

User Guide

GFK-3127A

Jan 2020

PACSystems™ Ethernet Switch

SLM084 User Manual



Warnings and Caution Notes as Used in this Publication

WARNING

Warning notices are used in this publication to emphasize that hazardous voltages, currents, temperatures, or other conditions that could cause personal injury exist in this equipment or may be associated with its use.

In situations where inattention could cause either personal injury or damage to equipment, a Warning notice is used.

CAUTION

Caution notices are used where equipment might be damaged if care is not taken.

Note: Notes merely call attention to information that is especially significant to understanding and operating the equipment.

These instructions do not purport to cover all details or variations in equipment, nor to provide for every possible contingency to be met during installation, operation, and maintenance. The information is supplied for informational purposes only, and Emerson makes no warranty as to the accuracy of the information included herein. Changes, modifications, and/or improvements to equipment and specifications are made periodically and these changes may or may not be reflected herein. It is understood that Emerson may make changes, modifications, or improvements to the equipment referenced herein or to the document itself at any time. This document is intended for trained personnel familiar with the Emerson products referenced herein.

Emerson may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not provide any license whatsoever to any of these patents.

Emerson provides the following document and the information included therein as-is and without warranty of any kind, expressed or implied, including but not limited to any implied statutory warranty of merchantability or fitness for particular purpose. If you purchased this product through an Authorized Channel Partner, please contact the seller directly.

Contents

Section 1: Getting to Know Your Switch	1
1.1 About the SLM084 Industrial Switch	1
1.2 Software Features	1
1.3 Hardware Features	2
Section 2: Hardware Installation	3
2.1 Installing Switch on DIN-Rail	3
2.2 Mount SLM084 on DIN-Rail	3
2.3 Wall Mounting Installation	4
Section 3: Hardware Overview	5
3.1 Front Panel	5
3.2 Front Panel LEDs	6
3.3 Top view Panel	7
Section 4: Cables	9
4.1 Ethernet Cables	9
4.2 1000/100BASE-TX/10BASE-T Pin Assignments	9
4.3 1000 Base-T RJ-45 Pin Assignments	10
4.4 10/100 Base-T MDI/MDI-X pins assignment	10
4.5 1000 Base-T MDI/MDI-X pins assignment	11
4.6 SFP	11
4.7 Console Cable	12
Section 5: Web Management	13
5.1 Configuration by Web Browser	13
5.1.1 About Web-based Management	13
5.2 Basic Setting	15
5.2.1 System Information	15

5.2.2	System Password	17
5.2.2.1	Authentication Method	18
5.3	IP Setting	20
5.3.1	HTTPS	21
5.3.2	SSH	22
5.3.3	LLDP.....	23
5.3.4	Modbus TCP.....	28
5.3.5	Backup/Restore Configuration	29
5.3.6	Firmware Update	29
5.3.7	DHCP Server.....	30
5.3.7.1	Setting.....	30
5.3.7.2	DHCP Dynamic Client List.....	30
5.3.7.3	DHCP Client List	31
5.3.8	Port Setting.....	31
5.3.8.1	Port Control	31
5.3.8.2	Port Trunk.....	34
5.3.8.2.1	Trunk Configuration.....	34
5.3.8.2.2	LACP Port Configuration	36
5.3.8.2.3	LACP System Status	38
5.3.8.2.4	LACP Status.....	39
5.3.8.2.5	LACP Statistics	40
5.3.8.3	Redundancy.....	43
5.3.8.3.1	Redundant Ring	43
5.3.9	MSTP.....	45
5.3.9.1	Bridge Settings.....	45
5.3.9.2	MSTI Mapping	47
5.3.9.3	MSTI Priorities	49
5.3.9.4	CIST Ports.....	50
5.3.9.5	MSTI Ports.....	52

5.3.9.6	STP Bridges	54
5.3.9.7	STP Port Status.....	55
5.3.9.8	STP Statistics.....	56
5.3.10	VLAN.....	57
5.3.10.1	VLAN Membership Configuration	57
5.3.10.2	VLAN Port Configuration	59
5.3.10.3	Private VLAN	61
5.3.11	SNMP	64
5.3.11.1	SNMP-System	64
5.3.11.2	SNMP-Communities.....	69
5.3.11.3	SNMP-Users	70
5.3.11.4	SNMP-Groups	73
5.3.11.5	SNMP-Views.....	74
5.3.11.6	SNMP-Accesses.....	75
5.3.12	Traffic Prioritization.....	77
5.3.12.1	Stom Control	77
5.3.12.2	Port Classification	79
5.3.12.3	Port Tag Remaking.....	83
5.3.12.4	Port DSCP	84
5.3.12.5	Port Policing.....	86
5.3.13	Queue Policing	87
5.3.13.1	Port Scheduler	89
5.3.13.2	Port Shaping	90
5.3.13.3	DSCP Based QoS.....	91
5.3.13.4	DSCP Translation.....	92
5.3.13.5	DSCP Classification.....	93
5.3.13.6	QoS Control List	94
5.3.13.6.1	QoS Counters.....	98
5.3.14	Multicast.....	101

5.3.14.1	IGMP Snooping	101
5.3.14.2	IGMP Snooping- VLAN Configuration-	102
5.3.14.3	IGMP Snooping Status	103
5.3.14.4	IGMP Snooping Groups Information	104
5.3.15	Security	106
5.3.15.1	Remote Control Security Configuration	106
5.3.15.2	ACL	107
5.3.15.2.1	Ports	107
5.3.15.2.2	Rate Limiters	109
5.3.15.2.3	ACL Control List	109
5.3.15.3	Authentication Server	120
5.3.15.3.1	Common Server Configuration	120
5.3.15.3.2	RADIUS Authentication Server Configuration	121
5.3.16	RADIUS Overview	124
5.3.16.1	RADIUS Details	126
5.3.16.2	NAS(802.1x)	129
5.3.17	Warning	142
5.3.17.1	Fault Alarm	142
5.3.18	System Warning	142
5.3.18.1	SYSLOG Setting	142
5.3.18.1.1	Event Selection	144
5.3.19	Monitor and Diag	145
5.3.19.1	MAC Table	145
5.3.19.1.1	Configuration	145
5.3.19.1.2	Aging Configuration	146
5.3.19.2	MAC Table Learning	147
5.3.19.3	Static MAC Table Configuration	148
5.3.19.4	MAC Table	149
5.3.20	Port Statistic	150

5.3.20.1	Traffic Overview	150
5.3.20.2	Detailed Statistics	151
5.3.20.3	Port Mirroring	153
5.3.20.4	System Log Information	155
5.3.20.5	Cable Diagnostics.....	157
5.3.20.6	SFP Monitor	158
5.3.20.7	Ping	159
5.3.20.8	Synchronization-PTP	160
5.3.20.9	Factory Defaults	165
5.3.20.10	System Reboot.....	166

Section 6: Command Line Interface Management 167

Section 7: Technical Specifications 192

General Contact Information	196
Technical Support.....	196

Section 1: Getting to Know Your Switch

1.1 About the SLM084 Industrial Switch

SLM084 is managed redundant ring Ethernet switch with 8x10/100/1000Base-T(X) ports and 12x100/1000Base-X SFP ports. With completely support of Ethernet Redundancy protocol, Redundant Ring (recovery time < 30ms over 250 units of connection) and MSTP (RSTP/STP compatible) can protect your mission-critical applications from network interruptions or temporary malfunctions with its fast recovery technology. And support wide operating temperature from -40 oC to 70 oC. SLM084 can also be managed centralized and convenient by PACSystems Ethernet Switch Configuration Tool, Except the Web-based interface and console (CLI) configuration. Therefore, the switch is one of the most reliable choice for highly-managed and Fiber Ethernet application.

1.2 Software Features

Support Redundant Ring (recovery time < 30ms over 250 units of connection) and MSTP(RSTP/STP compatible) for Ethernet Redundancy

- Support IEEE 1588v2 clock synchronization
- Support Modbus TCP protocol
- Support IEEE 802.3az Energy-Efficient Ethernet technology
- Provided HTTPS/SSH protocol to enhance network security
- Support SMTP client
- IGMP v2/v3 (IGMP snooping support) for filtering multicast traffic
- Support SNMP v1/v2c/v3 & RMON & 802.1Q VLAN Network Management
- Support ACL, TACACS+ and 802.1x User Authentication for security
- Supports 9.6K Bytes Jumbo Frame
- Multiple notification for warning of unexpected event
- Web-based ,Telnet, Console (CLI), and Windows utility (Open-Vision) configuration
- Support LLDP Protocol

- Rigid IP-30 housing design
- DIN-Rail and wall mounting enabled

1.3 Hardware Features

- Redundant DC power inputs
- Operating Temperature: -40 to 70°C
- Storage Temperature: -40 to 85 °C
- Operating Humidity: 5% to 95%, non-condensing
- Casing: IP-30
- 8 x 10/100/1000Base-T(X)
- 12 x 100/1000Base-X with SFP port
- Console Port
- Dimensions 96.4 (W) x 105.5 (D) x 154 (H) mm (3.8 x 4.15 x 6.06 inches)

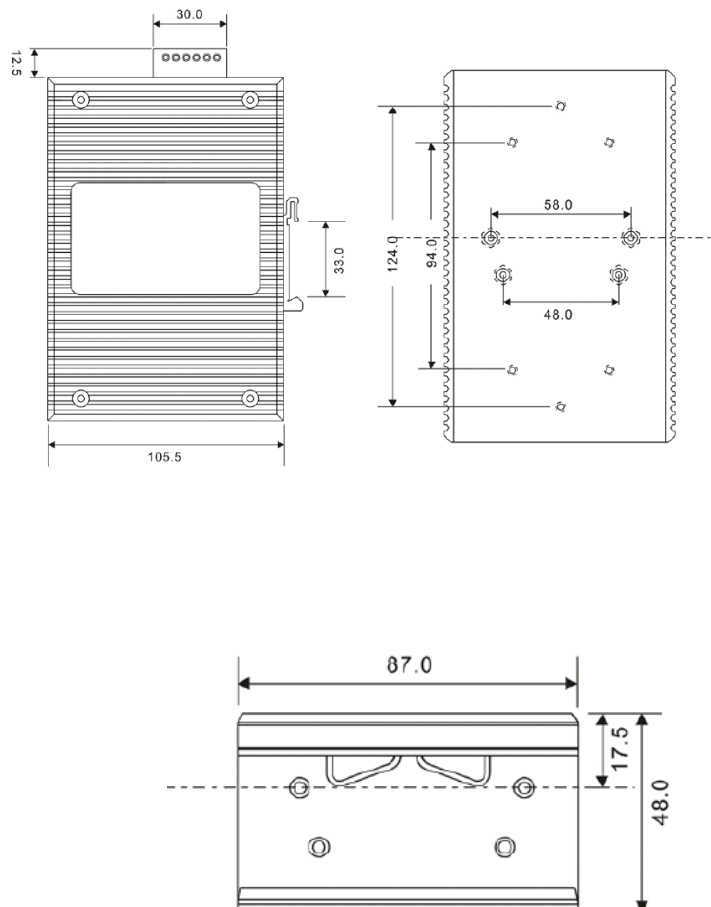
Section 2: Hardware Installation

2.1 Installing Switch on DIN-Rail

Each switch has a DIN-Rail kit on rear panel. The DIN-Rail kit helps switch to fix on the DIN-Rail. It is easy to install the switch on the DIN-Rail:

2.2 Mount SLM084 on DIN-Rail

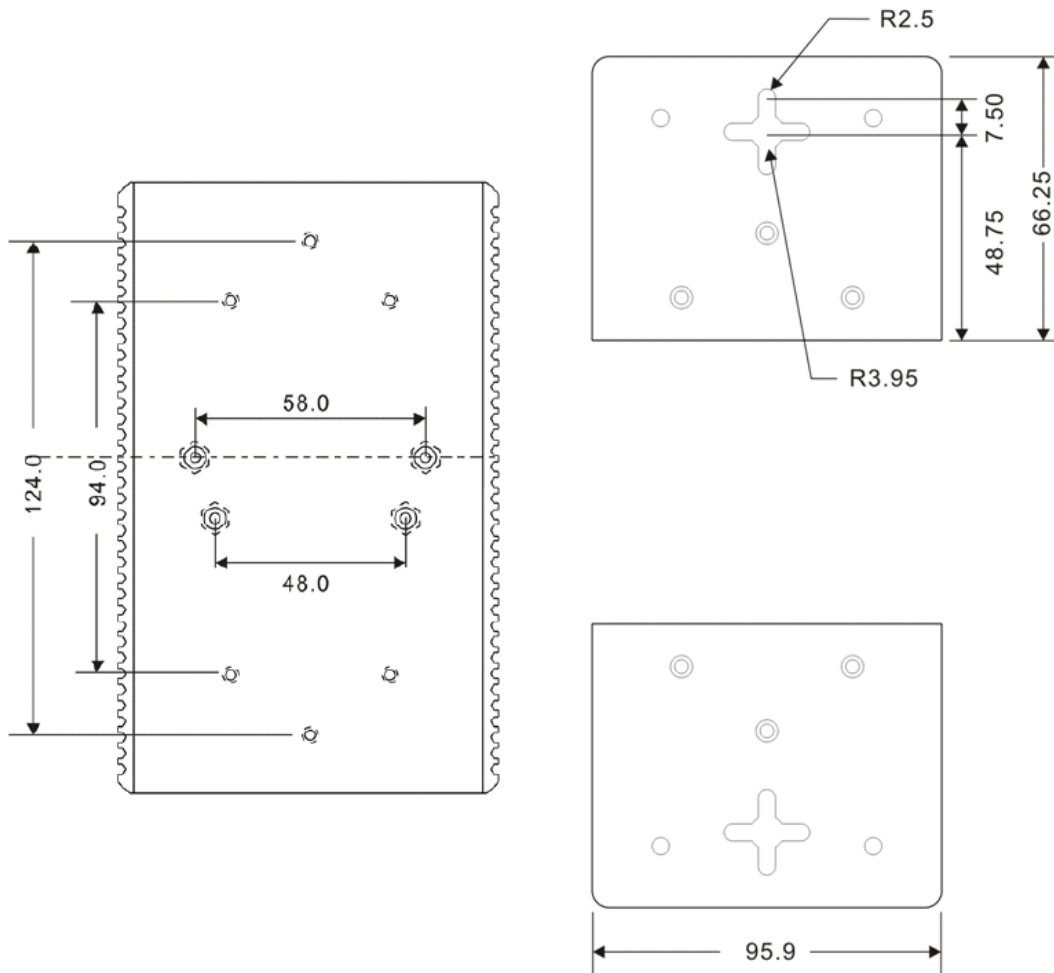
Figure 1: Din Rail Size



2.3 Wall Mounting Installation

Each switch has another installation method for users to fix the switch. A wall mount panel can be found in the package. The following steps show how to mount the switch on the wall:

Figure 2: Wall Mounting Size



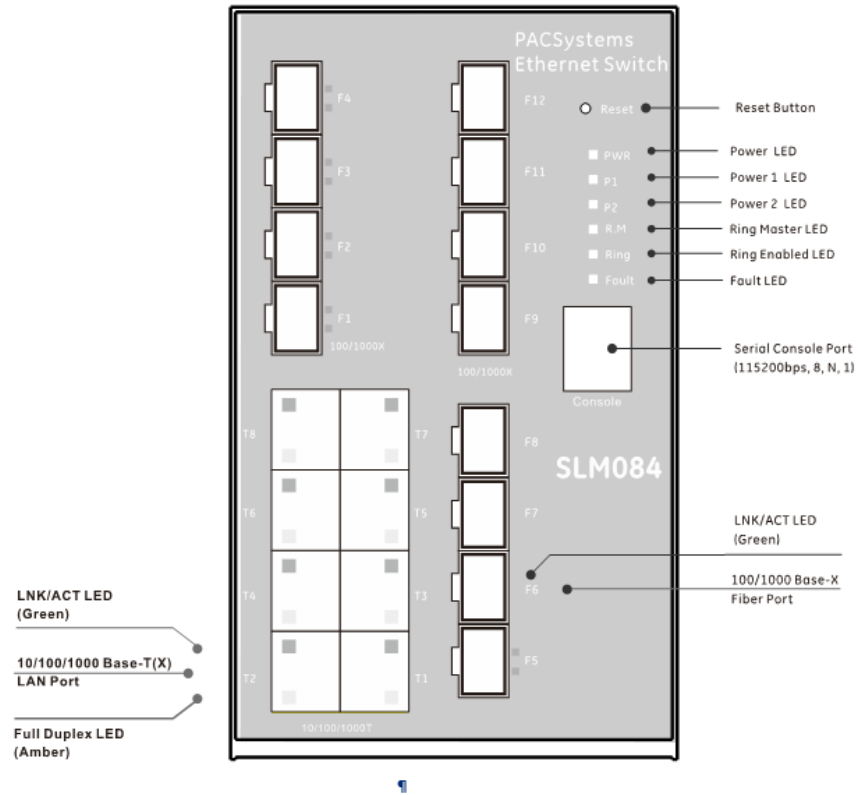
Section 3: Hardware Overview

3.1 Front Panel

The following table describes the labels that stick on the SLM084

Port	Description
SFP ports	12 X 100 /1000Base-X
Copper Port	8 X 10/100/1000Base-T(X)
Console	Use RS-232 with RJ-45 connector to manage switch.

Figure 3: Front Panel



3.2 Front Panel LEDs

LED	Color	Status	Description
PWR	Green	On	DC power module up
P1	Green	On	DC power module 1 activated.
P2	Green	On	DC Power module 2 activated.
R.M	Green	On	Ring Master.
Ring	Green	On	Ring enabled.

