3onedata

IES6306 Series
Industrial Ethernet Switch
User Manual

Document Version: 01

Issue Date: 11/22/2021

3onedata

Please scan our QR code for more details

3onedata
Make network communication more reliable

BlueEyes pro

Embedded Industrial Ethernet Switch Modules

Embedded Serial Device Server Modules

Industry-specialized Products
(Rail Transit, Power, Smart City, Pipe Gallery…)

Honor · Quality · Service

Layer 2 (Unmanaged) Managed Industrial Ethernet Switch

Layer 3 Managed Industrial Ethernet Switch

Industrial PoE Switch

BlueEyes Pro Management Software

VSP Virtual Serial Port Management Software

SNMP Management Software

Modbus Gateway

Serial Device Server

Media Converter

CAN Device Server

Interface Converter

Industrial Wireless Products

3onedata Co., Ltd.

Headquarter address:	3/B, Zone 1, Baiwangxin High Technology Industrial park, Nanshan District, Shenzhen, 518108 China
Technology support:	tech-support@3onedata.com
Service hotline:	+86-400-880-4496
E-mail:	sales@3onedata.com
Fax:	+86-0755-26703485
Website:	http://www.3onedata.com

Preface

The software user manual describes the industrial Ethernet switch:

- Product features
- Product network management configuration

Note

The screenshot reference model of this manual is 4 Gigabit PoE Ports + 2 2.5G SFP + 2 48VDC Power Inputs. Other series models have the same interface function and operation except for the following differences.

- Differences in Ethernet interfaces and types and quantities of power supplies.

Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers
- Hardware engineers

Conventions

Format	Description
" "	Words with "" represent the interface words. Fox example "Port number".
>	Multiple paths are separated by the symbol '>'. Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	It represents the words clicked to achieve hyperlink. Font color as: "Light blue".
About this chapter	The section 'about this chapter' provide links to various sections of this chapter, as well as links to the Principles Operations Section of this chapter.

Symbols

Format	Description
⚠ Notice	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
⚠ Warning	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
📄 Note	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.
🔑 Key	The tips of configuration and operation.
💡 Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

Revision Record

Version No.	Date	Revision note
01	2021-11-22	Product release

Contents

1 Log in the Web Interface

1.1 WEB Browsing System Requirement

While using managed industrial Ethernet switches, the system should meet the following conditions.

Hardware and software	System requirements
Resolution	1024x768 or above
Color	256 color or above
Browser	Internet Explorer 6.0 or above
Operating system	• Windows XP • Windows 7

1.2 Setting IP Address of PC

The switch default management as follows:

IP Settings	Default Value
IP Address	192.168.1.254
Subnet mask	255.255.255.0

When configuring a switch through the Web:

- Before making remote configuration, make sure that the route between the computer and the switch is reachable.
- Before local configuration, please make sure the IP address of the computer is on the same subnet to the one of switch.

Note:
When the switch is first configured. If it is configured locally, make sure the current computer network segment is 1.

Eg: Assume that the IP address of the current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

Operation Steps

Amendment steps as follow:

Step 1 Open "Control panel > Network connection > Local area connection > Properties > Internet protocol version (TCP/IPv4) Properties".

Step 2 Change the "5" selected by the red frame in the figure to "1".
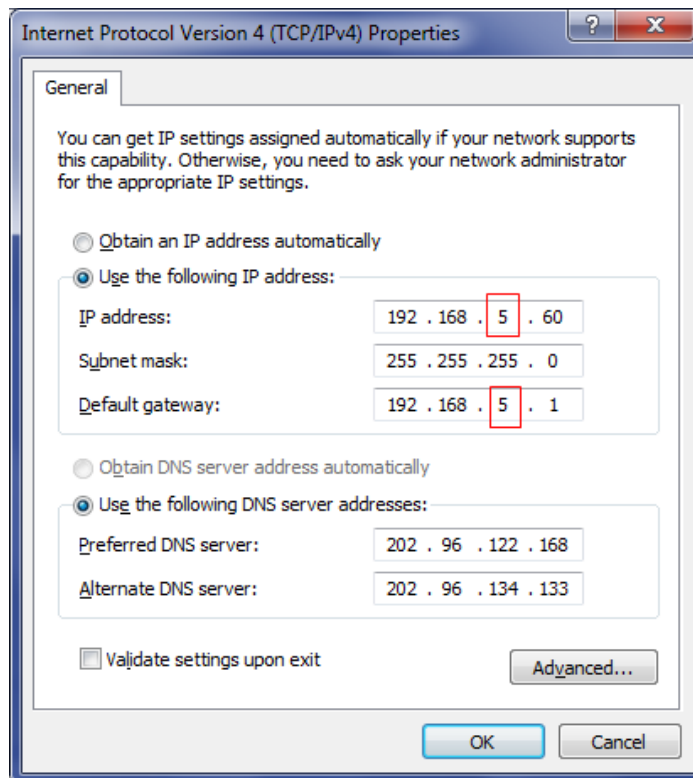
Step 3 Click "OK"

Step 4 End.

⚠️Notice

In windows system, if user adopts the advanced configuration function of IP address and accesses the switch device via setting IP dummy address, the following two managed functions can't be achieved: IGMP polling and IEEE 802.1x polling.

1.3   Log in the Web Configuration Interface

Operation Steps
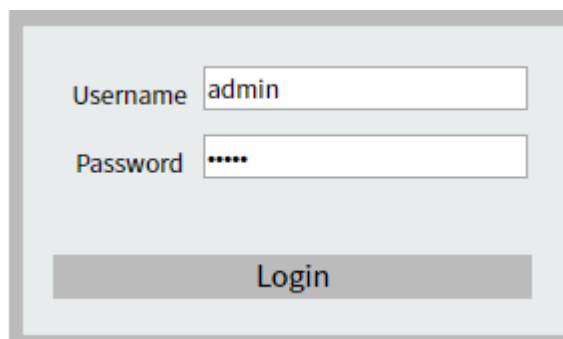
The initial password of the default user must be changed when logging in to the device for the first time. Login in the web configuration interface as follow:

Step 1 Run the computer browser.

Step 2 Enter the address of the switch "http://192.168.1.254" in the address bar of the browser.

Step 3 Click the Enter key.

Step 4 Pop-up dialog box as shown below, enter the user name and password in the login window.

Username	admin
Password	•••••

Login

Note:
- This switch supports one default user. This user has administrator privilege and can configure devices via WEB, TELNET, SSH, CLI, etc.
- The default username and password are "admin"; please strictly distinguish capital and small letter while entering.
- If you log in to the device for the first time, you will be prompted to change the default user's initial password. If the password has been modified through the WEB or CLI, the subsequent steps can be ignored and the modified password can be used to log in to the device directly.
- If the number of incorrect login information input reaches 5 times, the system will automatically lock the user for 5 minutes.

Step 5 Click "Login".

Step 6 Pop up a window as the figure below, enter the user name and new password on the login window.

Note:

- The device could be logged in for the first time by default username and initial password; After logging in, the system will prompt you to modify the default user's initial password, and you can log in normally after modification.
- The length of the new password string must be greater than or equal to 8 and be composed of two or more of uppercase letters, lowercase letters, numbers and special characters.
- After changing the password, save the current configuration on the "System Configuration > Save startup-config" page to take effect.

Step 7 Click "OK".

Step 8 Pop up a window as the figure below, enter the user name and password on the login window.

Step 9 Click the "login" button.

Step 10 End.

After login in successfully, user can configure relative parameters and information according to demands.

Note:

After logging in to the device, you can modify the IP address of the switch for ease of use.

2 System

2.1 System Information

2.1.1 System Information Configuration

The switch system information is provided here.

System Information >	System Information Configuration	System Information Monitoring	CPU Load

System Contact	
System Name	dut5
System Location	

Save   Reset

System Contact

The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

System Name

An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (09), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.

System Location

The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

2.1.2　System Information Monitor

The switch system information is provided here.

System Information >	System Information Configuration	System Information Monitoring	Sys Load	Auto-refresh ☐	Refresh

System	
Contact	
Name	
Location	
Hardware	
MAC Address	00-02-6f-01-02-03
Time	
System Date	1970-01-01T01:51:05+00:00 Synchronize PC time
System Uptime	0d 01:51:05
Software	
Software Version	5.2.2.B2021072100R1239D20000
Software Date	Jul 21 2021 09:05:33 by Jaguar

Contact

System contact configured by the path "System > System Information Configuration > System Administrator".

Name

System name configured by the path "System > System Information Configuration > Information > System Name".

Position

The location configured in "System > System Information Configuration > Information > System Location".

MAC Address

The MAC Address of this switch.

System Date

The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.

System Uptime

The period of time the device has been operational.

Software Version

The software version of this switch.

Software Date

The date when the switch software was produced.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

2.1.3 CPU Load

This page displays the CPU load, using an SVG graph.
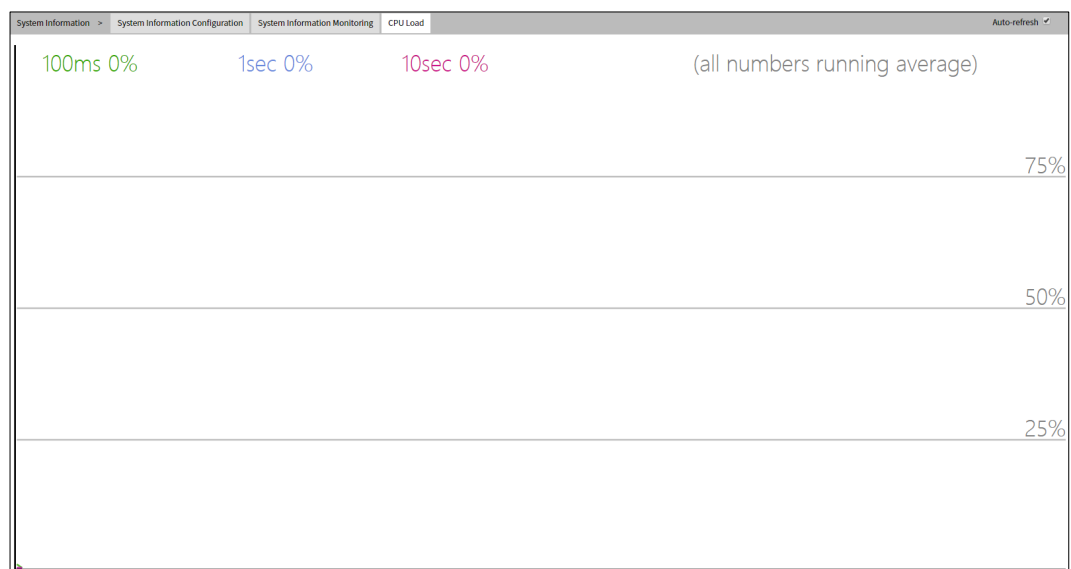
The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well. In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

2.2 IP

2.2.1 IP Configuration

Configure IP basic settings, control IP interfaces and IP routes.

The maximum number of interfaces supported is 8 and the maximum number of routes is 32.

Mode

Configure whether the IP stack should act as a Host or a Router. In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces.

IP Interfaces

Delete

Select this option to delete an existing IP interface.

VLAN

The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.

IPv4 DHCP Enabled

Enable the DHCPv4 client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol.

The DHCPv4 client will announce the configured System Name as hostname to provide DNS lookup.

IPv4 DHCP Fallback Timeout

The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fallback mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.

IPv4 DHCP Current Lease

For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.

IPv4 Address

The IPv4 address of the interface in dotted decimal notation.

If DHCP is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

IPv4 Mask Length

The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address.

If DHCP is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

DHCPv6 Enable

Enable the DHCPv6 client by checking this box. If this option is enabled, the system will configure the IPv6 address of the interface using the DHCPv6 protocol.

DHCPv6 Rapid Commit

Enable the DHCPv6 Rapid-Commit option by checking this box. If this option is enabled, the DHCPv6 client terminates the waiting process as soon as a Reply message with a Rapid Commit option is received.

This option is only manageable when DHCPv6 client is enabled.

DHCPv6 Current Lease

For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.

IPv6 Address

The IPv6 address of the interface. A IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80:: 215: c5ff: fe03:4dc7. The symbol is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once.

System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address.

The field may be left blank if IPv6 operation on the interface is not desired.

IPv6 Mask

The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for a IPv6 address.

The field may be left blank if IPv6 operation on the interface is not desired.

Resolving IPv6 DAD

The link-local address is formed from an interface identifier based on the hardware address which is supposed to be uniquely assigned. Once the DAD (Duplicate Address Detection) detects the address duplication, the operation on the interface SHOULD be disabled.

At this moment, manual intervention is required to resolve the address duplication. For example, check whether the loop occurs in the VLAN or there is indeed other device occupying the same hardware address as the device in the VLAN.

After making sure the specific link-local address is unique on the IPv6 link in use, delete and then add the specific IPv6 interface to restart the IPv6 operations on this interface.

IP Routes

Delete

Select this option to delete an existing IP route.

Internet

The destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0or IPv6:: notation.

Mask Length

The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid

values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).

Gateway

The IP address of the IP gateway. Valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.

Next Hop VLAN (Only for IPv6)

The VLAN ID (VID) of the specific IPv6 interface associated with the gateway.

The given VID ranges from 1 to 4095 and will be effective only when the corresponding IPv6 interface is valid.

If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway.

If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.

Buttons

Add new IP interface: click here to add new IP interface. A maximum of 8 interfaces is supported.

Add new IP route: click to add new IP route. A maximum of 32 routes is supported.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

2.2.2 IP Status Monitoring

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbour cache (ARP cache) status.

IP Interfaces

Interface

The name of the interface.

Type

The address type of the entry. This may be LINK or IPv4.

Address

The current address of the interface (of the given type).

Status

The status flags of the interface (and/or address).

IP Routes

Network

The destination IP network or host address of this route.

Gateway

The gateway address of this route.

Status

The status flags of the route.

Neighbour cache

IP Address

The IP address of the entry.

Link Address

The Link (MAC) address for which a binding to the IP address given exist.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

2.3   NTP Configuration

2.3.1   NTP Client Configuration

Configure NTP on this page.

Mode

Indicates the NTP mode operation. Possible modes are:

- Enabled: Enable NTP client mode operation.
- Disabled: Disable NTP client mode operation.

Server

Provide the IPv4 or IPv6 address of a NTP server. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating

each field (:). For example, fe80:: 215: c5ff: fe03:4dc7. The symbol is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'. In addition, it can also accept a domain name address.

NTP >	NTP Client Configuration	NTP Server Configuration
Mode	Disabled ▼	
Save	Reset	

2.3.2　NTP Server Configuration

Configure NTP server on this page.

NTP >	NTP Client Configuration	NTP Server Configuration
Mode	Disabled ▼	
Save	Reset	

Mode

Configure the NTP server mode, options are as follows:

- Enable: Enable NTP Server.
- Disable: Disable NTP Server.

2.4　Time Zone Configuration

Time Zone Configuration		
Time Zone Configuration		
Time Zone	None ▼	
Acronym		(2 - 16 characters)
Save	Reset	

• Time Zone
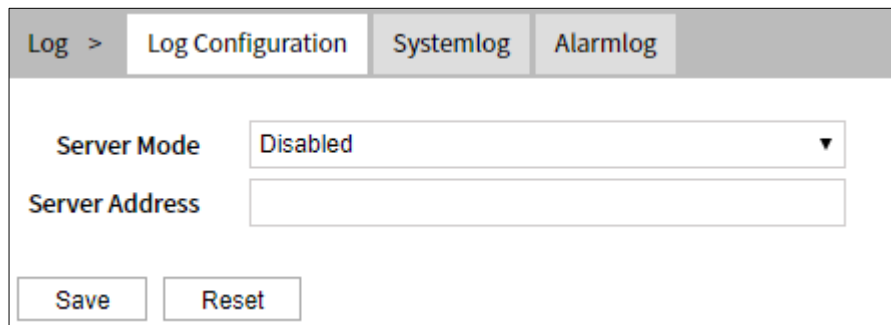
> Lists the various Time Zones worldwide. Select appropriate Time Zone from the drop down and click Save to set.

• Acronym

> User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range: Up to 16 characters).

2.5   System Log

2.5.1   Log Configuration

• Server Mode

> Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to the syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are:

- Enabled: Enable server mode operation.
- Disabled: Disable server mode operation.

2.5.2   System Information

> The switch system log information is provided here.

Log >	Log Configuration	Systemlog	Alarmlog		Auto-refresh ☐	Refresh	Clear	|<<	<<	>>	>>|

	Level	All	▼
	Clear Level	All	▼

The total number of entries is 6 for the given level.

