

PACSystems™ Industrial Managed Gigabit Ethernet Switch SLM168

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	7
1.1 About the SLM168 Industrial Switch	7
1.2 Software Features	7
1.1 Hardware Features	8
Section 2: Hardware Overview	9
2.1 Front Panel	9
2.2 Rear Panel	10
2.3 Rack-Mount Kit Assembly	11
2.4 Front Panel LEDs	11
Section 3: Cables	14
3.1 Ethernet Cables	14
3.1.1 10/100/1000BASE-T(X) Pin Assignments	14
3.2 SFP	17
Section 4: Web Management	18
4.1 Configuration by Web Browser	18
4.1.1 About Web-based Management	18
4.1.2 Basic Setting	20
4.1.2.1 System Information	20
4.1.2.2 Admin & Password	22
4.1.2.3 IP Setting	23
4.1.2.4 HTTPS	24
4.1.2.5 SSH	25
4.1.2.6 LLDP	26

4.1.2.7	Modbus TCP.....	32
4.1.3	Backup/Restore Configuration	33
4.1.3.1	Firmware Update	33
4.1.4	DHCP Server.....	34
4.1.4.1	Setting.....	34
4.1.4.2	DHCP Dynamic Client List.....	34
4.1.4.3	DHCP Client List	35
4.1.5	Port Setting.....	36
4.1.5.1	Port Control	36
4.1.5.2	Rate Limit.....	39
4.1.5.3	Port Trunk.....	41
4.1.5.3.1	Trunk Configuration.....	41
4.1.5.3.2	LACP Port Configuration	43
4.1.5.3.3	LACP System Status	45
4.1.5.3.4	LACP Statistics	48
4.1.6	Redundancy	49
4.1.6.1	Redundant Ring	49
4.1.7	MSTP.....	51
4.1.7.1	MSTI Mapping	52
4.1.7.2	MSTI Priorities	55
4.1.8	CIST Ports.....	56
4.1.8.1	MSTI Ports.....	59
4.1.9	STP Bridges	61
4.1.10	STP Port Status.....	62
4.1.11	STP Statistics.....	63

4.1.12	VLAN	64
4.1.12.1	VLAN Membership Configuration	64
4.1.12.2	Private VLAN	66
4.1.13	SNMP	69
4.1.13.1	SNMP-System	69
4.1.13.2	SNMP-Communities	73
4.1.14	SNMP-Users	74
4.1.14.1	SNMP-Groups	76
4.1.14.2	SNMP-Views	77
4.1.15	Traffic Prioritization	80
4.1.15.1	Storm Control	80
4.1.15.2	Port QoS	81
4.1.15.2.1	Port QoS Configuration	81
4.1.15.3	QoS Control List	82
4.1.15.4	Queuing Counters	85
4.1.15.5	Wizard	86
4.1.16	Multicast	87
4.1.16.1	IGMP Snooping	87
4.1.16.2	IGMP Snooping Status	89
4.1.17	Security	91
4.1.17.1	ACL	91
4.1.17.1.1	Ports	91
4.1.17.1.2	Rate Limiters	93
4.1.17.1.3	ACL Configuration	94
4.1.17.1.4	Wizard	105

4.1.17.2	802.1x	106
4.1.18	Client Configuration.....	119
4.1.19	RADIUS Authentication Server Configuration	121
4.1.20	Warning	127
4.1.20.1	System Warning.....	127
4.1.20.1.1	SYSLOG Setting.....	127
4.1.20.1.2	Event Selection	128
4.1.21	Monitor and Diag	130
4.1.21.1	MAC Table	130
4.1.21.1.1	Configuration	130
4.1.21.1.2	Aging Configuration.....	131
4.1.21.1.3	MAC Table Learning	131
4.1.21.1.4	Static MAC Table Configuration	132
4.1.21.1.5	MAC Table	133
4.1.21.2	Port Statistic	135
4.1.21.2.1	Traffic Overview.....	135
4.1.21.2.2	Detailed Statistics	137
4.1.21.3	Port Mirroring	140
4.1.21.4	System Log Information	142
4.1.21.5	Cable Diagnostics.....	144
4.1.21.6	Ping	146
4.1.22	Factory Defaults	147
Section 5: Command Line Interface Management		148
5.1	About CLI Management.....	148
5.1.1	Command Groups.....	152

Section 6: Technical Specifications	168
General Contact Information	0
Technical Support.....	0

Section 1: Getting to Know Your Switch

1.1 About the SLM168 Industrial Switch

SLM168 is managed redundant ring Ethernet switches with 16xGigabit combo ports and 8x100/1000Base-X SFP ports. With complete support of Ethernet Redundancy protocol, Redundant Ring (recovery time < 20ms over 250 units of connection) and MSTP/RSTP/STP (IEEE 802.1S/W/D) can protect your mission-critical applications from network interruptions or temporary malfunctions with its fast recovery technology. And all functions of SLM168 can also be managed centralized and convenient by PACSystems Ethernet Switch Configuration Tool or above, as well as the Web-based interface, console (CLI) configuration.

1.2 Software Features

- Fastest Redundant Ethernet Ring (Recovery time < 20ms over 250 units connection)
- Supports Ring Coupling, Dual Homing
- MSTP/RSTP/STP (IEEE 802.1S/W/D)
- Supports SNMPv1/v2/v3 & RMON & Port base/IEEE 802.1Q VLAN Network Management
- Event notification by Email, SNMP Trap and syslog Output
- Web-based and Console (CLI) configuration
- Enable/Disable ports, MAC based port security
- Port-based network access control (IEEE 802.1x)
- RADIUS centralized password management
- SNMPv3 encrypted authentication and access security
- Quality of Service (IEEE 802.1p) for real-time traffic
- VLAN (IEEE 802.1q) with support for double-tagging and GVRP
- IGMP Snooping for multicast filtering
- Port configuration, status, statistics, mirroring, and security

1.1 Hardware Features

- 16 x Combo ports with 10/100/1000Base-T(X) and 100/1000 Base-X SFP
- 8 x 100/1000Base-X SFP ports
- Console Port
- Operating Temperature: -40 to 70°C
- Storage Temperature: -40 to 85°C
- Operating Humidity: 5% to 95%, non-condensing
- Dimensions : 431 (W) x 342 (D) x 44 (H) mm

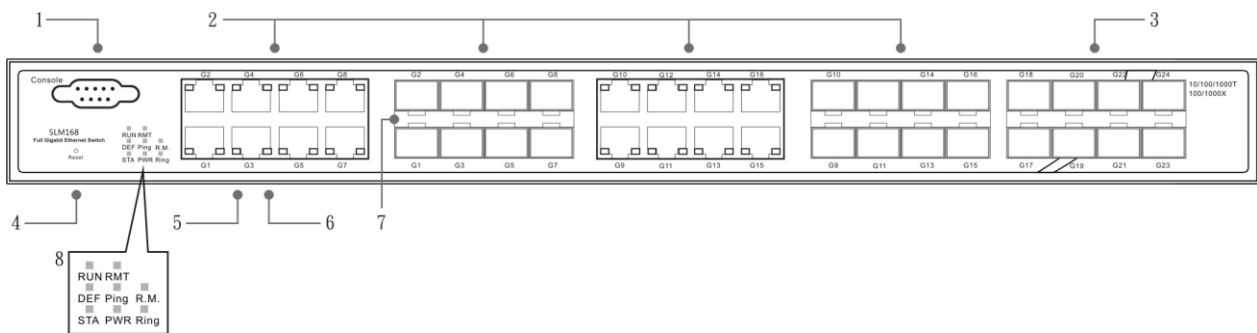
Section 2: Hardware Overview

2.1 Front Panel

The following table describes the labels that stick on the SLM168.

Port	Description
Combo ports	16 x 10/100/1000Base-T(X) Ethernet port and 100/1000Base-X SFP
SFP Port	8 x 100/1000Base-X SFP
Console	Use RS-232 with DB9 connector to manage switch.

Figure 1: SLM168



1. Console port (DB9)
2. 10/100/1000Base-T(X) Ethernet port and 100/1000Base-X SFP (combo port)
3. 100/1000Base-X Fiber port on SFP
4. Reset button: Push the button 3 seconds for reset; 5 seconds for factory default.
5. LED for Ethernet ports 1000Mbps Link/Act status
6. LED for Ethernet ports 10/100Mbps Link/Act status

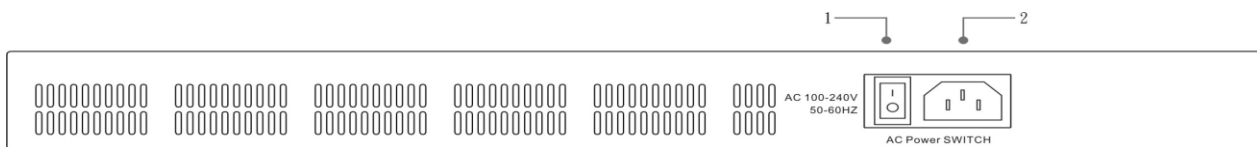
7. LED for SFP ports Link/Act status.
8. Front Panel LED Status:
 - LED for STA: Green : Indicates that the system ready. The LED is blinking when the system is upgrading firmware
 - LED for PWR: This LED lights on when the power module is activated.
 - LED for R.M. (Ring master): When the LED lights on, this switch is designated as the ring master of the Ring topology.
 - LED for Ring: When the led light on, the Redundant Ring is activated.
 - LED for DEF: System resets to default configuration.
 - LED for Ping: System is processing “PING” request.
 - LED for RUN: System is operating continuously.
 - LED for RMT: System is accessed remotely.

2.2 Rear Panel

The rare panel of SLM168 is showed as below:

1. Power Switch
2. Power input for AC 100V~240V / 50~60Hz.

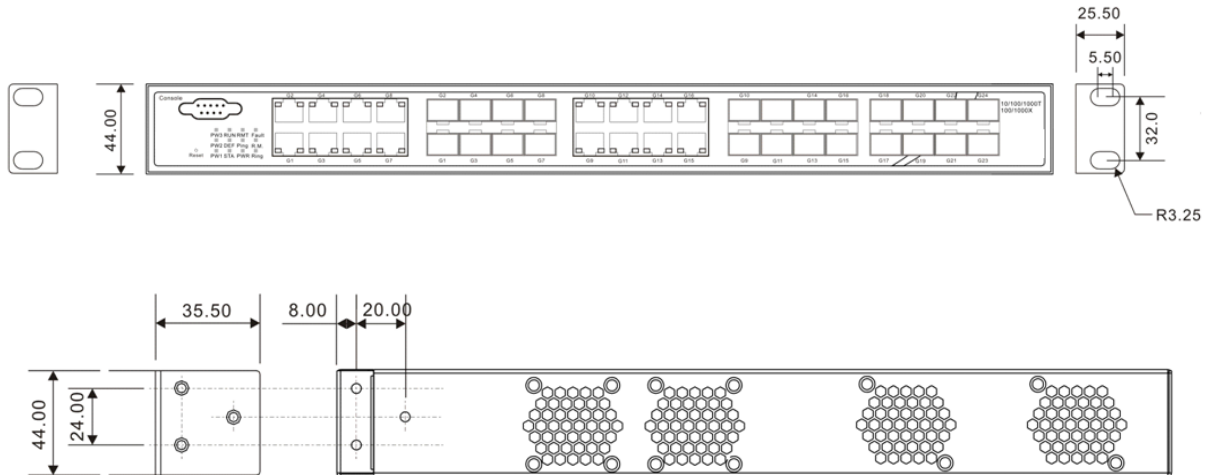
Figure 2: Rear Panel



2.3 Rack-Mount Kit Assembly

You can find the rack-mount kit and the screws in the packing box. Please assemble the rack-mount kit on the switch with screws as shown below:

Figure 3: Rack Mount Kit Assembly



2.4 Front Panel LEDs

LED	Color	Status	Description
PWR	Green	On	When the PWR links, the green led will be light on.
STA	Green	On	When the power module is in PWR UP state, the green LED lights on.
		Blinking	When the system is upgrading firmware
DEF	Green	On	System resets to default configuration.

LED	Color	Status	Description
RUN	Green	Slowly blinking	System is operating continuously.
PWR	Green	On	Power module activated.
Ping	Green	Blinking	When the led light on, System is processing “PING” request
RMT	Green	Blinking	System is accessed remotely.
Ring	Green	On	Ring enabled.
		Slowly blinking	Ring has only One link. (lacks one link to build the ring)
		Fast blinking	Ring work normally.
R.M	Green	On	When the system is operating in Redundant Ring Master mode
Fault	Amber	On	Indicates unexpected event occurred.
10/100/1000Base-T(X) Gigabit Ethernet ports			
LINK/ACT	Green	On	Port speed 1000M link up
		Blinking	Data Transmitted on 1000M
	Amber	On	Port speed 10/100M link

LED	Color	Status	Description
			up
		Blinking	Data Transmitted on 10/100M
SFP			
LINK/ACT	Green	On	Port link up.
		Blinking	Data transmitted

Section 3: Cables

3.1 Ethernet Cables

The SLM168 switches have 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 100-ohm UTP	UTP 100 m (328 ft)	RJ-45
1000BASE-TX	CAT 5/5e 100-ohm UTP	UTP 100 m (328 ft)	RJ-45

3.1.1 10/100/1000BASE-T(X) Pin Assignments

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

10/100 Base-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

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 SLM168 switches support 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:

10/100 Base-T MDI/MDI-X pin assignments

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)

3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

1000 Base-T MDI/MDI-X pin assignments

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.