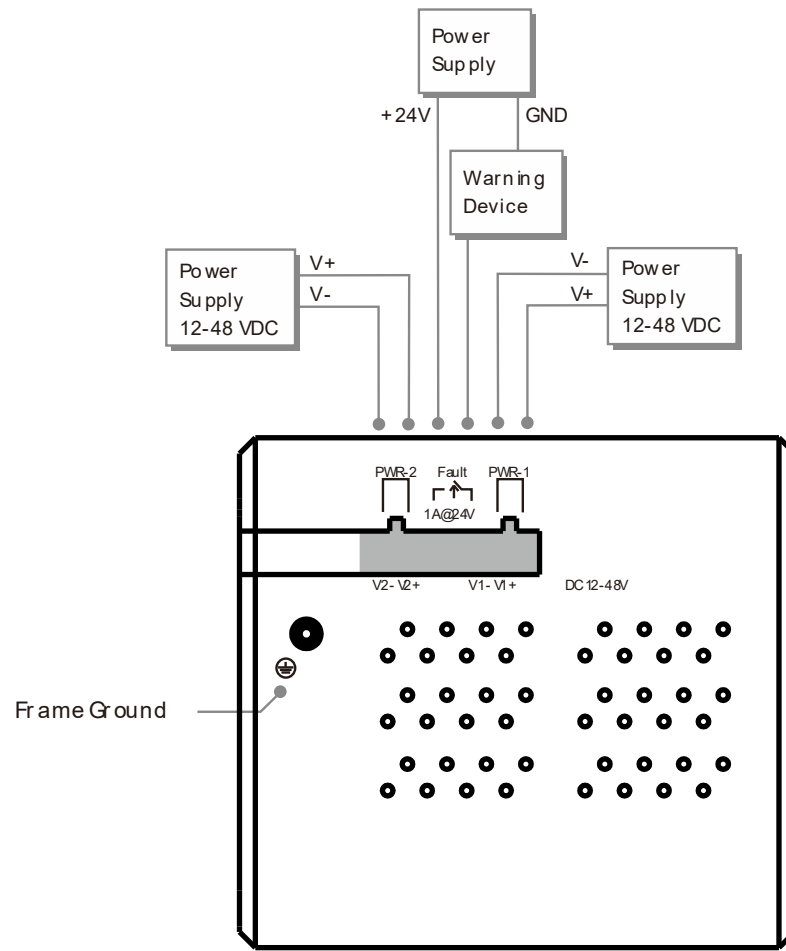
		Slowly blinking	Ring has only One link. (lack of one link to build the ring.)
		Fast blinking	Ring work normally.
Fault	Amber	On	Fault relay. Power failure or Port down/fail.
10/100/1000Base-T(X) Fast Ethernet ports			
LNK	Green	On	Port link up.
ACT	Green	Blinking	Data transmitted.
Full Duplex	Amber	On	Port works under full duplex.
SFP			
LNK	Green	On	Port link up.
ACT	Green	On	Data transmitted.

3.3 Top view Panel

The bottom panel component of SLM084 is showed as below:

1. Terminal block includes: PWR1, PWR2 (12-48V DC)
2. Ground wire

Figure 4: Top View Panel



Section 4: Cables

4.1 Ethernet Cables

The SLM084 has standard Ethernet ports. According to the link type, the switches use CAT 3, 4, 5, 5e UTP cables to connect to any other network device (PCs, servers, switches, routers, or hubs). Please refer to the following table for cable specifications.

Cable Types and Specifications

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45
1000BASE-TX	Cat. 5/Cat. 5e 100-ohm UTP	UTP 100 m (328ft)	RJ-45

4.2 1000/100BASE-TX/10BASE-T Pin Assignments

With 1000/100BASE-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-T 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

4.3 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 SLM084 switch supports auto MDI/MDI-X operation. You can use a straight-through cable to connect PC to switch. The following table below shows the 10BASE-T/ 100BASE-TX MDI and MDI-X port pin outs.

4.4 10/100 Base-T 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

4.5 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.

4.6 SFP

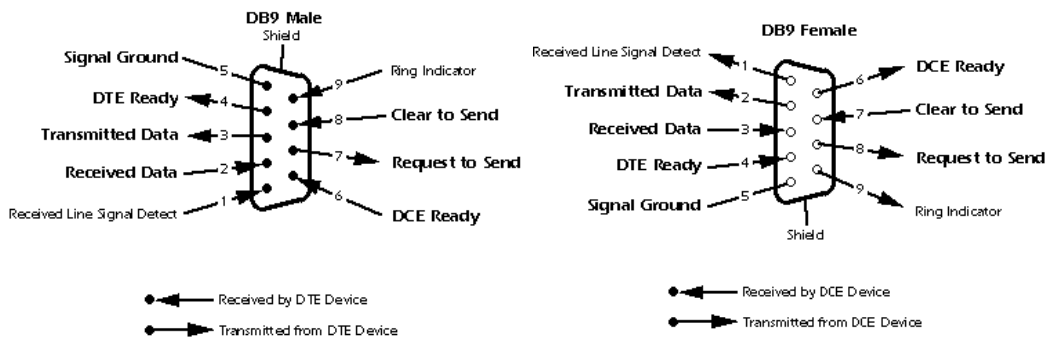
The Switch has fiber optical ports with SFP connectors. The fiber optical ports are in multi-mode (0 to 550M, 850 nm with 50/125 μm , 62.5/125 μm fiber) and single-mode with LC connector. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.

4.7 Console Cable

SLM084 switch can be management by console port. The DB-9 to RJ-45 cable can be found in the package. You can connect them to PC via a RS-232 cable with DB-9 female connector and the other end (RJ-45 connector) connects to console port of switch.

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

Figure 5: DB9 Male



Section 5: Web Management

WARNING

While making any establishment and upgrading firmware, please remove physical loop connection first.

Do NOT power off equipment while firmware is upgrading.

5.1 Configuration by Web Browser

This section introduces the configuration by 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 Microsoft Internet Explorer.

The Web-Based Management function supports Internet Explorer 5.0 or later. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

Note: By default, IE5.0 or later version does not allow Java Applets to open sockets. You need to explicitly modify the browser setting in order to enable Java Applets to use network ports.

Preparing for Web Management

The default value is as below:

IP Address: 192.168.0.100

Subnet Mask: **255.255.255.0**

User Name: **admin**

Password: **admin**

System Login

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

Figure 6: Enter Network Password



5.2 Basic Setting

5.2.1 System Information

Figure 7: Information Message

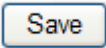
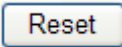
Information Message

System	
Name	SLM084
Description	Industrial 20-port managed Gigabit Ethernet switch with 8x10/100/1000Base-T(X) ports and 12x100/1000Base-X, SFP socket
Location	
Contact	
OID	1.3.6.1.4.1.25972.0.0.113
Hardware	
MAC Address	00-1e-94-01-b3-11
Time	
System Date	1970-01-01 00:21:38+00:00
System Uptime	0d 00:21:38
Software	
Kernel Version	v9.26
Software Version	v1.00
Software Date	2015-03-26T17:23:07+08:00

Auto-refresh Refresh

Enable Location Alert

Label	Description
System Name	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z, a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last

Label	Description
	character must not be a minus sign. The allowed string length is 0 to 255.
System Description	The device Description.
System Location	The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
System Timezone offset(minutes)	Provide the time-zone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

5.2.2

5.2.3 System Password

This page allows you to configure the system password required to access the web pages or log in from CLI.

System Password

Old User Name	<input type="text"/>
Old Password	<input type="password"/>
New User Name	<input type="text"/>
New Password	<input type="password"/>
Confirm New Password	<input type="password"/>

Label	Description
Old Password	Enter the current system password. If this is incorrect, the new password will not be set.
New Password	The system password. The allowed string length is 0 to 31, and the allowed content is the ASCII characters from 32 to 126.
Confirm password	Re-type the new password.
<input type="button" value="Save"/>	Click to save changes.

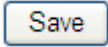
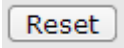
5.2.3.1 Authentication Method

This page allows you to configure how a user is authenticated when he logs into the switch via one of the management client interfaces.

Figure 8: Authentication Method Configuration

Authentication Method Configuration

Client	Authentication Method	Fallback
console	local ▼	<input type="checkbox"/>
telnet	local ▼	<input type="checkbox"/>
ssh	local ▼	<input type="checkbox"/>
web	local ▼	<input type="checkbox"/>

Label	Description
Client	The management client for which the configuration below applies.
Authentication Method	<p>Authentication Method can be set to one of the following values:</p> <p>none: authentication is disabled and login is not possible.</p> <p>local: use the local user database on the switch for authentication.</p> <p>radius: use a remote RADIUS server for authentication.</p>
Fallback	<p>Enable fallback to local authentication by checking this box.</p> <p>If none of the configured authentication servers are alive, the local user database is used for authentication.</p> <p>This is only possible if the Authentication Method is set to a value other than 'none' or 'local'.</p>
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

5.3 IP Setting

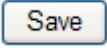
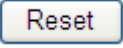
Configure the switch-managed IP information on this page.

Figure 9: IP Configuration

IP Configuration

	Configured	Current
DHCP Client	<input type="checkbox"/>	<input type="button" value="Renew"/>
IP Address	192.168.0.100	192.168.0.100
IP Mask	255.255.255.0	255.255.255.0
IP Router	0.0.0.0	0.0.0.0
VLAN ID	1	1
SNTP Server	0.0.0.0	

Label	Description
DHCP Client	Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
IP 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 192.168.10.1
IP Mask	Assign the subnet mask of the IP address. If DHCP client function is enabling, you do not need to assign the subnet mask
IP Router	Assign the network gateway for the switch. The default gateway is 192.168.10.254
VLAN ID	Provide the managed VLAN ID. The allowed range is 1 through 4095.
DNS Server	Provide the IP address of the DNS Server in dotted decimal notation.



Label	Description
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

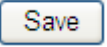
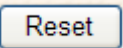
5.3.1 HTTPS

Figure 10: HTTPS Configuration

HTTPS Configuration

Mode | Enabled ▾

Label	Description
Mode	Indicates the HTTPS mode operation. When the current connection is HTTPS, to apply HTTPS disabled mode operation will automatically redirect web browser to an HTTP connection. Possible modes are: Enabled: Enable HTTPS mode operation. Disabled: Disable HTTPS mode operation.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

5.3.2 SSH

Figure 11: SSH Configuration

SSH Configuration

Mode

Label	Description
Mode	Indicates the SSH mode operation. Possible modes are: Enabled: Enable SSH mode operation. Disabled: Disable SSH mode operation.
<input type="button" value="Save"/>	Click to save changes.
<input type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

5.3.3 LLDP

LLDP Configuration

This page allows the user to inspect and configure the current LLDP port settings.

Figure 12: LLDP Configuration

LLDP Configuration

LLDP Parameters

Tx Interval	<input type="text" value="30"/>	seconds
--------------------	---------------------------------	---------

LLDP Port Configuration

Port	Mode
*	<> ▼
1	Enabled ▼
2	Enabled ▼
3	Enabled ▼
4	Enabled ▼
5	Enabled ▼
6	Enabled ▼
7	Enabled ▼

Label	Description
Port	The switch port number of the logical LLDP port.
Mode	<p>Select LLDP mode.</p> <p>Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.</p> <p>Tx only The switch will drop LLDP information received from neighbors, but will send out LLDP information.</p>

	<p>Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors.</p> <p>Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbors.</p>
--	---

LLDP Neighbor Information

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected. The columns hold the following information:

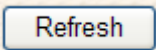
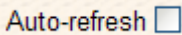
Figure 13: LLDP Neighbor Information

LLDP Neighbour Information

Auto-refresh Refresh

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

Label	Description
Local Port	The port on which the LLDP frame was received.
Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.
Remote Port ID	The Remote Port ID is the identification of the neighbor port.
System Name	System Name is the name advertised by the neighbor unit.
Port Description	Port Description is the port description advertised by the neighbor unit.
System Capabilites	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:

Label	Description
	<p>1. Other</p> <p>2. Repeater</p> <p>3. Bridge</p> <p>4. WLAN Access Point</p> <p>5. Router</p> <p>6. Telephone</p> <p>7. DOCSIS cable device</p> <p>8. Station only</p> <p>9. Reserved</p> <p>When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).</p>
Management Address	<p>Management Address is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address.</p>
	<p>Click to refresh the page immediately.</p>
	<p>Check this box to enable an automatic refresh of the page at regular intervals.</p>

Port Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole stack, switch, while local counters refer to counters for the currently selected switch.

Figure 14: LLDP Global Counters

Auto-refresh Refresh Clear

LLDP Global Counters

Global Counters	
Neighbour entries were last changed	1970-01-01 00:00:00+00:00 (2113 secs. ago)
Total Neighbours Entries Added	0
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

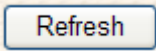
LLDP Statistics Local Counters

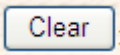
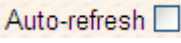
Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	69	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0

Global Counters

Label	Description
Neighbor entries were last changed at	Shows the time for when the last entry was last deleted or added.
Total Neighbors Entries Added	Shows the number of new entries added since switch reboot.
Total Neighbors Entries Deleted	Shows the number of new entries deleted since switch reboot.
Total Neighbors Entries Dropped	Shows the number of LLDP frames dropped due to that the entry table was full.
Total Neighbors Entries Aged Out	Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

Label	Description
Local Port	The port on which LLDP frames are received or transmitted.
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.
Rx Errors	The number of received LLDP frames containing some kind of error.
Frames Discarded	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.
Org. Discarded	The number of organizationally TLVs received.
Age-Outs	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.
	Click to refresh the page immediately.

Label	Description
	Clears the local counters. All counters (including global counters) are cleared upon reboot.
	Check this box to enable an automatic refresh of the page at regular intervals.

5.3.4 Modbus TCP

Support Modbus TCP. (About Modbus please reference <http://www.modbus.org/>)

Figure 15: Modbus TCP

MODBUS Configuration

Mode | Disabled ▼
 Save | Reset

The following table describes the labels in this screen.

Label	Description
Mode	Enable or Disable Modbus TCP function

5.3.5 Backup/Restore Configuration

You can save/view or load the switch configuration. The configuration file is in XML format with a hierarchy of tags:

Figure 16: Configuration Save

Configuration Save

Save Configuration

5.3.6 Firmware Update

This page facilitates an update of the firmware controlling the stack. switch.

Figure 17: Software Upload

Software Upload

选择文件 未选择任何文件

Upload

5.3.7 DHCP Server

5.3.7.1 Setting

The system provides with DHCP server function. Enable the DHCP server function, the switch system will be a DHCP server.

Figure 18: DHCP Server Configuration

DHCP Server Configuration

Enabled	<input type="checkbox"/>
Start IP Address	192.168.0.100
End IP Address	192.168.0.200
Subnet Mask	255.255.255.0
Router	192.168.0.254
DNS	192.168.0.254
Lease Time (sec.)	86400
TFTP Server	0.0.0.0
Boot File Name	

5.3.7.2 DHCP Dynamic Client List

When the DHCP server function is activated, the system will collect the DHCP client information and display in here.

Figure 19: DHCP Dynamic Client List

DHCP Dynamic Client List

No.	Select	Type	MAC Address	IP Address	Surplus Lease
<input type="button" value="Select/Clear All"/> <input type="button" value="Add to static Table"/> <input type="button" value="Delete"/>					

5.3.7.3 DHCP Client List

You can assign the specific IP address which is in the assigned dynamic IP range to the specific port. When the device is connecting to the port and asks for dynamic IP assigning, the system will assign the IP address that has been assigned before in the connected device.

Figure 20: DHCP Client List

DHCP Client List

MAC Address	<input type="text"/>
IP Address	<input type="text"/>

No.	Select	Type	MAC Address	IP Address	Surplus Lease
<input type="button" value="Delete"/> <input type="button" value="Select/Clear All"/>					

5.3.8 Port Setting

5.3.8.1 Port Control

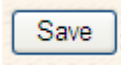
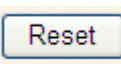
This page displays current port configurations. Ports can also be configured here.

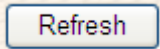
Figure 21: Port Configuration

Port Configuration

Refresh								
Port	Link	Speed		Flow Control			Maximum Frame Size	Power Control
		Current	Configured	Current Rx	Current Tx	Configured		
*			<>				9600	<>
1	1Gfdx	Auto	Auto	X	X		9600	Disabled
2	Down	Auto	Auto	X	X		9600	Disabled
3	Down	Auto	Auto	X	X		9600	Disabled
4	Down	Auto	Auto	X	X		9600	Disabled
5	Down	Auto	Auto	X	X		9600	Disabled
6	Down	Auto	Auto	X	X		9600	Disabled
7	Down	Auto	Auto	X	X		9600	Disabled
8	Down	Auto	Auto	X	X		9600	Disabled
9	Down	Auto	Auto	X	X		9600	
10	Down	Auto	Auto	X	X		9600	
11	Down	Auto	Auto	X	X		9600	
12	Down	Auto	Auto	X	X		9600	
13	Down	Auto	Auto	X	X		9600	
14	Down	Auto	Auto	X	X		9600	
15	Down	Auto	Auto	X	X		9600	

Label	Description
Port	This is the logical port number for this row.
Link	The current link state is displayed graphically. Green indicates the link is up and red that it is down.
Current Link Speed	Provides the current link speed of the port.
Configured Link Speed	<p>Select any available link speed for the given switch port.</p> <p>Auto Speed selects the highest speed that is compatible with a link partner.</p> <p>Disabled disables the switch port operation.</p> <p><> : configuration all port .</p>

Label	Description
Flow Control	<p>When Auto Speed is selected for a port, this section indicates the flow control capability that is advertised to the link partner.</p> <p>When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation.</p> <p>Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.</p>
Maximum Frame	<p>Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 9600 bytes.</p>
Power Control	<p>The Usage column shows the current percentage of the power consumption per port. The Configured column allows for changing the power savings mode parameters per port.</p> <p>Disabled: All power savings mechanisms disabled.</p> <p>ActiPHY: Link down power savings enabled.</p> <p>PerfectReach: Link up power savings enabled.</p> <p>Enabled: Both link up and link down power savings enabled.</p>
Total Power Usage	<p>Total power usage in board, measured in percent.</p>
	<p>Click to save changes.</p>
	<p>Click to undo any changes made locally and revert to previously saved values.</p>

Label	Description
	Click to refresh the page. Any changes made locally will be undone.