Start from ID 1 with 20 entries per page.

ID	Level	Time	Message
1	Informational	1970-01-01T00:00:00	IES6306
2	Informational	1970-01-01T00:00:02	SYS-BOOTING: Switch just made a cold boot.
3	Informational	1970-01-01T00:00:02	Restart Mode: cold.
4	Notice	1970-01-01T00:00:02	LINK-UPDOWN: Interface Vlan 1, changed state to down.
5	Notice	1970-01-01T00:00:04	LINK-UPDOWN: Interface 1/4, changed state to up.
6	Notice	1970-01-01T00:00:04	LINK-UPDOWN: Interface Vlan 1, changed state to up.

• **Syslog Level**

Indicates what kind of message will send to syslog server. Possible modes are:

- Error: Send the specific messages which severity code is less or equal than Error.
- Warning: Send the specific messages which severity code is less or equal than Warning.
- Notice: Send the specific messages which severity code is less or equal than Notice.
- Informational: Send the specific messages which severity code is less or equal than Informational.

Navigating the System Log Information Table

Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table.

The "Level" input field is used to filter the display system log entries.

The "Clear Level" input field is used to specify which system log entries will be cleared. To clear specific system log entries, select the clear level first then click the button "Delete" .

The "Start from ID" input field allow the user to change the starting point in this table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next entry match.

In addition, these input fields will upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

The   >>   will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<<   button to start over.

System Log Information Entry Columns

ID

The identification of the system log entry.

Level

The level of the system log entry. Info: The system log entry is belonged information level.

- Warning: The system log entry is belonged warning level.
- Error: The system log entry is belonged error level.

Time

The occurred time of the system log entry.

Message

The detailed message of the system log entry.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Updates the table entries, starting from the current entry.

Delete: Refresh the selected entries.

|<< : Updates the table entries, starting from the first available entry.

<< : Updates the table entries, ending at the last entry currently displayed.

>> : Updates the table entries, starting from the last entry currently displayed.

>>| : Updates the table entries, ending at the last available entry.

2.5.3　Alert Log

The switch system detailed log information is provided here.

| Log > | Log Configuration | Systemlog | Alarmlog | Auto-refresh ☐ | Refresh | |<< | << | >> | >>| |

The total number of entries is 3969 for the given level.

Start from ID 1 with 20 entries per page.

ID	Category	Level	Time	Product name	Message
1	Application	Warning	1970-01-01T15:42:41	IES6306	Interface GE 1/5, changed state to down.
2	Application	Warning	1970-01-01T15:42:43	IES6306	Interface GE 1/5, changed state to up.
3	Application	Warning	1970-01-01T15:42:47	IES6306	Interface GE 1/5, changed state to down.
4	Application	Warning	1970-01-01T15:42:50	IES6306	Interface GE 1/5, changed state to up.
5	Application	Warning	1970-01-01T15:42:51	IES6306	Interface GE 1/5, changed state to down.
6	Application	Warning	1970-01-01T15:42:52	IES6306	Interface GE 1/5, changed state to up.
7	Application	Warning	1970-01-01T15:42:53	IES6306	Interface GE 1/5, changed state to down.
8	Application	Warning	1970-01-01T15:42:56	IES6306	Interface GE 1/5, changed state to up.
9	Application	Warning	1970-01-01T15:42:57	IES6306	Interface GE 1/5, changed state to down.
10	Application	Warning	1970-01-01T15:43:00	IES6306	Interface GE 1/5, changed state to up.
11	Application	Warning	1970-01-01T15:43:03	IES6306	Interface GE 1/5, changed state to down.
12	Application	Warning	1970-01-01T15:43:04	IES6306	Interface GE 1/5, changed state to up.
13	Application	Warning	1970-01-01T15:43:05	IES6306	Interface GE 1/5, changed state to down.
14	Application	Warning	1970-01-01T15:43:06	IES6306	Interface GE 1/5, changed state to up.
15	Application	Warning	1970-01-01T15:43:07	IES6306	Interface GE 1/5, changed state to down.
16	Application	Warning	1970-01-01T15:43:11	IES6306	Interface GE 1/5, changed state to up.
17	Application	Warning	1970-01-01T15:43:14	IES6306	Interface GE 1/5, changed state to down.
18	Application	Warning	1970-01-01T15:43:16	IES6306	Interface GE 1/5, changed state to up.
19	Application	Warning	1970-01-01T15:43:18	IES6306	Interface GE 1/5, changed state to down.
20	Application	Warning	1970-01-01T15:43:23	IES6306	Interface GE 1/5, changed state to up.

Level

The severity level of the system log entry.

ID

The ID (>= 1) of the system log entry.

Message

The detailed message of the system log entry.

3 Port

3.1 Port

3.1.1 Port Settings

This feature displays current port configurations. Ports can also be configured using this feature.

Port

This is the logical port number for this row.

Description

The description of the port. It is an ASCII string no longer than 256 characters.

Link Status

The current link state is displayed graphically. Green indicates the link is up and red that it is down.

Current Link Speed

Current speed duplexes the current link speed of this port.

Configured Link Speed

Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are:

- Disable: Disable the switch port.
- Auto: Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner.
- 10Mbps HDX: Forces the cu port in 10 Mbps half duplex mode.

- 10Mbps FDX: Forces the cu port in 10 Mbps full duplex mode.

- 100Mbps HDX: Forces the cu port in 100 Mbps half duplex mode.

- 100Mbps FDX: Forces the cu port in 100 Mbps full duplex mode.

- 1Gbps FDX: Forces the port in 1 Gbps full duplex.

- 2.5Gbps FDX: The forced copper port is 2.5Gbps full duplex mode.

- SFP_Auto_AMS: Automatically determines the speed of the SFP. There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFPs might not be detectable. The port is set in AMS mode. Cu port is set in Auto mode.

- 100-FX: SFP port rate 100-FX. Cu port is disabled.

- 1000-X: SFP port rate 1000-FX. Cu port is disabled. Ports in AMS mode with 1000-X speed has Cu port preferred. Ports in AMS mode with 1000-X speed has fiber port preferred. Ports in AMS mode with 100-FX speed has fiber port preferred.

Advertise Duplex

When duplex is set as auto that is, Autonegotiation, the port will only advertise the specified duplex as either Fdx or Hdx to the link partner. By default, port will advertise all the supported duplexes if the Duplex is Auto.

Advertise Speed

When Speed is set as auto that is, Autonegotiation, the port will only advertise the specified speeds (10M 100M 1G) to the link partner. By default, port will advertise all the supported speeds if speed is set as Auto.

Flow Control

When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation.

PFC

When PFC (802.1Qbb Priority Flow Control) is enabled on a port then flow control on a priority level is enabled. Through the Priority field, range (one or more) of priorities can be configured. For example: '0-3, 7 'is equal to '0, 1, 2, 3, 7'. PFC is not supported through auto negotiation. PFC and Flowcontrol cannot both be enabled on the same port.

Maximum Frame Size

Enter the maximum frame size allowed for the switch port, including FCS. The range is 1518-10240 bytes.

Excessive Collision Mode

Configure port transmit collision behavior.

- Discard: Discard frame after 16 collisions (default).
- Restart: Restart backoff algorithm after 16 collisions.

Frame Length Check

Configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actually payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch. Note: No drop counters count frames dropped due to frame length mismatch

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page; any changes made locally will be undone.

3.1.2 Port Status

This page provides an overview of the current switch port states.
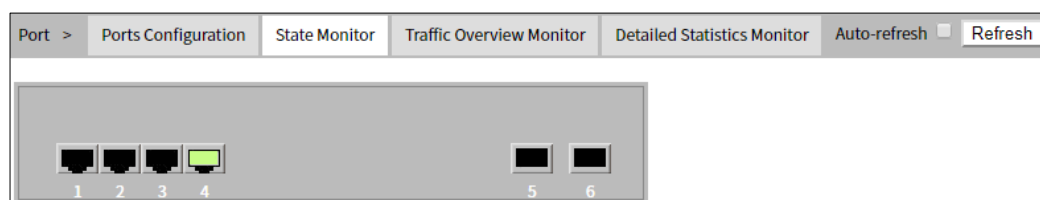
The port states are illustrated as follows:

State Disabled Down Link

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

3.1.3 Port Statistics Overview

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

The displayed counters are:

Port

The switch port number.

Note

The description of the port.

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.

Buttons

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

3.1.4　Detailed Port 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.

Port >	Ports Configuration	State Monitor	Traffic Overview Monitor	Detailed Statistics Monitor		Port 1 ▼ Auto-refresh☐ Refresh Clear

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
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 Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
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		

Receive Total and Transmit Total

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.

Receive and Transmit Size Counters

The number of received and transmitted good packets and bad packets. They are categorized according to their respective frame sizes.

Receive and Transmit Queue Counters

The number of received and transmitted packets per input and output queue.

Receive Error Counters

Rx Drops

The number of frames dropped due to lack of receive buffers or egress congestion.

Rx CRC/Alignment

The number of frames received with CRC or alignment errors.

Rx Undersize

The number of short 1 frames received with valid CRC.

Rx Oversize

The number of long 2 frames received with valid CRC.

Rx Fragments

The number of short 1 frames received with invalid CRC.

Rx Jabber

The number of long 2 frames received with invalid CRC.

Rx Filtered

The number of received frames filtered by the forwarding process.

1 Short frames are frames that are smaller than 64 bytes.

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

Transmit Error Counters

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.

Buttons

The port select box determines which port is affected by clicking the buttons.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

3.2 DDMI

3.2.1 DDMI Configuration

This page allows for configuring DDMI.

Mode

Indicates the DDMI mode operation. Possible modes are:

- Enabled: Enable DDMI mode operation.
- Disabled: Disable DDMI mode operation.

Buttons

Save: Click to save changes.

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

3.2.2 DDMI Overview Monitor

This page displays overview DDMI information.

Port

DDMI port.

Vendor

Indicates Vendor name SFP vendor name.

Part Number

Indicates Vendor PN Part number provided by SFP vendor.

Serial Number

Indicates Vendor SN Serial number provided by vendor.

Revision

Indicates Vendor rev Revision level for part number provided by vendor.

Data Code

Indicates Date code Vendor's manufacturing date code.

Transceiver

Indicates Transceiver compatibility.

3.3 Relay Alarm

On the page of "Relay", user can enable power supply, port alarm, and configure relevant alarm information.

Relay Configuration

Alarm Mode

Enable relay alarm or not, options as follows:

- Enable
- Disable

Power Mode Configuration

- Power

  Display power supply of the device, value is 1 or 2.

- Mode

  Enable the power supply alarm or not, options as follows:

  - Enable: when the power supply fails, power supply alarm will be triggered.
  - Disable

- Link

  Connection status of power supply, the device will automatically recognize and display, values include:

  - Fault
  - Normal.

Port Mode Configuration

- Port

  Display port number of the device, value range is: 110

- Mode

  Enable the port alarm or not, options as follows:

  - Enable: when the port is disconnected, port alarm will be triggered.
  - Disable

- Link

  Connection status of the port, the device will automatically recognize and display, values include:

  - Up: connection is normal.
  - Down: disconnected.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

4 Security

4.1 Users

This option provides an overview of the current users. Currently, the only way to log in as another user on the web server is to close and reopen the browser.

Users Configuration

User Name	Privilege Level
admin	15

Add New User

The displayed values for each user are:

User Name

The name identifying the user. This is also a link to edit a user.
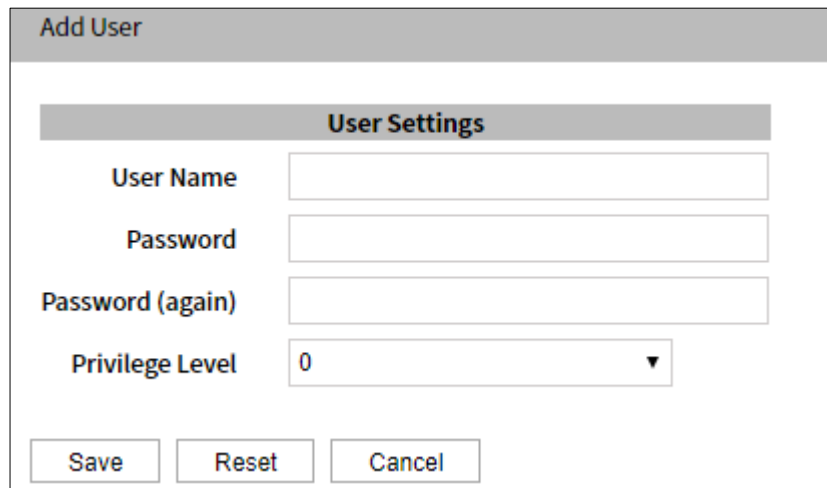
Privilege Level

The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, that is, that is granted the fully control of the device. However, other values need to refer to the privilege level of each group. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults, and so on) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

Buttons

Add a new user: Click this button to add a new user.

This page configures a user.

Add User

User Settings

User Name	
Password	
Password (again)	
Privilege Level	0 ▼

[Save] [Reset] [Cancel]

User Name

A string identifying the user name that this entry should belong to. The allowed string length is 1 to 31. The valid user name allows letters, numbers and underscores.

Password

The password of the user. The allowed string length is 0 to 31. Any printable characters including space is accepted.

Privilege Level

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

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

Clear: Click to undo any changes made locally and return to the Users.

Delete user: Delete the current user. This button is not available for new configurations (Add new user)

4.2　Privilege

This option provides an overview of the privilege levels configuration.

Privilege Level Configuration

Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5 ▼	10 ▼	5 ▼	10 ▼
Debug	15 ▼	15 ▼	15 ▼	15 ▼
DHCP	5 ▼	10 ▼	5 ▼	10 ▼
Diagnostics	5 ▼	10 ▼	5 ▼	10 ▼
ERPS	5 ▼	10 ▼	5 ▼	10 ▼
EVC	5 ▼	10 ▼	5 ▼	10 ▼
IP	5 ▼	10 ▼	5 ▼	10 ▼
IPMC_Snooping	5 ▼	10 ▼	5 ▼	10 ▼
JSON_RPC	5 ▼	10 ▼	5 ▼	10 ▼
JSON_RPC_Notification	5 ▼	10 ▼	5 ▼	10 ▼
LACP	5 ▼	10 ▼	5 ▼	10 ▼
LLDP	5 ▼	10 ▼	5 ▼	10 ▼
Loop_Protect	5 ▼	10 ▼	5 ▼	10 ▼
MAC_Table	5 ▼	10 ▼	5 ▼	10 ▼
Maintenance	15 ▼	15 ▼	15 ▼	15 ▼
Mirroring	5 ▼	10 ▼	5 ▼	10 ▼
NTP	5 ▼	10 ▼	5 ▼	10 ▼
Ports	5 ▼	10 ▼	1 ▼	10 ▼
PTP	5 ▼	10 ▼	5 ▼	10 ▼
QoS	5 ▼	10 ▼	5 ▼	10 ▼
Relay	5 ▼	10 ▼	5 ▼	10 ▼
Ring	5 ▼	10 ▼	5 ▼	10 ▼
Security	5 ▼	10 ▼	5 ▼	10 ▼
Spanning_Tree	5 ▼	10 ▼	5 ▼	10 ▼
System	5 ▼	10 ▼	1 ▼	10 ▼
VLANs	5 ▼	10 ▼	5 ▼	10 ▼

Save　　Reset

Group Name

The name identifying the privilege group. In most cases, a privilege level group consists of a single module (for example, LACP, RSTP or QoS), but a few of them contains more than one. The following description defines these privilege level groups in details:

- System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.
- Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.
- IP: Everything except ping.
- Port: Everything except VeriPHY.
- Diagnostic methods: 'ping' and VeriPHY.
- Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.

- Debug: Only present in CLI. Low Library.

Privilege Level

Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (for example, for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

4.3　Auth method

4.3.1　Authentication Method Configuration

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

Authentication Method Configuration

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

Command Authorization Method Configuration

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

Accounting Method Configuration

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

Save　Reset

The table has one row for each client type and a number of columns which are as follows:

Client

The management client for which the configuration below applies.

Method

Method can be set to one of the following values:

- No: Authentication is disabled and login is not possible.
- Local: Use the local user database on the switch for authentication.
- radius: Use one or more of the remote RADIUS servers for authentication.
- tacacs: Use one or more of the remote TACACS+ servers for authorization.

Methods that involves remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as local. This will enable the management client to log in via the local user database if none of the configured authentication servers are alive.

4.3.2 Command Authorization Method Configuration

The command authorization section allows you to limit the CLI commands available to a user. The table has one row for each client type and a number of columns which are as follows:

Client

The management client for which the configuration below applies.