3.2 SFP

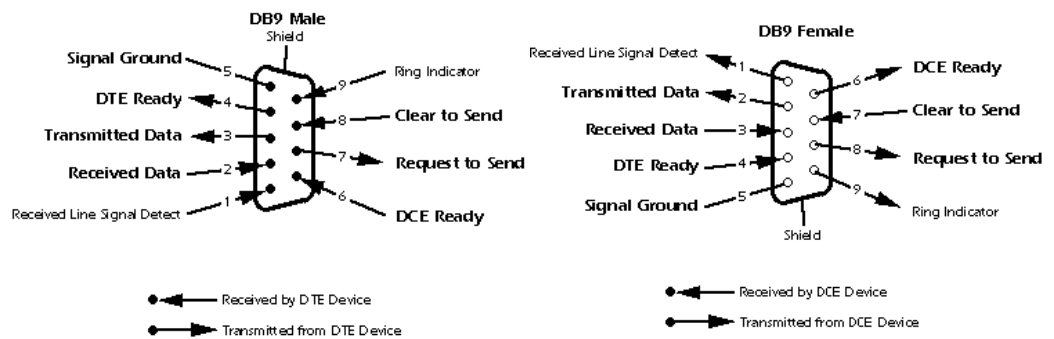
The Switch has fiber optical ports with SFP connectors. The fiber optical ports are in multi-mode (0 to 550 m, 850 nm with 50/125 μm, 62.5/125 μm fiber) and single-mode with LC connector. Please remember that the TX port of Switch A should be connected to the RX port of Switch B.

Console Cable

Each SLM168 switch can be managed by its console port. You can connect them to PC via an RS-232 cable with DB-9 female connector...

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

Figure 4: DB9 Pinout



Section 4: 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.

4.1 Configuration by Web Browser

This section introduces the configuration by Web browser.

4.1.1 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 values are shown as the following:

IP Address: 192.168.0.100

Subnet Mask: **255.255.255.0**

Default Gateway: **192.168.0.254**

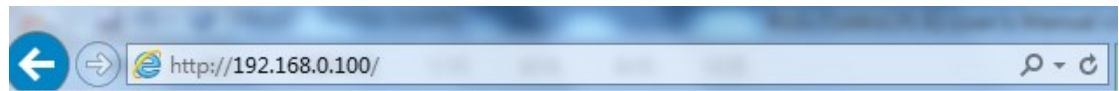
User Name: **admin**

Password: **admin**

System Login

1. Launch the Internet Explorer.
2. Type http:// or https:// and the IP address of the switch. Press “Enter”.

Figure 5: URL



3. The login screen appears.
4. Key in the username and password. The default username and password is “admin”.
5. Click “Enter” or “OK” button. Then the main interface of the Web-based management appears.

Figure 6: Main Interface

Open all

- System Information
- Basic Setting
- DHCP Server
- Port Setting
- Redundancy
- VLAN
- SNMP
- Traffic Prioritization
- Multicast
- Security
- Warning
- Monitor and Diag
- Factory Default
- System Reboot

Information Message

System	
Name	SLM168
Description	Industrial 24-port rack mount managed Gigabit Ethernet switch with 16xGigabit combo ports and 8x100/1000Base-X, SFP socket
Location	
Contact	
OID	1.3.6.1.4.1.25972.0.0.63
Hardware	
MAC Address	00-1e-94-94-3e-9e
Time	
System Date	1970-01-01 00:01:04 +0000
System Uptime	0d 00:01:04
Software	
Kernel Version	v7.12
Software Version	v1.00
Software Date	2014-04-18 12:08:24 +0800

Auto-refresh Refresh

Enable Location Alert

PACSystems™ Ethernet Switch
10/100/1000T
100/1000X

4.1.2 Basic Setting

4.1.2.1 System Information

The switch system information is provided here.

Figure 7: Information Message

Information Message

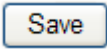
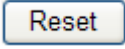
System	
Name	SLM168
Description	Industrial 24-port rack mount managed Gigabit Ethernet switch with 16xGigabit combo ports and 8x100/1000Base-X, SFP socket
Location	
Contact	
OID	1.3.6.1.4.1.25972.0.0.63
Hardware	
MAC Address	00-1e-94-94-3e-9e
Time	
System Date	1970-01-01 00:43:36 +0000
System Uptime	0d 00:43:36
Software	
Kernel Version	v7.12
Software Version	v1.00
Software Date	2014-04-18 12:08:24 +0800
Auto-refresh <input type="checkbox"/> Refresh	
Enable Location Alert	

Figure 8: System Information Configuration

System Information Configuration

System Name	SLM168
System Description	Industrial 24-port rack mount managed
System Location	
System Contact	
System Timezone Offset (minutes)	0
Save Reset	

Label	Description
System Name	An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name – a text string (0 to 255 characters) drawn from the alphabet (A-Z, a-z), digits (0-9), and the minus sign (-). No space characters are permitted as part of a name. The first character

Label	Description
	must be an alphabet, and the first or last character must not be a minus sign.
System Description	The administratively assigned description for this managed node. The allowed string length is 0 to 255, and the allowed contents are the ASCII characters from 32 to 126.
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 contents are 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 contents are the ASCII characters from 32 to 126.
Time Zone Offset	<p>Enter the name of contact person or organization</p> <p>Provide the time zone offset relative to UTC/GMT.</p> <p>The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes.</p>
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

4.1.2.2 Admin & Password

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

Figure 9: System Password

System Password

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

Label	Description
Old User Name	Enter the current system User Name. If this is incorrect, the new User name will not be set.
Old Password	Enter the current system password. If this is incorrect, the new password will not be set.
New User Name	Enter the new system User Name
New Password	Enter the new system password, and the password must meet the requirement : Minimum 8 characters; At least one Upper case letter. At least one numeric character. At least one special character such as @, #, \$,
Confirm password	Re-type the new password.
<input type="button" value="Save"/>	Click to save changes.

4.1.2.3 IP Setting

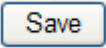
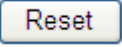
Configure the switch-managed IP information on this page.

Figure 10: 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		

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 192.168.0.100
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

Label	Description
IP Router	Assign the network gateway for the switch. The default gateway is 192.168.0.254
VLAN ID	Provide the managed VLAN ID. The allowed range is 1 through 4095.
SNTP Server	SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

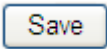
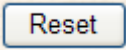
4.1.2.4 HTTPS

Figure 11: HTTPS Configuration

HTTPS Configuration

Mode | Enabled ▾

Save | Reset


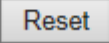
Label	Description
Mode	Indicates the HTTPS mode operation. Possible modes are: Enabled: Enable HTTPS mode operation. Disabled: Disable HTTPS mode operation.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

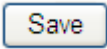
4.1.2.5 SSH

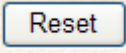
Figure 12: SSH Configuration

SSH Configuration

Mode | Disabled ▾

Label	Description
Mode	Indicates the SSH mode operation. Possible modes are: Enabled: Enable SSH mode operation. Disabled: Disable SSH mode operation.
	Click to save changes.

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

4.1.2.6 LLDP

LLDP Configuration

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

Figure 13: LLDP Configuration

LLDP Configuration

LLDP Parameters

Tx Interval seconds

Port	Mode
1	Enabled ▼
2	Enabled ▼
3	Enabled ▼
4	Enabled ▼
5	Enabled ▼
6	Enabled ▼
7	Enabled ▼
8	Enabled ▼
9	Enabled ▼
10	Enabled ▼
11	Enabled ▼
12	Enabled ▼
13	Enabled ▼
14	Enabled ▼
15	Enabled ▼
16	Enabled ▼
17	Enabled ▼
18	Enabled ▼
19	Enabled ▼
20	Enabled ▼
21	Enabled ▼
22	Enabled ▼
23	Enabled ▼
24	Enabled ▼

Label	Description
TX Interval	The LLDP Transmit interval time
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 14: LLDP Neighbor Information

LLDP Neighbor Information

Auto-refresh Refresh Open in new window

Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	Management Address
Port 14	00-1E-94-24-01-29	Port.02	SLM062	100TX	Bridge(+)	192.168.10.1 (IPv4) OID:

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 Capabilities	<p>System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:</p> <ol style="list-style-type: none"> 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved <p>When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).</p>

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

LLDP 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 15: LLDP Statistics

Auto-refresh Refresh Clear

Global Counters	
Neighbor entries were last changed at	1970-01-01 01:19:00 +0000 (295 sec. ago)
Total Neighbors Entries Added	1
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors 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	3	0	0	0	0	0	0	0	0
2	14	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	169	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	9	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	146	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	11	10	0	0	0	0	0	0	0
15	169	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
21	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0

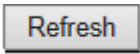
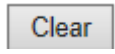
Global Counters

Label	Description
Neighbor entries were last changed at	Shows the time for when the last entry was last deleted or added. It is also shows the time since last change was detected.
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.

Label	Description
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	The number of well-formed TLVs, but with an unknown type

Label	Description
Unrecognized	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.
	Clears the local counters. All counters (including global counters) are cleared upon reboot.
Auto-refresh <input type="checkbox"/>	Check this box to enable an automatic refresh of the page at regular intervals.

4.1.2.7 Modbus TCP

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

Figure 16: Modbus TCP

MODBUS Configuration

Mode

The following table describes the labels in this screen.

Label	Description
Mode	Enable or Disable Modbus TCP function

4.1.3 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 17: Configuration Save

Configuration Save

Save configuration

Configuration Upload

浏览... Upload

4.1.3.1 Firmware Update

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

4.1.4 DHCP Server

4.1.4.1 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	192.168.10.100
End IP Address	192.168.10.200
Subnet Mask	255.255.255.0
Router	192.168.10.254
DNS	192.168.10.254
Lease Time (sec.)	86400
TFTP Server	0.0.0.0
Boot File Name	

4.1.4.2 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
1	<input type="checkbox"/>	dynamic	00-1e-94-24-01-29	192.168.10.100	86394
2	<input type="checkbox"/>	dynamic	6c-3e-6d-0a-3e-3a	192.168.10.101	94

4.1.4.3 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"/>

Add as Static

No.	Select	Type	MAC Address	IP Address	Surplus Lease
1		dynamic	00-1e-94-24-01-29	192.168.10.100	86362
2		dynamic	6c-3e-6d-0a-3e-3a	192.168.10.101	62

Delete Select/Clear All

4.1.5 Port Setting

4.1.5.1 Port Control

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

Figure 21: Port Configuration

Refresh

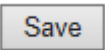
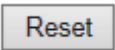
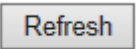
Auto Detect 100/1000 SFP Enabled ▾

Port	Link	Speed		Flow Control			Maximum Frame	Power Control
		Current	Configured	Current Rx	Current Tx	Configured		
1	● Down	100Mbps SFP	100Mbps SFP ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
2	● Down	100Mbps SFP	100Mbps SFP ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
3	● Down	Auto	Auto ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
4	● Down	Auto	Auto ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
5	● Down	Auto	Auto ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
6	● Down	Auto	Auto ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
7	● Down	Auto	Auto ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
8	● 1Gfdx	Auto	Auto ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
9	● Down	Auto	Auto ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
10	● 100fdx	Auto	Auto ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
11	● Down	Auto	Auto ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
12	● 1Gfdx	Auto	Auto ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
13	● Down	Auto	Auto ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
14	● 100fdx	Auto	Auto ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
15	● 1Gfdx	Auto	Auto ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
16	● Down	100Mbps SFP	100Mbps SFP ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
17	● Down	100Mbps SFP	100Mbps SFP ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
18	● Down	100Mbps SFP	100Mbps SFP ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
19	● Down	Auto	Auto ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
20	● Down	Auto	Auto ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
21	● Down	Auto	Auto ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
22	● Down	Auto	Auto ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
23	● Down	100Mbps SFP	100Mbps SFP ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾
24	● Down	100Mbps SFP	100Mbps SFP ▾	×	×	<input type="checkbox"/>	9600	Disabled ▾

Save Reset

Label	Description
Port	This is the logical port number for this row.
Link	The current link state is displayed graphically. Green indicates

Label	Description
	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>
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.</p> <p>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	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 9600 bytes.
Excessive Collision Mode	<p>Configure port transmit collision behavior.</p> <p>Discard: Discard frame after 16 collisions (default).</p> <p>Restart: Restart Backoff algorithm after 16 collisions.</p>

Label	Description
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	Total power usage in board, measured in percent.
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.
	Click to refresh the page.