5.3.8.2 Port Trunk

5.3.8.2.1 Trunk Configuration

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

Figure 22: Aggregation Mode Configuration

Aggregation Mode Configuration

Hash Code Contributors	
Source MAC Address	<input checked="" type="checkbox"/>
Destination MAC Address	<input type="checkbox"/>
IP Address	<input checked="" type="checkbox"/>
TCP/UDP Port Number	<input checked="" type="checkbox"/>

Label	Description
Source MAC Address	The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.
Destination MAC Address	The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.

IP Address	The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.
TCP/UDP Port Number	The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.

Figure 23: Aggregation Group Configuration

Aggregation Group Configuration

Group ID	Port Members																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Normal	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
9	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
10	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Save Reset

Label	Description
Group ID	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

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. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.
---------------------	---

5.3.8.2.2 LACP Port Configuration

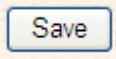
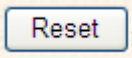
This page allows the user to inspect the current LACP port configurations, and possibly change them as well.

Figure 24: LACP Port Configuration

LACP Port Configuration

Port	LACP Enabled	Key		Role
*	<input type="checkbox"/>	<> ▼		<> ▼
1	<input type="checkbox"/>	Auto ▼		Active ▼
2	<input type="checkbox"/>	Auto ▼		Active ▼
3	<input type="checkbox"/>	Auto ▼		Active ▼
4	<input type="checkbox"/>	Auto ▼		Active ▼
5	<input type="checkbox"/>	Auto ▼		Active ▼
6	<input type="checkbox"/>	Auto ▼		Active ▼
7	<input type="checkbox"/>	Auto ▼		Active ▼
8	<input type="checkbox"/>	Auto ▼		Active ▼
9	<input type="checkbox"/>	Auto ▼		Active ▼
10	<input type="checkbox"/>	Auto ▼		Active ▼

Label	Description
Port	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
LACP Enabled	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. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.
Key	The Key value incurred by the port, range 1-65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb

Label	Description
	= 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
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).
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

5.3.8.2.3 LACP System Status

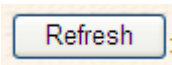
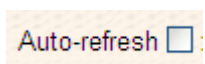
This page provides a status overview for all LACP instances.

LACP System Status

Auto-refresh Refresh

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

Label	Description
Aggr ID	The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'

Label	Description
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.
Last Changed	Shows which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID:Port".
	Click to refresh the page immediately.
	Check this box to enable an automatic refresh of the page at regular intervals.

5.3.8.2.4 LACP Status

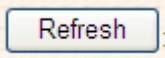
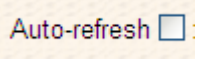
This page provides a status overview for LACP status for all ports.

Figure 25: LACP Status

LACP Status

Auto-refresh Refresh

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	No	-	-	-	-
6	No	-	-	-	-
7	No	-	-	-	-
8	No	-	-	-	-
-	..				

Label	Description
Port	The switch port number.
LACP	'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.
Key	The key assigned to this port. Only ports with the same key can aggregate together.
Aggr ID	The Aggregation ID assigned to this aggregation group.
Partner System ID	The partners System ID (MAC address).
Partner Port	The partners' port number connected to this port.
	Click to refresh the page immediately.
	Check this box to enable an automatic refresh of the page at regular intervals.

5.3.8.2.5 LACP Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. Global counters are counters that refer to the whole stack, switch, while local counters refer to counters for the currently selected switch.

Figure 26: LACP Statistics

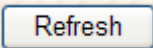
LACP Statistics

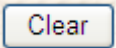
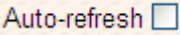
Auto-refresh Refresh Clear

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0

Global Counters

Label	Description
Neighbor entries were last changed at	Shows the time for when the last entry was last deleted or added.
Total Neighbors Entries Added	Shows the number of new entries added since switch reboot.
Total Neighbors Entries Deleted	Shows the number of new entries deleted since switch reboot.
Total Neighbors Entries Dropped	Shows the number of LLDP frames dropped due to that the entry table was full.
Total Neighbors Entries Aged Out	Shows the number of entries deleted due to Time-To-Live expiring.

Label	Description
Local Port	The port on which LLDP frames are received or transmitted.
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.
Rx Errors	The number of received LLDP frames containing some kind of error.
Frames Discarded	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.
Org. Discarded	The number of organizationally TLVs received.
Age-Outs	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.
	Click to refresh the page immediately.

Label	Description
	Clears the local counters. All counters (including global counters) are cleared upon reboot.
	Check this box to enable an automatic refresh of the page at regular intervals.

5.3.8.3 Redundancy

5.3.8.3.1 Redundant Ring

Ring is the most powerful Ring in the world. The recovery time of Ring is less than 10 ms. It can reduce unexpected damage caused by network topology change. Ring Supports 3 Ring topology: Ring, Coupling Ring and Dual Homing.

Figure 27: Redundant Ring

Redundant Ring Configuration

<input type="checkbox"/> Redundant Ring		
Ring Master	Disable ▼	This switch is Not a Ring Master.
1st Ring Port	Port 1 ▼	LinkDown
2nd Ring Port	Port 2 ▼	LinkDown
<input type="checkbox"/> Coupling Ring		
Coupling Port	Port 3 ▼	LinkDown
<input type="checkbox"/> Dual Homing		
Homing Port	Port 4 ▼	LinkDown
<input type="button" value="Save"/> <input type="button" value="Refresh"/>		

The following table describes the labels in this screen.

Label	Description
Redundant Ring	Mark to enable Ring.
Ring Master	There should be one and only one Ring Master in a ring. However if there are two or more switches which set Ring Master to enable, the switch with the lowest MAC address will be the actual Ring Master and others will be Backup Masters.
1st Ring Port	The primary port, when this switch is Ring Master.
2nd Ring Port	The backup port, when this switch is Ring Master.
Coupling Ring	Mark to enable Coupling Ring. Coupling Ring can be used to divide a big ring into two smaller rings to avoid effecting all switches when network topology change. It is a good application for connecting two Rings.
Coupling Port	Link to Coupling Port of the switch in another ring. Coupling Ring need four switch to build an active and a backup link. Set a port as coupling port. The coupled four ports of four switches will be run at active/backup mode.
Dual Homing	Mark to enable Dual Homing. By selecting Dual Homing mode, Ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work as active/backup mode, and connect each Ring to the normal switches in RSTP mode.
Apply	Click " Apply " to set the configurations.

Note: We don't suggest you to set one switch as a Ring Master and a Coupling Ring at the same time due to heavy load.

5.3.9 MSTP

5.3.9.1 Bridge Settings

This page allows you to configure RSTP system settings. The settings are used by all RSTP Bridge instances in the Switch Stack.

Figure 28: STP Bridge Configuration

STP Bridge Configuration

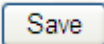
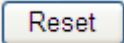
Basic Settings

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

Advanced Settings

Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	<input style="width: 80%;" type="text"/>

Label	Description
Protocol Version	The STP protocol version setting. Valid values are STP, RSTP and MSTP.
Forward Delay	The delay used by STP Bridges to transition Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be $\leq (FwdDelay-1)*2$.

Label	Description
Maximum Hop Count	This defines the initial value of remainingHops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range 4 to 30 seconds, and MaxAge must be $\leq (\text{FwdDelay} - 1) * 2$.
Transmit Hold Count	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

5.3.9.2 MSTI Mapping

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

Figure 29: MSTI Configuration

MSTI Configuration

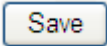
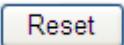
Add VLANs separated by spaces or comma.

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

Configuration Identification	
Configuration Name	00-1e-94-01-b3-11
Configuration Revision	0

MSTI Mapping	
MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Label	Description
Configuration Name	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is at most 32 characters.
Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
MSTI	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

Label	Description
VLANS Mapped	The list of VLAN's mapped to the MSTI. The VLANs must be separated with comma and/or space. A VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.)
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

5.3.9.3 MSTI Priorities

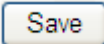
This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

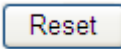
Figure 30: MSTI Configuration

MSTI Configuration

MSTI	Priority
∞	<> ▼
CIST	32768 ▼
MSTI1	32768 ▼
MSTI2	32768 ▼
MSTI3	32768 ▼
MSTI4	32768 ▼
MSTI5	32768 ▼
MSTI6	32768 ▼
MSTI7	32768 ▼

Save Reset

Label	Description
MSTI	The bridge instance. The CIST is the default instance, which is always active.
Priority	Controls the bridge priority. Lower numerical values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.
	Click to save changes.

Label	Description
	Click to undo any changes made locally and revert to previously saved values.

5.3.9.4 CIST Ports

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well. This page contains settings for physical and aggregated ports. The aggregation settings are stack global.

Figure 31: STP CIST Port Configuration

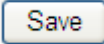
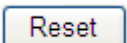
STP CIST Port Configuration

CIST Aggregated Port Configuration										
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point	
						Role	TCN			
-	<input type="checkbox"/>	Auto ▼	128 ▼	Non-Edge ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True ▼	

CIST Normal Port Configuration										
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point	
						Role	TCN			
*	<input type="checkbox"/>	<> ▼	<> ▼	<> ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<> ▼	
1	<input type="checkbox"/>	Auto ▼	128 ▼	Non-Edge ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	
2	<input type="checkbox"/>	Auto ▼	128 ▼	Non-Edge ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	
3	<input type="checkbox"/>	Auto ▼	128 ▼	Non-Edge ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	
4	<input type="checkbox"/>	Auto ▼	128 ▼	Non-Edge ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	
5	<input type="checkbox"/>	Auto ▼	128 ▼	Non-Edge ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	
6	<input type="checkbox"/>	Auto ▼	128 ▼	Non-Edge ▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	

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 path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D

Label	Description
	recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
OpenEdge (setate flag)	Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transitioning to the forwarding state is faster for edge ports (having operEdge true) than for other ports.
AdminEdge	Controls whether the operEdge flag should start as being set or cleared. (The initial operEdge state when a port is initialized).
AutoEdge	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.
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. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also know as Root Guard.
Restricted TCN	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause

Label	Description
	temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or is the physical link state for the attached LANs transitions frequently.
Point2Point	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

5.3.9.5 MSTI Ports

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well. A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for 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. The aggregation settings are stack global.

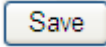
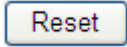
Figure 32: MSTI Port Configuration

MSTI Port Configuration

Select MSTI

MST1 ▼

Get

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. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

5.3.9.6 STP Bridges

This page provides a status overview for all STP bridge instances.

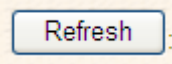
The displayed table contains a row for each STP bridge instance, where the column displays the following information:

Figure 33: STP Bridges

STP Bridges

Auto-refresh Refresh

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.00-1E-94-01-B3-11	32768.00-1E-94-01-B3-11	-	0	Steady	-

Label	Description
MSTI	The Bridge Instance. This is also a link to the STP Detailed Bridge Status.
Bridge ID	The Bridge ID of this Bridge instance.
Root ID	The Bridge ID of the currently elected root bridge.
Root Port	The switch port currently assigned the root port role.
Root Cost	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Topology Flag	The current state of the Topology Change Flag for this Bridge instance.
Topology Change Last	The time since last Topology Change occurred.
	Click to refresh the page immediately.

Label	Description
Auto-refresh <input type="checkbox"/>	Check this box to enable an automatic refresh of the page at regular intervals.

5.3.9.7 STP Port Status

This page displays the STP CIST port status for port physical ports in the currently selected switch.

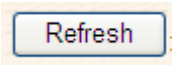
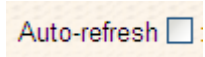
Figure 34: STP Port Status

STP Port Status

Auto-refresh Refresh

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-
11	Non-STP	Forwarding	-
12	Non-STP	Forwarding	-
13	Non-STP	Forwarding	-
14	Non-STP	Forwarding	-
15	Non-STP	Forwarding	-
16	Non-STP	Forwarding	-
17	Non-STP	Forwarding	-
18	Non-STP	Forwarding	-
19	Non-STP	Forwarding	-
20	Non-STP	Forwarding	-

Label	Description
Port	The switch port number of the logical STP port.
CIST Role	The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort.
State	The current STP port state of the CIST port. The port state can be one of the following values: Blocking Learning Forwarding.

Label	Description
Uptime	The time since the bridge port was last initialized.
	Click to refresh the page immediately.
	Check this box to enable an automatic refresh of the page at regular intervals.

5.3.9.8 STP Statistics

This page displays the RSTP port statistics counters for bridge ports in the currently selected switch.

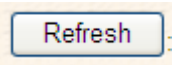
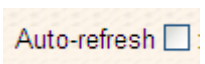
Figure 35: STP Statistics

STP Statistics

Auto-refresh Refresh Clear

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
No ports enabled										

Label	Description
Port	The switch port number of the logical RSTP port.
RSTP	The number of RSTP Configuration BPDU's received/transmitted on the port.
STP	The number of legacy STP Configuration BPDU's received/transmitted on the port.

Label	Description
TCN	The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
Discarded Unknown	The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
Discarded Illegal	The number of illegal Spanning Tree BPDU's received (and discarded) on the port.
	Click to refresh the page immediately.
	Check this box to enable an automatic refresh of the page at regular intervals.

5.3.10 VLAN

5.3.10.1 VLAN Membership Configuration

The VLAN membership configuration for the selected stack switch unit switch can be monitored and modified here. Up to 64 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

Figure 36: VLAN Membership Configuration

VLAN Membership Configuration

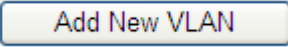
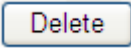
Refresh | << >>

Start from VLAN with entries per page.

Delete	VLAN ID	VLAN Name	Port Members																			
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
<input type="checkbox"/>	1	default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add New VLAN

Save Reset

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for 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	<p>Click  to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Legal values for a VLAN ID are 1 through 4095.</p> <p>The VLAN is enabled on the selected stack switch unit when you click on "Save". The VLAN is thereafter present on the other stack switch units, but with no port members.</p> <p>A VLAN without any port members on any stack unit will be deleted when you click "Save".</p> <p>The  button can be used to undo the addition of new VLANs.</p>

5.3.10.2 VLAN Port Configuration

Figure 37: Ethertype for Custom S-Ports 0X

Auto-refresh Refresh

Ethertype for Custom S-ports 0x

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN		Tx Tag
				Mode	ID	
*	<>	<input type="checkbox"/>	<>	<>	1	<>
1	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
2	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
3	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
4	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
5	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
6	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
7	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
8	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
9	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
10	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid

Label	Description
Ethertype for customer S-Ports	This field specifies the ether type used for Custom S-ports. This is a global setting for all the Custom S-ports.
Port	This is the logical port number of this row.
Port type	<p>Port can be one of the following types: Unaware, Customer port(C-port), Service port(S-port), Custom Service port(S-custom-port)</p> <p>If Port Type is Unaware, all frames are classified to the Port VLAN ID and tags are not removed.</p>
Ingress Filtering	Enable ingress filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded. By default, ingress filtering is disabled (no checkmark).
Frame Type	Determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port are discarded. By default, the field is set to All.
Port VLAN Mode	<p>Configures the Port VLAN Mode. The allowed values are None or Specific. This parameter affects VLAN ingress and egress processing.</p> <p>If None is selected, a VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN aware switches. Tx tag should be set to Untag_pvid when this mode is used.</p>

Label	Description
	If Specific (the default value) is selected, a Port VLAN ID can be configured (see below). Untagged frames received on the port are classified to the Port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with the classified VLAN ID is inserted in the frame.
Port VLAN ID	Configures the VLAN identifier for the port. The allowed values are from 1 through 4095. The default value is 1. Note: The port must be a member of the same VLAN as the Port VLAN ID.
Tx Tag	Determines egress tagging of a port. Untag_pvid - All VLANs except the configured PVID will be tagged. Tag_all - All VLANs are tagged. Untag_all - All VLANs are untagged.

5.3.10.3 Private VLAN

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.