Method

It can be set to one of the following values:

- no: Command authorization is disabled. User is granted access to CLI commands according to his privilege level.
- tacacs: Use one or more of the remote TACACS+ servers for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.

Cmd Lvl

Authorizes all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15.

Cfg Cmd

Also, authorizes configuration commands.

4.3.3 Accounting Method Configuration

The accounting section allows you to configure command and exec (login) accounting. The table has one row for each client type and a number of columns which are as follows:

Client

The management client for which the configuration below applies.

Method

Method can be set to one of the following values:

- No: Authentication is disabled.
- tacacs: Uses one or more of the remote TACACS+ servers for accounting.

Cmd Lvl

Enable statistics of all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15. Leave the field empty to disable command accounting.

Exec

Enables exec (login) accounting.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

4.4 SSH

This option allows you to configure SSH.

Mode

The Mode option indicates the SSH mode operation. Possible modes are:

- Enable: Enable SSH mode operation.
- Disabled: Disables SSH mode operation.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

4.5　HTTPS

This page allows you to configure the HTTPS settings and maintain the current certificate on the switch.

HTTPS Configuration		Refresh
Mode	Disabled ▼	
Automatic Redirect	Disabled ▼	
Certificate Maintain	None ▼	
Certificate Status	Switch secure HTTP certificate is presented	
Save　　Reset		

Mode

Indicate the HTTPS mode operation.

Possible modes are:

- Enabled: Enable HTTPS mode operation.
- Disabled: Disable HTTPS mode operation.

Automatic Redirect

Indicate the HTTPS redirect mode operation. It is only significant when "HTTPS Mode Enabled" is selected. When the redirect mode is enabled, the HTTP connection will be redirected to HTTPS connection automatically.

Notice that the browser may not allow the redirect operation due to the security consideration unless the switch certificate is trusted to the browser. You need to initialize the HTTPS connection manually for this case.

Possible modes are:

- Enable: Enable HTTPS redirect mode operation.

- Disable: Disable HTTPS redirect mode operation.

Certificate Maintain

The operation of certificate maintenance.

Possible operations are:

- None: No operation.
- Delete: Delete the current certificate.
- Upload: Upload a certificate PEM file. Possible methods are: Web Browser or URL.
- Generate: Generate a new self-signed RSA certificate.

Certificate Pass Phrase

Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.

Certificate Upload

Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem

Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g. Firefox v37 and Chrome v39.

Possible methods are:

- Web bowser: Upload a certificate via Web browser.
- URL: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name>. For example, tftp://10.10.10.10/new_image_path/new_image.dat,http://username:password@10.10.10.10:80/new_image_path/new_image.dat. Operation. For example: A valid file name is a text string drawn from alphabet (A-Za-z), digits (09), dot (.), hyphen (-), under score(_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.

Certificate Status

Display the current status of certificate on the switch.

Possible statuses are:

- Switch secure HTTP certificate is presented.
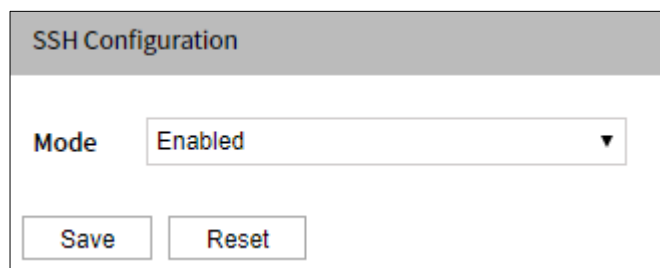- Switch secure HTTP certificate is not presented.
- Switch secure HTTP certificate is generating....

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

Auto-refresh: Click to refresh the page; any changes made locally will be undone.

4.6 Access Management

4.6.1 Access Management Configuration

This option allows you to configure access management. The maximum number of entries is 16. If the type of the application matches any one of the access management entries, it allows access to the switch.

Access Management >	Access Management Configuration	Access Management Statistics Monitor

Mode | Disabled ▼

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

Add New Entry

Save   Reset

Mode

Indicates the access management mode operation. Possible modes are:

- Enabled: Enables access management mode operation.
- Disable: Disable access management mode operation.

Delete

Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.

VLAN ID

Indicates the VLAN ID for the access management entry.

Start IP address

Indicates the start IP address for the access management entry.

Ending IP Address

Indicates the end IP address for the access management entry.

HTTP/HTTPS

Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.

SNMP

Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

TELNET/SSH

Indicates that the host can access the switch from TELNET/SSH interface if the host IP address matches the IP address range provided in the entry.

Buttons

Add new entry: Click to add a new access management entry.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

4.6.2 Access Management Statistics Monitoring

This page provides statistics for access management.

Interface

The interface type through which the remote host can access the switch.

Received Packets

Number of received packets from the interface when access management mode is enabled.

Allowed Packets

Number of allowed packets from the interface when access management mode is enabled.

Discarded Packets

Number of discarded packets from the interface when access management mode is enabled.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clear all statistics.

4.7   SNMP

4.7.1 System Configuration

This option allows you to system configure the SNMP feature.

Mode

Indicates the SNMP mode operation. Possible modes are:

- Enabled: Enables SNMP mode operation.
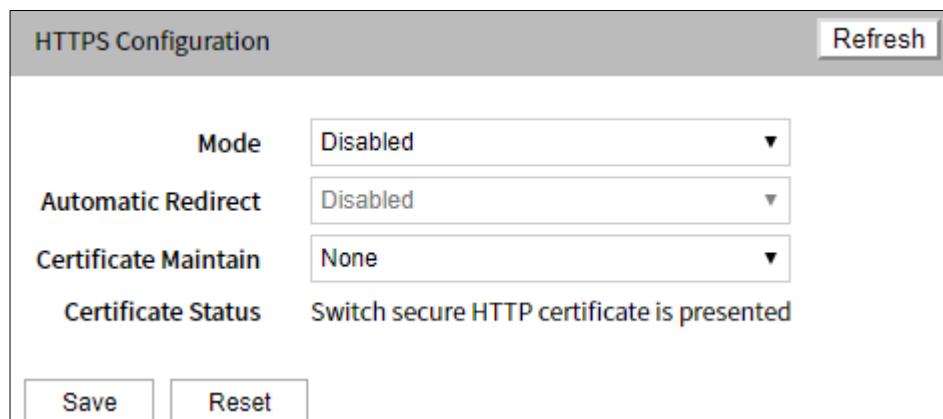- Disabled: Disables SNMP mode operation.

Version

Indicates the SNMP supported version. Possible versions are:

- SNMP v1: Sets SNMP supported version 1.
- SNMP v2c: Sets SNMP supported version 2c.
- SNMP v3: Set version 3 supported by SNMP.

Read Community

Indicates the community read access string to permit access to SNMP agent. The allowed string length is 1 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string is associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Write Community

Indicates the community write access string to permit access to SNMP agent. The allowed string length is 1 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. If SNMP version is SNMPv3, the community string is associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.

Engine ID

Indicates the SNMPv3 engine ID. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

4.7.2　Trap Configuration

This option allows you to configure the SNMP trap feature.

Global Settings

Mode

Indicates the trap mode operation. Possible modes are as follows:

- Enabled: Enables SNMP trap mode operation.
- Disabled: Disables SNMP trap mode operation.

Trap Destination Configurations

Configure trap destinations on this page.

Name

Indicates the name of the trap configuration.

Enable

Indicates the trap destination mode operation. Possible modes are as follows:

- Enabled: Enables SNMP trap mode operation.
- Disabled: Disables SNMP trap mode operation.

Version

Indicates the SNMP trap supported version. Possible versions are as follows:

- SNMPv1: Sets SNMP trap supported version 1.
- SNMPv2c: Sets SNMP trap supported version 2c.
- SNMPv3: Sets SNMP trap supported version 3.

Destination Address

Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w') as well as a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (09), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash. Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Destination port

Indicates the SNMP trap destination port. SNMP Agent sends an SNMP message via this port. The port range is 1~65535.

Buttons

Add new entry: Click to add a new user.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

4.7.2.1　SNMP Trap Configuration

Configure SNMP trap on this page.

Trap Config Name

Indicates which trap Configuration's name for configuring. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Trap Mode

Indicates the SNMP mode operation. Possible modes are:

Enabled: Enable SNMP mode operation.

Disabled: Disable SNMP mode operation.

Trap Version

Indicates the SNMP supported version. Possible versions are:

SNMP v1: Set SNMP supported version 1.

SNMP v2c: Set SNMP supported version 2c.

SNMP v3: Set version 3 supported by SNMP.

Trap Community

Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126.

Trap Destination Address

Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').

And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (09), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash.

Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Trap Destination port

Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

Trap Inform Mode

Indicates the SNMP trap inform mode operation. Possible modes are:

Enabled: Enable SNMP trap inform mode operation.

Disabled: Disable SNMP trap inform mode operation.

Trap Inform Timeout (seconds)

Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.

Trap Inform Retry Times

Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.

Trap Probe Security Engine ID

Indicates the SNMP trap probe security engine ID mode of operation. The possible values are:

Enabled: Enable SNMP trap probe security engine ID mode of operation.

Disabled: Disable SNMP trap probe security engine ID mode of operation.

Trap Security Engine ID

Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain

an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.

Trap Security Name

Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

SNMP Trap Event

Configure SNMP trap on this page.

System

Enable/disable that the Interface group's traps. Possible traps are:

Hot Start: Enable/disable warm start trap.

Cold Start: Enable/disable cold start trap.

Interface

Indicates that the Interface group's traps. Possible traps are: Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are:

Link Up: Enable/disable Link up trap.

Link Down: Enable/disable Link down trap.

LLDP: Enable/disable LLDP trap.

Authentication

Indicates that the authentication group's traps. Possible traps are:

SNMP Authentication Fail: Enable/disable SNMP trap authentication failure trap.

Enable

Indicates that the Switch group's traps. Possible traps are:

STP: Enable/disable STP trap.

RMON: Enable/disable RMON trap.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

4.7.3   SNMPv3 Community Configuration

This option allows you to configure SNMPv3 community table. The entry index key is Community.

Delete

Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.

Community

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

Source IP

Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.

Source Mask

Indicates the SNMP access source address mask.

Buttons

Add new community entry: Click to add a new community entry.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

4.7.4 User Configuration

This option allows you to configure SNMPv3 user table. The entry index keys are Engine ID and User Name.

Delete

Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.

Engine ID

An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is a local user; otherwise it is a remote user.

User Name

A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Level

Indicates the security model that this entry should belong to. Possible security models are:

- NoAuth, NoPriv: No authentication and no encryption.
- Auth, NoPriv: Authentication and no encryption.
- Auth, Priv: Authentication and encryption.

The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.

Authentication Mode

Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

- None: No authentication mode.
- MD5: An optional flag to indicate that this user uses MD5 authentication protocol.
- SHA: An optional flag to indicate that this user uses SHA authentication protocol.

The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.

Authentication Password

A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.

Privacy Protocol

Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

- None: No privacy protocol.
- DES: An optional flag to indicate that this user uses DES authentication protocol.
- AES: An optional flag to indicate that this user uses AES authentication protocol.

Privacy Password

A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

Add new user entry: Click to add new entry.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

4.7.5 Group Configuration

This option allows you to configure the SNMPv3 group table. The entry index keys are Security Model and Security Name.

Delete

Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.

Operation

Security Model

Indicates the security model that this entry should belong to. Possible security models are as follows:

- v1: Reserved for SNMPv1.
- v2c: Reserved for SNMPv2c.
- usm: User-based Security Model (USM).

Security Name

A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Group Name

A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

Add new group entry: Click to add a new community entry.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

4.7.6 View Configuration

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

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 ASCII characters from 33 to 126.

View Type

Indicates the view type that this entry should belong to. Possible view types are:

- The characteristics of OSPF fast convergence are as follows: An optional flag to indicate that this view subtree should be included.
- Exclude: An optional flag to indicate that this view subtree should be excluded.

In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.

OID Subtree

The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).

Buttons

Add new view entry: click to add a new view entry.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

4.7.7   Access Configuration

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

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 ASCII characters from 33 to 126.

Security Mode

Indicates the security model that this entry should belong to. Possible security models are:

- any: Any security model accepted(v1|v2c|usm).
- v1: Reserved for SNMPv1.
- v2c: Reserved for SNMPv2c.
- usm: User-based Security Model (USM).

Security Level

Indicates the security model that this entry should belong to. Possible security models are:

- NoAuth, NoPriv: No authentication and no encryption.
- Auth, NoPriv: Authentication and no encryption.
- Auth, Priv: Authentication and encryption.

Read View Name

The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Write View Name

The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

Add new access entry: click to add a new access entry.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

4.8 RMON

4.8.1 Statistical Group Configuration

Configure RMON Statistics table on this page. The entry index key is ID.

Delete

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

ID

Indicates the index of the entry. The range is from 1 to 65535.

Data Source

Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.

Buttons

Add new entry: Click to add a new community entry.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

4.8.2 History Configuration

Configure RMON History table on this page. The entry index key is ID.

RMON >	Statistics Configuration	History Configuration	Alarm Configuration	Event Configuration	Statistics Monitor	History Monitor	Alarm Monitor	Event Monitor

Delete   ID   Data Source   Interval   Buckets   Buckets Granted

Add New Entry	Save	Reset

Delete

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

ID

Indicates the index of the entry. The range is from 1 to 65535.

Data Source

Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.

Interval

Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.

Buckets

Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.

Buckets Granted

The number of data shall be saved in the RMON.

Buttons

Add new entry: Click to add a new community entry.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

4.8.3 Alarm configuration

Configure RMON Alarm table on this page. The entry index key is ID.

RMON >	Statistics Configuration	History Configuration	Alarm Configuration	Event Configuration	Statistics Monitor	History Monitor	Alarm Monitor	Event Monitor

Delete   ID   Interval   Variable   Sample Type   Value   Startup Alarm   Rising Threshold   Rising Index   Falling Threshold   Falling Index

Add New Entry	Save	Reset

Delete

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

ID

Indicates the index of the entry. The range is from 1 to 65535.

Sampling interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.

Variable

Indicates the particular variable to be sampled, the possible variables are:

- InOctets: The total number of octets received on the interface, including framing characters.

- InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol.

- InNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.

- InDiscards: The number of inbound packets that are discarded even the packets are normal.

- InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

- InUnknownProtos: the number of the inbound packets that were discarded because of the unknown or un-support protocol.

- OutOctets: The number of octets transmitted out of the interface , including framing characters.

- OutUcastPkts: The number of uni-cast packets that request to transmit.

- OutNUcastPkts: The number of broad-cast and multi-cast packets that request to transmit.

- OutDiscards: The number of outbound packets that are discarded even the packets are normal.

- OutErrors: The number of outbound packets that could not be transmitted because of errors.

- OutQLen: The length of the output packet queue (in packets).

Sampling Type

The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

- Absolute: Direct sampling.

- Increment: Calculate the difference between samples (default).

Variable

The value of the statistic during the last sampling period.

Startup Alarm

The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are:

- RisingTrigger alarm when the first value is larger than the rising threshold.
- FallingTrigger alarm when the first value is less than the falling threshold.
- RisingOrFallingTrigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).

Rising Threshold

Rising threshold value (-2147483648-2147483647).

Rising Index

Rising event index (165535).

Falling Threshold

Falling threshold value (-2147483648-2147483647)

Falling Index

Falling event index (165535).

Buttons

Add new entry: Click to add a new community entry.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

4.8.4 Link Event Configuration

Configure RMON Event table on this page. The entry index key is ID.

Delete

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

ID

Indicates the index of the entry. The range is from 1 to 65535.

Description

Indicates this event, the string length is from 0 to 127, default is a null string.

Type

Indicates the notification of the event, the possible types are:

- No: No operations.
- log: Create SNMP log entry when the event is triggered.
- snmptrap: Send SNMP trap when the event is triggered.
- logandtrap: Create SNMP log entry and sent SNMP trap when the event is triggered.

Community

Specify the community when trap is sent, the string length is from 0 to 127, default is "public".

Event Last Time

Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons

Add new entry: Click to add a new community entry.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

4.8.5 Statistics Monitoring

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Alarm 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 Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

The "Start from Control Index" allows the user to select the starting point in the Alarm table. Clicking the "Refresh" button will update the displayed table starting from that or the next closest Statistics table match.

The [>>] will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the [|<<] button to start over.

The displayed counters are:

| RMON > | Statistics Configuration | History Configuration | Alarm Configuration | Event Configuration | Statistics Monitor | History Monitor | Alarm Monitor | Event Monitor | Auto-refresh | Refresh | |<< | >> |

Start from Control Index 0 with 20 entries per page.

| ID | Data Source(ifIndex) | Drop | Octets | Pkts | Broad-cast | Multi-cast | CRC Errors | Under-size | Over-size | Frag | Jabb | Coll | Bytes | 65~127 | 128~255 | 256~511 | 512~1023 | 1024~1588 |

ID

Indicates the index of Statistics entry.