4.1.5.2 Rate Limit

Configure the switch port rate limit for Policers and Shapers on this page.

Figure 22: Rate Limit Configuration

Rate Limit Configuration

Port	Policer Enabled	Policer Rate	Policer Unit	Shaper Enabled	Shaper Rate	Shaper Unit
1	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
2	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
3	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
4	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
5	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
6	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
7	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
8	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
9	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
10	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
11	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
12	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
13	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
14	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
15	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
16	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
17	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
18	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
19	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
20	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
21	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
22	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
23	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼
24	<input type="checkbox"/>	500	kbps ▼	<input type="checkbox"/>	500	kbps ▼

Save Reset

Label	Description
Port	The logical port for the settings contained in the same row.
Policer Enabled	Enable or disable the port policer. The default value is

Label	Description
	"Disabled".
Policer Rate	Configure the rate for the port policer. The default value is "500". This value is restricted to 500-1000000 when the "Policer Unit" is "kbps", and it is restricted to 1-1000 when the "Policer Unit" is "Mbps"
Policer Unit	Configure the unit of measure for the port policer rate as kbps or Mbps. The default value is "kbps".
Shaper Enabled	Enable or disable the port shaper. The default value is "Disabled".
Shaper Rate	Configure the rate for the port shaper. The default value is "500". This value is restricted to 500-1000000 when the "Policer Unit" is "kbps", and it is restricted to 1-1000 when the "Policer Unit" is "Mbps"
Shaper Unit	Configure the unit of measure for the port shaper rate as kbps or Mbps. The default value is "kbps".
<input data-bbox="428 1297 532 1346" type="button" value="Save"/>	Click to save changes.
<input data-bbox="433 1430 545 1478" type="button" value="Reset"/>	Click to undo any changes made locally and revert to previously saved values.

4.1.5.3 Port Trunk

4.1.5.3.1 Trunk Configuration

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

Figure 23: 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 24: Aggregation Group Configuration

Aggregation Group Configuration

Open in new window

Group ID	Port Members																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
11	<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"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
12	<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"/>	<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.

4.1.5.3.2 LACP Port Configuration

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

Figure 25: LACP Port Configuration

LACP Port Configuration

Port	LACP Enabled	Key		Role
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 ▼
11	<input type="checkbox"/>	Auto	▼	Active ▼
12	<input type="checkbox"/>	Auto	▼	Active ▼
13	<input type="checkbox"/>	Auto	▼	Active ▼
14	<input type="checkbox"/>	Auto	▼	Active ▼
15	<input type="checkbox"/>	Auto	▼	Active ▼
16	<input type="checkbox"/>	Auto	▼	Active ▼
17	<input type="checkbox"/>	Auto	▼	Active ▼
18	<input type="checkbox"/>	Auto	▼	Active ▼
19	<input type="checkbox"/>	Auto	▼	Active ▼
20	<input type="checkbox"/>	Auto	▼	Active ▼
21	<input type="checkbox"/>	Auto	▼	Active ▼
22	<input type="checkbox"/>	Auto	▼	Active ▼
23	<input type="checkbox"/>	Auto	▼	Active ▼
24	<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 = 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).
<div data-bbox="428 1488 532 1535" style="border: 1px solid gray; padding: 2px; display: inline-block;">Save</div>	Click to save changes.
<div data-bbox="433 1619 545 1665" style="border: 1px solid gray; padding: 2px; display: inline-block;">Reset</div>	Click to undo any changes made locally and revert to previously saved values.

4.1.5.3.3 LACP System Status

This page provides a status overview for all LACP instances.

Figure 26: LACP System Status

LACP System Status

Auto-refresh Refresh Open in new window

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'
Partner System ID	The system ID (MAC address) of the aggregation partner.
Partner Key	The Key that the partner has assigned to this aggregation ID.
Last Changed	The time since this aggregation changed.
Local Ports	Shows which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID:Port"
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
Auto-refresh <input type="checkbox"/>	Check this box to enable an automatic refresh of the page at regular intervals.

LACP Status

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

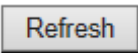
Figure 27: LACP Status

LACP Status

Auto-refresh Refresh Open in new window

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	-	-	-	-
9	No	-	-	-	-
10	No	-	-	-	-
11	No	-	-	-	-
12	No	-	-	-	-
13	No	-	-	-	-
14	No	-	-	-	-
15	No	-	-	-	-
16	No	-	-	-	-
17	No	-	-	-	-
18	No	-	-	-	-
19	No	-	-	-	-
20	No	-	-	-	-
21	No	-	-	-	-
22	No	-	-	-	-
23	No	-	-	-	-
24	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

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

4.1.5.3.4 LACP Statistics

This page provides an overview for LACP statistics for all ports.

Figure 28: LACP Statistics

LACP Statistics

Auto-refresh Refresh Clear

Port	LACP Transmitted	LACP Received	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
21	0	0	0	0
22	0	0	0	0
23	0	0	0	0
24	0	0	0	0

Label	Description
Port	The switch port number
LACP Transmitted	Shows how many LACP frames have been sent from each port
LACP Received	Shows how many LACP frames have been received at each port.

Label	Description
Discarded	Shows how many unknown or illegal LACP frames have been discarded at each port.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
Auto-refresh <input type="checkbox"/>	Check this box to enable an automatic refresh of the page at regular intervals.
<input type="button" value="Clear"/>	Clears the counters for all ports

4.1.6 Redundancy

4.1.6.1 Redundant Ring

Redundant Ring is one of the most powerful Ring in the world. The recovery time of Ring is less than 20 ms. It can reduce unexpected damage caused by network topology change. Ring Supports 3 Ring topology: Redundant Ring, Coupling Ring and Dual Homing.

Figure 29: Redundant Ring Configuration

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.
1 st Ring Port	The primary port, when this switch is Ring Master.
2 nd 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.

4.1.7 MSTP

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 30: STP Bridge Configuration

STP Bridge Configuration

Basic Settings

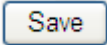
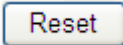
Protocol Version	MSTP ▼
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

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: 100%;" type="text"/>

Save Reset

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 Max Age must be $\leq (FwdDelay-1) * 2$.

Label	Description
Maximum Hop Count	This defines the initial value of remaining Hops 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 Max Age 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.

4.1.7.1 MSTI Mapping

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

Figure 31: MSTI Mapping

MSTI Configuration

Add VLANs separated by spaces or comma.

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

Configuration Identification

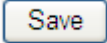
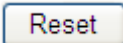
Configuration Name	00-1e-94-94-3e-9e
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MST1	
MST2	
MST3	
MST4	
MST5	
MST6	
MST7	

Save

Reset

Label	Description
Configuration Name	The name identification 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.
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.

4.1.7.2 MSTI Priorities

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

Figure 32: MSTI Configuration

MSTI Configuration

MSTI Priority Configuration

MSTI	Priority
CIST	128 ▼
MST1	128 ▼
MST2	128 ▼
MST3	128 ▼
MST4	128 ▼
MST5	128 ▼
MST6	128 ▼
MST7	128 ▼

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.
<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.

4.1.8 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 33: STP CIST Ports Configuration

STP CIST Ports Configuration

CIST Aggregated Ports Configuration

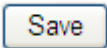
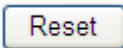
Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
-	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True

CIST Normal Ports Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
1	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
5	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
7	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
8	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
9	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
10	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
11	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
12	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
13	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
14	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
15	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
16	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
17	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
18	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
19	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
20	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
21	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
22	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
23	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
24	<input type="checkbox"/>	Auto	128	Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Save Reset

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 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).
Open Edge(set ate 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.
Admin Edge	Controls whether the operEdge flag should start as being set or cleared. (The initial operEdge state when a port is initialized).
Auto Edge	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

Label	Description
	<p>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 known as Root Guard.</p>
Restricted TCN	<p>If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistent incorrectly learned station location information. 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.</p>
Point2Point	<p>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.</p>
	<p>Click to save changes.</p>
	<p>Click to undo any changes made locally and revert to previously saved values.</p>

4.1.8.1 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 34: MSTI Port Configuration

MSTI Port Configuration

Select MSTI

MST1
MST2
MST3
MST4
MST5
MST6
MST7

Get

MST1 MSTI Port Configuration

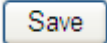
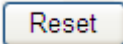
MST1 Aggregated Ports Configuration

Port	Path Cost		Priority
-	Auto		128

MST1 Normal Ports Configuration

Port	Path Cost		Priority
1	Auto		128
2	Auto		128
3	Auto		128
4	Auto		128
5	Auto		128
6	Auto		128
7	Auto		128
8	Auto		128
9	Auto		128
10	Auto		128
11	Auto		128
12	Auto		128
13	Auto		128
14	Auto		128
15	Auto		128
16	Auto		128
17	Auto		128
18	Auto		128
19	Auto		128
20	Auto		128
21	Auto		128
22	Auto		128
23	Auto		128
24	Auto		128

Save
Reset

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.

4.1.9 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 35: STP Bridges

STP Bridges

Auto-refresh Refresh

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	80:00-00:1E:94:94:3E:9E	80:00-00:1E:94:94:3E:9E	-	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.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
Auto-refresh <input type="checkbox"/>	Check this box to enable an automatic refresh of the page at regular intervals.

4.1.10 STP Port Status

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

Figure 36: STP Port Status

STP Port Status

Auto-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	-
21	Non-STP	Forwarding	-
22	Non-STP	Forwarding	-
23	Non-STP	Forwarding	-
24	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.
Uptime	The time since the bridge port was last initialized.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
Auto-refresh <input type="checkbox"/>	Check this box to enable an automatic refresh of the page at regular intervals.

4.1.11 STP Statistics

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

Figure 37: 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.
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.
<input type="button" value="Refresh"/>	Click to refresh the page immediately.
Auto-refresh <input type="checkbox"/>	Check this box to enable an automatic refresh of the page at regular intervals.

4.1.12 VLAN

4.1.12.1 VLAN Membership Configuration

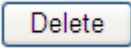
The VLAN membership configuration for the selected stack switch unit switch can be monitored and modified here. Up to 64 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN.

Figure 38: VLAN

VLAN Membership Configuration

		Port Members																							
Delete	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
<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"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" 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"/>	<input type="checkbox"/>
<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" 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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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 <input type="button" value="Add New VLAN"/> to add a new VLAN ID. An empty row is added to the table, and the VLAN can be

Label	Description
	<p>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>

4.1.12.2 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 39: Private VLAN

Private VLAN Membership Configuration

[Open in new window](#)

		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	21	22	23	24
<input type="checkbox"/>	1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

[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

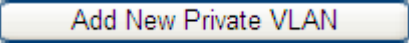

	members, and all boxes are unchecked.
Adding a New Static Entry	<p>Click  to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click "OK" to discard 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  button can be used to undo the addition of new Private VLANs.</p>

Figure 40: Port Isolation Configuration

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	21	22	23	24
<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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Label	Description
Port Members	<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>

4.1.13 SNMP

4.1.13.1 SNMP-System

Figure 41: 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>
Read Community	<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>
Write	<p>Indicates the community write access string to permit access to</p>

Label	Description
Community	SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. 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.
Engine ID	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.

Figure 42: 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	Indicates the SNMP trap mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.

Label	Description
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'. 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> <p>Enabled: Enable SNMP trap authentication failure.</p> <p>Disabled: Disable SNMP trap authentication failure.</p>
Trap Link-up and Link-down	<p>Indicates the SNMP trap link-up and link-down mode operation.</p> <p>Possible modes are:</p>

Label	Description
	<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>
Trap Inform Mode	<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>
Trap Inform Timeout(seconds)	<p>Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.</p>
Trap Inform Retry Times	<p>Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.</p>
Trap Probe Security Engine ID	<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>
Trap Security Engine ID	<p>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</p>

	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.

4.1.13.2 SNMP-Communities

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

Figure 43: SNMPv3

SNMPv3 Communities 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

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

4.1.14 SNMP-Users

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

Figure 44: SNMPv3

SNMPv3 Users 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 simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Level	Indicates the security model that this entry should belong to. Possible security models are: NoAuth, NoPriv: None authentication and none privacy.

Label	Description
	<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>
Authentication Protocol	<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>
Authentication Password	<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>
Privacy Protocol	<p>Indicates the privacy protocol that this entry should belong to.</p> <p>Possible privacy protocols are:</p> <p>None: None privacy protocol.</p> <p>DES: An optional flag to indicate that this user using DES authentication protocol.</p>
Privacy Password	<p>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.</p>

4.1.14.1 SNMP-Groups

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

Figure 45: SNMPv3 Groups Configuration

SNMPv3 Groups 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

Add new group

Save

Reset

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.