A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

Figure 38: Private VLAN Membership Configuration

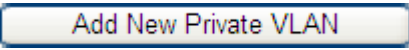
Auto-refresh Refresh

Private VLAN Membership Configuration

		Port Members																			
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add New Private VLAN

Save Reset

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Private VLAN ID	Indicates the ID of this particular private VLAN.
MAC Address	The MAC address for the entry.
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.
Adding a New Static Entry	Click  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

Label	Description
	<p>the incorrect entry, or click "Cancel" to return to the editing and make a correction.</p> <p>The Private VLAN is enabled when you click "Save".</p> <p>The <input type="button" value="Delete"/> button can be used to undo the addition of new Private VLANs.</p>

Figure 39: Port Isolation Configuration

Auto-refresh

Port Isolation Configuration

Port Number																			
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Label	Description
<p>Port Members</p>	<p>A check box is provided for each port of a private VLAN.</p> <p>When checked, port isolation is enabled for that port.</p> <p>When unchecked, port isolation is disabled for that port.</p> <p>By default, port isolation is disabled for all ports.</p>

5.3.11 SNMP

5.3.11.1 SNMP-System

Figure 40: SNMP System Configuration

SNMP System Configuration

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

Label	Description
Mode	<p>Indicates the SNMP mode operation. Possible modes are:</p> <p>Enabled: Enable SNMP mode operation.</p> <p>Disabled: Disable SNMP mode operation.</p>
Version	<p>Indicates the SNMP supported version. Possible versions are:</p> <p>SNMP v1: Set SNMP supported version 1.</p> <p>SNMP v2c: Set SNMP supported version 2c.</p> <p>SNMP v3: Set SNMP supported version 3.</p>

Label	Description
<p>Read Community</p>	<p>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.</p> <p>The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using USM for authentication and privacy and the community string will associated with SNMPv3 communities table</p>
<p>Write Community</p>	<p>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.</p> <p>The field only suits to SNMPv1 and SNMPv2c. SNMPv3 is using USM for authentication and privacy and the community string will associated with SNMPv3 communities table.</p>
<p>Engine ID</p>	<p>Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.</p>

Figure 41: SNMP Trap Configuration

SNMP Trap Configuration

Trap Mode	Disabled ▼
Trap Version	SNMP v1 ▼
Trap Community	public
Trap Destination Address	
Trap Authentication Failure	Enabled ▼
Trap Link-up and Link-down	Enabled ▼
Trap Inform Mode	Enabled ▼
Trap Inform Timeout (seconds)	1
Trap Inform Retry Times	5

Label	Description
Trap Mode	<p>Indicates the SNMP trap mode operation. Possible modes are:</p> <p>Enabled: Enable SNMP trap mode operation.</p> <p>Disabled: Disable SNMP trap mode operation.</p>
Trap Version	<p>Indicates the SNMP trap supported version. Possible versions are:</p> <p>SNMP v1: Set SNMP trap supported version 1.</p> <p>SNMP v2c: Set SNMP trap supported version 2c.</p> <p>SNMP v3: Set SNMP trap supported version 3.</p>
Trap Community	<p>Indicates the community access string when send SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.</p>
Trap Destination Address	<p>Indicates the SNMP trap destination address.</p> <p>Trap Destination IPv6 Address</p>
Trap Destination IPv6 Address	<p>Provide the trap destination IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, 'fe80:215:c5ff:fe03:4dc7'.</p> <p>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 only appear once. It also used a following legally IPv4 address. For example, ':::192.1.2.34'.</p>
Trap Authentication Failure	<p>Indicates the SNMP entity is permitted to generate authentication failure traps. Possible modes are:</p>

Label	Description
	<p>Enabled: Enable SNMP trap authentication failure.</p> <p>Disabled: Disable SNMP trap authentication failure.</p>
<p>Trap Link-up and Link-down</p>	<p>Indicates the SNMP trap link-up and link-down mode operation. Possible modes are:</p> <p>Enabled: Enable SNMP trap link-up and link-down mode operation.</p> <p>Disabled: Disable SNMP trap link-up and link-down mode operation.</p>
<p>Trap Inform Mode</p>	<p>Indicates the SNMP trap inform mode operation. Possible modes are:</p> <p>Enabled: Enable SNMP trap inform mode operation.</p> <p>Disabled: Disable SNMP trap inform mode operation.</p>
<p>Trap Inform Timeout(seconds)</p>	<p>Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.</p>
<p>Trap Inform Retry Times</p>	<p>Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.</p>
<p>Trap Probe Security Engine ID</p>	<p>Indicates the SNMP trap probe security engine ID mode of operation. Possible values are:</p> <p>Enabled: Enable SNMP trap probe security engine ID mode of operation.</p> <p>Disabled: Disable SNMP trap probe security engine ID mode of operation.</p>

Label	Description
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 between 10 and 64 hexadecimal digits, 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.

5.3.11.2 SNMP-Communities

Configure SNMPv3 communities table on this page. The entry index key is Community.

Figure 42: SNMPv3 Community Configuration

SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
<input type="checkbox"/>	public	0.0.0.0	0.0.0.0
<input type="checkbox"/>	private	0.0.0.0	0.0.0.0

Add New Entry

Save

Reset

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.

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 the ASCII characters from 33 to 126.
Source IP	Indicates the SNMP access source address.
Source Mask	Indicates the SNMP access source address mask.

5.3.11.3 SNMP-Users

Configure SNMPv3 users table on this page. The entry index keys are Engine ID and User Name.

Figure 43:SNMPv3 User Configuration

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, 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

Label	Description
	<p>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.</p>
<p>User Name</p>	<p>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 the ASCII characters from 33 to 126.</p>
<p>Security Level</p>	<p>Indicates the security model that this entry should belong to. Possible security models are:</p> <p>NoAuth, NoPriv: None authentication and none privacy.</p> <p>Auth, NoPriv: Authentication and none privacy.</p> <p>Auth, Priv: Authentication and privacy.</p> <p>The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.</p>
<p>Authentication Protocol</p>	<p>Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:</p> <p>None: None authentication protocol.</p> <p>MD5: An optional flag to indicate that this user using MD5 authentication protocol.</p> <p>SHA: An optional flag to indicate that this user using SHA authentication protocol.</p> <p>The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.</p>
<p>Authentication Password</p>	<p>A string identifying the authentication pass 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 the ASCII characters from 33 to 126.</p>

Label	Description
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are: None: None privacy protocol. DES: An optional flag to indicate that this user using DES authentication protocol.
Privacy Password	A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126.

5.3.11.4 SNMP-Groups

Configure SNMPv3 groups table on this page. The entry index keys are Security Model and Security Name.

Figure 44:SNMPv3 Group Configuration

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group
<input type="checkbox"/>	usm	default_user	default_rw_group

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
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 the 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 the ASCII characters from 33 to 126.

5.3.11.5 SNMP-Views

Configure SNMPv3 views table on this page. The entry index keys are View Name and OID Subtree.

Figure 45: SNMPv3 View Configuration

SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
<input type="checkbox"/>	default_view	included ▼	.1

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
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 the ASCII characters from 33 to 126.
View Type	<p>Indicates the view type that this entry should belong to. Possible view types are:</p> <p>included: An optional flag to indicate that this view subtree should be included.</p> <p>excluded: An optional flag to indicate that this view subtree should be excluded.</p> <p>General, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID subtree overstep the 'excluded' view entry.</p>
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(*)

5.3.11.6 SNMP-Accesses

Configure SNMPv3 accesses table on this page. The entry index keys are Group Name, Security Model and Security Level.

Figure 46: SNMP3v3 Access Configuraiton

SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	default_ro_group	any	NoAuth, NoPriv	default_view ▼	None ▼
<input type="checkbox"/>	default_rw_group	any	NoAuth, NoPriv	default_view ▼	default_view ▼

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
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 the ASCII characters from 33 to 126.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: any: Accepted any security model (v1 v2c usm). v1: Reserved for SNMPv1. v2c: Reserved for SNMPv2c. usm: User-based Security Model (USM).
Security Level	Indicates the security model that this entry should belong to. Possible security models are:

Label	Description
	<p>NoAuth, NoPriv: None authentication and none privacy.</p> <p>Auth, NoPriv: Authentication and none privacy.</p> <p>Auth, Priv: Authentication and privacy.</p>
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 the 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 the ASCII characters from 33 to 126.

5.3.12 Traffic Prioritization

5.3.12.1 Storm Control

There is a unicast storm rate control, multicast storm rate control, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

The rate is 2^n , where n is equal to or less than 15, or "No Limit". The unit of the rate can be either pps (packets per second) or kpps (kilopackets per second). The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

Note: Frames, which are sent to the CPU of the switch are always limited to approximately 4 kpps. For example, broadcasts in the management VLAN are limited to this rate. The management VLAN is configured on the IP setup page.

Figure 47: Storm Control Configuration

Storm Control Configuration

Frame Type	Enable	Rate (pps)
Unicast	<input type="checkbox"/>	1 ▼
Multicast	<input type="checkbox"/>	1 ▼
Broadcast	<input type="checkbox"/>	1 ▼

Save Reset

Label	Description
Frame Type	The settings in a particular row apply to the frame type listed here: unicast, multicast, or broadcast.
Status	Enable or disable the storm control status for the given frame type.
Rate	The rate unit is packet per second (pps), configure the rate as 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. The 1 kpps is actually 1002.1 pps.

5.3.12.2 Port Classification

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

Figure 48: QoS Ingress Port Classification

QoS Ingress Port Classification

Port	QoS class	DP level	PCP	DEI	Tag Class.	DSCP Based
*	<> ▼	<> ▼	<> ▼	<> ▼		<input type="checkbox"/>
1	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
2	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
3	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
4	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
5	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
6	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
7	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
8	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
9	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
10	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
11	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
12	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
13	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
14	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>
15	0 ▼	0 ▼	0 ▼	0 ▼	Disabled	<input type="checkbox"/>

Label	Description
Port	The port number for which the configuration below applies
QoS Class	Controls the default QoS class. All frames are classified to a QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

Label	Description
	<p>If the port is VLAN aware and the frame is tagged, then the frame is classified to a QoS class that is based on the PCP value in the tag as shown below. Otherwise the frame is classified to the default QoS class.</p> <p>PCP value: 0 1 2 3 4 5 6 7</p> <p>QoS class: 1 0 2 3 4 5 6 7</p> <p>If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a QoS class that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default QoS class.</p> <p>The classified QoS class can be overruled by a QCL entry.</p> <p>Note: If the default QoS class has been dynamically changed, then the actual default QoS class is shown in parentheses after the configured default QoS class.</p>
<p>DP level</p>	<p>Controls the default Drop Precedence Level.</p> <p>All frames are classified to a DP level.</p>

Label	Description
	<p>If the port is VLAN aware and the frame is tagged, then the frame is classified to a DP level that is equal to the DEI value in the tag. Otherwise the frame is classified to the default DP level.</p> <p>If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DP level that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DP level.</p> <p>The classified DP level can be overruled by a QCL entry.</p>
<p>PCP</p>	<p>Controls the default PCP value.</p> <p>All frames are classified to a PCP value.</p> <p>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.</p>
<p>DEI</p>	<p>Controls the default DEI value.</p> <p>All frames are classified to a DEI value.</p>

Label	Description
	<p>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.</p>
<p>Tag Class</p>	<p>Shows the classification mode for tagged frames on this port.</p> <p>Disabled: Use default QoS class and DP level for tagged frames.</p> <p>Enabled: Use mapped versions of PCP and DEI for tagged frames.</p> <p>Click on the mode in order to configure the mode and/or mapping.</p> <p>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 QoS class and DP level.</p>
<p>DSCP Based</p>	<p>Click to Enable DSCP Based QoS Ingress Port Classification.</p>

5.3.12.3 Port Tag Remaking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.

Figure 49: 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
13	Classified
14	Classified
15	Classified
16	Classified
17	Classified
18	Classified
19	Classified
20	Classified

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.

5.3.12.4 Port DSCP

This page allows you to configure the basic QoS Port DSCP Configuration settings for all switch ports.

Figure 50: Port DSCP

QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input type="checkbox"/>	<> ▼	<> ▼
1	<input type="checkbox"/>	Disable ▼	Disable ▼
2	<input type="checkbox"/>	Disable ▼	Disable ▼
3	<input type="checkbox"/>	Disable ▼	Disable ▼
4	<input type="checkbox"/>	Disable ▼	Disable ▼
5	<input type="checkbox"/>	Disable ▼	Disable ▼
6	<input type="checkbox"/>	Disable ▼	Disable ▼
7	<input type="checkbox"/>	Disable ▼	Disable ▼
8	<input type="checkbox"/>	Disable ▼	Disable ▼
9	<input type="checkbox"/>	Disable ▼	Disable ▼
10	<input type="checkbox"/>	Disable ▼	Disable ▼
11	<input type="checkbox"/>	Disable ▼	Disable ▼
12	<input type="checkbox"/>	Disable ▼	Disable ▼
13	<input type="checkbox"/>	Disable ▼	Disable ▼
14	<input type="checkbox"/>	Disable ▼	Disable ▼

Label	Description
Port	The Port column shows the list of ports for which you can configure dscp ingress and egress settings.
Ingress	<p>In Ingress settings you can change ingress translation and classification settings for individual ports.</p> <p>There are two configuration parameters available in Ingress:</p> <ol style="list-style-type: none"> 1. Translate 2. Classify
1. Translate	To Enable the Ingress Translation click the checkbox.
2. Classify	<p>Classification for a port have 4 different values.</p> <ul style="list-style-type: none"> •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	<p>Port Egress Rewriting can be one of -</p> <ul style="list-style-type: none"> •Disable: No Egress rewrite. •Enable: Rewrite enabled without remapping.

Label	Description
	<ul style="list-style-type: none"> •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 DPO' 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 DPO' table or from the 'DSCP Translation->Egress Remap DP1' table.

5.3.12.5 Port Policing

This page allows you to configure the Policer settings for all switch ports.

Figure 51: QoS Ingress Port Policers

QoS Ingress Port Policers

Port	Enabled	Rate	Unit	Flow Control
*	<input type="checkbox"/>	500	<> ▼	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
8	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
9	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
10	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
11	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
12	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
13	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
14	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
15	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>
16	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>

Label	Description
Port	The port number for which the configuration below applies
Enable	Controls whether the policer is enabled on this switch port.
Rate	Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps".
Unit	Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps".
Flow Control	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

5.3.13 Queue Policing

This page allows you to configure the Queue Policer settings for all switch ports.

Figure 52: Qos Ingress Queue Policers

QoS Ingress Queue Policers

Port	Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Label	Description
Port	The port number for which the configuration below applies.
Enable(E)	Controls whether the queue policer is enabled on this switch port.
Rate	Controls the rate for the queue policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps", and it is restricted to 1-3300 when the "Unit" is "Mbps". 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. The default value is "kbps". This field is only shown if at least one of the queue policers are enabled.

5.3.13.1 Port Scheduler

This page provides an overview of QoS Egress Port Schedulers for all switch ports.

Figure 53: 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	-	-	-	-	-	-

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.

5.3.13.2 Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports.

Figure 54: QoS Egress Port Shapers

QoS Egress Port Shapers

Port	Shapers								Port	
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7		
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
11	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
12	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
13	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
14	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
15	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
16	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
17	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
18	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
19	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
20	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

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.
Mode	Shows "disabled" or actual queue shaper rate - e.g. "800 Mbps".
Qn	Shows "disabled" or actual port shaper rate - e.g. "800 Mbps".

5.3.13.3 DSCP Based QoS

This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.

Figure 55 DSCP-Based QoS Ingress Classification

DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
∞	<input type="checkbox"/>	<> ▼	<> ▼
0 (BE)	<input type="checkbox"/>	0 ▼	0 ▼
1	<input type="checkbox"/>	0 ▼	0 ▼
2	<input type="checkbox"/>	0 ▼	0 ▼
3	<input type="checkbox"/>	0 ▼	0 ▼
4	<input type="checkbox"/>	0 ▼	0 ▼
5	<input type="checkbox"/>	0 ▼	0 ▼
6	<input type="checkbox"/>	0 ▼	0 ▼
7	<input type="checkbox"/>	0 ▼	0 ▼
8 (CS1)	<input type="checkbox"/>	0 ▼	0 ▼
9	<input type="checkbox"/>	0 ▼	0 ▼
10 (AF11)	<input type="checkbox"/>	0 ▼	0 ▼

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 value can be any of (0-7)
DPL	Drop Precedence Level (0-1)

5.3.13.4 DSCP Translation

This page allows you to configure the basic QoS DSCP Translation settings for all switches. DSCP translation can be done in Ingress or Egress.

Figure 56: DSCP Transition

DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<> ▼	<input type="checkbox"/>	<> ▼	<> ▼
0 (BE)	0 (BE) ▼	<input type="checkbox"/>	0 (BE) ▼	0 (BE) ▼
1	1 ▼	<input type="checkbox"/>	1 ▼	1 ▼
2	2 ▼	<input type="checkbox"/>	2 ▼	2 ▼
3	3 ▼	<input type="checkbox"/>	3 ▼	3 ▼
4	4 ▼	<input type="checkbox"/>	4 ▼	4 ▼
5	5 ▼	<input type="checkbox"/>	5 ▼	5 ▼
6	6 ▼	<input type="checkbox"/>	6 ▼	6 ▼
7	7 ▼	<input type="checkbox"/>	7 ▼	7 ▼
8 (CS1)	8 (CS1) ▼	<input type="checkbox"/>	8 (CS1) ▼	8 (CS1) ▼
9	9 ▼	<input type="checkbox"/>	9 ▼	9 ▼
10 (AF11)	10 (AF11) ▼	<input type="checkbox"/>	10 (AF11) ▼	10 (AF11) ▼
11	11 ▼	<input type="checkbox"/>	11 ▼	11 ▼
12 (AF12)	12 (AF12) ▼	<input type="checkbox"/>	12 (AF12) ▼	12 (AF12) ▼
13	13 ▼	<input type="checkbox"/>	13 ▼	13 ▼
14 (AF13)	14 (AF13) ▼	<input type="checkbox"/>	14 (AF13) ▼	14 (AF13) ▼
15	15 ▼	<input type="checkbox"/>	15 ▼	15 ▼
16 (CS2)	16 (CS2) ▼	<input type="checkbox"/>	16 (CS2) ▼	16 (CS2) ▼

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

Label	Description
1. Translate	DSCP at Ingress side can be translated to any of (0-63) DSCP values.
2.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.
1.Remap DP0	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.
2.Remap DP1	Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

5.3.13.5 DSCP Classification

This page allows you to configure the mapping of QoS class and Drop Precedence Level to DSCP value.