Data Source(ifIndex)

The port ID which wants to be monitored.

Drop

The total number of events in which packets were dropped by the probe due to lack of resources.

Octets

The total number of octets of data (including those in bad packets) received on the network.

Pkts

The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast

The total number of good packets received that were directed to the broadcast address.

Multicast

The total number of good packets received that were directed to a multicast address.

CRC Errors

Total number of packets received. Eight-bit byte with length (excluding the frame part, but including FCS octets) between 64 and 1518, but there is an integer (FCS error) bad frame check sequence (FCS) of eight-bit byte or a bad FCS eight-bit byte which is not an integer (alignment error).

Under-size

The total number of packets received that were less than 64 octets.

Over-size

The total number of packets received that were longer than 1518 octets.

Frag.

The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.

The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.

The best estimate of the total number of collisions on this Ethernet segment.

64

The total number of packets (including bad packets) received that were 64 octets in length.

65~127

The total number of packets (including bad packets) received that were between 65 to 127 octets in length.

128~255

The total number of packets (including bad packets) received that were between 128 to 255 octets in length.

256~511

The total number of packets (including bad packets) received that were between 256 to 511 octets in length.

512~1023

The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.

1024~1588

The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

|<< : Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.

\>> : Updates the table, starting with the entry after the last entry currently displayed.

4.8.6 History Monitoring

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History 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 History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

The "Start from History Index and Sample Index" allows the user to select the starting point in the History table. Clicking the "Refresh" button will update the displayed table starting from that or the next closest History table match.

The ⟩⟩ will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached, the text "No other entries" is shown in the displayed table. Use the |⟨⟨ button to start over.

The displayed fields are:

RMON >	Statistics Configuration	History Configuration	Alarm Configuration	Event Configuration	Statistics Monitor	History Monitor	Alarm Monitor	Event Monitor	Auto-refresh ☐ Refresh	|<<	>>

Start from Control Index 0 to 0 with 20 entries per page.

Interval Variable Sample Type Drop Octets Pkts Broad-cast Multi-cast CRC Errors Under-size Over-size Frag Jabb Coll Utilization

History Index

Indicates the index of History control entry.

Sample Index

Indicates the index of the data entry associated with the control entry.

Sample Start

The value of sysUpTime at the start of the interval over which this sample was measured.

Drop

The total number of events in which packets were dropped by the probe due to lack of resources.

Octets

The total number of octets of data (including those in bad packets) received on the network.

Pkts

The total number of packets (including bad packets, broadcast packets, and multicast packets) received.

Broadcast

The total number of good packets received that were directed to the broadcast address.

Multicast

The total number of good packets received that were directed to a multicast address.

CRCErrors

Total number of packets received. Eight-bit byte with length (excluding the frame part, but including FCS octets) between 64 and 1518, but there is an integer (FCS error) bad frame check sequence (FCS) of eight-bit byte or a bad FCS eight-bit byte which is not an integer (alignment error).

Undersize

The total number of packets received that were less than 64 octets.

Oversize

The total number of packets received that were longer than 1518 octets.

Frag.

The number of frames which size is less than 64 octets received with invalid CRC.

Jabb.

The number of frames which size is larger than 64 octets received with invalid CRC.

Coll.

The best estimate of the total number of collisions on this Ethernet segment.

Utilization

The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

|<< : Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.

\>> : Updates the table, starting with the entry after the last entry currently displayed.

4.8.7 Alarm Monitoring

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Alarm 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 Alarm table. The first displayed will be the one with the lowest ID found in the Alarm table.

The "Start from Control Index" allows the user to select the starting point in the Alarm table. Clicking the "Refresh" button will update the displayed table starting from that or the next closest Statistics table match.

The ⟩⟩ will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |⟨⟨ button to start over.

The displayed fields are:

ID

Indicates the index of Alarm control entry.

Interval

Indicates the interval in seconds for sampling and comparing the rising and falling threshold.

Variable

Indicates the particular variable to be sampled

Sample Type

The method of sampling the selected variable and calculating the value to be compared against the thresholds.

Value

The value of the statistic during the last sampling period.

Startup Alarm

The alarm that may be sent when this entry is first set to valid.

Rising Threshold

Rising threshold value.

Rising Index

Rising event index.

Falling Threshold

Falling threshold value.

Falling Index

Falling event index.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

|<< : Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.
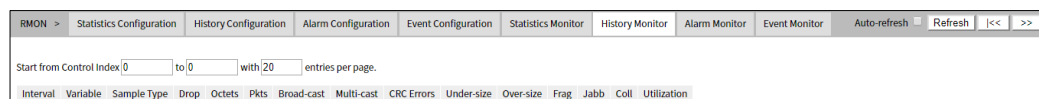
\>\> : Updates the table, starting with the entry after the last entry currently displayed.

4.8.8 Event Monitoring

This page provides an overview of RMON event entries. Each page shows up to 99 entries from the event 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 Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table.

The "from event index and log index" input field allows the user to select a starting point in the Event table. Clicking the "Refresh" button will update the displayed table starting from that or the next closest Event table match.

The \>\> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

The displayed fields are:

Event Index

Indicates the index of the event entry.

Log Index

Indicates the index of the log entry.

LogTime

Indicates Event log time

LogDescription

Indicates the Event description.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

[|<<]: Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.

[>>]: Updates the table, starting with the entry after the last entry currently displayed.

5 Secure Network

5.1   Port Limit Control

This page allows you to configure the Port Security Limit Control system and port settings.

Limit Control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Limit Control is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken. The action can be one of the four different actions as described below.

The Limit Control module utilizes a lower-layer module, Port Security module, which manages MAC addresses learnt on the port.

The Limit Control configuration consists of two sections, a system- and a port-wide.

5.1.1 System Configuration

Mode

Indicates if Limit Control is globally enabled or disabled on the switch. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.

Aging Enabled

If checked, secured MAC addresses are subject to aging as discussed under Aging Period .

Aging Period

If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality.

The Aging Period can be set to a number between 10 and 10,000,000 seconds.

To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

5.1.2 Port Configuration

The table has one row for each port on the switch and a number of columns, which are:

Port

The port number for which the configuration below applies.

Mode

Controls whether Limit Control is enabled on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Notice that other modules may

still use the underlying port security features without enabling Limit Control on a given port.

Limit

The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

ACTION

If Limit is reached, the switch can take one of the following actions:

- None: Do not allow more than Limit MAC addresses on the port, but take no further action.
- Trap: If Limit + 1 MAC addresses is seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit gets exceeded.
- Shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new address will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port:

  1) Boot the switch,

  2) Disable and re-enable Limit Control on the port or the switch,

  3) Click the Reopen button.

- Trap & Shutdown: If Limit + 1 MAC addresses is seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.

Status

This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values:

- Disabled: Limit Control is either globally disabled or disabled on the port.
- Ready: The limit is not yet reached. This can be shown for all actions.
- Limit Reached: Indicates that this port has reached its limit. This state can only be shown if Action is set to None or Trap.
- Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.

Re-open Button

If a port is shutdown by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Action section.

Note that clicking the reopen button causes the page to be refreshed, so non-committed changes will be lost.

Buttons

Refresh: Click to refresh the page. Note that non-committed changes will be lost.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

5.2 Port Security

Port Security Switch Status

This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections - one with a legend of user modules and one with the actual port status.

5.2.1 Switch Monitoring

User Module Legend

The legend shows all user modules that may request Port Security services.

User Module Name

The full name of a module that may request Port Security services.

Abbr

A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

Port Status

The table has one row for each port on the switch and a number of columns, which are:

Port

The port number for which the status applies. Click the port number to see the status for this particular port.

Users

Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.

Status

Shows the current state of the port. It can take one of four values:

- Disabled: No user modules are currently using the Port Security service.

- Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive.

- Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in.

- Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration Web-page.

MAC Count (Current, Limit)

The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) and the maximum number of MAC addresses that can be learned on the port, respectively.

If no user modules are enabled on the port, the Current column will show a dash (-).

If the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

5.2.2 Port Monitoring

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

MAC Address & VLAN ID

The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.

Status

Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.

Time of Addition

Shows the date and time when this MAC address was first seen on the port.

Age/Hold

If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise a new age period will begin.

If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Buttons

Use the port select box to select which port to show status for.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

5.3   NAS

5.3.1 Network Access Server Configuration

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 "Configuration→Security→AAA" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as shall be explored below.

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 supplicant 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.

The NAS configuration consists of two sections, a system- and a port-wide.

System Configuration

Mode

Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.

Reauthentication Enabled

If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled

ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached.

For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).

Reauthentication Period

Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.

EAPOL Timeout

Determines the time for retransmission of Request Identity EAPOL frames.

Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.

Aging Period

This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

• Single 802.1X

• Multi 802.1X

• MAC-Based Auth.

When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.

If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries.

For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.

Hold Time

This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:

• Single 802.1X

• Multi 802.1X

• MAC-Based Auth.

If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time.

The Hold Time can be set to a number between 10 and 1000000 seconds.

RADIUS-Assigned QoS Enabled

RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description).

The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.

RADIUS-Assigned VLAN Enabled

RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description).

The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determine whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.

Guest VLAN Enabled

A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below.

The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.

Guest VLAN ID

This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled.

Valid values are in the range [1; 4095].

Max. Reauth. Count

The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled.

Valid values are in the range [1; 255].

Allow Guest VLAN if EAPOL Seen

The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port.

The value can only be changed if the Guest VLAN option is globally enabled.

Port Configuration

The table has one row for each port on the switch and a number of columns, which are:

Port

The port number for which the configuration below applies.

Admin State

If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:

- Force Authorized

  In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication.

- Force Unauthorized

  In this mode, the switch will send one EAPOL Failure frame when the port link

comes up, and any client on the port will be disallowed network access.

- Port-based 802.1X

  In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch 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 AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the 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.

- MAC-based Auth.

  Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on

behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

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

The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.

Port Status

The current state of the port. It can undertake one of the following values:

- Globally Disabled: NAS is globally disabled.
- Link Down: NAS is globally enabled, but there is no link on the port.
- Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.
- Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.
- X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

Restart

Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.

Clicking these buttons will not cause settings changed on the page to take effect.

- Reauthenticate: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.

  The button only has effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

- Reinitialize: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

Buttons

Refresh: Click to refresh the page.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

5.3.2 Network Access Server Switch Status

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

Network Access Server Switch Status >	NAS Configuration	Switch Monitor	Port Monitor	Auto-refresh ☐ Refresh

Port	Admin State	Port State	Last Source	Last ID
1	Force Authorized	Globally Disabled		
2	Force Authorized	Globally Disabled		
3	Force Authorized	Globally Disabled		
4	Force Authorized	Globally Disabled		
5	Force Authorized	Globally Disabled		
6	Force Authorized	Globally Disabled		

Port

The switch port number. Click to navigate to detailed NAS statistics for this port.

Admin State

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

Port Status

The current state of the port. Refer to NAS Port State for a description of the individual states.

Last Source

The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.

Last ID

The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

QoS Class

QoS Class assigned to the port by the RADIUS server if enabled.

Port VLAN ID

The VLAN ID that NAS places port in. The field is blank, if the Port VLAN ID is not overridden by NAS.

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

5.3.3 NAS Statistics

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X 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.

Port Status

Admin State

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

Port Status

The current state of the port. Refer to NAS Port State for a description of the individual states.

5.4 ACL

5.4.1 Port Configuration

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.

Port

The switch port number.

Policy ID

Select the policy to apply to this port. The allowed values are 0 through 255. The default value is 0.

ACTION

Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".

Rate Limiter ID

Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled".

EVC Policer

Select whether EVC policer is enabled or disabled. The default value is "Disabled". Note that ACL rate limiter and EVC policer can not both be enabled.

EVC Policer ID

Select which EVC policer ID to apply on this port. The allowed values are Disabled or the values 1 through 256.

Port Redirect

Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".

Mirroring

Specify the mirror operation of this port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

Logging

Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC. The allowed values are:

Enabled: Frames received on the port are stored in the System Log.

Disabled: Frames received on the port are not logged.

The default value is "Disabled". Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.

Shutdown

Specify the port shut down operation of this port. The allowed values are:

Enable: If a frame is received on the port, the port will be disabled.

Disabled: Port shut down is disabled.

The default value is "Disabled".

Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).

Status

Specify the port state of this port. The allowed values are:

Enabled: To reopen ports by changing the volatile port configuration of the ACL user module.

Disabled: To close ports by changing the volatile port configuration of the ACL user module.

The default value is "Enabled".

Counter

Counts the number of frames that match this ACE.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

Refresh: Click to refresh the page; any changes made locally will be undone.

Clear: Click to clear the counters.

5.4.2 Rate Limiter Configuration

Configure the rate limiter for the ACL of the switch.

Rate Limiter ID

The rate limiter ID for the settings contained in the same row and its range is 1 to 16.

Speed

The valid rate is 0-3276700pps.

or 0, 100, 200, 300, ..., 1000000 in kbps.

Unit

Specify the rate unit. The allowed values are:

pps: Packets per second.

kbps: Kbits per second.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

5.4.3 Access Control List Configuration

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 256 on each switch.

Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.

ACL >	Port Configuration	Rate Limiters Configuration	Access Control List Configuration	ACL Status Monitor	Auto-refresh ☐	Refresh	Clear	Remove All

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

ACE
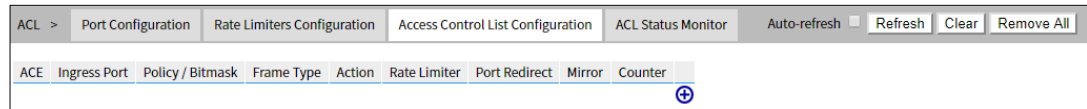
Indicates the ACE ID.

Ingress

Indicates the ingress port of the ACE. The possible values are:

All: The ACE will match all ingress port.

Port: The ACE will match a specific ingress port.

Policy / Bitmask

Indicates the policy number and bitmask of the ACE.

Frame Type

Indicates the frame type of the ACE. The possible values are:

Any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

IPv4/ICMP: ACE will match IPv4 frames with ICMP protocol.

IPv4/UDP: ACE will match IPv4 frames with UDP protocol.

IPv4/TCP: ACE will match IPv4 frames with TCP protocol.

IPv4/Other: ACE will match IPv4 frames, which are not ICMP/UDP/TCP.

IPv6: The ACE will match all IPv6 standard frames.

ACTION

Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter

Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

Port Redirect

Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.

Mirroring

Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are:

Enable: Frames received on the port are mirrored.

Disable: Frames received on the port are not mirrored.

The default value is "Disabled".

Counter

The counter indicates the number of times the ACE was hit by a frame.

Modification Buttons

You can modify each ACE (Access Control Entry) in the table using the following buttons:

:Add: Inserts a new ACE before the current row.

Edit: Edits the ACE row.

Up: Moves the ACE up the list.

:down: Moves the ACE down the list.

:Delete: Delete ACE.

Add: The lowest plus sign adds a new entry at the bottom of the ACE listings.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page; any changes made locally will be undone.

Clear: Click to clear the counters.

Clear all: click to delete all ACEs.

5.4.4 ACL Status Monitoring

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

ACL >	Port Configuration	Rate Limiters Configuration		Access Control List Configuration		ACL Status Monitor	combined ▼	Auto-refresh ☐	Refresh

User	ACE	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
netmanager	1	IPv4/UDP 65530-65534	Permit	Disabled	Disabled	Yes	0	No
mstp	1	ARP	Permit	Disabled	Disabled	Yes	20018	No
ring	1	LLC	Deny	Disabled	Disabled	Yes	0	No
ring	2	LLC	Permit	Disabled	Disabled	Yes	0	No

User

Indicates the ACL user.

ACE

Indicates the ACE ID on local switch.

Frame Type

Indicates the frame type of the ACE. The possible values are:

Any: The ACE will match any frame type.

EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

IPv4/ICMP: ACE will match IPv4 frames with ICMP protocol.

IPv4/UDP: ACE will match IPv4 frames with UDP protocol.

IPv4/TCP: ACE will match IPv4 frames with TCP protocol.

IPv4/Other: ACE will match IPv4 frames, which are not ICMP/UDP/TCP.

IPv6: The ACE will match all IPv6 standard frames.

ACTION

Indicates the forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.

Deny: Frames matching the ACE are dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter

Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.

CPU

Forward packet that matched the specific ACE to CPU.

Counter

The counter indicates the number of times the ACE was hit by a frame.