4.1.14.2 SNMP-Views

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

SNMPv3 Views 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(*).
-------------	---

4.1.2.1 SNMP-Accesses

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

Figure 46: SNMPv3 Accesses Configuration

SNMPv3 Accesses 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	<p>Indicates the security model that this entry should belong to.</p> <p>Possible security models are:</p> <p>any: Accepted any security model (v1 v2c usm).</p> <p>v1: Reserved for SNMPv1.</p> <p>v2c: Reserved for SNMPv2c.</p> <p>usm: User-based Security Model (USM).</p>
Security Level	Indicates the security model that this entry should belong to.

	<p>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>
Read View Name	<p>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.</p>
Write View Name	<p>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.</p>

4.1.15 Traffic Prioritization

4.1.15.1 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

Storm Control Configuration

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

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.

4.1.15.2 Port QoS

This page allows you to configure QoS settings for each port.

Frames can be classified by 4 different QoS classes: Low, Normal, Medium, and High.

The classification is controlled by a QCL that is assigned to each port.

A QCL consists of an ordered list of up to 12 QCEs.

Each QCE can be used to classify certain frames to a specific QoS class.

This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority.

Frames not matching any of the QCEs are classified to the default QoS class for the port.

4.1.15.2.1 Port QoS Configuration

Figure 48: Port QoS Configuration

Port QoS Configuration

Ingress Configuration				Egress Configuration				
Port	Default Class	QCL #	Tag Priority	Queuing Mode	Queue Weighted			
					Low	Normal	Medium	High
1	Low	1	0	Strict Priority	1	2	4	8
2	Low	1	0	Strict Priority	1	2	4	8
3	Low	1	0	Strict Priority	1	2	4	8
4	Low	1	0	Strict Priority	1	2	4	8
5	Low	1	0	Strict Priority	1	2	4	8
6	Low	1	0	Strict Priority	1	2	4	8
7	Low	1	0	Strict Priority	1	2	4	8
8	Low	1	0	Strict Priority	1	2	4	8
9	Low	1	0	Strict Priority	1	2	4	8
10	Low	1	0	Strict Priority	1	2	4	8
11	Low	1	0	Strict Priority	1	2	4	8
12	Low	1	0	Strict Priority	1	2	4	8
13	Low	1	0	Strict Priority	1	2	4	8
14	Low	1	0	Strict Priority	1	2	4	8
15	Low	1	0	Strict Priority	1	2	4	8
16	Low	1	0	Strict Priority	1	2	4	8
17	Low	1	0	Strict Priority	1	2	4	8
18	Low	1	0	Strict Priority	1	2	4	8
19	Low	1	0	Strict Priority	1	2	4	8
20	Low	1	0	Strict Priority	1	2	4	8
21	Low	1	0	Strict Priority	1	2	4	8
22	Low	1	0	Strict Priority	1	2	4	8
23	Low	1	0	Strict Priority	1	2	4	8
24	Low	1	0	Strict Priority	1	2	4	8

Save Reset

Label	Description
Port	<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>
Default Class	Configure the default QoS class for the port, that is, the QoS class for frames not matching any of the QCEs in the QCL.
QCL#	Select which QCL to use for the port.
Tag Priority	Select the default tag priority for this port when adding a Tag to the untagged frames.
Queuing Mode	Select which Queuing mode for this port.
Queue Weighted	Setting Queue weighted (Low=Normal, Medium=High) if the "Queuing Mode" is "Weighted".

4.1.15.3 QoS Control List

This page lists the QCEs for a given QCL.

Frames can be classified by 4 different QoS classes: Low, Normal, Medium, and High.

The classification is controlled by a QoS assigned to each port.

A QCL consists of an ordered list of up to 12 QCEs.

Each QCE can be used to classify certain frames to a specific QoS class.







This classification can be based on parameters such as VLAN ID, UDP/TCP port, IPv4/IPv6 DSCP or Tag Priority. Frames not matching any of the QCEs are classified to the default QoS Class for the port.

Figure 49: QCE Configuration

QCE Configuration

QCE Type	Ethernet Type ▾
Ethernet Type Value	0x FFFF
Traffic Class	Low ▾

Label	Description
QCL#	Select a QCL to display a table that lists all the QCEs for that particular QCL.
QCE Type	<p>Specifies which frame field the QCE processes to determine the QoS class of the frame.</p> <p>The following QCE types are supported:</p> <p>Ethernet Type: The Ethernet Type field. If frame is tagged, this is the Ethernet Type that follows the tag header.</p> <p>VLAN ID: VLAN ID. Only applicable if the frame is VLAN tagged.</p> <p>TCP/UDP Port: IPv4 TCP/UDP source/destination port.</p> <p>DSCP: IPv4 and IPv6 DSCP.</p> <p>ToS: The 3 precedence bit in the ToS byte of the IPv4/IPv6 header (also known as DS field).</p> <p>Tag Priority: User Priority. Only applicable if the frame is VLAN</p>

Label	Description
	tagged or priority tagged.
Type Value	<p>Indicates the value according to its QCE type.</p> <p>Ethernet Type: The field shows the Ethernet Type value.</p> <p>VLAN ID: The field shows the VLAN ID.</p> <p>TCP/UDP Port: The field shows the TCP/UDP port range.</p> <p>DSCP: The field shows the IPv4/IPv6 DSCP value.</p>
Traffic Class	The QoS class associated with the QCE.
Modification Buttons	<p>You can modify each QCE in the table using the following buttons:</p> <ul style="list-style-type: none">  : Inserts a new QCE before the current row.  : Edits the QCE.  : Moves the QCE up the list.  : Moves the QCE down the list.  : Deletes the QCE.  : The lowest plus sign adds a new entry at the bottom of the list of QCL.

4.1.15.4 Queuing Counters

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

Figure 50: Queuing Counters

Queuing Counters

Auto-refresh Refresh Clear

Port	Low Queue		Normal Queue		Medium Queue		High Queue	
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit
1	0	14	0	0	0	0	0	3
2	0	67	0	0	0	0	0	14
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	178128	239086	0	0	0	0	0	707
9	0	0	0	0	0	0	0	0
10	0	32345	0	0	0	0	0	312
11	0	0	0	0	0	0	0	0
12	207136	169865	0	0	0	0	0	404
13	0	0	0	0	0	0	0	0
14	1040	33805	0	0	0	0	247	316
15	75769	74825	0	0	0	0	0	14210
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0

Label	Description
Port	The logical port for the settings contained in the same row.
Low Queue	There are 4 QoS queues per port with strict or weighted queuing scheduling. This is the lowest priority queue.
Normal Queue	This is the normal priority queue of the 4 QoS queues. It has higher priority than the "Low Queue".
Medium Queue	This is the medium priority queue of the 4 QoS queues. It has higher priority than the "Normal Queue".
High Queue	This is the highest priority queue of the 4 QoS queues.
Receive / Transmit	The number of received and transmitted packets per port.

4.1.15.5 Wizard

This handy wizard helps you set up a QCL quickly.

Figure 51: Wizard

Welcome to the QCL Configuration Wizard!

Please select an action:

- Set up IP Cam High Performance**
Increase IP Cam performance.
- Set up Port Policies**
Group ports into several types according to different QCL policies.
- Set up Typical Network Application Rules**
Set up the specific QCL for different typical network application quality control.
- Set up ToS Precedence Mapping**
Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.
- Set up VLAN Tag Priority Mapping**
Set up the traffic class mapping to the user priority value (3 bits) when receiving VLAN tagged packets.

To continue, click Next.

Next >

Label	Description
Set up Port Policies	Group ports into several types according to different QCL policies.
Set up Typical Network Application Rules	Set up the specific QCL for different typical network application quality control.
Set up ToS Precedence Mapping	Set up the traffic class mapping to the precedence part of ToS (3 bits) when receiving IPv4/IPv6 packets.
Set up VLAN Tag Priority Mapping	Set up the traffic class mapping to the User Priority value (3 bits) when receiving VLAN tagged packets.

4.1.16 Multicast

4.1.16.1 IGMP Snooping

This page provides IGMP Snooping related configuration.

Figure 52: IGMP Snooping

Global Configuration	
Snooping Enabled	<input type="checkbox"/>
Unregistered IPMC Flooding enabled	<input type="checkbox"/>

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

Port Related Configuration

Port	Router Port	Fast Leave
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"/>
7	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="checkbox"/>	<input type="checkbox"/>
15	<input type="checkbox"/>	<input type="checkbox"/>
16	<input type="checkbox"/>	<input type="checkbox"/>
17	<input type="checkbox"/>	<input type="checkbox"/>
18	<input type="checkbox"/>	<input type="checkbox"/>
19	<input type="checkbox"/>	<input type="checkbox"/>
20	<input type="checkbox"/>	<input type="checkbox"/>
21	<input type="checkbox"/>	<input type="checkbox"/>
22	<input type="checkbox"/>	<input type="checkbox"/>
23	<input type="checkbox"/>	<input type="checkbox"/>
24	<input type="checkbox"/>	<input type="checkbox"/>

Label	Description
Snooping Enabled	Enable the Global IGMP Snooping.
Unregistered IPMC Flooding enabled	Enable unregistered IPMC traffic flooding.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping.
IGMP Querier	Enable the IGMP Querier in the VLAN. The Querier will send out if no Querier received in 255 seconds after IGMP Querier Enabled. Each Querier's interval is 125 second, and it will stop act as an IGMP Querier if received any Querier from other devices.
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.

4.1.16.2 IGMP Snooping Status

Figure 53: IGMP Snooping

Auto-refresh Refresh Clear Open in new window

IGMP Snooping Status

Statistics

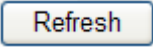
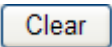
VLAN ID	Querier Status	Querier Transmit	Querier Receive	V1 Reports Receive	V2 Reports Receive	V3 Reports Receive	V2 Leave Receive
1	IDLE	0	0	0	0	0	0
50	IDLE	0	0	0	0	0	0

IGMP Groups

VLAN ID	Groups	Port Members																							
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
No IGMP groups																									

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-
17	-
18	-
19	-
20	-
21	-
22	-
23	-
24	-

Label	Description
VLAN ID	The VLAN ID of the entry.
Groups	The present IGMP groups. Max. are 128 groups for each VLAN.
Port Members	The ports that are members of the entry.
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.
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.
	Click to refresh the page immediately.
	Clears all Statistics counters.
Auto-refresh <input type="checkbox"/>	Check this box to enable an automatic refresh of the page at regular intervals.

4.1.17 Security

4.1.17.1 ACL

4.1.17.1.1 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 54: ACL Ports Configuration

ACL Ports Configuration

Refresh Clear

Port	Policy ID	Action	Rate Limiter ID	Port Copy	Logging	Shutdown	Counter
1	1	Permit	Disabled	Disabled	Disabled	Disabled	0
2	1	Permit	Disabled	Disabled	Disabled	Disabled	0
3	1	Permit	Disabled	Disabled	Disabled	Disabled	0
4	1	Permit	Disabled	Disabled	Disabled	Disabled	0
5	1	Permit	Disabled	Disabled	Disabled	Disabled	0
6	1	Permit	Disabled	Disabled	Disabled	Disabled	0
7	1	Permit	Disabled	Disabled	Disabled	Disabled	0
8	1	Permit	Disabled	Disabled	Disabled	Disabled	178128
9	1	Permit	Disabled	Disabled	Disabled	Disabled	0
10	1	Permit	Disabled	Disabled	Disabled	Disabled	0
11	1	Permit	Disabled	Disabled	Disabled	Disabled	0
12	1	Permit	Disabled	Disabled	Disabled	Disabled	207136
13	1	Permit	Disabled	Disabled	Disabled	Disabled	0
14	1	Permit	Disabled	Disabled	Disabled	Disabled	1301
15	1	Permit	Disabled	Disabled	Disabled	Disabled	77493
16	1	Permit	Disabled	Disabled	Disabled	Disabled	0
17	1	Permit	Disabled	Disabled	Disabled	Disabled	0
18	1	Permit	Disabled	Disabled	Disabled	Disabled	0
19	1	Permit	Disabled	Disabled	Disabled	Disabled	0
20	1	Permit	Disabled	Disabled	Disabled	Disabled	0
21	1	Permit	Disabled	Disabled	Disabled	Disabled	0
22	1	Permit	Disabled	Disabled	Disabled	Disabled	0
23	1	Permit	Disabled	Disabled	Disabled	Disabled	0
24	1	Permit	Disabled	Disabled	Disabled	Disabled	0

Save Reset

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

4.1.17.1.2 Rate Limiters

Configure the rate limiter for the ACL of the switch.

Figure 55: ACL Rate Limiter Configuration

ACL Rate Limiter Configuration

Rate Limiter ID	Rate (pps)
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1

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.