Figure 57: DSCP Classification

DSCP Classification

QoS Class	DPL	DSCP
<>	<>	<>
0	0	0 (BE) ▼
0	1	0 (BE) ▼
1	0	0 (BE) ▼
1	1	0 (BE) ▼
2	0	0 (BE) ▼
2	1	0 (BE) ▼
3	0	0 (BE) ▼
3	1	0 (BE) ▼
4	0	0 (BE) ▼
4	1	0 (BE) ▼
5	0	0 (BE) ▼
5	1	0 (BE) ▼
6	0	0 (BE) ▼
6	1	0 (BE) ▼
7	0	0 (BE) ▼
7	1	0 (BE) ▼

Save Reset

Label	Description
QoS Class	Actual QoS class
DPL	Actual Drop Precedence Level.
DSCP	Select the classified DSCP value (0-63).

5.3.13.6 QoS Control List

This page allows to edit|insert a single QoS Control Entry at a time. A QCE consists of several parameters. These parameters vary according to the frame type that you select.

Figure 58: QoS Control List Configuration

QoS Control List Configuration

QCE#	Port	Frame Type	SMAC	DMAC	VID	PCP	DEI	Action		
								Class	DPL	DSCP
+										

Label	Description
Port Members	Check the checkbox button to include the port in the QCL entry. By default all ports are included.
Key Parameters	<p>Key configuration is described as below:</p> <p>Tag Value of Tag field can be 'Any', 'Untag' or 'Tag'.</p> <p>VID Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.</p> <p>PCP Priority Code Point: Valid value 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'.</p> <p>DEI Drop Eligible Indicator: Valid value of DEI can be any of values between 0, 1 or 'Any'.</p> <p>SMAC Source MAC address: 24 MS bits (OUI) or 'Any'.</p> <p>DMAC Type Destination MAC type: possible values are unicast(UC), multicast(MC), broadcast(BC) or 'Any'.</p> <p>Frame Type Frame Type can have any of the following values:</p> <ol style="list-style-type: none"> 1. Any 2. Ethernet 3. LLC 4. SNAP 5. IPv4

Label	Description
	<p>6. IPv6</p> <p>Note: All frame types are explained below.</p>
1.Any	Allow all types of frames.
2. Ethernet	Ethernet Type Valid Ethernet type can have a value within 0x600-0xFFFF or 'Any' but excluding 0x800(IPv4) and 0x86DD(IPv6), default value is 'Any'.
3.LLC	<p>SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'.</p> <p>DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'.</p> <p>Control Valid Control field can vary from 0x00 to 0xFF or 'Any', the default value is 'Any'.</p>
4.SNAP	PID Valid PID(a.k.a Ethernet type) can have value within 0x00-0xFFFF or 'Any', default value is 'Any'.
5.IPv4	<p>Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'.</p> <p>Source IP Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero.</p>

Label	Description
	<p>DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.</p> <p>IP Fragment Ipv4 frame fragmented option: yes no any.</p> <p>Sport Source TCP/UDP port(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.</p> <p>Dport Destination TCP/UDP port(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP</p>
<p>6.IPv6</p>	<p>Protocol IP protocol number: (0-255, TCP or UDP) or 'Any'.</p> <p>Source IP IPv6 source address: (a.b.c.d) or 'Any', 32 LS bits.</p> <p>DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.</p> <p>Sport Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.</p> <p>Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.</p>
<p>Action Parameters</p>	<p>Class QoS class: (0-7) or 'Default'.</p> <p>DP Valid Drop Precedence Level can be (0-1) or 'Default'.</p> <p>DSCP Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.</p>

Label	Description
	'Default' means that the default classified value is not modified by this QCE.

5.3.13.6.1 QoS Counters

This page provides statistics for the different queues for all switch ports.

Figure 59: Queueing Counters

Queueing Counters

Auto-refresh Refresh Clear

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	195398	0	0	0	0	0	0	0	0	0	0	0	0	0	0	167538
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Label	Description
Port	The logical port for the settings contained in the same row.
Qn	There are 8 QoS queues per port. Q0 is the lowest priority queue.
Rx / Tx	The number of received and transmitted packets per queue.

5.1.1.1 QCL Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

Figure 60: QoS Control List Status

Combined ▾
Auto-refresh
Resolve Conflict
Refresh

QoS Control List Status

User	QCE#	Frame Type	Port	Action			Conflict
				Class	DPL	DSCP	
No entries							

Label	Description
User	Indicates the QCL user.
QCE#	Indicates the index of QCE.
Frame Type	<p>Indicates the type of frame to look for incoming frames. Possible frame types are:</p> <p>Any: The QCE will match all frame type.</p> <p>Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed.</p> <p>LLC: Only (LLC) frames are allowed.</p> <p>SNAP: Only (SNAP) frames are allowed.</p> <p>IPv4: The QCE will match only IPV4 frames.</p>

Label	Description
	IPv6: The QCE will match only IPV6 frames.
Port	Indicates the list of ports configured with the QCE.
Action	<p>Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.</p> <p>There are three action fields: Class, DPL and DSCP.</p> <p>Class: Classified QoS class; if a frame matches the QCE it will be put in the queue.</p> <p>DPL: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column.</p> <p>DSCP: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column.</p>
Conflict	Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

5.3.14 Multicast

5.3.14.1 IGMP Snooping

This page provides IGMP Snooping related configuration.

Figure 61: IGMP Snooping Configuration

IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input checked="" type="checkbox"/>

Port Related Configuration

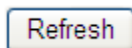
Port	Router Port	Fast Leave
*	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>

Label	Description
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMCv4 Flooding enabled	Enable unregistered IPMC traffic flooding.
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.

5.3.14.2 IGMP Snooping- VLAN Configuration-

Each page shows up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the



button will update the displayed table starting from that or the next closest VLAN Table match.



The button will use the last entry of the currently displayed entry as a basis for the next lookup.

When the end is reached the text "No more entries" is shown in the displayed table. Use the



button to start over.

Figure 62: IGMP Snooping VLAN Configuration

IGMP Snooping VLAN Configuration

Refresh |<< >>

Start from VLAN with entries per page.

Delete	VLAN ID	Snooping Enabled	IGMP Querier
Add New IGMP VLAN			

Save Reset

Label	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enable	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.

Label	Description
IGMP Querier	Enable the IGMP Querier in the VLAN.

5.3.14.3 IGMP Snooping Status

This page provides IGMP Snooping status.

Figure 63: IGMP Snooping Status

Auto-refresh Refresh Clear

IGMP Snooping Status

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	-

Label	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	Working Querier Version currently.
Host Version	Working Host Version currently.
Querier Status	Show the Querier status is "ACTIVE" or "IDLE".
Querier Receive	The number of Transmitted Querier.
V1 Reports Receive	The number of Received V1 Reports.

Label	Description
V2 Reports Receive	The number of Received V2 Reports.
V3 Reports Receive	The number of Received V3 Reports.
V2 Leave Receive	The number of Received V2 Leave.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
<input type="button" value="Clear"/>	Clears all Statistics counters.
Auto-refresh <input type="checkbox"/>	Check this box to enable an automatic refresh of the page at regular intervals.
Port	Switch Port number
Status	Indicate whether specific port is a router port or not .

5.3.14.4 IGMP Snooping Groups Information

Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group.

Figure 64: IGMP Snooping Group Information

IGMP Snooping Group Information

Auto-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	13	14	15	16	17	18	19	20
No more entries																					

Label	Description
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group..

5.3.15 Security

5.3.15.1 Remote Control Security Configuration

Remote Control Security allows you limit the remote access of management interface. When enabled, the request of client which is not in the allow list will be rejected.

Figure 65: Remote Control Security Configuration

Remote Control Security Configuration

Mode

Delete Port IP Web Telnet SNMP

Label	Description
Port	Port number of remote client.
IP Address	IP address of remote client. Keeps this field "0.0.0.0" means "Any IP".
Web	Check this item to enable Web management interface.
Telnet	Check this item to enable Telnet management interface.
SNMP	Check this item to enable SNMP management interface
Delete	Check this item to delete.

5.3.15.2 ACL

5.3.15.2.1 Ports

Configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

Figure 66: ACL Ports Configuration

ACL Ports Configuration

Refresh Clear

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	208902
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

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 1 through 8. The default value is 1.
Action	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".
Rate Limiter ID	Select which rate limiter to apply to this port. The allowed values are Disabled or the values 1 through 15. The default value is "Disabled".
Port Copy	Select which port frames are copied to. The allowed values are Disabled or a specific port number. The default value is "Disabled".

Label	Description
Logging	<p>Specify the logging operation of this port. The allowed values are:</p> <p>Enabled: Frames received on the port are stored in the System Log.</p> <p>Disabled: Frames received on the port are not logged.</p> <p>The default value is "Disabled". Please note that the System Log memory size and logging rate is limited.</p>
Shutdown	<p>Specify the port shut down operation of this port. The allowed values are:</p> <p>Enabled: If a frame is received on the port, the port will be disabled.</p> <p>Disabled: Port shut down is disabled.</p> <p>The default value is "Disabled".</p>
Counter	Counts the number of frames that match this ACE.

5.3.15.2.2 Rate Limiters

Configure the rate limiter for the ACL of the switch.

Figure 67: ACL Rate Limiter Configuration

ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	1	<> ▼
1	1	pps ▼
2	1	pps ▼
3	1	pps ▼
4	1	pps ▼
5	1	pps ▼
6	1	pps ▼
7	1	pps ▼
8	1	pps ▼
9	1	pps ▼
10	1	pps ▼
11	1	pps ▼
12	1	pps ▼
13	1	pps ▼
14	1	pps ▼
15	1	pps ▼
16	1	pps ▼

Save Reset

Label	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate	The rate unit is packet per second (pps), configure the rate as 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. The 1 kpps is actually 1002.1 pps.

5.3.15.2.3 ACL Control List

Configure an ACE (Access Control Entry) on this page.

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type that you selected.

A frame that hits this ACE matches the configuration that is defined here.

Figure 68: Access Control List Configuration

Auto-refresh Refresh Clear Remove All

Access Control List Configuration

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

Label	Description
Ingress Port	<p>Select the ingress port for which this ACE applies.</p> <p>Any: The ACE applies to any port.</p> <p>Port n: The ACE applies to this port number, where n is the number of the switch port.</p> <p>Policy n: The ACE applies to this policy number, where n can range from 1 through 8.</p>
Frame Type	<p>Select the frame type for this ACE. These frame types are mutually exclusive.</p> <p>Any: Any frame can match this ACE.</p> <p>Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications should be greater than or equal to 1536 decimal (equal to 0600 hexadecimal).</p>

Label	Description
	<p>ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with Ethernet type.</p> <p>IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with Ethernet type.</p>
Action	<p>Specify the action to take with a frame that hits this ACE.</p> <p>Permit: The frame that hits this ACE is granted permission for the ACE operation.</p> <p>Deny: The frame that hits this ACE is dropped.</p>
Rate Limiter	<p>Specify the rate limiter in number of base units. The allowed range is 1 to 15. Disabled indicates that the rate limiter operation is disabled.</p>
Port Copy	<p>Frames that hit the ACE are copied to the port number specified here. The allowed range is the same as the switch port number range. Disabled indicates that the port copy operation is disabled.</p>
Logging	<p>Specify the logging operation of the ACE. The allowed values are:</p> <p>Enabled: Frames matching the ACE are stored in the System Log.</p> <p>Disabled: Frames matching the ACE are not logged.</p> <p>Please note that the System Log memory size and logging rate is limited.</p>
Shutdown	<p>Specify the port shut down operation of the ACE. The allowed values are:</p> <p>Enabled: If a frame matches the ACE, the ingress port will be disabled.</p> <p>Disabled: Port shut down is disabled for the ACE.</p>
Counter	<p>The counter indicates the number of times the ACE was hit by a frame.</p>

Figure 69: MAC Parameters

MAC Parameters

SMAC Filter	Specific ▼
SMAC Value	00-00-00-00-00-01
DMAC Filter	MC ▼

Label	Description
SMAC Filter	<p>(Only displayed when the frame type is Ethernet Type or ARP.)</p> <p>Specify the source MAC filter for this ACE.</p> <p>Any: No SMAC filter is specified. (SMAC filter status is "don't-care".)</p> <p>Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.</p>
SMAC Value	<p>When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this SMAC value.</p>
DMAC Filter	<p>Specify the destination MAC filter for this ACE.</p> <p>Any: No DMAC filter is specified. (DMAC filter status is "don't-care".)</p> <p>MC: Frame must be multicast.</p> <p>BC: Frame must be broadcast.</p> <p>UC: Frame must be unicast.</p> <p>Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.</p>

Label	Description
DMAC Value	When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this DMAC value.

Figure 70: VLAN Parameters

VLAN Parameters

802.1Q Tagged	Any ▼
VLAN ID Filter	Any ▼
Tag Priority	Any ▼

Label	Description
VLAN ID Filter	Specify the VLAN ID filter for this ACE. Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".) Specific: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.
VLAN ID	When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.
Tag Priority	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value Any means that no tag priority is specified (tag priority is "don't-care".)

Figure 71: IP Parameters

IP Parameters

IP Protocol Filter	Any ▼
IP TTL	Any ▼
IP Fragment	Any ▼
IP Option	Any ▼
SIP Filter	Any ▼
DIP Filter	Any ▼

Save Reset Cancel

Label	Description
IP Protocol Filter	<p>Specify the IP protocol filter for this ACE.</p> <p>Any: No IP protocol filter is specified ("don't-care").</p> <p>Specific: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.</p> <p>ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file.</p> <p>UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file.</p> <p>TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.</p>
IP TTL	<p>Specify the Time-to-Live settings for this ACE.</p> <p>zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.</p> <p>non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.</p>

Label	Description
	Any: Any value is allowed ("don't-care").
IP Fragment	<p>Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.</p> <p>No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.</p> <p>Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>
IP Option	<p>Specify the options flag setting for this ACE.</p> <p>No: IPv4 frames where the options flag is set must not be able to match this entry.</p> <p>Yes: IPv4 frames where the options flag is set must be able to match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>
SIP Filter	<p>Specify the source IP filter for this ACE.</p> <p>Any: No source IP filter is specified. (Source IP filter is "don't-care".)</p> <p>Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.</p> <p>Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.</p>
DIP Filter	Specify the destination IP filter for this ACE.

Label	Description
	<p>Any: No destination IP filter is specified. (Destination IP filter is "don't-care".)</p> <p>Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.</p> <p>Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.</p>

Figure 72: ARP Parameters

ARP Parameters

ARP/RARP	Any ▼
Request/Reply	Any ▼
Sender IP Filter	Any ▼
Target IP Filter	Any ▼

ARP Sender MAC Match	Any ▼
RARP Target MAC Match	Any ▼
IP/Ethernet Length	Any ▼
IP	Any ▼
Ethernet	Any ▼

Label	Description
ARP/RARP	<p>Specify the available ARP/RARP opcode (OP) flag for this ACE.</p> <p>Any: No ARP/RARP OP flag is specified. (OP is "don't-care".)</p> <p>ARP: Frame must have ARP/RARP opcode set to ARP.</p> <p>RARP: Frame must have ARP/RARP opcode set to RARP.</p> <p>Other: Frame has unknown ARP/RARP Opcode flag.</p>
Request/Reply	<p>Specify the available ARP/RARP opcode (OP) flag for this ACE.</p> <p>Any: No ARP/RARP OP flag is specified. (OP is "don't-care".)</p> <p>Request: Frame must have ARP Request or RARP Request OP flag set.</p> <p>Reply: Frame must have ARP Reply or RARP Reply OP flag.</p>
Sender IP Filter	<p>Specify the sender IP filter for this ACE.</p> <p>Any: No sender IP filter is specified. (Sender IP filter is "don't-care".)</p> <p>Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.</p> <p>Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.</p>
Sender IP Address	<p>When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.</p>
Sender IP Mask	<p>When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.</p>
Target IP Filter	<p>Specify the target IP filter for this specific ACE.</p>

Label	Description
	<p>Any: No target IP filter is specified. (Target IP filter is "don't-care".)</p> <p>Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears. Network: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.</p>
Target IP Adress	When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.
Target IP Mask	When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.
ARP SMAC Match	<p>Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.</p> <p>0: ARP frames where SHA is not equal to the SMAC address.</p> <p>1: ARP frames where SHA is equal to the SMAC address.</p> <p>Any: Any value is allowed ("don't-care").</p>
RARP SMAC Match	<p>Specify whether frames can hit the action according to their target hardware address field (THA) settings.</p> <p>0: RARP frames where THA is not equal to the SMAC address.</p> <p>1: RARP frames where THA is equal to the SMAC address.</p> <p>Any: Any value is allowed ("don't-care").</p>
IP/Ethernet Length	Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.

Label	Description
	<p>0: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must not match this entry.</p> <p>1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>
<p style="text-align: center;">IP</p>	<p>Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.</p> <p>0: ARP/RARP frames where the HLD is equal to Ethernet (1) must not match this entry.</p> <p>1: ARP/RARP frames where the HLD is equal to Ethernet (1) must match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>
<p style="text-align: center;">Ethernet</p>	<p>Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.</p> <p>0: ARP/RARP frames where the PRO is equal to IP (0x800) must not match this entry.</p> <p>1: ARP/RARP frames where the PRO is equal to IP (0x800) must match this entry.</p> <p>Any: Any value is allowed ("don't-care").</p>

5.3.15.3 Authentication Server

5.3.15.3.1 Common Server Configuration

This page allows you to configure the Authentication Servers

Figure 73: Authentication Server Configuration

Authentication Server Configuration

Common Server Configuration

Timeout	15	seconds
Dead Time	300	seconds

Label	Description
Timeout	<p>The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server.</p> <p>If the server does not reply within this time frame, we will consider it to be dead and continue with the next enabled server (if any).</p> <p>RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.</p>
Dead Time	<p>The Dead Time, which can be set to a number between 0 and 3600 seconds, 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.</p> <p>Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.</p>

5.3.15.3.2 RADIUS Authentication Server Configuration

The table has one row for each RADIUS Authentication Server and a number of columns, which are:

Figure 74: RADIUS Authentication Server Configuration

RADIUS Authentication Server Configuration

#	Enabled	IP Address	Port	Secret
1	<input type="checkbox"/>		1812	<input type="password"/>
2	<input type="checkbox"/>		1812	<input type="password"/>
3	<input type="checkbox"/>		1812	<input type="password"/>
4	<input type="checkbox"/>		1812	<input type="password"/>
5	<input type="checkbox"/>		1812	<input type="password"/>

Label	Description
#	The RADIUS Authentication Server number for which the configuration below applies.
Enabled	Enable the RADIUS Authentication Server by checking this box.
IP Address	The IP address or hostname of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation.
Port	The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.
Secret	The secret - up to 29 characters long - shared between the RADIUS Authentication Server and the switch stack.