Conflicts

Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons

The select box determines which ACL user is affected by clicking the buttons.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

5.5　RADIUS

5.5.1　RADIUS Server Configuration

This page allows you to configure the RADIUS servers.

Global Configuration

These setting are common for all of the RADIUS servers.

Timeout

Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.

Retransmit

Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.

Deadtime

Deadtime, which can be set to a number between 0 to 1440 分, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

Key

The secret key - up to 63 characters long - shared between the RADIUS server and the switch.

NAS-IP-Address (Attribute 4)

The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-IPv6-Address (Attribute 95)

The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.

NAS-Identifier (Attribute 32)

The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Server Configuration

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

Delete

To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.

Hostname

The IP address or hostname of the RADIUS server.

Auth Port

The UDP port to use on the RADIUS server for authentication. Set to 0 to disable authentication.

Acct Port

The UDP port to use on the RADIUS server for accounting. Set to 0 to disable accounting.

Timeout

This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Retransmit

This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

Key

This optional setting overrides the global key. Leaving it blank will use the global key.

Adding a New Server

Add new server: Click to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported.

Delete: The button can be used to undo the addition of the new server.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

RADIUS Server Status Overview

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

RADIUS >	RADIUS Server Configuration	RADIUS Server Status Overview Monitor	RADIUS Authentication Statistics Monitor	Auto-refresh ☐ Refresh

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

RADIUS Servers

#

The RADIUS server number. Click to navigate to detailed statistics for this server.

IP Address

The IP address of this server.

Authentication Port

UDP port number for authentication.

Authentication Status

The current status of the server. This field takes one of the following values:

- Disabled: The server is disabled.
- Not Ready: The server is enabled, but IP communication is not yet up and running.
- Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
- Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Accounting Port

Billing UDP port number.

Accounting Status

The current status of the server. This field takes one of the following values:

- Disabled: The server is disabled.
- Not Ready: The server is enabled, but IP communication is not yet up and running.
- Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.
- Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

5.5.2 RADIUS Authentication Statistics Link Monitoring

This page provides detailed statistics for a particular RADIUS server.

RADIUS Authentication Statistics

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.

Packet Counters

RADIUS authentication server packet counter. There are seven receive and four transmit counters.

Direction	Name	RFC4668 Name	Description
Received	**Access Accepts**	radiusAuth ClientExtA ccessAcce pts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Received	**Access Rejects**	radiusAuth ClientExtA ccessReje	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.

Direction	Name	RFC4668 Name	Description
		cts	
Received	**Access Challenges**	radiusAuth ClientExtA ccessChall enges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Received	**Malformed Access Responses**	radiusAuth ClientExtM alformedAc cessRespo nses	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.
Received	**Bad Authenticators**	radiusAuth ClientExtB adAuthenti cators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Received	**Unknown Types**	radiusAuth ClientExtU nknownTy pes	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Received	**Packets Dropped**	radiusAuth ClientExtP acketsDrop ped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Transmitted	**Access Requests**	radiusAuth ClientExtA ccessRequ ests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Transmitted	**Access Retransmissions**	radiusAuth ClientExtA	The number of RADIUS Access-Request packets retransmitted to

Direction	Name	RFC4668 Name	Description
		ccessRetra nsmissions	the RADIUS authentication server.
Transmitted	**Pending Requests**	radiusAuth ClientExtP endingReq uests	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.
Transmitted	**Timeouts**	radiusAuth ClientExtTi meouts	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.

Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4668 Name	Description
IP Address	-	IP address and UDP port of the authentication server.
Status	-	Shows the state of the server. It adopts one of the following values: □ Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP

Name	RFC4668 Name	Description
		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.

RADIUS Accounting Statistics

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB.

Use the server select box to switch between the backend servers to show details for.

Packet Counters

RADIUS accounting server packet counter. There are five receive and four transmit counters.

Direction	Name	RFC4670 Name	Description
Received	Responses	radiusAccClient ExtResponses	The number of RADIUS packets (valid or invalid) received from the

Direction	Name	RFC4670 Name	Description
			server.
Received	Malformed Responses	radiusAccClient ExtMalformedR esponses	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.
Received	Bad Authenticators	radiusAcctClient ExtBadAuthenti cators	The number of RADIUS packets containing invalid authenticators received from the server.
Received	Unknown Types	radiusAccClient ExtUnknownTy pes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Received	Packets Dropped	radiusAccClient ExtPacketsDrop ped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Transmitt ed	Requests	radiusAccClient ExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Transmitt ed	Retransmissions	radiusAccClient ExtRetransmissi ons	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Transmitt ed	Pending Requests	radiusAccClient ExtPendingReq uests	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.
Transmitt ed	Timeouts	radiusAccClient ExtTimeouts	The number of accounting timeouts to the server. After a timeout, the

Direction	Name	RFC4670 Name	Description
			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.

Other Info

This section contains information about the state of the server and the latest round-trip time.

Name	RFC4670 Name	Description
IP Address	-	IP address and UDP port for the accounting server in question.
Status	-	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.

Name	RFC4670 Name	Description
Round-Trip Time	radiusAccClientExt RoundTripTime	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.

Buttons

The server select box determines which server is affected by clicking the buttons.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

5.6 Ethernet Services

5.6.1 Port Configuration

This page displays current EVC port configurations. The settings can also be configured here.

Port

The switch port number.

DEI Mode

The DEI mode for an NNI port determines whether frames transmitted on the port will have the DEI field in the outer tag marked based on the colour of the frame. The allowed values are:

- Coloured: The DEI is 1 for yellow frames and 0 for green frames.
- Fixed: The DEI value is determined by ECE rules.

Tag Mode

The tag mode specifying whether the EVC classification must be based on the outer or inner tag. This can be used on NNI ports connected to another service provider, where an outer "tunnel" tag is added together with the inner tag identifying the EVC. The allowed values are:

- Inner: Enable inner tag in EVC classification.
- Outer: Enable outer tag in EVC classification.

Address Mode

The IP/MAC address mode specifying whether the EVC classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses. The allowed values are:

- Source: Enable SMAC/SIP matching.
- Destination: Enable DMAC/DIP matching.

Buttons

Save: Click to save changes.

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

5.6.2 L2CP Configuration

This page displays current EVC L2CP configurations. The settings can also be configured here.

| L2CP Port Configuration > | Ports Configuration | L2CP Configuration | Bandwidth Profilesn Configuration | EVCs Configuration | ECEs Configuration | EVC Statistics Monitor | ▼ | Refresh |

DMAC	L2CP Mode
01-80-C2-00-00-00	Peer ▼
01-80-C2-00-00-01	Peer ▼
01-80-C2-00-00-02	Peer ▼
01-80-C2-00-00-03	Peer ▼
01-80-C2-00-00-04	Peer ▼
01-80-C2-00-00-05	Peer ▼
01-80-C2-00-00-06	Peer ▼
01-80-C2-00-00-07	Peer ▼
01-80-C2-00-00-08	Peer ▼
01-80-C2-00-00-09	Peer ▼
01-80-C2-00-00-0A	Peer ▼
01-80-C2-00-00-0B	Peer ▼
01-80-C2-00-00-0C	Peer ▼
01-80-C2-00-00-0D	Peer ▼
01-80-C2-00-00-0E	Peer ▼
01-80-C2-00-00-0F	Peer ▼
01-80-C2-00-00-20	Forward ▼
01-80-C2-00-00-21	Forward ▼
01-80-C2-00-00-22	Forward ▼
01-80-C2-00-00-23	Forward ▼
01-80-C2-00-00-24	Forward ▼
01-80-C2-00-00-25	Forward ▼
01-80-C2-00-00-26	Forward ▼
01-80-C2-00-00-27	Forward ▼
01-80-C2-00-00-28	Forward ▼
01-80-C2-00-00-29	Forward ▼
01-80-C2-00-00-2A	Forward ▼
01-80-C2-00-00-2B	Forward ▼
01-80-C2-00-00-2C	Forward ▼
01-80-C2-00-00-2D	Forward ▼
01-80-C2-00-00-2E	Forward ▼
01-80-C2-00-00-2F	Forward ▼

DMAC

The destination BPDU MAC addresses (01-80-C2-00-00-0X) and GARP (01-80-C2-00-00-2X) MAC addresses for the settings contained in the same row.

L2CP Mode

The L2CP mode for the specific port. Possible values are:

- Peer: Allow to peer L2CP frames.
- Forward: Allow to forward L2CP frames.

Buttons

Port 1 ▼: the port select box determines which port is affected by clicking the buttons.

Refresh: Click to refresh the page.

Save: Click to save changes.

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

5.6.3 Bandwidth Limitation Subset

This page displays current EVC ingress bandwidth profile configurations. These policers may be used to limit the traffic received on UNI ports. The settings can also be configured here.

Start from Policer ID

The start Policer ID for displaying the table entries. The allowed range is from 1 through 256.

Entry

The number of entries per page. The allowed range is from 2 through 256.

Policer ID

The Policer ID is used to identify one of the 256 policers.

State

The administrative state of the bandwidth profile. The allowed values are:

- Enabled: The bandwidth profile enabled.
- Disabled: The bandwidth profile is disabled.

Type

The policer type of the bandwidth profile. The allowed values are:

- MEF: MEF ingress bandwidth profile.
- Single: Single bucket policer.

Policer Mode

The colour mode of the bandwidth profile. The allowed values are:

- Coupled: Colour-aware mode with coupling enabled.
- Aware: Colour-aware mode with coupling disabled.

Rate Type

The rate type of the bandwidth profile. The allowed values are:

- Data: Specify that this bandwidth profile operates on data rate.
- Line: Specify that this bandwidth profile operates on line rate.

CIR

The Committed Information Rate of the bandwidth profile. The allowed range is from 0 through 10000000 kilobit per second.

CBS

The Committed Burst Size of the bandwidth profile. The allowed range is from 0 through 100000 bytes.

EIR

The Excess Information Rate for MEF type bandwidth profile. The allowed range is from 0 through 10000000 kilobit per second.

EBS

The Excess Burst Size for MEF type bandwidth profile. The allowed range is from 0 through 100000 bytes.

Buttons

Refresh: Refresh the displayed table starting from the input fields.

|<<: Updates the table, starting with the first entry in the table.

<<: Updates the table, ending at the entry before the first entry currently displayed.

>>: Updates the table, starting with the entry after the last entry currently displayed.

>>|: Updates the table, ending at the last entry in the table.

Save: Click to save changes.

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

5.6.4 EVCs Configuration

This page displays current EVC configurations. On this system, only Provider Bridge based EVCs are supported.

EVC ID

The EVC ID identifies the EVC. The range is from 1 through 256.

Name

The name for the EVC.

VID

The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The range is from 1 through 4095.

IVID

The Internal/classified VLAN ID in the PB network. The range is from 1 through 4095.

Learning

The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports. Possible values are:

- Enabled: Learning is enabled (MAC addresses are learned).
- Disabled: Learning is disabled (MAC addresses are not learned).

Inner Tag Type

The inner tag type is used to determine whether an inner tag is inserted in frames forwarded to NNI ports. Possible values are:

- None: An inner tag is not inserted.
- C-tag: An inner C-tag is inserted.
- S-tag: An inner S-tag is inserted.
- S-custom-tag: An inner tag is inserted and the tag type is determined by the VLAN port configuration of the NNI.

Inner Tag VID Mode

The inner VID Mode affects the VID in the inner and outer tag. Possible values are:

- Normal: The VID of the two outer tags aren't swapped.
- Tunnel: The VID of the two outer tags are swapped, so that the VID of the outer tag is taken from the Inner Tag configuration and the VID of the inner tag is the EVC VID. In this mode, the NNI ports are normally configured to do EVC classification based on the inner tag.

Inner Tag VID

The Inner tag VLAN ID. The allowed range is from 0 through 4095.

Inner Tag PCP/DEI Preservation

The inner tag PCP and DEI preservation. Possible values are:

- Preserved: The inner tag PCP and DEI is preserved.
- Fixed: The inner tag PCP and DEI is fixed.

Inner Tag PCP

The inner tag PCP value. The allowed range is from 0 through 7.

Inner Tag DEI

The inner tag DEI value. The allowed value is 0 or 1.

Outer Tag VID

The EVC outer tag VID for UNI ports. The allowed range is from 0 through 4095.

NNI Ports

The list of Network to Network Interfaces for the EVC.

Modification Buttons

You can modify each EVC in the table using the following buttons:

ⓔ:Edit the EVC entry.

ⓧ:Delete the EVC entry.

⊕:Add new EVC entry.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

Remove all: Click to remove all EVCs.

This page displays current EVC configurations. The settings can also be configured here.

NNI Ports

The list of Network to Network Interfaces for the EVC.

EVC ID

The EVC ID identifies the EVC. The allowed range is from 1 through 256.

Name

The name for the EVC. It is case sensitive and can contain up to 256 characters combination of alphanumeric and special characters.

VID

The VLAN ID in the PB network. It may be inserted in a C-tag, S-tag or S-custom tag depending on the NNI port VLAN configuration. The allowed range is from 1 through 4095.

IVID

The Internal/classified VLAN ID in the PB network. The allowed range is from 1 through 4095.

Learning

The learning mode for the EVC controls whether source MAC addresses are learned for frames matching the EVC. Learning may be disabled if the EVC only includes two UNI/NNI ports. Possible values are:

- Enabled: Learning is enabled (MAC addresses are learned).
- Disabled: Learning is disabled (MAC addresses are not learned).

Inner Tag

Type

The inner tag type is used to determine whether an inner tag is inserted in frames forwarded to NNI ports. Possible values are:

- None: An inner tag is not inserted.
- C-tag: An inner C-tag is inserted.
- S-tag: An inner S-tag is inserted.
- S-custom-tag: An inner tag is inserted and the tag type is determined by the VLAN port configuration of the NNI.

VID Mode

The inner VID Mode affects the VID in the inner and outer tag. Possible values are:

- Normal: The VID of the two outer tags aren't swapped.
- Tunnel: The VID of the two outer tags are swapped, so that the VID of the outer tag is taken from the Inner Tag configuration and the VID of the inner tag is the EVC VID. In this mode, the NNI ports are normally configured to do EVC classification based on the inner tag.

VLAN ID

The Inner tag VLAN ID. The allowed range is from 1 through 4095.

PCP/DEI Preservation

The inner tag PCP and DEI preservation. Possible values are:

- Preserved: The inner tag PCP and DEI is preserved.
- Fixed: The inner tag PCP and DEI is fixed.

PCP

The inner tag PCP value. The allowed range is from 0 through 7.

DEI

The inner tag DEI value. The allowed value is 0 or 1.

Outer Tag

VLAN ID

The EVC outer tag VID for UNI ports. The allowed range is from 1 through 4095.

Buttons

Save: Click to save changes.

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

Cancel: Return to the previous page; any changes made locally will be undone.

5.6.5 ECEs Configuration

This page displays the current EVC Control Entries (ECEs). The settings can also be configured here.

ECE ID

The ECE ID identifies the ECE. Unique ECE IDs are automatically assigned to ECEs added. The possible range is from 1 through 256.

Ingress Matching

UNI Ports

The list of User Network Interfaces for the ECE.

Tag Type

The tag type for the ECE. Possible values are:

- Any: The ECE will match both tagged and untagged frames.
- Untagged: The ECE will match untagged frames only.
- C-Tagged: The ECE will match custom tagged frames only.
- S-Tagged: The ECE will match service tagged frames only.
- Tagged: The ECE will match tagged frames only.

VID

The VLAN ID for the ECE. It only significant if tag type 'Tagged' is selected. Possible values are:

- Specific: The range is from 0 through 4095.
- Any: The ECE will match any VLAN ID.

PCP

The PCP value for the ECE. It only significant if tag type 'Tagged' is selected. Possible values are:

- Specific: The ECE will match a specific PCP in the range 0 through 7.

- Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.
- Any: The ECE will match any PCP value.

DEI

The DEI value for the ECE. It only significant if tag type 'Tagged' is selected. The possible values is: 0, 1 or Any.

Frame Type

The frame type for the ECE. Possible values are:

- Any: The ECE will match any frame type.
- IPv4: The ECE will match IPv4 frames only.
- IPv6: The ECE will match IPv6 frames only.

Actions

Direction

The EVCs and ECEs are used to setup flows in one or both directions as determined by the ECE Direction parameter. If the ECE is bidirectional, the ingress rules of the NNI ports will be setup to match the traffic being forwarded to NNI ports. Possible values are:

- Both: Bidirectional.
- UNI-to-NNI: Unidirectional from UNI to NNI.
- NNI-to-UNI: Unidirectional from NNI to UNI.