4.1.17.1.3 ACL Configuration

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 56: ACE Configuration

ACE Configuration

Ingress Port	Any ▾
Frame Type	Any ▾

Action	Permit ▾
Rate Limiter	Disabled ▾
Port Copy	Disabled ▾
Logging	Disabled ▾
Shutdown	Disabled ▾
Counter	0

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> <p>ARP: Only ARP frames can match this ACE. Notice the ARP frames</p>

Label	Description
	<p>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 57: MAC Parameters

MAC Parameters

SMAC Filter	Specific ▼
SMAC Value	00-00-00-00-00-01
DMAC Filter	Specific ▼
DMAC Value	00-00-00-00-00-02

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>

Label	Description
	<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>
DMAC Value	<p>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.</p>

Figure 58: VLAN Parameters

VLAN Parameters

VLAN ID Filter	Specific ▾
VLAN ID	1
Tag Priority	Any ▾

Label	Description
VLAN ID Filter	<p>Specify the VLAN ID filter for this ACE.</p> <p>Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)</p> <p>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.</p>
VLAN ID	<p>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.</p>
Tag Priority	<p>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</p>

	"don't-care".)
--	----------------

Figure 59: IP Parameters

IP Parameters

IP Protocol Filter	Other ▾
IP Protocol Value	255
IP TTL	Non-zero ▾
IP Fragment	Any ▾
IP Option	Any ▾
SIP Filter	Any ▾
DIP Filter	Any ▾

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 Protocol Value	<p>When "Specific" is selected for the IP protocol value, you can enter a specific value.. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value.</p>

Label	Description
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> <p>Any: Any value is allowed ("don't-care").</p>
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>

Label	Description
	<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>
SIP Address	When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.
SIP Mask	When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
DIP Filter	<p>Specify the destination IP filter for this ACE.</p> <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>
DIP Address	When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.
DIP Mask	When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

Figure 60: ARP Parameters

ARP Parameters

ARP/RARP	Other ▾	ARP SMAC Match	Any ▾
Request/Reply	Request ▾	RARP SMAC Match	Any ▾
Sender IP Filter	Network ▾	IP/Ethernet Length	Any ▾
Sender IP Address	192.168.1.1	IP	Any ▾
Sender IP Mask	255.255.255.0	Ethernet	Any ▾
Target IP Filter	Any ▾		

Save Reset Cancel

Label	Description
ARP/RARP	Specify the available ARP/RARP opcode (OP) flag for this ACE. Any: No ARP/RARP OP flag is specified. (OP is "don't-care".) ARP: Frame must have ARP/RARP opcode set to ARP. RARP: Frame must have ARP/RARP opcode set to RARP. Other: Frame has unknown ARP/RARP opcode flag.
Request/Reply	Specify the available ARP/RARP opcode (OP) flag for this ACE. Any: No ARP/RARP OP flag is specified. (OP is "don't-care".) Request: Frame must have ARP Request or RARP Request OP flag set. Reply: Frame must have ARP Reply or RARP Reply OP flag.
Sender IP Filter	Specify the sender IP filter for this ACE. Any: No sender IP filter is specified. (Sender IP filter is "don't-care".) Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears. 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

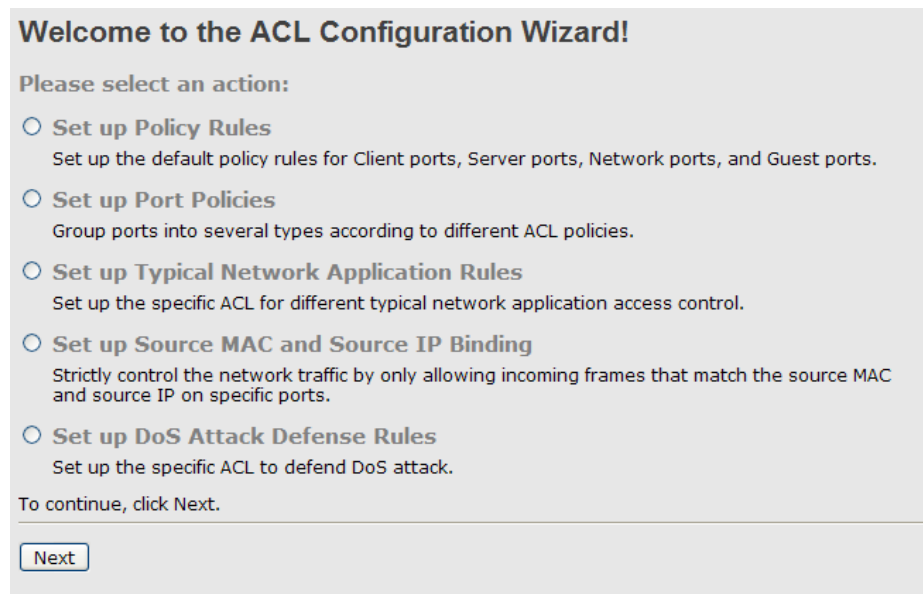
Label	Description
	that appear.
Sender IP Address	When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.
Sender IP Mask	When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.
Target IP Filter	Specify the target IP filter for this specific ACE. Any: No target IP filter is specified. (Target IP filter is "don't-care".) 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.
Target IP Address	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	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. 0: ARP frames where SHA is not equal to the SMAC address. 1: ARP frames where SHA is equal to the SMAC address. Any: Any value is allowed ("don't-care").
RARP SMAC Match	Specify whether frames can hit the action according to their target hardware address field (THA) settings. 0: RARP frames where THA is not equal to the SMAC address. 1: RARP frames where THA is equal to the SMAC address. Any: Any value is allowed ("don't-care").
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. 0: ARP/RARP frames where the HLN is equal to Ethernet (0x06)

Label	Description
	<p>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>
IP	<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>
Ethernet	<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>

4.1.17.1.4 Wizard

This handy wizard helps you set up an ACL quickly

Figure 61: Wizard



Label	Description
Set up Policy Rules	Set up the default policy rules for Client ports, Server ports, Network ports and Guest ports.
Set up Port Policies	Group ports into several types according to different ACL policies.
Set up Typical Network Application Rules	Set up the specific ACL for different typical network application access control.
Set up Source MAC and Source IP Binding	Strictly control the network traffic by only allowing incoming frames that match the source IP and source MAC on specific port.
Set up Dos Attack Defense Rules	Set up the specific ACL to defend DoS attack.

4.1.17.2 802.1x

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 802.1X authentication.

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 are 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 are 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 62: Port Security Configuration

Port Security Configuration

System Configuration

Mode	Disabled <input type="button" value="v"/>
Reauthentication Enabled	<input type="checkbox"/>
Reauthentication Period	3600 seconds
EAP Timeout	30 seconds
Age Period	300 seconds
Hold Time	10 seconds

Port Configuration

Port	Admin State	Port State	Max Clients		Restart	
1	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
2	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
3	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
4	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
5	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
6	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
7	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
8	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
9	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
10	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
11	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
12	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
13	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
14	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
15	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
16	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
17	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
18	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
19	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
20	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
21	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
22	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
23	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	Reauthenticate	Reinitialize
24	Authorized <input type="button" value="v"/>	Disabled	All <input type="button" value="v"/>	96	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 between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Age Period below).</p>
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.
EAP Timeout	Determines the time the switch shall wait for the supplicant response before retransmitting a packet. Valid values are in the range 1 to 255 seconds. This has no effect for MAC-based ports.
Age Period	<p>This setting applies to ports running MAC-based authentication, only.</p> <p>Suppose a client is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch that runs MAC-based authentication, and suppose the client gets</p>

Label	Description
	<p>successfully authenticated. Now assume that the client powers down his PC. What should make the switch forget about the authenticated client? Reauthentication will not solve this problem, since this doesn't require the client to be present, as discussed under Reauthentication Enabled above. The solution is aging of authenticated clients. The Age Period, which can be set to a number between 10 and 1000000 seconds, works like this: A timer is started when the client gets authenticated. After half the age period, the switch starts looking for frames sent by the client. If another half age period elapses and no frames are seen, the client is considered removed from the system, and it will have to authenticate again the next time a frame is seen from it. If, on the other hand, the client transmits a frame before the second half of the age period expires, the switch will consider the client alive, and leave it authenticated. Therefore, an age period of T will require the client to send frames more frequent than T/2 for him to stay authenticated.</p>
Hold Time	<p>This setting applies to ports running MAC-based authentication, only.</p> <p>If the RADIUS server denies a client access, or a RADIUS server request times out (according to the timeout specified on the Authentication configuration page), the client is put on hold in the Unauthorized state. In this state, frames from the client will not cause the switch to attempt to reauthenticate the client. The Hold Time, which can be set to a number between 10 and 1000000 seconds, determines the time after an EAP Failure indication or RADIUS timeout that a client is not</p>

Label	Description
	allowed access.
Port	The port number for which the configuration below applies.
Admin State	<p>Sets the authentication mode to one of the following options (only used when 802.1X or MAC-based authentication is globally enabled):</p> <p>Auto: Requires an 802.1X-aware client (supplicant) to be authorized by the authentication server. Clients that are not 802.1X-aware will be denied access.</p> <p>Authorized: Forces the port to grant access to all clients, 802.1X-aware or not. The switch transmits an EAPOL Success frame when the port links up.</p> <p>Unauthorized: Forces the port to deny access to all clients, 802.1X-aware or not. The switch transmits an EAPOL Failure frame when the port links up.</p> <p>MAC-Based: Enables MAC-based authentication on the port. The switch doesn't transmit or accept EAPOL frames on the port. Flooded frames and broadcast traffic will be transmitted on the port, whether or not clients are authenticated on the port, whereas unicast traffic against an unsuccessfully authenticated client will be dropped. Clients that are not (yet) successfully authenticated will not be allowed to transmit frames of any kind.</p>
Port State	<p>The current state of the port. It can undertake one of the following values:</p> <p>Disabled: 802.1X and MAC-based authentication is globally</p>

Label	Description
	<p>disabled.</p> <p>Link Down: 802.1X or MAC-based authentication is enabled, but there is no link on the port.</p> <p>Authorized: The port is authorized. This is the case when 802.1X authentication is enabled, the port has link, and the Admin State is "Auto" and the supplicant is authenticated or the Admin State is "Authorized".</p> <p>Unauthorized: The port is unauthorized. This is the case when 802.1X authentication is enabled, the port has link, and the Admin State is "Auto", but the supplicant is not (yet) authenticated or the Admin State is "Unauthorized".</p> <p>X Auth/Y Unauth: X clients are currently authorized and Y are unauthorized. This state is shown when 802.1X and MAC-based authentication is globally enabled and the Admin State is set to "MAC-Based".</p>
Max Clients	<p>This setting applies to ports running MAC-based authentication, only.</p> <p>The maximum number of clients allowed on a given port can be configured through the list-box and edit-control for this setting. Choosing the value "All" from the list-box allows the port to consume up to 48 client state-machines. Choosing the value "Specific" from the list-box opens up for entering a specific number of maximum clients on the port (1 to 48).</p> <p>The switch is "born" with a pool of state-machines, from which all ports draw whenever a new client is seen on the port. When a given port's maximum is reached (both authorized and</p>

Label	Description
	<p>unauthorized clients count), further new clients are disallowed access. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available state-machines.</p>
Restart	<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 "Auto" or "MAC-Based".</p> <p>Clicking these buttons will not cause settings changed on the page to take effect.</p> <p>Reauthenticate: Schedules a reauthentication to whenever the quiet-period of the port runs out (port-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.</p> <p>The button only has effect for successfully authenticated ports/clients and will not cause the port/client to get temporarily unauthorized.</p> <p>Reinitialize: Forces a reinitialization of the port/clients and thereby a reauthentication immediately. The port/clients will transfer to the unauthorized state while the reauthentication is ongoing.</p>

Figure 63: Port Security Status

Port Security Status

Auto-refresh Refresh

Port	State	Last Source	Last ID
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		
21	Disabled		
22	Disabled		
23	Disabled		
24	Disabled		

Label	Description
Port	The switch port number. Click to navigate to detailed 802.1X statistics for this port.
State	The current state of the port. Refer to IEEE 802.1X Port State for a description of the individual states.
Last Source	The source MAC address carried in the most recently received EAPOL frame for port-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 Resp/ID EAPOL frame for port-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 64: 802.1X Statistics Port 1

802.1X Statistics Port 1

Port 1	Auto-refresh <input type="checkbox"/>	Refresh	Clear
Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	Total	0
Response ID Responses	0	Request ID Requests	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		
Receive Backend Server Counters		Transmit Backend Server Counters	
Access Challenges	0	Responses	0
Other Requests	0		
Auth. Successes	0		
Auth. Failures	0		
Last Supplicant Info			
Version			0
Source Identity			