5.1.1.1.1 RADIUS Accounting Server Configuration

Figure 75: RADIUS Accounting Server Configuration

RADIUS Accounting Server Configuration

#	Enabled	IP Address	Port	Secret
1	<input type="checkbox"/>		1813	<input type="password"/>
2	<input type="checkbox"/>		1813	<input type="password"/>
3	<input type="checkbox"/>		1813	<input type="password"/>
4	<input type="checkbox"/>		1813	<input type="password"/>
5	<input type="checkbox"/>		1813	<input type="password"/>

Label	Description
#	The RADIUS Accounting Server number for which the configuration below applies.
Enabled	Enable the RADIUS Accounting Server by checking this box.
IP Address	The IP address or hostname of the RADIUS Accounting Server. IP address is expressed in dotted decimal notation.
Port	The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.
Secret	The secret - up to 29 characters long - shared between the RADIUS Accounting Server and the switch stack.

5.3.16 RADIUS Overview

This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page.

RADIUS Authentication Servers

Figure 76: RADIUS Authentication Server Status Overview

RADIUS Authentication Server Status Overview

Auto-refresh Refresh

#	IP Address	Status
1	0.0.0.0:1812	Disabled
2	0.0.0.0:1812	Disabled
3	0.0.0.0:1812	Disabled
4	0.0.0.0:1812	Disabled
5	0.0.0.0:1812	Disabled

Label	Description
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
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.

Label	Description
	<p>Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.</p> <p>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.</p>

RADIUS Accounting Servers

Figure 77: RADIUS Accounting Server Status Overview

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:1813	Disabled
2	0.0.0.0:1813	Disabled
3	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
5	0.0.0.0:1813	Disabled

Label	Description
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
Status	The current status of the server. This field takes one of the following values:

Label	Description
	<p>Disabled: The server is disabled.</p> <p>Not Ready: The server is enabled, but IP communication is not yet up and running.</p> <p>Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.</p> <p>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.</p>

5.3.16.1 RADIUS Details

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for. The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for.

Figure 78: RADIUS Authentication Statistics for Server #1

RADIUS Authentication Statistics for Server #1

Server #1 ▾	Auto-refresh <input type="checkbox"/>	Refresh	Clear
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		0.0.0.0:1812	
State		Disabled	
Round-Trip Time		0 ms	

Label	Description
Packet Counters	RADIUS authentication server packet counter. There are seven receive and four transmit counters.
Other Info	This section contains information about the state of the server and the latest round-trip time.

Figure 79: RADIUS ACcounting Statistics for Server #1

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	0.0.0.0:1813		
State	Disabled		
Round-Trip Time	0 ms		

Label	Description
Packet Counters	RADIUS accounting server packet counter. There are five receive and four transmit counters.
Other Info	This section contains information about the state of the server and the latest

5.3.16.2 NAS(802.1x)

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the Authentication configuration page.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X software installed on his system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1 X authentications.

Overview of 802.1X (Port-Based) Authentication

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch is special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server is RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the Authentication configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames

at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Overview of MAC-Based Authentication

Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using static entries into the MAC Table. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users, equipment whose MAC address is a valid RADIUS user can be used by anyone, and only the MD5-Challenge method is supported.

The 802.1X and MAC-Based Authentication configuration consists of two sections, a system- and a port-wide

Figure 80: Network Access Server Configuration

Refresh

Network Access Server Configuration

System Configuration

Mode	Disabled ▼	
Reauthentication Enabled	<input type="checkbox"/>	
Reauthentication Period	3600	seconds
EAPOL Timeout	30	seconds
Aging Period	300	seconds
Hold Time	10	seconds

Port Configuration

Port	Admin State	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

Label	Description
Mode	Indicates if 802.1X and MAC-based authentication is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
Reauthentication Enabled	<p>If checked, 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.</p> <p>For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication</p>

Label	Description
	between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Age 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.
Age Period	<p>This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:</p> <ul style="list-style-type: none"> • MAC-Based Auth. <p>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.</p> <p>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.</p>
Hold Time	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

Label	Description
	<ul style="list-style-type: none"> • MAC-Based Auth. <p>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.</p> <p>The switch will ignore new frames coming from the client during the hold time.</p> <p>The Hold Time can be set to a number between 10 and 1000000 seconds.</p>
Port	The port number for which the configuration below applies.
Admin State	<p>If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:</p> <p>Force Authorized</p> <p>In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.</p> <p>Force Unauthorized</p> <p>In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access.</p> <p>Port-based 802.1X</p>

Label	Description
	<p>In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch is special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server is RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.</p> <p>When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.</p> <p>Note: Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the</p>

Label	Description
	<p>supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.</p> <p>Single 802.1X</p> <p>In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant.</p> <p>Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.</p> <p>Multi 802.1X</p>

Label	Description
	<p>In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Multi 802.1X variant.</p> <p>Multi 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.</p> <p>In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.</p> <p>The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.</p> <p>MAC-based Auth.</p>

Label	Description
	<p>Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.</p> <p>When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard.</p> <p>The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is</p>

Label	Description
	<p>supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.</p>
<p>Port State</p>	<p>The current state of the port. It can undertake one of the following values:</p> <p>Globally Disabled: NAS is globally disabled.</p> <p>Link Down: NAS is globally enabled, but there is no link on the port.</p> <p>Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.</p> <p>Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.</p> <p>X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.</p>
<p>Restart</p>	<p>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.</p> <p>Clicking these buttons will not cause settings changed on the page to take effect.</p> <p>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.</p> <p>The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.</p>

Label	Description
	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.

Switch

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

Figure 81: Network Access Server Switch Status

Network Access Server Switch Status

Auto-refresh Refresh

Port	Admin State	Port State	Last Source	Last 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		

Label	Description
Port	The switch port number. Click to navigate to detailed 802.1X 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.

Label	Description
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.

This page provides detailed IEEE 802.1X statistics for a specific switch port running port-based authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only. Use the port select box to select which port details to be displayed.

Figure 82: NAS Statistics Port 1

NAS Statistics Port 1

Port 1 ▾ Auto-refresh Refresh

Port State

Admin State Force Authorized
Port State Globally Disabled

Label	Description
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.

Label	Description
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
EAPOL Counters	<p>These supplicant frame counters are available for the following administrative states:</p> <ul style="list-style-type: none"> • Force Authorized • Force Unauthorized • 802.1X
Backend Server Counters	<p>These backend (RADIUS) frame counters are available for the following administrative states:</p> <ul style="list-style-type: none"> • 802.1X • MAC-based Auth.
Last Supplicant/Client Info	<p>Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:</p> <ul style="list-style-type: none"> • 802.1X • MAC-based Auth.

5.3.17 Warning

5.3.17.1 Fault Alarm

When any selected fault event is happened, the Fault LED in switch panel will light up and the electric relay will signal at the same time.

5.3.18 System Warning

5.3.18.1 SYSLOG Setting

The SYSLOG is a protocol to transmit event notification messages across networks. Please refer to RFC 3164 - The BSD SYSLOG Protocol

Figure 83: System Log Configuration

System Log Configuration

Server Mode	Disabled ▾
Server Address	0.0.0.0

The following table describes the labels in this screen.

Label	Description
Server Mode	<p>Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are:</p> <p>Enabled: Enable server mode operation.</p> <p>Disabled: Disable server mode operation.</p>
SYSLOG Server IP Address	<p>Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a host name.</p>

5.3.18.1.1 Event Selection

SYSLOG and SMTP are the two warning methods that supported by the system. Check the corresponding box to enable system event warning method you wish to choose. Please note that the checkbox cannot be checked when SYSLOG or SMTP is disabled.

Figure 84: System Warning

System Warning - Event Selection

System Events	SYSLOG
System Start	<input type="checkbox"/>
Power Status	<input type="checkbox"/>
SNMP Authentication Failure	<input type="checkbox"/>
Redundant Ring Topology Change	<input type="checkbox"/>

Port	SYSLOG	Port	SYSLOG
1	Disabled ▼	2	Disabled ▼
3	Disabled ▼	4	Disabled ▼
5	Disabled ▼	6	Disabled ▼
7	Disabled ▼	8	Disabled ▼
9	Disabled ▼	10	Disabled ▼
11	Disabled ▼	12	Disabled ▼
13	Disabled ▼	14	Disabled ▼
15	Disabled ▼	16	Disabled ▼
17	Disabled ▼	18	Disabled ▼
19	Disabled ▼	20	Disabled ▼

The following table describes the labels in this screen.

Label	Description
System Cold Start	Alert when system restart
Power Status	Alert when a power up or down
SNMP Authentication Failure	Alert when SNMP authentication failure.

Label	Description
Redundant Ring Topology Change	Alert when Redundant Ring topology changes.
Port Event SYSLOG / SMTP event	<ul style="list-style-type: none"> ■ Disable ■ Link Up ■ Link Down ■ Link Up & Link Down
Apply	Click “Apply” to activate the configurations.
Help	Show help file.

5.3.19 Monitor and Diag

5.3.19.1 MAC Table

5.3.19.1.1 Configuration

The MAC Address Table is configured on this page. Set timeouts for entries in the dynamic MAC Table and configure the static MAC table here.

Figure 85: MAC Address Table Configuration

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	<input type="checkbox"/>
Aging Time	300 seconds

MAC Table Learning

	Port Members																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Auto	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Static MAC Table Configuration

			Port Members																			
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Add New Static Entry																						
Save			Reset																			

5.3.19.1.2 Aging Configuration

By default, dynamic entries are removed from the MAC after 300 seconds. This removal is also called aging.

Configure aging time by entering a value here in seconds; for example, **Age time** seconds.

The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking **Disable automatic aging.**

5.3.19.2 MAC Table Learning

If the learning mode for a given port is grayed 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:

Figure 86: MAC Table Learning

MAC Table Learning

	Port Members																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Auto	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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.

5.3.19.3 Static MAC Table Configuration

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

The maximum of 64 entries is for the whole stack, and not per switch.

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

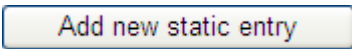
Figure 87: Static MAC Table Configuration

Static MAC Table Configuration

			Port Members																			
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

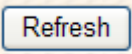
Add New Static Entry

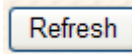
Save Reset


Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for 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  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".

5.3.19.4 MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "Start from MAC address" and "VLAN" input fields allow the user to select the starting point in the MAC Table. Clicking the  button will update the displayed table starting from that

or the closest next MAC Table match. In addition, the two input fields will - upon a  button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The  will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "no more entries" is shown in the displayed table.






Use the  button to start over.

Figure 88: MAC Address Table

MAC Address Table

Auto-refresh    

Start from VLAN and MAC address with entries per page.

Type	VLAN	MAC Address	CPU	Port Members																			
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Static	1	00-1E-94-01-B3-11	✓																				
Dynamic	1	68-F7-28-D0-C5-78	✓																				
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	

Label	Description
Type	Indicates whether the entry is a static or 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.

5.3.20 Port Statistic

5.3.20.1 Traffic Overview

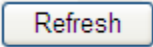
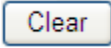
This page provides an overview of general traffic statistics for all switch ports.

Figure 89: Port Statistics Overview

Port Statistics Overview

Auto-refresh Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	7852	5732	1544400	3322541	0	0	0	0	144
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0

Label	Description
Port	The logical port for the settings contained in the same row.
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions per port.
Drops	The number of frames discarded due to ingress or egress congestion.
Filtered	The number of received frames filtered by the forwarding process.
Auto-refresh <input type="checkbox"/>	Check this box to enable an automatic refresh of the page at regular intervals.
	Updates the counters entries, starting from the current entry ID.
	Flushes all counters entries.

5.3.20.2 Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Detailed Statistics-Receive & Transmit Total

Figure 90: Detailed Port Statistics - Port 1

Detailed Port Statistics Port 1

Port 1 Auto-refresh

Receive Total		Transmit Total	
Rx Packets	8507	Tx Packets	6222
Rx Octets	1676114	Tx Octets	3601902
Rx Unicast	8154	Tx Unicast	6170
Rx Multicast	144	Tx Multicast	52
Rx Broadcast	209	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	5386	Tx 64 Bytes	91
Rx 65-127 Bytes	246	Tx 65-127 Bytes	459
Rx 128-255 Bytes	27	Tx 128-255 Bytes	2739
Rx 256-511 Bytes	2812	Tx 256-511 Bytes	282
Rx 512-1023 Bytes	36	Tx 512-1023 Bytes	1783
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	868
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	8507	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	6222
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	144		

Label	Description
Rx and Tx Packets	The number of received and transmitted (good and bad) packets.
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
Rx and Tx Unicast	The number of received and transmitted (good and bad) unicast packets.
Rx and Tx Multicast	The number of received and transmitted (good and bad) multicast packets.
Rx and Tx Broadcast	The number of received and transmitted (good and bad) broadcast packets.

Label	Description
Rx and Tx Pause	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
Rx Drops	The number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short 1 frames received with valid CRC.
Rx Oversize	The number of long 2 frames received with valid CRC.
Rx Fragments	The number of short 1 frames received with invalid CRC.
Rx Jabber	The number of long 2 frames received with invalid CRC.
Rx Filtered	The number of received frames filtered by the forwarding process.
Tx Drops	The number of frames dropped due to output buffer congestion.
Tx Late / Exc.Coll.	The number of frames dropped due to excessive or late collisions.

Short frames are frames that are smaller than 64 bytes.

Long frames are frames that are longer than the configured maximum frame length for this port.

5.3.20.3 Port Mirroring

Configure port Mirroring on this page.

To debug network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow.

The traffic to be copied to the mirror port is selected as follows:

All frames received on a given port (also known as ingress or source mirroring).

All frames transmitted on a given port (also known as egress or destination mirroring).

Port to mirror also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this port. Disabled disables mirroring.

Figure 91: Mirror Configuration

Mirror Configuration

Port to mirror to Disabled ▼

Mirror Port Configuration

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

Label	Description
Port	The logical port for the settings contained in the same row.
Mode	<p>Select mirror mode.</p> <p>Rx only : Frames received at this port are mirrored to the mirror port. Frames transmitted are not mirrored.</p> <p>Tx only : Frames transmitted from this port are mirrored to the mirror port. Frames received are not mirrored.</p>

Label	Description
	<p>Disabled : Neither frames transmitted nor frames received are mirrored.</p> <p>Enabled : Frames received and frames transmitted are mirrored to the mirror port.</p> <p>Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames for the mirror port. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.</p>

5.3.20.4 System Log Information

The switch system log information is provided here.

Figure 92: System Log Information

System Log Information

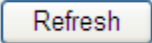
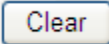




Auto-refresh Refresh Clear |<< << >> >>|

The total number of entries is 0 for the given level.

Start from ID with entries per page.

ID	Time	Message
No system log entries		

Label	Description
ID	The ID (≥ 1) of the system log entry.
Level	The level of the system log entry. The following level types are supported:

Label	Description
	<p>Info: Information level of the system log.</p> <p>Warning: Warning level of the system log.</p> <p>Error: Error level of the system log.</p> <p>All: All levels.</p>
Time	The time of the system log entry.
Message	The MAC Address of this switch.
Auto-refresh <input type="checkbox"/>	Check this box to enable an automatic refresh of the page at regular intervals.
	Updates the system log entries, starting from the current entry ID.
	Flushes all system log entries.
	Updates the system log entries, starting from the first available entry ID.
	Updates the system log entries, ending at the last entry currently displayed.
	Updates the system log entries, starting from the last entry currently displayed.
	Updates the system log entries, ending at the last available entry ID.

5.3.20.5 Cable Diagnostics

This page is used for running the VeriPHY Cable Diagnostics.

Figure 93: VeriPHY Cable Diagnostics

VeriPHY Cable Diagnostics

Port

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	--	--	--	--	--	--	--	--

Press 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.

Label	Description
Port	The port where you are requesting VeriPHY Cable Diagnostics.
Cable Status	Port: Port number. Pair: The status of the cable pair. Length: The length (in meters) of the cable pair.