EVC ID

The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. Possible values are:

- Specific: The range is from 1 through 256.
- None: The ECE does not map to an EVC.

Tag Pop Count

The ingress tag pop count for the ECE. The possible range is from 0 through 2.

Policy ID

The ACL Policy ID for the ECE. The range is from 0 through 255.

Class

The traffic class for the ECE. The range is from 0 through 7.

Egress Outer Tag

Mode

The outer tag for nni-to-uni direction for the ECE. Possible values are:

- Enable: Enable outer tag for nni-to-uni direction for the ECE.

- Disable: Disable outer tag for nni-to-uni direction for the ECE.

PEC/DEI Preservation

The outer tag PCP and DEI preservation for the ECE. Possible values are:

- Preserved: The outer tag PCP and DEI are preserved.
- Fixed: The outer tag PCP and DEI are fixed.

PCP

The outer tag PCP value for the ECE. The possible range is from 0 through 7.

DEI

The outer tag DEI value for the ECE. The possible value is 0 or 1.

Conflict

Indicates the hardware status of the specific ECE. The specific ECE is not applied to the hardware due to hardware limitations.

Modification Buttons

You can modify each ECE (EVC Control Entry) in the table using the following buttons:

⊕: Inserts a new ECE before the current row.

ⓔ: Edits the ECE row.

⬆: Moves the ECE up the list.

⬇: Moves the ECE down the list.

⊗: Deletes the ECE.

⊕: The lowest plus sign adds a new entry at the bottom of the ECE listings.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

Remove all: Click to remove all ECEs.

This page displays current ECE configurations. The settings can also be configured here.

UNI Ports

The list of User Network Interfaces for the ECE.

Ingress Matching

Tag Type

The tag type for matching the ECE. Possible values are:

- Any: The ECE will match both tagged and untagged frames.
- Untagged: The ECE will match untagged frames only.
- C-Tagged: The ECE will match custom tagged frames only.
- S-Tagged: The ECE will match service tagged frames only.
- Tagged: The ECE will match tagged frames only.

VLAN ID Filter

The VLAN ID filter for matching the ECE. It only significant if tag type 'Tagged' is selected. Possible values are:

- Any: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)

- Specific: If you want to filter a specific VLAN ID value with this ECE, choose this value. A field for entering a specific value appears.
- Range: If you want to filter a specific VLAN ID range filter with this ECE, choose this value. A field for entering a range appears.

VLAN ID Value

When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is from 0 through 4095.

VLAN ID Range

When "Range" is selected for the VLAN ID filter, you can enter a specific range. The allowed range is from 0 through 4095.

PCP

The PCP value for matching the ECE. It only significant if tag type 'Tagged' is selected. Possible values are:

- Any: The ECE will match any PCP value.
- Specific: The ECE will match a specific PCP in the range 0 through 7.
- Range: The ECE will match PCP values in the selected range 0-1, 2-3, 4-5, 6-7, 0-3 or 4-7.

DEI

The DEI value for matching the ECE. It only significant if tag type 'Tagged' is selected. The allowed value is: 0, 1 or Any.

Frame Type

The frame type for the ECE. Possible values are:

- Any: The ECE will match any frame type.
- IPv4: The ECE will match IPv4 frames only.
- IPv6: The ECE will match IPv6 frames only.

IP Parameters

Protocol

The IP protocol for matching the ECE. Possible values are:

- Any: No protocol filter is specified. (Protocol filter status is "don't-care".)
- UDP: Specify the UDP for matching the ECE.
- TCP: Specify the TCP for matching the ECE.
- Other: If you want to filter a specific protocol value with this ECE, choose this value. A field for entering a specific value appears.

Protocol Value

When "other" is selected for the protocol filter, you can enter a specific value. The allowed value is from 0 through 255.

SIP/DIP Filter

The source/destination IP address for matching the ECE. It depends on by the port address mode, when port address mode is set to 'Source' then the field is used for source address. Similarly when port address mode is set to 'Destination' then the field is used for destination address. Possible values are:

- Any: No SIP/DIP filter is specified. (SIP/DIP filter status is "don't-care".)
- Host: When "IPv4" is selected for the Frame Type, if you want to filter a specific host address with this ECE, choose this value. A field for entering a host address appears.
- Network: When "IPv4" is selected for the Frame Type, if you want to filter a specific network address with this ECE, choose this value. Two fields for entering a specific network address and network mask appears.
- Specific: When "IPv6" is selected for the Frame Type, if you want to filter a specific network address with this ECE, choose this value. Two fields for entering a specific network address and network mask appears.

SIP/DIP Address

When "IPv4" is selected for the Frame Type and "Host" or "Network" is selected for the SIP/DIP filter, you can enter a specific host or network address. When "IPv6" is selected for the Frame Type, the field only supported 32 bits for IPv6 address.

SIP/DIP Mask

When "IPv4" is selected for the Frame Type and "Host" or "Network" is selected for the SIP/DIP filter, you can enter a specific network mask. When "IPv6" is selected for the Frame Type, the field only supported 32 bits for IPv6 address mask.

DSCP Filter

The DSCP filter for matching the ECE. Possible values are:

- Any: No DSCP filter is specified. (DSCP filter status is "don't-care".)
- Specific: If you want to filter a specific DSCP value with this ECE, choose this value. A field for entering a specific value appears.
- Range: If you want to filter a specific DSCP range filter with this ECE, choose this value. A field for entering a range appears.

DSCP Value

When "Specific" is selected for the DSCP filter, you can enter a specific value. The allowed value is from 0 through 63.

DSCP Range

When "Range" is selected for the DSCP filter, you can enter a specific range. The allowed range is from 0 through 63.

Fragment

The IPv4 Fragment for matching the ECE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. Possible values are:

- Any: The ECE will match any MF bit.
- Non-Fragment: 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.
- Fragment: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.

UDP/TCP Parameters

Source Port Filter

The TCP/UDP source port for matching the ECE. It only significant if protocol filter 'UDP' or 'TCP' is selected. Possible values are:

- Any: No TCP/UDP source port filter is specified. (Source port filter status is "don't-care".)
- Specific: If you want to filter a specific TCP/UDP source port No. Use this ECE, choose this value. A field for entering a specific No. appears.
- Range: If you want to filter a specific TCP/UDP source port range filter with this ECE, choose this value. A field for entering a range appears.

Source Port No.

When "Specific" is selected for the source port filter, you can enter a specific value. The allowed value is from 0 through 65535.

Source Port Range

When "Range" is selected for the source port filter, you can enter a specific range. The allowed range is from 0 through 65535.

Destination Port Filter

The TCP/UDP destination port for matching the ECE. It only significant if protocol filter 'UDP' or 'TCP' is selected. The possible values are:

Any: No TCP/UDP destination port filter is specified. (Destination port filter status is "don't-care").

Specific: If you want to filter a specific TCP/UDP destination port No. Use this ECE, choose this value. A field for entering a specific No. appears.

Range: If you want to filter a specific TCP/UDP destination port range filter with this ECE, choose this value. A field for entering a range appears.

Destination Port No.

When "Specific" is selected for the destination port filter, you can enter a specific value. The allowed value is from 0 through 65535.

Destination Port Range

When "Range" is selected for the destination port filter, you can enter a specific range. The allowed range is from 0 through 65535.

MAC Parameters

SMAC Filter

The source MAC address for matching the ECE. Possible values are:

- Any: No SMAC filter is specified. (SMAC filter status is "don't-care".)
- Specific: If you want to filter a specific SMAC value with this ECE, choose this value. A field for entering a specific value appears.

SMAC Value

When "Specific" is selected for the SMAC filter, you can enter a specific value. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit).

DMAC Type

The destination MAC address type for matching the ECE. Possible values are:

- Any: No DMAC type is specified. (DMAC filter status is "don't-care".)
- Unicast: Frame must be unicast.
- Multicast: Frame must be multicast.
- Broadcast: Frame must be broadcast.

Action

Direction

The EVCs and ECEs are used to setup flows in one or both directions as determined by the ECE Direction parameter. If the ECE is bidirectional, the ingress rules of the NNI ports will be setup to match the traffic being forwarded to NNI ports. Possible values are:

- Both: Bidirectional.
- UNI-to-NNI: Unidirectional from UNI to NNI.
- NNI-to-UNI: Unidirectional from NNI to UNI.

EVC ID Filter

The EVC ID for the ECE. The ECE is only active when mapping to an existing EVC. Possible values are:

- Any: No EVC ID filter is specified. (EVC ID filter status is "don't-care".)

- Specific: If you want to filter a specific EVC ID with this ECE, choose this value. A field for entering a specific value appears.

EVC ID Value

When "Specific" is selected for the VLAN ID filter, you can enter a specific value. The allowed value is from 1 through 256.

Tag Pop Count

The ingress tag pop count for the ECE. The allowed range is from 0 through 2.

Policy ID

The ACL Policy ID for the ECE for matching ACL rules. The allowed range is from 0 through 255.

Class

The traffic class for the ECE. The allowed range is from 0 through 7 or disabled.

Egress Outer Tag

Mode

The outer tag for nni-to-uni direction for the ECE. Possible values are:

- Enable: Enable outer tag for nni-to-uni direction for the ECE.
- Disable: Disable outer tag for nni-to-uni direction for the ECE.

PEC/DEI Preservation

The outer tag PCP and DEI preservation for the ECE. Possible values are:

- Preserved: The outer tag PCP and DEI is preserved.
- Fixed: The outer tag PCP and DEI is fixed.

PCP

The outer tag PCP value for the ECE. The allowed range is from 0 through 7.

DEI

The outer tag DEI value for the ECE. The allowed value is 0 or 1.

Buttons

Save: Click to save changes.

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

Cancel: Return to the previous page; any changes made locally will be undone.

5.6.6 EVC Statistics

This page provides NNI port traffic statistics for the selected EVC. It also shows counters for UNI ports of ECEs mapping to the EVC. And the MPLS Pseudo-Wires counters are included when the PW ID is attached to the selected EVC.

| ECE Statistics > | Ports Configuration | L2CP Configuration | Bandwidth Profilesn Configuration | EVCs Configuration | ECEs Configuration | EVC Statistics Monitor | Port 1 ▼ | Auto-refresh ☐ | Refresh | Clear |

Class	Green Frames		Yellow Frames		Red Frames	Discarded Frames	
	Rx	Tx	Rx	Tx	Rx	Green	Yellow
0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0

Class

The traffic class for the EVC.

Green Frames Rx

The number of green received.

Green Frames Tx

The number of green transmitted.

Yellow Frames Rx

The number of yellow received.

Yellow Frames Tx

The number of yellow transmitted.

Red Frames Rx

The number of red received.

Discarded Frames Green

The number of discarded in the green color.

Discarded Frames Yellow

The number of discarded in the yellow color.

Buttons

Port 1▼:The port select box determines which port is affected by clicking the buttons.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for the selected port.

5.7 TACACS+ Server Configuration

This page allows you to configure the TACACS+ servers.

Global Configuration

These setting are common for all of the TACACS+ servers.

Timeout

Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.

Deadtime

Deadtime, which can be set to a number between 0 to 1440 分, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

Key

The secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Server Configuration

The table has one row for each TACACS+ server and a number of columns, which are:

Delete

To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.

Hostname

The IP address or hostname of the TACACS+ server.

Port

The TCP port to use on the TACACS+ server for authentication.

Timeout

This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.

Key

This optional setting overrides the global key. Leaving it blank will use the global key.

Adding a New Server

Click "Add new server" to add a new TACACS + server. An empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported.

The "Delete" button can be used to undo the addition of the new server.

Buttons

Save: Click to save changes.

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

6 Layer 2 Protocol

6.1 MAC

6.1.1 MAC Address Table 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.

Aging Configuration

By default, dynamic entries are removed from the MAC table 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.

MAC Table Learning

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

Each port can do learning based upon the following settings:

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.

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

Delete

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

VLAN ID

The VLAN ID of the entry.

MAC Address

The MAC address of the entry.

Port Members

Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Add New Static Entry

Click to add a new entry to the static MAC table. "Add new static entry" specifies the VLAN ID, MAC address, and port members for the new entry. Click "Apply".

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.1.2 MAC Address Table Monitoring

Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Navigating the 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 "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The ⏵⏵ will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

MAC Table Columns

Type

Indicates whether the entry is a static or a dynamic entry.

MAC Address

The MAC address of the entry.

VLAN

The VLAN ID of the entry.

Port Members

The ports that are members of the entry.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.

Clear: refresh all dynamic entries.

| << |: Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.

| >> |: Updates the table, starting with the entry after the last entry currently displayed.

6.2 VlAN

VLAN is Virtual Local Area Network. VLAN is the data switching technology that logically (note: not physically) divides the LAN device into each network segment (or smaller LAN) to achieve the virtual working group (unit).

VLAN advantages mainly include:

- Port isolation. Ports in different VLAN, even in the same switch, can't intercommunicate. Such a physical switch can be used as multiple logical switches.
- Network security. Different VLAN can't directly communicate with each other, which has eradicated the insecurity of broadcast information.
- Flexible management. Changing the network user belongs to needn't to change ports or connection; only needs to change the firmware configuration.

That is, ports within the same VLAN can intercommunicate; otherwise, ports can't communicate with each other. A VLAN is identified with VLAN ID, and ports with the same VLAN ID belong to a same VLAN.

6.2.1 VLAN

Function Description

On the "Vlan-config" page, user can create VLAN and edit VLAN description.

Operation Path

Open in order: "Layer 2 Configuration > VLAN Configuration > Vlan-config".

Interface Description

Vlan configuration interface as follows:

The main element configuration description of Vlan configuration interface.

Interface Element	Description
Add	Click "Add" to add VLAN entry.
Delete	Check VLAN entry and click "delete" button to delete VLAN entry.
VLAN	VLAN ID number, value range is 1-4094.
Description	VLAN ID description, maximum 16 characters.
Untagged Port	Untagged port member to conduct untagged process to sending data frame.
Tagged Port	Tag port member to conduct tagged process to sending data frame.
Status	Status type: ● Static; ● Dynamic.

6.2.2 Access

Function Description

On the "Access Configuration" page, user can configure the port VLAN mode (access, trunk, Hybird), and port VLAN ID: PVID.

Operation Path

Open in order: "Layer 2 Configuration > VLAN Configuration > Access Configuration".

Interface Description

Access configuration interface as follow:

The main element configuration description of Access configuration interface.

Interface Element	Description
Configuration	Check the entries of Vlan value that need to be reset, click "Config" button to reset Vlan value.
Mode setting	There are three port link types that the switch supports: ● Trunk: port can belong to multiple VLAN, Trunk port can allow the messages of multiple VLANs to pass with Tag, but only allow the messages of one VLAN to transmit without tag (strip Tag) from this kind of interface. Commonly used in the connection between network devices. ● Hybrid: port can belong to multiple VLANs. Hybrid port

Interface Element	Description
	allows messages of multiple VLANs to pass with tag, and allows the messages sent from this kind of interface to configure whether the messages of some VLANs is with tag (not strip Tag) or not (strip Tag) . It could be used in the connection between network devices, as well as user devices.
Port	The corresponding port name of the device Ethernet port.
Port VLAN ID	Port Default Vlan ID, which is the default VLAN of the port. Default is 1, value range is 1-4094. Note: Each port has a PVID property, when the port receives Untag messages, it adds Tag mark on them according to PVID. When the port transmits data message with the same Tag mark as PVID, it would erase the Tag mark and then transmit the message. The PVID of all ports default to 1.

6.2.3 Trunk

Function Description

On the "Trunk configuration" page, user can configure port pvid value and tagVLAN, as well as transforming the value of Trunk type to Access or Hybrid type.

Operation Path

Open in order: "Layer 2 Configuration > VLAN Configuration > Trunk-configuration".

Interface Description

Trunk configuration interface as follows:

The main element configuration description of Trunk configuration interface:

Interface Element	Description
Configuration	Check the entries that need to be reconfigured, click "configure" to reset VLAN value.
Mode setting	Click mode setting to set the type to access or hybrid • Access: port only belongs to 1 VLAN(which is the default VLAN), all ports of the switch are Access mode by default and all PVID are 1. • Hybrid: port can belong to multiple VLANs. Hybrid port allows messages of multiple VLANs to pass with tag, and allows the messages sent from this kind of interface to configure whether the messages of some VLANs is with tag (not strip Tag) or not (strip Tag) . It could be used in the connection between network devices, as well as user devices.
Port	The corresponding port name of the device Ethernet port.
pvid	VLAN ID number, value range is 1-4094.
TagVLAN	The tagged value, an individual number or range ("-" represents range). For example: 9 or 10-15.