Label	Description																																																
EAPOL Counters	<p>These counters are not available for MAC-based ports.</p> <p>Supplicant frame counter statistics. There are seven receive frame counters and three transmit frame counters.</p> <table border="1"> <thead> <tr> <th colspan="4">EAPOL Counters</th> </tr> <tr> <th>Direction</th> <th>Name</th> <th>IEEE Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Rx</td> <td>Total</td> <td>dot1xAuthEapolFramesRx</td> <td>The number of valid EAPOL frames of any type that have been received by the switch.</td> </tr> <tr> <td>Rx</td> <td>Response ID</td> <td>dot1xAuthEapolRespIdFramesRx</td> <td>The number of valid EAP Resp/ID frames that have been received by the switch.</td> </tr> <tr> <td>Rx</td> <td>Responses</td> <td>dot1xAuthEapolRespFramesRx</td> <td>The number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch.</td> </tr> <tr> <td>Rx</td> <td>Start</td> <td>dot1xAuthEapolStartFramesRx</td> <td>The number of EAPOL Start frames that have been received by the switch.</td> </tr> <tr> <td>Rx</td> <td>Logoff</td> <td>dot1xAuthEapolLogoffFramesRx</td> <td>The number of valid EAPOL logoff frames that have been received by the switch.</td> </tr> <tr> <td>Rx</td> <td>Invalid Type</td> <td>dot1xAuthInvalidEapolFramesRx</td> <td>The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.</td> </tr> <tr> <td>Rx</td> <td>Invalid Length</td> <td>dot1xAuthEapolLengthErrorFramesRx</td> <td>The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.</td> </tr> <tr> <td>Tx</td> <td>Total</td> <td>dot1xAuthEapolFramesTx</td> <td>The number of EAPOL frames of any type that have been transmitted by the switch.</td> </tr> <tr> <td>Tx</td> <td>Request ID</td> <td>dot1xAuthEapolReqIdFramesTx</td> <td>The number of EAP initial request frames that have been transmitted by the switch.</td> </tr> <tr> <td>Tx</td> <td>Requests</td> <td>dot1xAuthEapolReqFramesTx</td> <td>The number of valid EAP Request frames (other than initial request frames) that have been transmitted by the switch.</td> </tr> </tbody> </table>	EAPOL Counters				Direction	Name	IEEE Name	Description	Rx	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.	Rx	Response ID	dot1xAuthEapolRespIdFramesRx	The number of valid EAP Resp/ID frames that have been received by the switch.	Rx	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch.	Rx	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.	Rx	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL logoff frames that have been received by the switch.	Rx	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.	Rx	Invalid Length	dot1xAuthEapolLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.	Tx	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.	Tx	Request ID	dot1xAuthEapolReqIdFramesTx	The number of EAP initial request frames that have been transmitted by the switch.	Tx	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAP Request frames (other than initial request frames) that have been transmitted by the switch.
EAPOL Counters																																																	
Direction	Name	IEEE Name	Description																																														
Rx	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.																																														
Rx	Response ID	dot1xAuthEapolRespIdFramesRx	The number of valid EAP Resp/ID frames that have been received by the switch.																																														
Rx	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Resp/ID frames) that have been received by the switch.																																														
Rx	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.																																														
Rx	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL logoff frames that have been received by the switch.																																														
Rx	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.																																														
Rx	Invalid Length	dot1xAuthEapolLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.																																														
Tx	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.																																														
Tx	Request ID	dot1xAuthEapolReqIdFramesTx	The number of EAP initial request frames that have been transmitted by the switch.																																														
Tx	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAP Request frames (other than initial request frames) that have been transmitted by the switch.																																														
Backend Server Counters	<p>Backend server frame counter statistics.</p> <p>For MAC-based ports there are two tables containing backend server counters. The left-most shows a summary of all backend</p>																																																

Label	Description																												
	<p>server counters on this port. The right-most shows backend server counters for the currently selected client, or dashes if no client is selected or available. A client can be selected from the list of authorized/unauthorized clients below the two counter tables.</p> <p>There are slight differences in the interpretation of the counters between port- and MAC-based authentication as shown below.</p> <table border="1" data-bbox="662 674 1487 1140"> <thead> <tr> <th colspan="4">Backend Server Counters</th> </tr> <tr> <th>Direction</th> <th>Name</th> <th>IEEE Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Rx</td> <td>Access Challenges</td> <td>dot1xAuthBackendAccessChallenges</td> <td>Port-based: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. MAC-based: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).</td> </tr> <tr> <td>Rx</td> <td>Other Requests</td> <td>dot1xAuthBackendOtherRequestsToSupplicant</td> <td>Port-based: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. MAC-based: Not applicable.</td> </tr> <tr> <td>Rx</td> <td>Auth. Successes</td> <td>dot1xAuthBackendAuthSuccesses</td> <td>Port- and MAC-based: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.</td> </tr> <tr> <td>Rx</td> <td>Auth. Failures</td> <td>dot1xAuthBackendAuthFails</td> <td>Port- and MAC-based: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.</td> </tr> <tr> <td>Tx</td> <td>Responses</td> <td>dot1xAuthBackendResponses</td> <td>Port-based: Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. MAC-based: Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.</td> </tr> </tbody> </table>	Backend Server Counters				Direction	Name	IEEE Name	Description	Rx	Access Challenges	dot1xAuthBackendAccessChallenges	Port-based: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. MAC-based: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).	Rx	Other Requests	dot1xAuthBackendOtherRequestsToSupplicant	Port-based: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. MAC-based: Not applicable.	Rx	Auth. Successes	dot1xAuthBackendAuthSuccesses	Port- and MAC-based: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.	Rx	Auth. Failures	dot1xAuthBackendAuthFails	Port- and MAC-based: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.	Tx	Responses	dot1xAuthBackendResponses	Port-based: Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. MAC-based: Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.
Backend Server Counters																													
Direction	Name	IEEE Name	Description																										
Rx	Access Challenges	dot1xAuthBackendAccessChallenges	Port-based: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. MAC-based: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).																										
Rx	Other Requests	dot1xAuthBackendOtherRequestsToSupplicant	Port-based: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. MAC-based: Not applicable.																										
Rx	Auth. Successes	dot1xAuthBackendAuthSuccesses	Port- and MAC-based: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.																										
Rx	Auth. Failures	dot1xAuthBackendAuthFails	Port- and MAC-based: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.																										
Tx	Responses	dot1xAuthBackendResponses	Port-based: Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. MAC-based: Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.																										
Last Supplicant/Client Info	<p>For MAC-based ports, this section is embedded in the backend server counter's section.</p> <p>Information about the last supplicant/client that attempted to authenticate.</p> <table border="1" data-bbox="662 1461 1487 1675"> <thead> <tr> <th colspan="4">Last Supplicant/Client Info</th> </tr> <tr> <th>Name</th> <th>IEEE Name</th> <th></th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Version</td> <td>dot1xAuthLastEapolFrameVersion</td> <td></td> <td>Port-based: The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable.</td> </tr> <tr> <td>Source</td> <td>dot1xAuthLastEapolFrameSource</td> <td></td> <td>Port-based: The source MAC address carried in the most recently received EAPOL frame. MAC-based: Not applicable.</td> </tr> <tr> <td>Identity or (Last) Client</td> <td>-</td> <td></td> <td>Port-based: The user name (supplicant identity) carried in the most recently received Resp/ID EAPOL frame. MAC-based: The MAC address of the last client that attempted to authenticate (left-most table), or the MAC address of the currently selected client (right-most table).</td> </tr> </tbody> </table>	Last Supplicant/Client Info				Name	IEEE Name		Description	Version	dot1xAuthLastEapolFrameVersion		Port-based: The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable.	Source	dot1xAuthLastEapolFrameSource		Port-based: The source MAC address carried in the most recently received EAPOL frame. MAC-based: Not applicable.	Identity or (Last) Client	-		Port-based: The user name (supplicant identity) carried in the most recently received Resp/ID EAPOL frame. MAC-based: The MAC address of the last client that attempted to authenticate (left-most table), or the MAC address of the currently selected client (right-most table).								
Last Supplicant/Client Info																													
Name	IEEE Name		Description																										
Version	dot1xAuthLastEapolFrameVersion		Port-based: The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable.																										
Source	dot1xAuthLastEapolFrameSource		Port-based: The source MAC address carried in the most recently received EAPOL frame. MAC-based: Not applicable.																										
Identity or (Last) Client	-		Port-based: The user name (supplicant identity) carried in the most recently received Resp/ID EAPOL frame. MAC-based: The MAC address of the last client that attempted to authenticate (left-most table), or the MAC address of the currently selected client (right-most table).																										
Clients attached to this port	<p>This table is only available for MAC-based ports</p> <p>Each row in the table represents a MAC-based client on the port, and there are three parameters for each client:</p>																												

Label	Description
	<p>MAC Address:</p> <p>Shows the MAC address of the client, which is also used as the password in the authentication process against the backend server. Clicking the link causes the client's backend server counters to be shown in the right-most backend server counters table above. If no clients are attached, it shows No clients attached.</p> <p>State:</p> <p>Shows whether the client is authorized or unauthorized. As long as the backend server hasn't successfully authenticated a client, it is unauthorized.</p> <p>Last Authentication:</p> <p>Show the date and time of the last authentication of the client. This gets updated for every re-authentication of the client.</p>

4.1.18 Client Configuration

Figure 65: Authentication Configuration

Authentication Configuration

Client Configuration

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

RADIUS Authentication Server Configuration

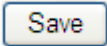
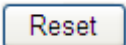
#	Enabled	IP Address	Port	Secret
1	<input type="checkbox"/>		1812	
2	<input type="checkbox"/>		1812	
3	<input type="checkbox"/>		1812	
4	<input type="checkbox"/>		1812	
5	<input type="checkbox"/>		1812	

RADIUS Accounting Server Configuration

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

Save Reset

Label	Description
Client	The 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 stack for</p>

	<p>authentication.</p> <p>Radius : use a remote RADIUS server for authentication.</p> <p>Tacacs+ : use a remote TACACS+ 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 something else than 'none or 'local'.</p>
	Click to save changes.
	Click to undo any changes made locally and revert to previously saved values.

4.1.19 RADIUS Authentication Server Configuration

Label	Description
#	The RADIUS Authentication Server number for which the configuration below applies.
Enable	Enable the RADIUS Authentication Server by checking this box.
IP Address	<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 something else than 'none' or 'local'.</p>

Figure 66: 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.
State	<p>The current state of the server. This field takes one of the following values:</p> <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 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>

Figure 67: 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.
State	<p>The current state of the server. This field takes one of the following values:</p> <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>

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 68: RADIUS Authentication Statistics

RADIUS Authentication Statistics for Server #1 (0.0.0.0:1812)

Server #1 Auto-refresh

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			
State			Disabled
Round-Trip Time			0 ms

Label	Description																																																
Packet Counters	<p>RADIUS authentication server packet counter. There are seven receive and four transmit counters.</p> <table border="1"> <thead> <tr> <th>Direction</th> <th>Name</th> <th>RFC4668 Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Rx</td> <td>Access Accepts</td> <td>radiusAuthClientExtAccessAccepts</td> <td>The number of RADIUS Access-Accept packets (valid or invalid) received from the server.</td> </tr> <tr> <td>Rx</td> <td>Access Rejects</td> <td>radiusAuthClientExtAccessRejects</td> <td>The number of RADIUS Access-Reject packets (valid or invalid) received from the server.</td> </tr> <tr> <td>Rx</td> <td>Access Challenges</td> <td>radiusAuthClientExtAccessChallenges</td> <td>The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.</td> </tr> <tr> <td>Rx</td> <td>Malformed Access Responses</td> <td>radiusAuthClientExtMalformedAccessResponses</td> <td>The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length, Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.</td> </tr> <tr> <td>Rx</td> <td>Bad Authenticators</td> <td>radiusAuthClientExtBadAuthenticators</td> <td>The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.</td> </tr> <tr> <td>Rx</td> <td>Unknown Types</td> <td>radiusAuthClientExtUnknownTypes</td> <td>The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.</td> </tr> <tr> <td>Rx</td> <td>Packets Dropped</td> <td>radiusAuthClientExtPacketsDropped</td> <td>The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.</td> </tr> <tr> <td>Tx</td> <td>Access Requests</td> <td>radiusAuthClientExtAccessRequests</td> <td>The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.</td> </tr> <tr> <td>Tx</td> <td>Access Retransmissions</td> <td>radiusAuthClientExtAccessRetransmissions</td> <td>The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.</td> </tr> <tr> <td>Tx</td> <td>Pending Requests</td> <td>radiusAuthClientExtPendingRequests</td> <td>The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.</td> </tr> <tr> <td>Tx</td> <td>Timeouts</td> <td>radiusAuthClientExtTimeouts</td> <td>The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.</td> </tr> </tbody> </table>	Direction	Name	RFC4668 Name	Description	Rx	Access Accepts	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.	Rx	Access Rejects	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.	Rx	Access Challenges	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.	Rx	Malformed Access Responses	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length, Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.	Rx	Bad Authenticators	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.	Rx	Unknown Types	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.	Rx	Packets Dropped	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.	Tx	Access Requests	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.	Tx	Access Retransmissions	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.	Tx	Pending Requests	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.	Tx	Timeouts	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
Direction	Name	RFC4668 Name	Description																																														
Rx	Access Accepts	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.																																														
Rx	Access Rejects	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.																																														
Rx	Access Challenges	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.																																														
Rx	Malformed Access Responses	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length, Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.																																														
Rx	Bad Authenticators	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.																																														
Rx	Unknown Types	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.																																														
Rx	Packets Dropped	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.																																														
Tx	Access Requests	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.																																														
Tx	Access Retransmissions	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.																																														
Tx	Pending Requests	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.																																														
Tx	Timeouts	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.																																														

Label	Description									
Other Info	<p>This section contains information about the state of the server and the latest round-trip time.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>RFC4668 Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>State</td> <td>-</td> <td>Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.</td> </tr> <tr> <td>Round-Trip Time</td> <td>radiusAuthClientExtRoundTripTime</td> <td>The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.</td> </tr> </tbody> </table>	Name	RFC4668 Name	Description	State	-	Shows the state of the server. It takes one of the following values: Disabled : The selected server is disabled. Not Ready : The server is enabled, but IP communication is not yet up and running. Ready : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left) : Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.	Round-Trip Time	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.
Name	RFC4668 Name	Description								
State	-	Shows the state of the server. It takes one of the following values: Disabled : The selected server is disabled. Not Ready : The server is enabled, but IP communication is not yet up and running. Ready : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left) : Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.								
Round-Trip Time	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.								