5.3.20.6 SFP Monitor

The DDM function can pass SFP module which supports DDM function, measure the temperature of the apparatus .And manage and set up event alarm module through DDM WEB

Figure 94: SFP Monitor

SFP Monitor

Auto-refresh Refresh

Port No.	Temperature (°C)	Vcc (V)	TX Bias (mA)	TX Power (mW)	(dBm)	RX Power (mW)	(dBm)
9	N/A	N/A	N/A	N/A	N/A	N/A	N/A
10	N/A	N/A	N/A	N/A	N/A	N/A	N/A
11	N/A	N/A	N/A	N/A	N/A	N/A	N/A
12	N/A	N/A	N/A	N/A	N/A	N/A	N/A
13	N/A	N/A	N/A	N/A	N/A	N/A	N/A
14	N/A	N/A	N/A	N/A	N/A	N/A	N/A
15	N/A	N/A	N/A	N/A	N/A	N/A	N/A
16	N/A	N/A	N/A	N/A	N/A	N/A	N/A
17	N/A	N/A	N/A	N/A	N/A	N/A	N/A
18	N/A	N/A	N/A	N/A	N/A	N/A	N/A
19	N/A	N/A	N/A	N/A	N/A	N/A	N/A
20	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Warning Temperature :

°C(0~100)

Event Alarm :

Syslog

5.3.20.7 Ping

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

Figure 95: ICMP Ping

ICMP Ping

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

Start

After you press , 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING6 server ::10.10.132.20
```

```
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
```

```
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
```

```
64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms
```

```
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms
```

```
64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms
```

```
Sent 5 packets, received 5 OK, 0 bad
```

You can configure the following properties of the issued ICMP packets:

Label	Description
IP Address	The destination IP Address.
Ping Size	The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.

5.3.20.8 Synchronization-PTP

Overview of MAC-Based Authentication

This page allows the user to configure and inspect the current PTP clock settings.

PTP External Clock Mode

Figure 96: PTP External Clock Mode

PTP External Clock Mode

One_PPS_Mode	Disable ▼
External Enable	False ▼
VCXO Enable	False ▼
Clock Frequency	1

Label	Description
One_pps_mode	<p>This Selection box will allow you to select the One_pps_mode configuration.</p> <p>The following values are possible:</p> <ol style="list-style-type: none"> 1. Output : Enable the 1 pps clock output 2. Input : Enable the 1 pps clock input 3. Disable : Disable the 1 pps clock in/out-put
External Enable	<p>This Selection box will allow you to configure the External Clock output.</p> <p>The following values are possible:</p> <ol style="list-style-type: none"> 1. True : Enable the external clock output 2. False : Disable the external clock output
VCXO_Enable	<p>This Selection box will allow you to configure the External VCXO rate adjustment.</p> <p>The following values are possible:</p> <ol style="list-style-type: none"> 1. True : Enable the external VCXO rate adjustment 2. False : Disable the external VCXO rate adjustment
Clock Frequency	<p>This will allow to set the Clock Frequency.</p> <p>The possible range of values are 1 - 25000000 (1 - 25MHz)</p>

PTP Clock Configuration

Figure 97: PTP Clock Configuration

PTP Clock Configuration

			Port List																				
Delete	Clock Instance	Device Type	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
No Clock Instances Present																							
<input type="button" value="Add New PTP Clock"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>																							

Label	Description
Delete	Check this box and click on 'Save' to delete the clock instance.
Clock Instance	Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to edit the Clock details.
Device Type	Indicates the Type of the Clock Instance. There are five Device Types. 1. Ord-Bound - clock's Device Type is Ordinary-Boundary Clock. 2. P2p Transp - clock's Device Type is Peer to Peer Transparent Clock. 3. E2e Transp - clock's Device Type is End to End Transparent Clock. 4. Master Only - clock's Device Type is Master Only. 5. Slave Only - clock's Device Type is Slave Only.
Port List	Set check mark for each port configured for this Clock Instance.

Label	Description
2 Step Flag	Static member: defined by the system, true if two-step Sync events and Pdelay_Resp events are used
Clock Identity	It shows unique clock identifier
One Way	If true, one-way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.
Protocol	<p>Transport protocol used by the PTP protocol engine</p> <p>Ethernet PTP over Ethernet multicast</p> <p>ip4multi PTP over IPv4 multicast</p> <p>ip4uni PTP over IPv4 unicast</p> <p>Note : IPv4 unicast protocol only works in Master only and Slave only clocks</p> <p>See parameter Device Type</p> <p>In a unicast Slave only clock you also need configure which master clocks to request Announce and Sync messages from. See: Unicast Slave Configuration</p>
VLAN Tag Enable	<p>Enables the VLAN tagging for the PTP frames.</p> <p>Note: Packets are only tagged if the port is configured for vlan tagging. i.e:</p> <p>Port Type != Unaware and PortVLAN mode == None, and the port is member of the VLAN.</p>

Label	Description
VID	VLAN Identifier used for tagging the PTP frames.
PCP	Priority Code Point value used for PTP frames.

5.3.20.9 Factory Defaults

You can reset the configuration of the stack switch on this page. Only the IP configuration is retained.

Figure 98: Factory Defaults

Factory Defaults



- Keep IP
- Keep User/Password

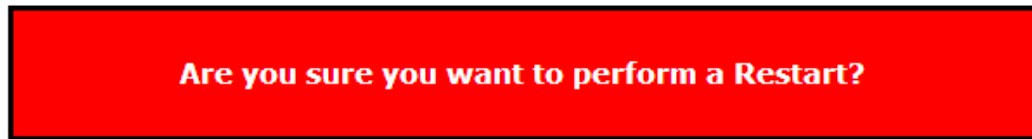
Label	Description
<input type="button" value="Yes"/>	Click to reset the configuration to Factory Defaults.
<input type="button" value="No"/>	Click to return to the Port State page without resetting the configuration

5.3.20.10 System Reboot

You can reset the stack switch on this page. After reset, the system will boot normally as if you had powered-on the devices

Figure 99: Restart Device

Restart Device



Label	Description
<input type="button" value="Yes"/>	Click to reboot device.
<input type="button" value="No"/>	Click to return to the Port State page without rebooting.

Section 6: Command Line Interface Management

Besides WEB-base management, SLM084 also support CLI management. You can use console or telnet to management switch by CLI.

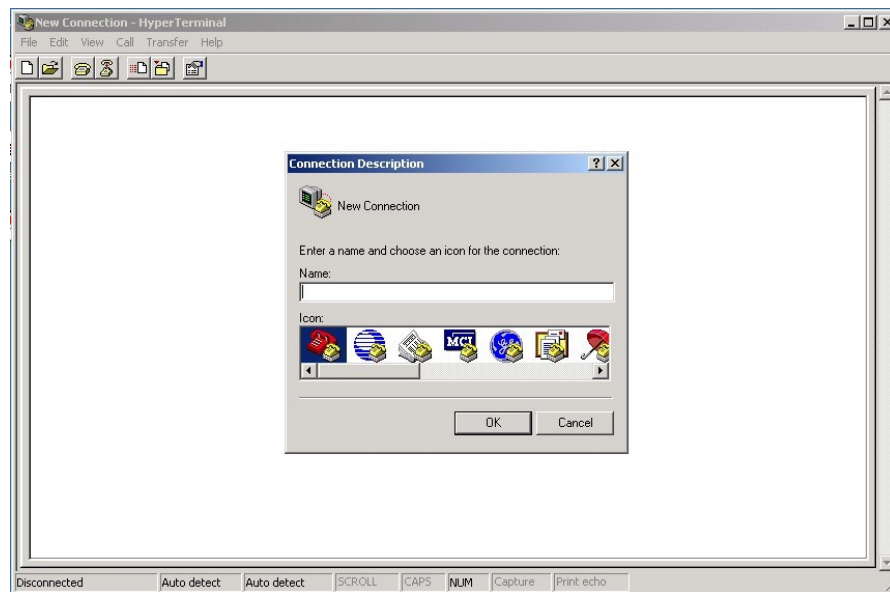
CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

Before Configuring by RS-232 serial console, use an RJ45 to DB9-F cable to connect the Switches' RS-232 Console port to your PC's COM port.

Follow the steps below to access the console via RS-232 serial cable.

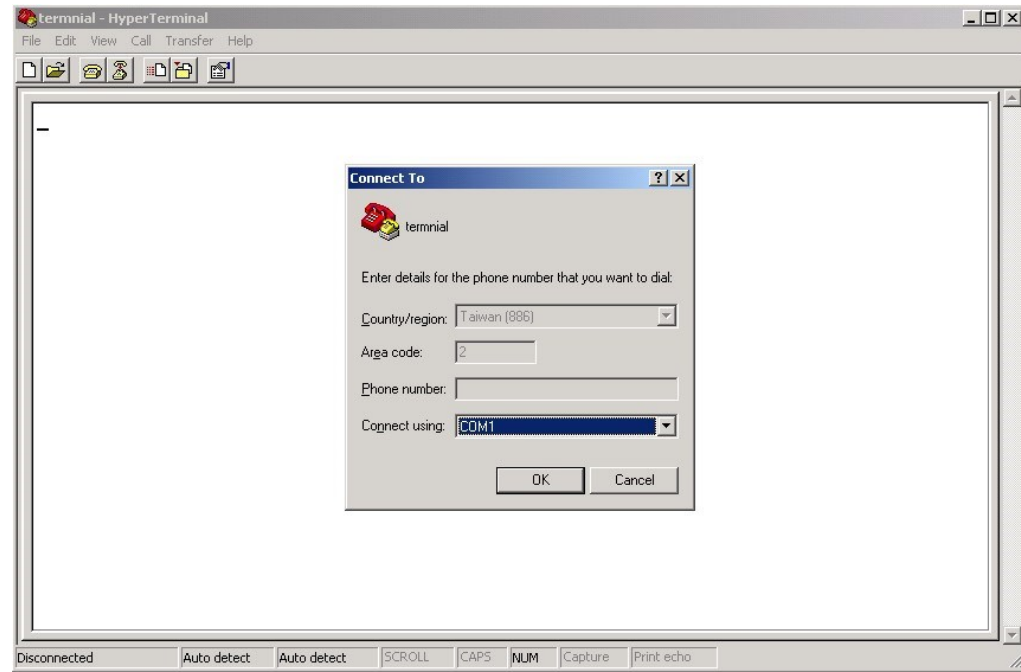
1. From the Windows desktop, click on Start -> Programs -> Accessories -> Communications -> Hyper Terminal
2. Input a name for new connection

Figure 100: Connection Description



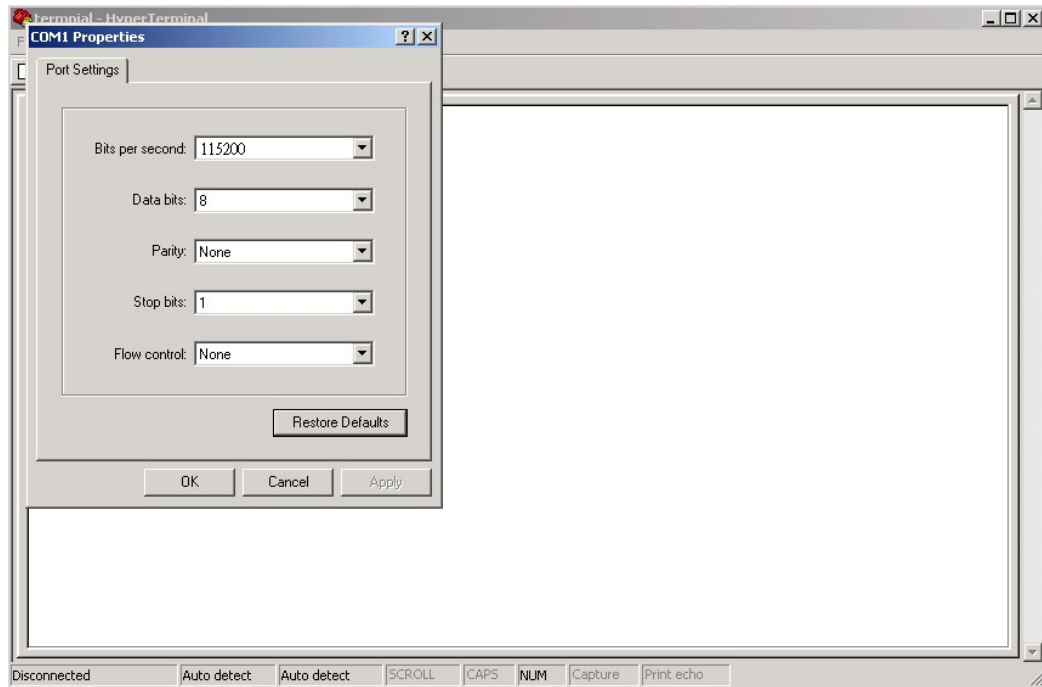
3. Select to use COM port number

Figure 101:COM Port Numbers



- The COM port properties setting, 115200 for Bits per second, 8 for Data bits, None for Parity, 1 for Stop bits and none for Flow control.

Figure 102: COM Port Settings



- 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”.

Figure 103: SLM084 Command Line Interface

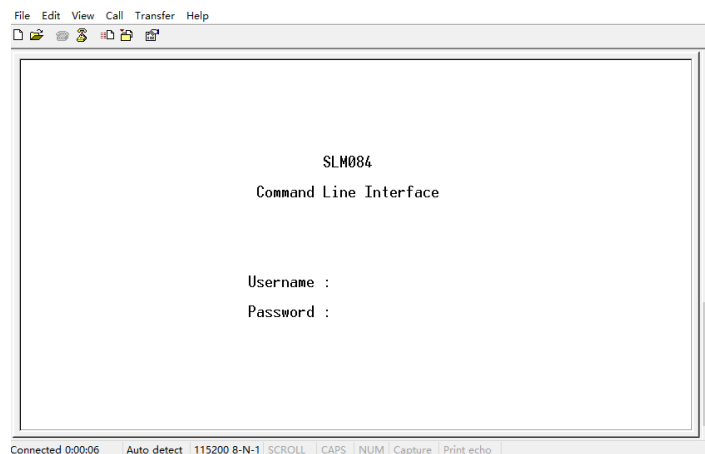


Figure 104: Command Groups