6.2.4　Hybrid

Function Description

On the "Hybrid Configuration" page, user can configure Hybrid relative parameters.

Operation Path

Open in order: "Layer 2 Configuration > VLAN Configuration > Hybrid Configuration".

Interface Description

Hybrid configuration interface as follow:

The main element configuration description of Hybrid configuration interface.

Interface Element	Description
Configuration	Check the entries that need to be reconfigured, click "configure" to reset VLAN value.
Mode setting	Click mode setting to set the type to access or trunk ● Access: port only belongs to 1 VLAN(which is the default VLAN), all ports of the switch are Access mode by default and all PVID are 1. ● Trunk: port can belong to multiple VLAN, Trunk port can allow the messages of multiple VLANs to pass with Tag, but only allow the messages of one VLAN to transmit without tag (strip Tag) from this kind of interface. Commonly used in the connection between network devices.
Port	The corresponding port name of the device Ethernet port.
pvid	VLAN ID number, value range is 1-4094.
untagVLAN	The untagged value, an individual number or range ("-" represents range). For example: 9 or 10-15
tagVLAN	The tagged value, an individual number or range ("-" represents range). For example: 9 or 10-15

Process for Port Receiving and Sending Message

Interface type	Process for Receiving Untagged Message	Process for Receiving Tagged Message	The process of transmit frame
Access		● Receive the	Strip the PVID Tag of the

Interface type	Process for Receiving Untagged Message	Process for Receiving Tagged Message	The process of transmit frame
interface	Receive this message and tag it with default VLAN ID.	message when the VLAN ID is the same as default VLAN ID. • Discard the message when the VLAN ID is different from the default VLAN ID.	message first, then transmit it.
Trunk interface		• Receive this message when the VLAN ID is in the list of VLAN ID that allow to pass through the interface. • Discard this message when the VLAN ID is not in the list of VLAN ID that allow to pass through the interface.	• When the VLAN ID is the same as the default VLAN ID, and it is the VLAN ID allowed to pass through the interface, it would strip the Tag and send this message. • When the VLAN ID is different from the default VLAN ID, and it's the VLAN ID allowed to pass through the interface, it would remain its original Tag and send the message.
Hybrid interface			When the VLAN ID is the one allowed to pass through the interface, it would send this message. It could be set to whether to carry Tag

Interface type	Process for Receiving Untagged Message	Process for Receiving Tagged Message	The process of transmit frame
			during transmission.

6.3   DHCP Server

6.3.1   Mode Setting

This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN.

Global Mode

Configure operation mode to enable/disable DHCP server per system.

Mode

Configure the operation mode per system. Possible modes are:

- Enabled: Enable DHCP server per system.
- Disabled: Disable DHCP server per system.

VLAN Mode

Configure operation mode to enable/disable DHCP server per VLAN.

VLAN Range

Indicate the VLAN range in which DHCP server is enabled or disabled. The first VLAN ID must be smaller than or equal to the second VLAN ID. BUT, if the VLAN range contains only 1 VLAN ID, then you can just input it into either one of the first and second VLAN ID or both.

On the other hand, if you want to disable existed VLAN range, then you can follow the steps.

1Click to add new VLAN range "Add Vlan range".

2Input the VLAN range that you want to disable.

3Choose Mode to be disabled.

4Press "Save" to apply the change.

Then, you will see the disabled VLAN range is removed from the DHCP Server mode configuration page.

Mode

Indicate the operation mode per VLAN. Possible modes are:

Enabled: Enable DHCP server per VLAN.

Disabled: Disable DHCP server per VLAN.

Buttons

Add VLAN range: click to add new VLAN range.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.3.2   Reserve IP configuration

This page configures excluded IP addresses. DHCP server will not allocate these excluded IP addresses to DHCP client.

Excluded IP Address

Configure excluded IP addresses.

IP Range

Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. BUT, if the IP range contains only 1 excluded IP, then you can just input it to either one of the first and second excluded IP or both.

Buttons

Add IP range: Click to add a new excluded IP range.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.3.3 DHCP Pool Configuration

This page manages DHCP pools. According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client.

Pool Setting

Add or delete pools.

Adding a pool and giving a name is to create a new pool with "default" configuration. If you want to configure all settings including type, IP subnet mask and lease time, you can click the pool name to go into the configuration page.

Name

Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page.

Type

Display which type of the pool is.

Network: the pool defines a pool of IP addresses to service more than one DHCP client.

Host: the pool services for a specific DHCP client identified by client identifier or hardware address.

If "-" is displayed, it means not defined.

IP

Display network number of the DHCP address pool.

If "-" is displayed, it means not defined.

Subnet Mask

Display subnet mask of the DHCP address pool.

If "-" is displayed, it means not defined.

Lease Time

Display lease time of the pool.

Buttons

Add new address pool: click to add a DHCP pool.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.3.3.1   DHCP Pool Configuration

This page configures all settings of a DHCP pool.

DHCP Pool Configuration		
Pool		
Name	test ▼	
Setting		
Pool Name	test	
Type	None ▼	
IP		
Subnet Mask		
Lease Time	1	days (0-365)
	0	hours (0-23)
	0	minutes (0-59)
Domain Name		
Broadcast Address		
Default Router	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
DNS Server	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
NTP Server	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
NetBIOS Node Type	None ▼	
NetBIOS Scope		
NetBIOS Name Server	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
NIS Domain Name		
NIS Server	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
	0.0.0.0	
Client Identifier	None ▼	
Hardware Address		
Client Name		
Vendor 1 Class Identifier		
Vendor 1 Specific Information		
Vendor 2 Class Identifier		
Vendor 2 Specific Information		
Vendor 3 Class Identifier		
Vendor 3 Specific Information		
Vendor 4 Class Identifier		
Vendor 4 Specific Information		
Pool Option 66		
Pool Sname		
Pool File (67)		

Save   Reset

Pool

Select a pool to configure the settings.

Name

Select a pool by pool name.

Setting

Configure pool settings.

Name

Display the selected pool name.

Type

Specify which type of the pool is.

Network: the pool defines a pool of IP addresses to service more than one DHCP client.

Host: the pool services for a specific DHCP client identified by client identifier or hardware address.

IP

Specify network number of the DHCP address pool.

Subnet Mask

DHCP option 1.

Specify subnet mask of the DHCP address pool.

Lease Time

DHCP option 51, 58 and 59.

Specified Lease Time. Allow the client to request a lease time for the IP address. If all are 0's, then it means the lease time is infinite.

Domain Name

DHCP option 15.

Specify domain name that client should use when resolving hostname via DNS.

Broadcast Address

DHCP option 28.

Specify the broadcast address in use on the client's subnet.

Default Router

DHCP option 3.

Specify a list of IP addresses for routers on the client's subnet.

DNS Server

DHCP option 6.

Specify a list of Domain Name System name servers available to the client.

NTP Server

DHCP option 42.

Specify a list of IP addresses indicating NTP servers available to the client.

NetBIOS Node Type

DHCP option 46.

Specify NetBIOS node type option to allow Netbios over TCP/IP clients which are configurable to be configured as described in RFC 1001/1002.

NetBIOS Scope

DHCP option 47.Specify the NetBIOS over TCP/IP scope parameter for the client as specified in RFC 1001/1002.

NetBIOS Name Server

DHCP option44.

Specify a list of NBNS name servers listed in order of preference.

NIS Domain Name

DHCP option 40. Specify the name of NIS domain of the client.

NIS Server

DHCP option41.

Specify a list of IP addresses indicating NIS servers available to the client.

Client Identifier

DHCP option61.

Specify client's unique identifier to be used when the pool is the type of host.

Hardware Address

Specify client's hardware(MAC) address to be used when the pool is the type of host.

Client Name

DHCP option 12.

Specify the name of client to be used when the pool is the type of host.

Vendor / Class Identifier

DHCP option 60.Specify to be used by DHCP client to optionally identify the vendor type and configuration of a DHCP client. DHCP server will deliver the corresponding option 43 specific information to the client that sends option 60 vendor class identifier.

Vendor / Specific Information

DHCP option 43.

Specify vendor specific information according to option 60 vendor class identifier.

Pool Option 66

Server address is used to specify the domain name of the TFTP server assigned to the client.

Pool Sname

TFTP server address specifies the address of the TFTP server assigned to the client.

Pool File （67）

Set boot filename option to specify the boot filename assigned to the client.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.3.4 Statistics Monitoring

DHCP Server Statistics

This page displays the database counters and the number of DHCP messages sent and received by DHCP server.

Database Counters

Display counters of various databases.

Pool

Number of pools.

Excluded IP Address

Number of excluded IP address ranges.

Declined IP Address

Number of declined IP addresses.

Binding Counters

Display counters of various databases.

Automatic Binding

Number of bindings with network-type pools.

Manual Binding

Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type.

Expired Binding

Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.

DHCP Message Received Counters

Display counters of DHCP messages received by DHCP server.

DISCOVER

Number of DHCP DISCOVER messages received.

REQUEST

Number of DHCP REQUEST messages received.

DECLINE

Number of DHCP DECLINE messages received.

RELEASE

Number of DHCP RELEASE messages received.

INFORM

Number of DHCP INFORM messages received.

DHCP Message Sent Counters

Display counters of DHCP messages sent by DHCP server.

OFFER

Number of DHCP OFFER messages sent.

ACK

Number of DHCP ACK messages sent.

NAK

Number of DHCP NAK messages sent.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Click to clear DHCP Message Received Counters and DHCP Message Sent Counters.

6.3.5 Binding Monitoring

DHCP Server Binding IP

This page displays bindings generated for DHCP clients.

DHCP Server Binding IP >	Mode Configuration	Excluded IP Configuration	Pool Configuration	Statistics Monitor	Binding Monitor	Declined IP Monitor	Auto-refresh ☐	Refresh	Clear Selected	Clear Automatic	Clear Manual	Clear Expired
Binding IP Address												
Delete	IP	Type	State	Pool Name	Server ID							

Binding IP Address

Display all bindings.

IP

IP address allocated to DHCP client.

Type

Type of binding. Possible types are Automatic, Manual, Expired.

Status

State of binding. Possible states are Committed, Allocated, Expired.

Pool Name

The pool that generates the binding.

Server ID

Server IP address to service the binding.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear selected: click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is Expired, then it is freed.

Clear Automatic: Click to clear all automatic bindings and change them to expired bindings.

Clear Manual: Click to clear all manual bindings and change them to expired bindings.

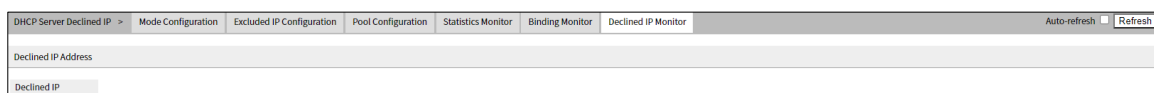Clear Expired: Click to clear all expired bindings and free them.

6.3.6 Conflict Monitoring

DHCP Server Declined IP

This page displays declined IP addresses.

Declined IP Addresses

Display IP addresses declined by DHCP clients.

DHCP Server Declined IP >	Mode Configuration	Excluded IP Configuration	Pool Configuration	Statistics Monitor	Binding Monitor	Declined IP Monitor	Auto-refresh ☐ Refresh
Declined IP Address							
Declined IP							

Declined IP

List of IP addresses declined.

Buttons

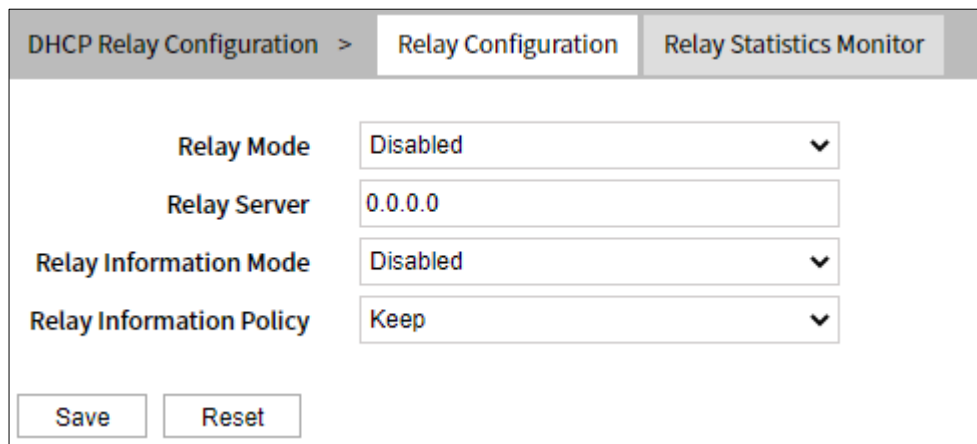Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

6.4 DHCP Relay

6.4.1 Relay Configuration

A DHCP relay agent is used to forward and to transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such

condition, please make sure the switch configuration of VLAN interface IP address and PVID (Port VLAN ID) correctly.

DHCP Relay Configuration >	Relay Configuration	Relay Statistics Monitor

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

Save   Reset

Relay Mode

Indicates the DHCP relay mode operation.

Possible modes are:

- Enabled: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.
- Disabled: Disable DHCP relay mode operation.

Relay Server

Indicates the DHCP relay server IP address.

Relay Information Mode

Indicates the DHCP relay information mode option operation. The option 82 circuit ID format as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID(in standalone device it always equal 0, in stackable device it means switch ID), and the last two characters are the port number. For example, "00030108" means the DHCP message receive form VLAN ID 3, switch ID 1, port No 8. And the option 82 remote ID value is equal the switch MAC address.

Possible modes are:

- Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes

it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.

- Disable: Disable DHCP relay information mode operation.

Relay Information Policy

Indicates the DHCP relay information option policy. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:

- Replace: Replace the original relay information when a DHCP message that already contains it is received.

- Keep: Keep the original relay information when a DHCP message that already contains it is received.

- Delete: Drop the package when a DHCP message that already contains relay information is received.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.4.2 Relay Statistics Monitoring

This page provides statistics for DHCP relay.

Server Statistics

Transmit to Server

The number of packets that are relayed from client to server.

Transmit Error

The number of packets that resulted in errors while being sent to clients.

Receive from Server

The number of packets received from server.

Receive Missing Agent Option

The number of packets received without agent information options.

Receive Missing Circuit ID

The number of packets received with the Circuit ID option missing.

Receive Missing Remote ID

The number of packets received with the Remote ID option missing.

Receive Bad Circuit ID

The number of packets whose Circuit ID option did not match known circuit ID.

Receive Bad Remote ID

The number of packets whose Remote ID option did not match known Remote ID.

Client Statistics

Transmit to Client

The number of relayed packets from server to client.

Transmit Error

The number of packets that resulted in error while being sent to servers.

Receive from Client

The number of received packets from server.

Receive Agent Option

The number of received packets with relay agent information option.

Replace Agent Option

The number of packets which were replaced with relay agent information option.

Keep Agent Option

The number of packets whose relay agent information was retained.

Drop Agent Option

The number of packets that were dropped which were received with relay agent information.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clear all statistics.

6.5 DHCP Snooping

6.5.1 Listening Configuration

Configure DHCP Snooping on this page.

Snooping Mode

Indicates the DHCP snooping mode operation. Possible modes are:

- Enabled: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

- Disabled: Disable DHCP snooping mode operation.

Port Mode Configuration

Indicates the DHCP snooping port mode. Possible port modes are:

- Trusted: Configures the port as trusted source of the DHCP messages.

- Untrusted: Configures the port as untrusted source of the DHCP messages.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.5.2 Listening Table Monitoring

This page display the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

Dynamic DHCP Snooping Table >	Snooping Configuration	Snooping Table Monitor	Auto-refresh ☐	Refresh	I<<	>>

Start from , MAC address 00-00-00-00-00-00 , VLAN 0 with 20 entries per page.

MAC Address	VLAN ID	Source Port	IP Address	IP Subnet Mask	DHCP Server

No more entries

Navigating the DHCP snooping Table

Each page shows up to 99 entries from the Dynamic DHCP snooping 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 Dynamic DHCP snooping Table.

The "MAC address" and "VLAN" input fields allows the user to select the starting point in the Dynamic DHCP snooping Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next Dynamic DHCP snooping Table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The ▢ >> will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the ▢ I<< button to start over.

DHCP snooping Table Columns

MAC Address

User MAC address of the entry.

VLAN ID

VLAN-ID in which the DHCP traffic is permitted.

Source Port

Switch Port Number for which the entries are displayed.

IP Address

User IP address of the entry.

IP Subnet Mask

User IP subnet mask of the entry.

DHCP Server Address

DHCP Server address of the entry.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Refresh the displayed table starting from the input fields.