Figure 69: RADIUS Accounting Statistics

RADIUS Accounting Statistics for Server #1 (0.0.0.0:1813)

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			
State			Disabled
Round-Trip Time			0 ms

Label	Description
Packet Counters	RADIUS accounting server packet counter. There are five receive and four transmit counters.

	<table border="1"> <thead> <tr> <th>Direction</th> <th>Name</th> <th>RFC4670 Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Rx</td> <td>Responses</td> <td>radiusAccClientExtResponses</td> <td>The number of RADIUS packets (valid or invalid) received from the server.</td> </tr> <tr> <td>Rx</td> <td>Malformed Responses</td> <td>radiusAccClientExtMalformedResponses</td> <td>The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.</td> </tr> <tr> <td>Rx</td> <td>Bad Authenticators</td> <td>radiusAccClientExtBadAuthenticators</td> <td>The number of RADIUS packets containing invalid authenticators received from the server.</td> </tr> <tr> <td>Rx</td> <td>Unknown Types</td> <td>radiusAccClientExtUnknownTypes</td> <td>The number of RADIUS packets of unknown types that were received from the server on the accounting port.</td> </tr> <tr> <td>Rx</td> <td>Packets Dropped</td> <td>radiusAccClientExtPacketsDropped</td> <td>The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.</td> </tr> <tr> <td>Tx</td> <td>Requests</td> <td>radiusAccClientExtRequests</td> <td>The number of RADIUS packets sent to the server. This does not include retransmissions.</td> </tr> <tr> <td>Tx</td> <td>Retransmissions</td> <td>radiusAccClientExtRetransmissions</td> <td>The number of RADIUS packets retransmitted to the RADIUS accounting server.</td> </tr> <tr> <td>Tx</td> <td>Pending Requests</td> <td>radiusAccClientExtPendingRequests</td> <td>The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.</td> </tr> <tr> <td>Tx</td> <td>Timeouts</td> <td>radiusAccClientExtTimeouts</td> <td>The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.</td> </tr> </tbody> </table>	Direction	Name	RFC4670 Name	Description	Rx	Responses	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.	Rx	Malformed Responses	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.	Rx	Bad Authenticators	radiusAccClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.	Rx	Unknown Types	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.	Rx	Packets Dropped	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.	Tx	Requests	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.	Tx	Retransmissions	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.	Tx	Pending Requests	radiusAccClientExtPendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.	Tx	Timeouts	radiusAccClientExtTimeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
Direction	Name	RFC4670 Name	Description																																						
Rx	Responses	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.																																						
Rx	Malformed Responses	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.																																						
Rx	Bad Authenticators	radiusAccClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.																																						
Rx	Unknown Types	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.																																						
Rx	Packets Dropped	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.																																						
Tx	Requests	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.																																						
Tx	Retransmissions	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.																																						
Tx	Pending Requests	radiusAccClientExtPendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.																																						
Tx	Timeouts	radiusAccClientExtTimeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.																																						
<p>Other Info</p>	<p>This section contains information about the state of the server and the latest</p> <table border="1"> <thead> <tr> <th>Name</th> <th>RFC4670 Name</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>State</td> <td>-</td> <td>Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.</td> </tr> <tr> <td>Round-Trip Time</td> <td>radiusAccClientExtRoundTripTime</td> <td>The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.</td> </tr> </tbody> </table>	Name	RFC4670 Name	Description	State	-	Shows the state of the server. It takes one of the following values: Disabled : The selected server is disabled. Not Ready : The server is enabled, but IP communication is not yet up and running. Ready : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left) : Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.	Round-Trip Time	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.																															
Name	RFC4670 Name	Description																																							
State	-	Shows the state of the server. It takes one of the following values: Disabled : The selected server is disabled. Not Ready : The server is enabled, but IP communication is not yet up and running. Ready : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left) : Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.																																							
Round-Trip Time	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.																																							

4.1.20 Warning

4.1.20.1 System Warning

4.1.20.1.1 SYSLOG Setting

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

Figure 70: Syslog Server

Syslog Server

IP Address	0.0.0.0
<input type="button" value="Save"/>	<input type="button" value="Reset"/>

Label	Description
SYSLOG Server IP Address	The remote SYSLOG Server IP address.

4.1.20.1.2 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 71: 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
21	Disabled	22	Disabled
23	Disabled	24	Disabled

Save Reset

Label	Description
System Event	
System Start	Alert when system restart
Power Status	Alert when a power up or down
SNMP Authentication Failure	Alert when SNMP authentication failure.
Redundant Ring Topology Change	Alert when Redundant Ring topology changes.
Port Event SYSLOG / SMTP event	Disable Link Up Link Down Link Up & Link Down

4.1.21 Monitor and Diag

4.1.21.1 MAC Table

4.1.21.1.1 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 72: MAC Address Table

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	<input type="checkbox"/>
Age 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	21	22	23	24
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"/>	<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"/>	<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"/>	<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	21	22	23	24

Add new static entry

Save Reset

4.1.21.1.2 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**.

4.1.21.1.3 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 73: 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	21	22	23	24
Auto	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

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.

4.1.21.1.4 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 74: Static MAC Table

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	21	22	23	24
Delete	<input type="text" value="1"/>	<input type="text" value="00-00-00-00-00-00"/>	<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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete	<input type="text" value="2"/>	<input type="text" value="00-00-00-00-00-00"/>	<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"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Add new static entry"/>																										
<input type="button" value="Save"/>			<input type="button" value="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".

4.1.21.1.5 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.

4.1.21.2 Port Statistic

4.1.21.2.1 Traffic Overview

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

Figure 76: Port Statistics Overview

Port Statistics Overview

Auto-refresh Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive	Transmit	Receive
1	0	17	0	1982	0	0	0	0	0
2	0	81	0	8021	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	178129	239793	25937786	294189111	1	0	0	0	1
9	0	0	0	0	0	0	0	0	0
10	0	34319	0	3614995	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	207136	170269	287964364	14775980	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	1332	35789	426610	3780392	0	0	0	0	0
15	81854	92792	11408309	26673364	6	0	0	0	14
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
21	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0
24	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.
<input type="button" value="Refresh"/>	Updates the counters entries, starting from the current entry ID.
<input type="button" value="Clear"/>	Flushes all counters entries.

4.1.21.2.2 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 77: Detailed Port Statistics Port 1

Detailed Port Statistics Port 1

Port 1

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	17
Rx Octets	0	Tx Octets	1982
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	12
Rx Broadcast	0	Tx Broadcast	5
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	2
Rx 65-127 Bytes	0	Tx 65-127 Bytes	9
Rx 128-255 Bytes	0	Tx 128-255 Bytes	6
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Low	0	Tx Low	14
Rx Normal	0	Tx Normal	0
Rx Medium	0	Tx Medium	0
Rx High	0	Tx High	3
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	0		

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.
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/Alignmen t	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

Label	Description
	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.

4.1.21.3 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 78: Mirror Configuration

Mirror Configuration

Port to mirror to

Port	Mode
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 ▾
21	Disabled ▾
22	Disabled ▾
23	Disabled ▾
24	Disabled ▾

Label	Description
Port to mirror to	The mirror port which the port Frames are mirrored to
Port	The port which will be mirrored
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> <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>

4.1.21.4 System Log Information

The switch system log information is provided here.

Figure 79: System Log Information

System Log Information


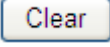




Auto-refresh Refresh Clear |<< << >> >>| Open in new window
Level All ▾

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

Start from ID with entries per page.

ID	Level	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: Info: Information level of the system log. Warning: Warning level of the system log. Error: Error level of the system log. All: All levels.
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

Label	Description
	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.

4.1.21.5 Cable Diagnostics

This page is used for running the VeriPHY Cable Diagnostics.

Figure 80: VeriPHY Cable Diagnostics

VeriPHY Cable Diagnostics

Open in new window

Port All ▾

Start

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
1	--	--	--	--	--	--	--	--
2	--	--	--	--	--	--	--	--
3	--	--	--	--	--	--	--	--
4	--	--	--	--	--	--	--	--
5	--	--	--	--	--	--	--	--
6	--	--	--	--	--	--	--	--
7	--	--	--	--	--	--	--	--
8	--	--	--	--	--	--	--	--
9	--	--	--	--	--	--	--	--
10	--	--	--	--	--	--	--	--
11	--	--	--	--	--	--	--	--
12	--	--	--	--	--	--	--	--
13	--	--	--	--	--	--	--	--
14	--	--	--	--	--	--	--	--
15	--	--	--	--	--	--	--	--
16	--	--	--	--	--	--	--	--
17	--	--	--	--	--	--	--	--
18	--	--	--	--	--	--	--	--
19	--	--	--	--	--	--	--	--
20	--	--	--	--	--	--	--	--
21	--	--	--	--	--	--	--	--
22	--	--	--	--	--	--	--	--
23	--	--	--	--	--	--	--	--
24	--	--	--	--	--	--	--	--

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.

4.1.21.6 Ping

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

Figure 81: ICMP Ping

ICMP Ping

IP Address	0.0.0.0
Ping Size	64

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.

4.1.22 Factory Defaults

You can reset the configuration of the stack switch on this page.

Figure 82: Factory Defaults

Factory Defaults



- Keep IP
- Keep User/Password

Label	Description
Keep IP	Reset the configuration to Factory Defaults except IP address
Keep User/Password	Reset the configuration to Factory Defaults except User and Password
<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

Section 5: Command Line Interface Management

5.1 About CLI Management

Besides WEB-base management, SLM168 also support CLI management. You can use Serial Console or SSH to management switch by CLI.