```
Command Groups:
-----
System      : System settings and reset options
IP          : IP configuration and Ping
Port        : Port management
MAC         : MAC address table
ULAN        : Virtual LAN
PULAN       : Private ULAN
Security    : Security management
STP         : Spanning Tree Protocol
Aggr        : Link Aggregation
LACP        : Link Aggregation Control Protocol
LLDP        : Link Layer Discovery Protocol
PoE         : Power Over Ethernet
QoS         : Quality of Service
Mirror      : Port mirroring
Config      : Load/Save of configuration via TFTP
Firmware    : Download of firmware via TFTP
PTP         : IEEE1588 Precision Time Protocol
Loop Protect : Loop Protection
IPMC        : MLD/IGMP Snooping
Fault       : Fault Alarm Configuration
Event       : Event Selection
DHCP Server : DHCP Server Configuration
Ring        : Ring Configuration
Chain       : Chain Configuration
RCS         : Remote Control Security
Fastrecovery : Fast-Recovery Configuration
SFP         : SFP Monitor Configuration
DeviceBinding : Device Binding Configuration
MRP         : MRP Configuration
Modbus      : Modbus TCP Configuration
```

System

System>	Configuration [all] [<port_list>]
	Reboot
	Restore Default [keep_ip]
	Contact [<contact>]
	Name [<name>]
	Location [<location>]
	Description [<description>]
	Password <password>
	Username [<username>]
	Timezone [<offset>]
	Log [<log_id>] [all info warning error] [clear]

IP

IP>	Configuration
	DHCP [enable disable]
	Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]
	Ping <ip_addr_string> [<ping_length>]
	SNTP [<ip_addr_string>]

Port

port>	Configuration [<port_list>] [up down]
	Mode [<port_list>] [auto 10hdx 10fdx 100hdx 100fdx 1000fdx sfp_auto_ams]
	Flow Control [<port_list>] [enable disable]
	State [<port_list>] [enable disable]
	MaxFrame [<port_list>] [<max_frame>]
	Power [<port_list>] [enable disable actiphy dynamic]
	Excessive [<port_list>] [discard restart]
	Statistics [<port_list>] [<command>] [up down]
	VeriPHY [<port_list>]
	SFP [<port_list>]

MAC

MAC>	Configuration [<port_list>]
	Add <mac_addr> <port_list> [<vid>]
	Delete <mac_addr> [<vid>]
	Lookup <mac_addr> [<vid>]
	Agetime [<age_time>]
	Learning [<port_list>] [auto disable secure]
	Dump [<mac_max>] [<mac_addr>] [<vid>]
	Statistics [<port_list>]

	Flush
--	-------

VLAN

VLAN>	Configuration [<port_list>]
	PVID [<port_list>] [<vid> none]
	FrameType [<port_list>] [all tagged untagged]
	IngressFilter [<port_list>] [enable disable]
	tx_tag [<port_list>] [untag_pvid untag_all tag_all]
	PortType [<port_list>] [unaware c-port s-port s-custom-port]
	EtypeCustomSport [<etype>]
	Add <vid> <name> [<ports_list>]
	Forbidden Add <vid> <name> [<port_list>]
	Delete <vid> <name>
	Forbidden Delete <vid> <name>
	Forbidden Lookup [<vid>] [(name <name>)]
	Lookup [<vid>] [(name <name>)] [combined static nas all]
	Name Add <name> <vid>
	Name Delete <name>
	Name Lookup [<name>]
	Status [<port_list>] [combined static nas mstp all conflicts]

Private VLAN

PVLAN>	Configuration [<port_list>]
	Add <pvlan_id> [<port_list>]
	Delete <pvlan_id>
	Lookup [<pvlan_id>]
	Isolate [<port_list>] [enable disable]

Security

Security >	Switch	Switch security setting
	Network	Network security setting
	AAA	Authentication, Authorization and Accounting setting

Security Switch

Security/switch>	Password <password>	
	Auth	Authentication
	SSH	Secure Shell
	HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
	RMON	Remote Network Monitoring

Security Switch Authentication

Security/switch/auth>	Configuration
	Method [console telnet ssh web] [none local radius] [enable disable]

Security Switch SSH

Security/switch/ssh>	Configuration
	Mode [enable disable]

Security Switch HTTPS

Security/switch/ssh>	Configuration
	Mode [enable disable]

Security Switch RMON

Security/switch/rmon>	Statistics Add <stats_id> <data_source>
	Statistics Delete <stats_id>
	Statistics Lookup [<stats_id>]
	History Add <history_id> <data_source> [<interval>] [<buckets>]
	History Delete <history_id>
	History Lookup [<history_id>]
	Alarm Add <alarm_id> <interval> <alarm_variable> [absolute delta]<rising_threshold> <rising_event_index> <falling_threshold> <falling_event_index> [rising falling both]
	Alarm Delete <alarm_id>
	Alarm Lookup [<alarm_id>]

Security Network

Security/Network>	Psec	V
	NAS	Network Access Server (IEEE 802.1X)
	ACL	Access Control List
	DHCP	Dynamic Host Configuration Protocol

Security Network Psec

Security/Network/Psec>	Switch [<port_list>]
	Port [<port_list>]

Security Network NAS

Security/Network/NAS>	Configuration [<port_list>]
	Mode [enable disable]
	State [<port_list>] [auto authorized unauthorized macbased]
	Reauthentication [enable disable]
	ReauthPeriod [<reauth_period>]
	EapolTimeout [<eapol_timeout>]
	Agetime [<age_time>]
	Holdtime [<hold_time>]
	Authenticate [<port_list>] [now]
	Statistics [<port_list>] [clear eapol radius]

Security Network ACL

Security/Network/ACL>	Configuration [<port_list>]
	Action [<port_list>] [permit deny] [<rate_limiter>][<port_redirect>] [<mirror>] [<logging>] [<shutdown>]
	Policy [<port_list>] [<policy>]
	Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]
	Add [<ace_id>] [<ace_id_next>][<(port <port_list>)>] [<(policy <policy> <policy_bitmask>)>][<tagged>] [<vid>] [<tag_prio>] [<dmac_type>][<(etype <etype> [<smac>] [<dmac>))>] (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>]) [permit deny] [<rate_limiter>] [<port_redirect>] [<mirror>] [<logging>][<shutdown>]
	Delete <ace_id>
	Lookup [<ace_id>]
	Clear
	Status [combined static loop_protect dhcp ptp ipmc conflicts]
	Port State [<port_list>] [enable disable]

Security Network DHCP

Security/Network/DHCP>	Configuration
	Mode [enable disable]
	Server [<ip_addr>]
	Information Mode [enable disable]
	Information Policy [replace keep drop]
	Statistics [clear]

Security Network AAA

Security/Network/AAA>	Configuration
	Timeout [<timeout>]
	Deadtime [<dead_time>]
	RADIUS [<server_index>] [enable disable] [<ip_addr_string>] [<secret>] [<server_port>]
	ACCT_RADIUS [<server_index>] [enable disable] [<ip_addr_string>] [<secret>] [<server_port>]
	Statistics [<server_index>]

STP

STP>	Configuration
	Version [<stp_version>] Non-certified release, v
	Txhold [<holdcount>]lt 15:15:15, Dec 6 2007
	MaxAge [<max_age>]
	FwdDelay [<delay>]
	bpduFilter [enable disable]
	bpduGuard [enable disable]
	recovery [<timeout>]
	CName [<config-name>] [<integer>]
	Status [<msti>] [<port_list>]
	Msti Priority [<msti>] [<priority>]
	Msti Map [<msti>] [clear]
	Msti Add <msti> <vid>
	Port Configuration [<port_list>]
	Port Mode [<port_list>] [enable disable]
	Port Edge [<port_list>] [enable disable]
	Port AutoEdge [<port_list>] [enable disable]
	Port P2P [<port_list>] [enable disable auto]

	Port RestrictedRole [<port_list>] [enable disable]
	Port RestrictedTcn [<port_list>] [enable disable]
	Port bpduGuard [<port_list>] [enable disable]
	Port Statistics [<port_list>]
	Port Mcheck [<port_list>]
	Msti Port Configuration [<msti>] [<port_list>]
	Msti Port Cost [<msti>] [<port_list>] [<path_cost>]
	Msti Port Priority [<msti>] [<port_list>] [<priority>]

Aggr

	Configuration
	Add <port_list> [<aggr_id>]
Aggr>	Delete <aggr_id>
	Lookup [<aggr_id>]
	Mode [smac dmac ip port] [enable disable]

LACP

	Configuration [<port_list>]
	Mode [<port_list>] [enable disable]
	Key [<port_list>] [<key>]
LACP>	Role [<port_list>] [active passive]

	Status [<port_list>]
	Statistics [<port_list>] [clear]

LLDP

LLDP>	Configuration [<port_list>]
	Mode [<port_list>] [enable disable]
	Statistics [<port_list>] [clear]
	Info [<port_list>]

QoS

QoS>	DSCP Map [<dscp_list>] [<class>] [<dpl>]
	DSCP Translation [<dscp_list>] [<trans_dscp>]
	DSCP Trust [<dscp_list>] [enable disable]
	DSCP Classification Mode [<dscp_list>] [enable disable]
	DSCP Classification Map [<class_list>] [<dpl_list>] [<dscp>]
	DSCP EgressRemap [<dscp_list>] [<dpl_list>] [<dscp>]
	Storm Unicast [enable disable] [<packet_rate>]
	Storm Multicast [enable disable] [<packet_rate>]
	Storm Broadcast [enable disable] [<packet_rate>]
QCL Add [<qce_id>] [<qce_id_next>]	

	<p>[<port_list></p> <p>[<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type>]</p> <p>[(etype [<etype>]) </p> <p>(LLC [<DSAP>] [<SSAP>] [<control>]) </p> <p>(SNAP [<PID>]) </p> <p>(ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) </p> <p>(ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])</p> <p>[<class>] [<dp>] [<classified_dscp>]</p>
	QCL Delete <qce_id>
	QCL Lookup [<qce_id>]
	QCL Status [combined static conflicts]
	QCL Refresh

Mirror

	Configuration [<port_list>]
Mirror>	Port [<port> disable]
	Mode [<port_list>] [enable disable rx tx]

Dot1x

	Configuration [<port_list>]
Dot1x>	Mode [enable disable]

	State [<port_list>] [macbased auto authorized unauthorized]
	Authenticate [<port_list>] [now]
	Reauthentication [enable disable]
	Period [<reauth_period>]
	Timeout [<eapol_timeout>]
	Statistics [<port_list>] [clear eapol radius]
	Clients [<port_list>] [all <client_cnt>]
	Agetime [<age_time>]
	Holdtime [<hold_time>]

IGMP

	Configuration [<port_list>]
	Mode [enable disable]
	State [<vid>] [enable disable]
	Querier [<vid>] [enable disable]
IGMP>	Fastleave [<port_list>] [enable disable]
	Router [<port_list>] [enable disable]
	Flooding [enable disable]
	Groups [<vid>]
	Status [<vid>]

ACL

ACL>	Configuration [<port_list>]
	Action [<port_list>] [permit deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]
	Policy [<port_list>] [<policy>]
	Rate [<rate_limiter_list>] [<packet_rate>]
	Add [<ace_id>] [<ace_id_next>] [switch (port <port>) (policy <policy>)] [<vid>] [<tag_prio>] [<dmac_type>] [(etype [<etype>] [<smac>] [<dmac>]) (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>)] (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>)] (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>)] (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>)] (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>)) [permit deny] [<rate_limiter>] [<port_copy>] [<logging>] [<shutdown>]
	Delete <ace_id>
Lookup [<ace_id>]	
Clear	

Mirror

Mirror>	Configuration [<port_list>]
---------	-----------------------------

	Port [<port> disable]
	Mode [<port_list>] [enable disable rx tx]

Config

Config>	Save <ip_server> <file_name>
	Load <ip_server> <file_name> [check]

Firmware

Firmware>	Load <ip_addr_string> <file_name>
-----------	-----------------------------------

SNMP

SNMP>	Trap Inform Retry Times [<retries>]
	Trap Probe Security Engine ID [enable disable]
	Trap Security Engine ID [<engineid>]
	Trap Security Name [<security_name>]
	Engine ID [<engineid>]
	Community Add <community> [<ip_addr>] [<ip_mask>]
	Community Delete <index>
	Community Lookup [<index>]
	User Add <engineid> <user_name> [MD5 SHA] [<auth_password>] [DES] [<priv_password>]

	User Delete <index>
	User Changekey <engineid> <user_name> <auth_password> [<priv_password>]
	User Lookup [<index>]
	Group Add <security_model> <security_name> <group_name>
	Group Delete <index>
	Group Lookup [<index>]
	View Add <view_name> [included excluded] <oid_subtree>
	View Delete <index>
	View Lookup [<index>]
	Access Add <group_name> <security_model> <security_level> [<read_view_name>] [<write_view_name>]
	Access Delete <index>
	Access Lookup [<index>]

Firmware

Firmware>	Load <ip_addr_string> <file_name>
-----------	-----------------------------------

PTP

PTP>	Configuration [<clockinst>]
	PortState <clockinst> [<port_list>] [enable disable internal]

	ClockCreate <clockinst> [<devtype>] [<twostep>] [<protocol>] [<oneway>] [<clockid>] [<tag_enable>] [<vid>] [<prio>]
	ClockDelete <clockinst> [<devtype>]
	DefaultDS <clockinst> [<priority1>] [<priority2>] [<domain>]
	CurrentDS <clockinst>
	ParentDS <clockinst>
	Timingproperties <clockinst> [<utcoffset>] [<valid>] [<leap59>] [<leap61>] [<timetrac>] [<freqtrac>] [<ptptimescale>] [<timesource>]
	PTP PortDataSet <clockinst> [<port_list>] [<announceintv>] [<announceto>] [<syncintv>] [<delaymech>] [<minpdelayreqintv>] [<delayasymmetry>] [<ingresslatency>]
	LocalClock <clockinst> [update show ratio] [<clockratio>]
	Filter <clockinst> [<def_delay_filt>] [<period>] [<dist>]
	Servo <clockinst> [<displaystates>] [<ap_enable>] [<ai_enable>] [<ad_enable>] [<ap>] [<ai>] [<ad>]
	SlaveTableUnicast <clockinst>
	UniConfig <clockinst> [<index>] [<duration>] [<ip_addr>]
	ForeignMasters <clockinst> [<port_list>]
	EgressLatency [show clear]
	MasterTableUnicast <clockinst>
	ExtClockMode [<one_pps_mode>] [<ext_enable>] [<clockfreq>] [<vcxo_enable>]
	OnePpsAction [<one_pps_clear>]

	DebugMode <clockinst> [<debug_mode>]
	Wireless mode <clockinst> [<port_list>] [enable disable]
	Wireless pre notification <clockinst> <port_list>
	Wireless delay <clockinst> [<port_list>] [<base_delay>] [<incr_delay>]

Fault

Fault>	Alarm PortLinkDown [<port_list>] [enable disable]
	Alarm PowerFailure [pwr1 pwr2 pwr3] [enable disable]

Event

Event>	Configuration
	Syslog SystemStart [enable disable]
	Syslog PowerStatus [enable disable]
	Syslog SnmpAuthenticationFailure [enable disable]
	Syslog RingTopologyChange [enable disable]
	Syslog Port [<port_list>] [disable linkup linkdown both]
	SMTP SystemStart [enable disable]
	SMTP PowerStatus [enable disable]
	SMTP SnmpAuthenticationFailure [enable disable]
	SMTP RingTopologyChange [enable disable]
SMTP Port [<port_list>] [disable linkup linkdown both]	

DHCP Server

DHCP Server>	Mode [enable disable]
	Setup [<ip_start>] [<ip_end>] [<ip_mask>] [<ip_router>] [<ip_dns>] [<ip_tftp>] [<lease>] [<bootfile>]

Ring

Ring>	Mode [enable disable]
	Master [enable disable]
	1stRingPort [<port>]
	2ndRingPort [<port>]
	Couple Mode [enable disable]
	Couple Port [<port>]
	Dualhoming Mode [enable disable]
	Dualhoming Port [<port>]

RCS

RCS>	Mode [enable disable]
	Add [<ip_addr>] [<port_list>] [web_on web_off] [telnet_on telnet_off] [snmp_on snmp_off]
	Del <index>
	Configuration

SFP

SFP>	syslog [enable disable]
	temp [<temperature>]
	Info

Modbus

Modbus>	Status
	Mode [enable disable]

Section 7: Technical Specifications

SLM084	Description
Physical Ports	
10/100/1000Base-T(X) Ports in RJ45 Auto MDI/MDIX	8
100/1000Base-X with SFP port	12
Technology	
Ethernet Standards	<p>IEEE 802.3 for 10Base-T</p> <p>IEEE 802.3u for 100Base-TX and 100Base-FX</p> <p>IEEE 802.3ab for 1000Base-T</p> <p>IEEE 802.z for 1000Base-X</p> <p>IEEE 802.3x for Flow control</p> <p>IEEE 802.3ad for LACP (Link Aggregation Control Protocol)</p> <p>IEEE 802.1p for COS (Class of Service)</p> <p>IEEE 802.1Q for VLAN Tagging</p> <p>IEEE 802.1w for RSTP (Rapid Spanning Tree Protocol)</p> <p>IEEE 802.1s for MSTP (Multiple Spanning Tree Protocol)</p> <p>IEEE 802.1x for Authentication</p> <p>IEEE 802.1AB for LLDP (Link Layer Discovery Protocol)</p>
MAC Table	8k
Priority Queues	8

Processing	Store-and-Forward
Switch Properties	<p>Switching latency: 7 us</p> <p>Switching bandwidth: 40Gbps</p> <p>Max. Number of Available VLANs: 256</p> <p>IGMP multicast groups: 128 for each VLAN</p> <p>Port rate limiting: User Define</p>
Jumbo frame	Up to 9.6K Bytes
Security Features	<p>Device Binding security feature</p> <p>Enable/disable ports, MAC based port security</p> <p>Port based network access control (802.1x)</p> <p>VLAN (802.1Q) to segregate and secure network traffic</p> <p>Radius centralized password management</p> <p>SNMPv3 encrypted authentication and access security</p> <p>Https / SSH enhance network security</p>
Software Features	<p>STP/RSTP/MSTP (IEEE 802.1D/w/s)</p> <p>Redundant Ring (Redundant Ring) with recovery time less than 30ms over 250 units</p> <p>TOS/Diffserv supported</p> <p>Quality of Service (802.1p) for real-time traffic</p> <p>VLAN (802.1Q) with VLAN tagging and GVRP supported</p> <p>IGMP Snooping</p> <p>Port configuration, status, statistics, monitoring, security</p> <p>DHCP Server/Client/Relay</p> <p>SMTP Client</p> <p>Modbus TCP</p>

Network Redundancy	Redundant Ring MSTP (RSTP/STP compatible)
RS-232 Serial Console Port	RS-232 in RJ45 connector with console cable. 115200bps, 8, N, 1
LED indicators	
Power Indicator (PWR)	Green : Power LED x 2
Ring Master Indicator (R.M.)	Green : Indicates that the system is operating in Redundant Ring Master mode
Redundant Ring Indicator (Ring)	Green : Indicates that the system operating in Redundant Ring mode Green Blinking : Indicates that the Ring is broken.
Fault Indicator (Fault)	Amber : Indicate unexpected event occurred
10/100/1000Base-T(X) RJ45 Port Indicator	Green for 1000Mbps Link/Act indicator. Amber for duplex indicator
100/1000Base-X SFP Port Indicator	Green for port Link/Act.
Fault contact	
Relay	Relay output to carry capacity of 1A at 24VDC
Power	
Redundant Input power	Dual DC inputs. 12~48VDC on 6-pin terminal block
Power consumption (Typ.)	10 Watts
Overload current protection	Present
Reverse Polarity Protection	Present
Physical Characteristic	

Enclosure	IP-30
Dimension (W x D x H)	96.4 (W) x 105.5 (D) x 154 (H) mm (3.8 x 4.15 x 6.06 inch)
Weight (g)	1210 g
Environmental	
Storage Temperature	-40 to 85°C (-40 to 185°F)
Operating Temperature	-40 to 70°C (-40 to 158°F)
Operating Humidity	5% to 95% Non-condensing
Regulatory approvals	
EMI	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD) EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS), EN61000-4-8, EN61000-4-11
Shock	IEC60068-2-27
Free Fall	IEC60068-2-32
Vibration	IEC60068-2-6
Safety	EN60950-1
Warranty	5 years

General Contact Information

Home link: <http://www.emerson.com/industrial-automation-controls>

Knowledge Base: <https://www.emerson.com/industrial-automation-controls/support>

Technical Support

Americas

Phone: 1-888-565-4155

1-434-214-8532 (If toll free option is unavailable)

Customer Care (Quotes/Orders>Returns): customercare.mas@emerson.com

Technical Support: support.mas@emerson.com

Europe

Phone: +800-4444-8001

+420-225-379-328 (If toll free option is unavailable)

Customer Care (Quotes/Orders>Returns): customercare.emea.mas@emerson.com

Technical Support: support.mas.emea@emerson.com

Asia

Phone: +86-400-842-8599

+65-6955-9413 (All other Countries)

Customer Care (Quotes/Orders>Returns): customercare.cn.mas@emerson.com

Technical Support: support.mas.apac@emerson.com

Any escalation request should be sent to: mas.sfdcescalation@emerson.com

Note: If the product is purchased through an Authorized Channel Partner, please contact the seller directly for any support.

Emerson reserves the right to modify or improve the designs or specifications of the products mentioned in this manual at any time without notice. Emerson does not assume responsibility for the selection, use or maintenance of any product. Responsibility for proper selection, use and maintenance of any Emerson product remains solely with the purchaser.

© 2020 Emerson. All rights reserved. Emerson Terms and Conditions of Sale are available upon request. The Emerson logo is a trademark and service mark of Emerson Electric Co. All other marks are the property of their respective owners.