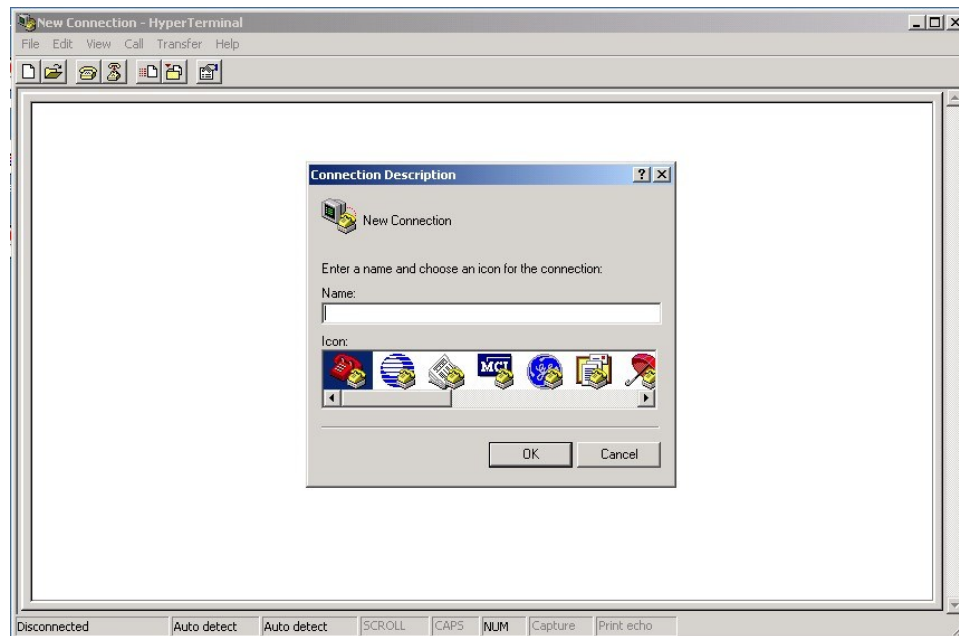
CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

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

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

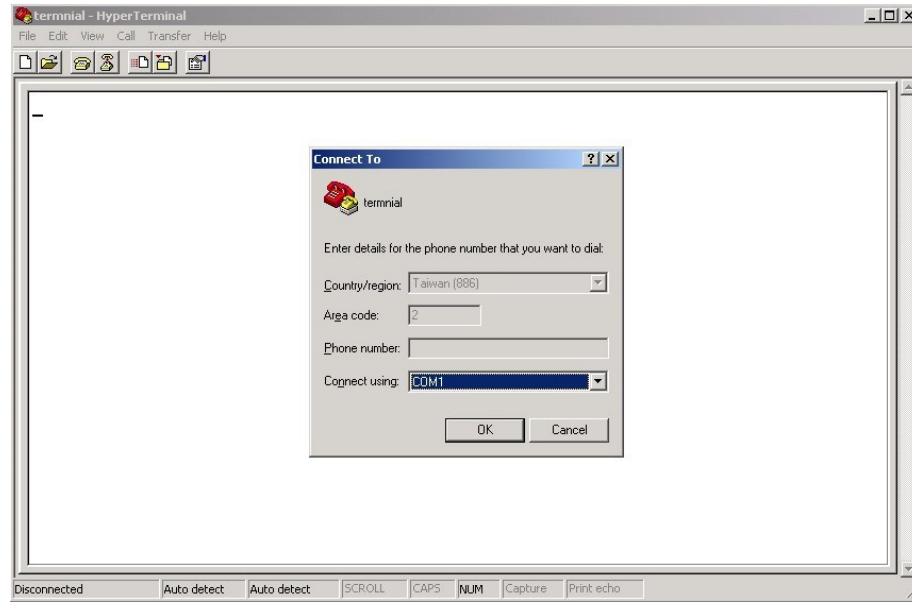
1. From the Windows desktop, click on Start -> Programs -> Accessories -> Communications -> Hyper Terminal
2. Input a name for new connection

Figure 83: Input Name



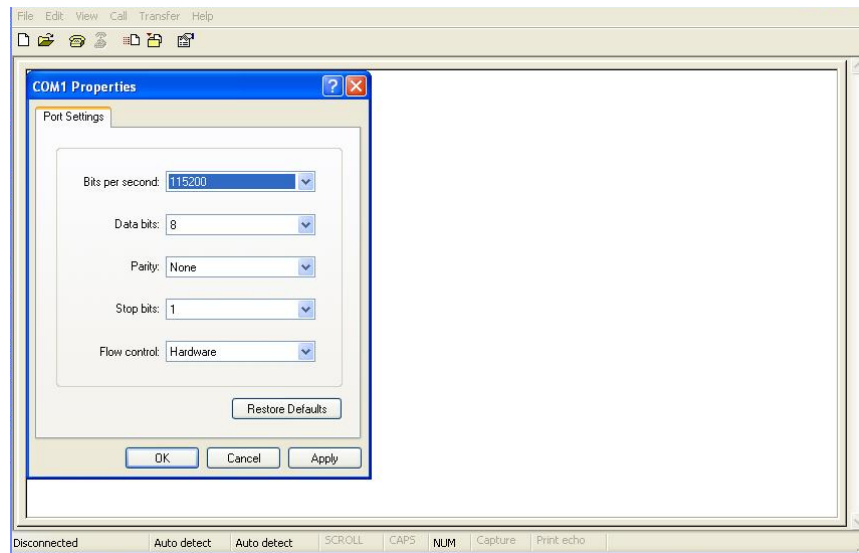
3. Select to use COM port number

Figure 84: COM1 Port



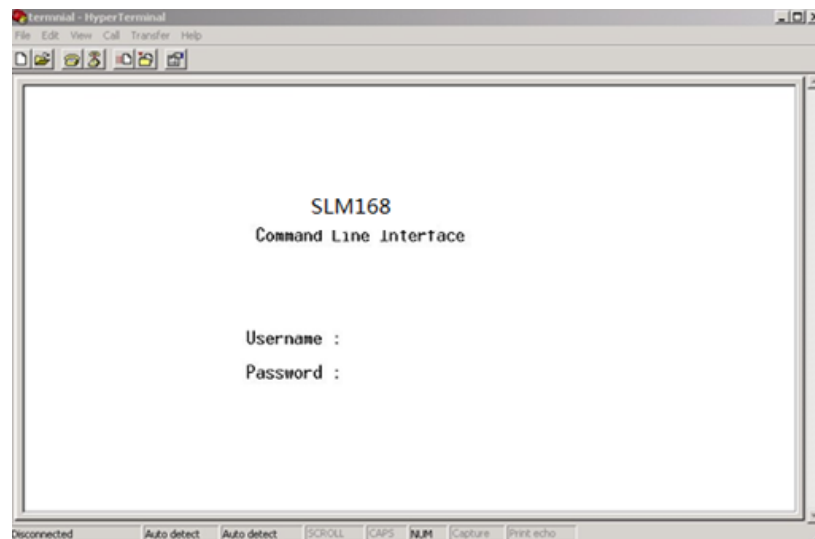
4. The COM port properties setting, 115200 for Bits per second, 8 for Data bits, None for Parity, 1 for Stop bits and none for Flow control.

Figure 85: COM port Properties



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

Figure 86: SLM168



CLI Management by SSH

Users can use “SSH” to configure the switches.

The default value is as below:

IP Address: 192.168.0.100

Subnet Mask: **255.2e55.255.0**

IP Router: **0.0.0.0**

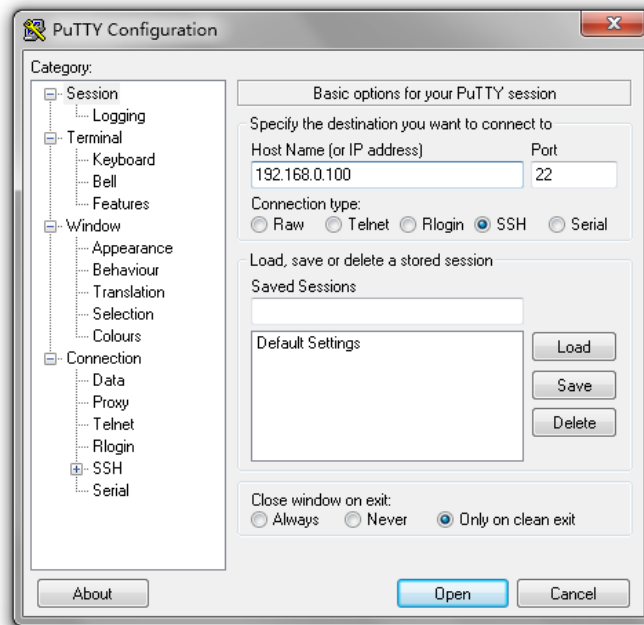
User Name: **admin**

Password: **admin**

Follow the steps below to access the console via SSH. You can Use “Putty” or other SSH Tool to connect switch. We will use the “PuTTY “ to introduce the SSH connection as below.

1. Input the switch IP address and Port, then click “Open” button.

Figure 87: PuTTY Configuration



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

5.1.1 Command Groups

Figure 88: Command Groups

```
Command Groups :
-----
System      : System settings and reset options
Syslog      : Syslog Server Configuration
IP          : IP configuration and Ping
Auth        : Authentication
Port        : Port management
Aggr        : Link Aggregation
LACP        : Link Aggregation Control Protocol
STP         : Spanning Tree Protocol
Dot1x       : IEEE 802.1X port authentication
IGMP        : Internet Group Management Protocol snooping
LLDP        : Link Layer Discovery Protocol
MAC         : MAC address table
ULAN        : Virtual LAN
PULAN       : Private ULAN
QoS         : Quality of Service
ACL         : Access Control List
Mirror      : Port mirroring
Config      : Load/Save of configuration via TFTP
SNMP        : Simple Network Management Protocol
Firmware    : Download of firmware via TFTP
Fault       : Fault Alarm 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]

Syslog

Syslog>	ServerConfiguration [<ip_addr>]
---------	---------------------------------

IP

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

	SNTP [<ip_addr_string>]
--	-------------------------

Auth

Auth>	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>]
	Client [console telnet ssh web] [none local radius] [enable disable]
	Statistics [<server_index>]

Port

Port>	Configuration [<port_list>]
	State [<port_list>] [enable disable]
	Mode [<port_list>] [10hdx 10fdx 100hdx 100fdx 1000fdx auto]
	Flow Control [<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>]
	VeriPHY [<port_list>]

Aggr

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

LACP

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

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>]

Dot1x

Dot1x>	Configuration [<port_list>]
	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

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

	Groups [<vid>]
	Status [<vid>]

LLDP

LLDP>	Configuration [<port_list>]
	Mode [<port_list>] [enable disable rx tx]
	Optional_TLV [<port_list>][port_descr sys_name sys_descr sys_capa mgmt_addr] [enable disable]
	Interval [<interval>]
	Hold [<hold>]
	Delay [<delay>]
	Reinit [<reinit>]
	Info [<port_list>]
	Statistics [<port_list>] [clear]

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

	Configuration [<port_list>]
	Aware [<port_list>] [enable disable]
	PVID [<port_list>] [<vid> none]
VLAN>	FrameType [<port_list>] [all tagged]
	Add <vid> [<port_list>]
	Delete <vid>
	Lookup [<vid>]

PVLAN

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

QoS

QoS>	Configuration [<port_list>]
	Classes [<class>]
	Default [<port_list>] [<class>]
	Tagprio [<port_list>] [<tag_prio>]
	QCL Port [<port_list>] [<qcl_id>]
	QCL Add [<qcl_id>] [<qce_id>] [<qce_id_next>] (etype <etype>) (vid <vid>) (port <udp_tcp_port>) (dscp <dscp>) (tos <tos_list>) (tag_prio <tag_prio_list>) <class>
	QCL Delete <qcl_id> <qce_id>
	QCL Lookup [<qcl_id>] [<qce_id>]
	Mode [<port_list>] [strict weighted]
	Weight [<port_list>] [<class>] [<weight>]
	Rate Limiter [<port_list>] [enable disable] [<bit_rate>]
	Shaper [<port_list>] [enable disable] [<bit_rate>]
	Storm Unicast [enable disable] [<packet_rate>]

	Storm Multicast [enable disable] [<packet_rate>]
	Storm Broadcast [enable disable] [<packet_rate>]

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]

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>
-----------	-----------------------------------

Fault

Fault>	Alarm PortLinkDown [<port_list>] [enable disable]
	Alarm PowerFailure [pwr] [enable disable]

Section 6: Technical Specifications

Switch Model	SLM168
Physical Ports	
Gigabit Combo port with 10/100/1000Base-T(X) and 100/1000Base-X SFP ports	16
100/1000Base-X with SFP port	8
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 802.1D for STP (Spanning Tree Protocol)</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	4
Processing	Store-and-Forward
Switch Properties	<p>Switching latency: 7 us</p> <p>Switching bandwidth: 48Gbps</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 9K Bytes
Security Features	<p>IP Police 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>
Software Features	<p>STP/RSTP/MSTP (IEEE 802.1D/w/s)</p> <p>Redundant Ring (Redundant Ring) with recovery time less than 20ms 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>IP-based bandwidth management</p> <p>Application-based QoS management</p> <p>DOS/DDOS auto prevention</p> <p>Port configuration, status, statistics, monitoring, security</p> <p>DHCP Client/Server</p>
Network Redundancy	<p>Redundant Ring</p> <p>STP</p> <p>RSTP</p> <p>MSTP</p>
RS-232 Serial Console Port	RS-232 in DB9 connector with console cable. 115200bps, 8, N, 1
LED indicators	
Power Indicator (PWR)	Green : Power indicator for AC
System Ready Indicator (STA)	Green : Indicates that the system ready. The LED is blinking when the system is upgrading firmware
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.
System Running Indicator (RUN)	Green : System is operating continuously
Supervisor Login Indicator (RMT)	Green : System is accessed remotely
Reset To Default Running Indicator (DEF)	Green : System resets to default configuration
Ping Command To The Switch Indicator (Ping)	Green : System is processing "PING" request
10/100/1000Base-T(X) RJ45 Port Indicator	Green for 1000Mbps Link/Act indicator Amber for 10/100Mbps Link/Act indicator
100/1000Base-X SFP Port Indicator	Green for port Link/Act.
Power	
Input power	100~240VAC with power cord
Power consumption (Typ.)	33 Watts
Overload current protection	Present
Physical Characteristic	
Enclosure	19 inches rack mountable
Dimension (W x D x H)	431 (W) x 342 (D) x 44 (H) mm

Weight (g)	4350g
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.