Clear: refresh all dynamic entries.

|<< : Updates the table starting from the first entry in the Dynamic DHCP snooping Table.

>> : Updates the table, starting with the entry after the last entry currently displayed.

6.6　DHCP Detailed Statistics

This page provides statistics for DHCP snooping. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. And clear the statistics on specific port may not take effect on global statistics since it gathers the different layer overview.

Receive and Transmit Packets

Rx and Tx Discover

The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer

The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request

The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline

The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK

The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK

The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release

The number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform

The number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query

The number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned

The number of lease unassigned (option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown

The number of lease unknown (option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active

The number of lease active (option 53 with value 13) packets received and transmitted.

Rx Discarded checksum error

The number of discard packet that IP/UDP checksum is error.

Rx Discarded from Untrusted

The number of discarded packet that are coming from untrusted port.

Buttons

The DHCP user select box determines which user is affected by clicking the buttons.

The port select box determines which port is affected by clicking the buttons.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

6.7 LLDP

6.7.1 LLDP Configuration

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

LLDP Configuration >	LLDP Configuration	Neighbors Monitor	Port Statistics Monitor	

LLDP Parameters

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

LLDP Interface Configuration

			Optional TLVs				
Interface	Mode	CDP aware	Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
*	<>	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/1	Disabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/2	Disabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/3	Disabled	☐	☑	☑	☑	☑	☑
GigabitEthernet 1/4	Disabled	☐	☑	☑	☑	☑	☑
2.5GigabitEthernet 1/1	Disabled	☐	☑	☑	☑	☑	☑
2.5GigabitEthernet 1/2	Disabled	☐	☑	☑	☑	☑	☑

Save   Reset

6.7.1.1 LLDP Parameters

Send interval

The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds.

Tx Hold

Each LLDP frame contains information about how long time the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.

Tx Delay

If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds.

Tx Reinit

When a interface is disabled, LLDP is disabled or the switch is rebooted, a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

6.7.1.2   LLDP Interface Configuration

Interface

The switch interface name of the logical LLDP interface.

Mode

Select LLDP mode.

Rx only The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.

Tx only The switch will drop LLDP information received from neighbors, but will send out LLDP information.

Disabled The switch will not send out LLDP information, and will drop LLDP information received from neighbors.

Enabled The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

CDP Aware

Select CDP awareness.

The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the interface is enabled.

Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.

CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.

CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table.

CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.

CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.

Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.

If all interfaces have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one interface has CDP awareness enabled all CDP frames are terminated by the switch.

Note: When CDP awareness on an interface is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.

Port Description

Optional TLV: When checked the "port description" is included in LLDP information transmitted.

Sys Name

Optional TLV: When checked the "system name" is included in LLDP information transmitted.

Sys Descr

Optional TLV: When checked the "system description" is included in LLDP information transmitted.

Sys Capa

Optional TLV: When checked the "system capability" is included in LLDP information transmitted.

Management Address

Optional TLV: When checked the "management address" is included in LLDP information transmitted.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.7.2 Neighbor Monitoring

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

Local Interface

The interface on which the LLDP frame was received.

Chassis ID

The Chassis ID is the identification of the neighbor's LLDP frames.

Port ID

The Port ID is the identification of the neighbor port.

Port Description

Port Description is the port description advertised by the neighbor unit.

System Name

System Name is the name advertised by the neighbor unit.

System Capabilities

System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:

1other

2Repeater

3Bridge

4Wireless network node

5Router

6Telephone

7DOCSIS cable device

8Station only

9Reserved

When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).

Management Address

Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

6.7.3 Port Statistics Monitoring

This page provides an overview of all LLDP traffic.

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

Global Counters

Clear global counters

If "Clear global counters" is checked, the global counters will be cleared when is clicked.

Neighbor entries were last changed

Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the 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.

Total Neighbors Entries Dropped

Shows the number of LLDP frames dropped due to the entry table being full.

Total Neighbors Entries Aged Out

Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each interface. The columns hold the following information:

Local Interface

The interface on which LLDP frames are received or transmitted.

Tx Frames

The number of LLDP frames transmitted on the interface.

Rx Frames

The number of LLDP frames received on the interface.

Rx Errors

The number of received LLDP frames containing some kind of error.

Frames Discarded

If a LLDP frame is received on a interface, 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 interface's link is down, an LLDP shutdown frame is received, or when the entry ages out.

TLVs Discarded

Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized

The number of well-formed TLVs, but with an unknown type value.

Org. Discarded Packets

If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.

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.

Clear

If checked the counters for the specific interface are cleared when is pressed.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

Clear: Clear the counters which have the corresponding checkbox checked.

6.8　Storm Policing

Global Storm Policer Configuration

Global storm policers for the switch are configured on this page.

There is a unicast storm policer, multicast storm policer, and a broadcast storm policer.

These only affect flooding frames, that is, (VLAN ID, DMAC) paired frames do not exist in the MAC address table.

The displayed settings are:

Global Storm Policer Configuration			
Frame Type	Enable	Rate	Unit
Unicast	☐	1	fps ▼
Multicast	☐	1	fps ▼
Broadcast	☐	1	fps ▼

Save　Reset

Frame Type

The frame type for which the configuration below applies.

Enable

Enable or disable the global storm policer for the given frame type.

Rate

Controls the rate for the global storm policer. This value is restricted to 1-1024000 when "Unit" is fps, and 1-1024 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the global storm policer.

Unit

Controls the unit of measure for the global storm policer rate as fps or kfps.

Buttons

Save: Click to save changes.

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

6.9   Loop Protection

6.9.1   Loop Protection Configuration

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

General Settings

Enable Loop Protection

Controls whether loop protections is enabled (as a whole).

Transmission Time

The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds. Default value is 5 seconds.

Shutdown Time

The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart). Default value is 180 seconds.

Port Configuration

Port

The switch port number.

Enable

Controls whether loop protection is enabled on this switch port.

ACTION

Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log or Log Only.

Tx Mode

Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.9.2 Loop Protection Status

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

Loop protection port status is:

Loop Protection >	Loop Protection Configuration	Loop Protection Status	Auto-refresh ☐	Refresh

Port	Action	Tx Mode	Loops	Status	Loop	Time of Last Loop

No ports enabled

Port

The switch port number of the logical port.

ACTION

The currently configured port action.

Transmit

The currently configured port transmit mode.

Loops

The number of loops detected on this port.

Status

The current loop protection status of the port.

Loop

Whether a loop is currently detected on the port.

Time of Last Loop

The time of the last loop event detected.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to enable an automatic refresh of the page at regular intervals.

6.10   Static Aggregation

6.10.1 Aggregation Mode Configuration

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

6.10.1.1   Hash Code Contributors

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.

6.10.1.2 Aggregation Group Configuration

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.

Configured ports

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.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.10.2 Aggregation Status

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

Static AGGR >	Static Aggregation Mode Configuration	Aggregation Status Monitor	Auto-refresh ☐	Refresh

Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports

No aggregation groups

Aggregation Group Status

Aggr ID

The Aggregation ID associated with this aggregation instance.

Name

Name of the Aggregation group ID.

Type

Type of the Aggregation group(Static or LACP).

Speed

Speed of the Aggregation group.

Configured ports

Configured member ports of the Aggregation group.

Aggregated ports

Aggregated member ports of the Aggregation group.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Automatic refresh occurs every 3 seconds.

6.11 LACP

6.11.1 LACP Configuration

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

LACP >	LACP Configuration	System Status Monitor	Port Status Monitor	Port Statistics Monitor

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

Save   Reset

Port

The switch port number.

Enable

Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner.

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).

Timeout

The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.

Prio

The priority of the control port, range 1-65535. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.11.2 System Status Monitoring

This page provides a status overview for all LACP instances.

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.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Automatic refresh occurs every 3 seconds.

6.11.3 Port State Monitoring

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

| LACP > | LACP Configuration | System Status Monitor | Port Status Monitor | Port Statistics Monitor | Auto-refresh ☐ | Refresh |

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Prio
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-

Port

The switch port number.

LACP

'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other port leaves. Meanwhile it's LACP status is disabled.

Key

The key assigned to this port. Only ports with the same key can aggregate together.

Aggr ID

The Aggregation ID assigned to this aggregation group.

Partner System ID

The system ID (MAC address) of the partner.

Partner port

The partner's port number connected to this port.

Partner priority

The partner's port priority.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Automatic refresh occurs every 3 seconds.

6.11.4 Port Monitoring Statistics

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

LACP >	LACP Configuration	System Status Monitor	Port Status Monitor	Port Statistics Monitor	Auto-refresh ☐	Refresh	Clear

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0

Port

The switch port number.

LACP Received

Shows how many LACP frames have been received at each port.

LACP Transmitted

Shows how many LACP frames have been sent from each port.

Discarded

Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

6.12 Spanning Tree

6.12.1 Bridge Setting Configuration

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

6.12.1.1 Basic Settings

Protocol Version

The MSTP / RSTP / STP protocol version setting. Valid values are STP, RSTP and MSTP.

Bridge Priority

Controls the bridge priority. Lower numeric 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.

For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

Hello Time

The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds, default is 2 seconds.

Note: Changing this parameter from the default value is not recommended, and may have adverse effects on your network.

Forward Delay

The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age

The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.

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 to. Valid values are in the range 6 to 40 hops.

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.

6.12.1.2 Advanced Settings

Edge Port BPDU Filtering

Control whether a port explicitly configured as Edge will transmit and receive BPDUs.

BPDU Guard

Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

Port Error Recovery

Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

Port Error Recovery Timeout

The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.12.2 MSTI Mapping Configuration

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

6.12.2.1   Configuration Identification

Domain Name

The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

Configuration Revision

The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

6.12.2.2   MSTI Mapping

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 VLANs mapped to the MSTI. The VLANs can be given as a single (xx, xx being between 1 and 4094) VLAN, or a range (xx-yy), each of which 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.) Example: 2,5,20-40.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.12.3 MSTI Priority Configuration

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

MSTI

The Bridge Instance. The CIST is the default instance, which is always active.

Priority

Controls the bridge priority. Lower numeric 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.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.12.4 CIST Port Configuration

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

Spanning tree >	Bridge Settings Configuration	MSTI Mapping Configuration	MSTI Priorities Configuration	CIST Ports Configuration	MSTI Ports Configuration	Bridge Status Monitor	Port Status Monitor	Port Statistics Monitor

CIST Aggregated Port Configuration

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

CIST Normal Port Configuration

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

Save   Reset

This page contains settings for physical and aggregated ports.

Port

The switch port number.

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 favour 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).

operEdge (state flag)

Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.

AdminEdge

Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).

AutoEdge

Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.

Restricted Role

If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence 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.

Restricted TCN

If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect 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 the physical link state of the attached LANs transits frequently.

BPDU Guard

If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting.
A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Point-to-Point

Controls whether the port connects to a point-to-point LAN rather than to 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.

Buttons

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

6.12.5 MSTI port configuration

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

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

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

Spanning tree >	Bridge Settings Configuration	MSTI Mapping Configuration	MSTI Priorities Configuration	CIST Ports Configuration	MSTI Ports Configuration	Bridge Status Monitor	Port Status Monitor	Port Statistics Monitor

Select MSTI

MST1 ▼	Get

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 favour 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).

Buttons

Get: Click to retrieve settings for a specific MSTI.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.12.6 Bridge Status Monitoring

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

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

Spanning tree >	Bridge Settings Configuration	MSTI Mapping Configuration	MSTI Priorities Configuration	CIST Ports Configuration	MSTI Ports Configuration	Bridge Status Monitor	Port Status Monitor	Port Statistics Monitor	Auto-refresh ☐	Refresh

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last Time
		ID	Port	Cost		
CIST	32768.00-22-6F-00-66-33	32768.00-22-6F-00-66-33	-	0	Steady	-

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.

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 of this Bridge instance.

Topology Change Last

The time since last Topology Change occurred.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Spanning tree >	Bridge Settings Configuration	MSTI Mapping Configuration	MSTI Priorities Configuration	CIST Ports Configuration	MSTI Ports Configuration	Bridge Status Monitor	Port Status Monitor	Port Statistics Monitor	Auto-refresh ☐	Refresh

STP Bridge Status

Bridge Instance	CIST
Bridge ID	32768.00-22-6F-00-66-33
Root ID	32768.00-22-6F-00-66-33
Root Cost	0
Root Port	-
Regional Root	32768.00-22-6F-00-66-33
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last Time	-

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime

No ports or aggregations active

6.12.6.1 STP Bridge Status

Bridge Instance

The Bridge instance - CIST, MST1, ...

Bridge ID

The Bridge ID of this Bridge instance.

Root ID

The Bridge ID of the currently elected root bridge.

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.

Regional Root

The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (For the CIST instance only).

Internal Root Cost

The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (For the CIST instance only).

Topology Flag

The current state of the Topology Change Flag of this Bridge instance.

Topology Change Count

The number of times where the topology change flag has been set (during a one-second interval).

Topology Change Last

The time passed since the Topology Flag was last set.

CIST Ports & Aggregations State

6.12.6.2 CSTI port and aggregation state

Port

The switch port number.

Port ID

The port id as used by the STP protocol. This is the priority part and the logical port index of the bridge port.

Role

The current STP port role. The port role can be one of the following values: Alternate Port, Backup Port, Root Port, Designated Port.

Status

The current STP port state. The port state can be one of the following values: Discarding Learning Forwarding.

Cost

The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value.

Edge

The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.

Point-to-Point

The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.

Uptime

The time since the bridge port was last initialized.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

6.12.7 Port State Monitoring

This page displays the STP CIST port status for physical ports of the switch. STP port state:

Port

The switch port number.

CIST Role

The current STP port role of the CIST port. The port role can be one of the following values: Alternate Port Backup Port Root Port Designated Port.

Port Status

The current STP port state of the CIST port. The port state can be one of the following values: Discarding Learning Forwarding.

Uptime

The time since the bridge port was last initialized.

Buttons

Refresh: Click to refresh the page immediately.

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

6.12.8 Port Statistics Monitoring

This page displays the STP port statistics counters of bridge ports in the switch.

The STP port statistics counters are:

Port

The switch port number.

MSTP

The number of MSTP BPDU's received/transmitted on the port.

RSTP

The number of RSTP 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.

Buttons

Refresh: Click to refresh the page immediately.

Clear: Click to reset the counters.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

6.13 Ring

6.13.1 Ring Configuration

This page provides ring related configurations.

It provides automatic recovery and reconnection mechanism for the disconnected Ethernet network, which has link redundancy and self-recovery ability in case of network interruption or network failure.

Global Mode

Enable/Disable the Global mode.

The ring configuration only takes effect when the global mode is enabled.

Delete

Check the corresponding check box to delete an entry. It will be deleted during the next Save operation.

Groups

Support ring group 1-4, it can create 4 ring networks at the same time.

Network ID

When multiple switch devices constitute a ring network, the current ring identification of the ring is network identification; the network identifications of different ring network are different.

Type

According to the scene environment requirement, choose different ring type.

Single: Single ring, it adopts a continuous ring to connect each device together.

Couple: Coupling ring is a redundant structure proposed to connect two independent networks.

Chain: The chain, it enhances the flexibility that user builds any type of redundant network topology structure via a kind of advanced software technology.

Dual-homing: Two adjacent rings share a switch; users can carry the same switch on two different networks or two different switching devices on the same network.

Port1

The network port 1 on the switch device used to form the ring network.

Port2

The network port 2 on the switch device used to form the ring network.

Hello Time

Hello_time is the sending time interval of Hello packet; via the ring port, CPU sends information packet to adjacent device for confirming the connection is normal or not.

Master/Slave

Single ring has master/slave device option. One-Master Multi-Slave mode is recommended in one single ring. When the device is set as master device and one end of it is backup link, it can enable backup link to ensure the normal operation of the network when failure occurs in ring network.

Note:

Some products don't support Master-slave option, so their ring network is non-master station structure.

Buttons

Add new entry: Click to add a new loop entry. Specify the ID and configure the new entry. Click "Save".

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.13.2 Loop Monitoring

This page displays the ring status.

Ring >	Ring Configuration	Ring Monitor				Auto-refresh ☐	Refresh

Group ID	Network ID	Master/Slave	Port1	Port2	Port1 Statu	Port2 Status
1	1	Slave	5	6	Blocking	Blocking

Group ID

Group ID of the ring network.

Network ID

The current ring identification of the ring is network ID.

Master/Slave

Single ring has master/slave device option. One-Master Multi-Slave mode is recommended in one single ring. When the device is set as master device and one end of it is backup link, it can enable backup link to ensure the normal operation of the network when failure occurs in ring network.

Note:

Some products don't support Master-slave option, so their ring network is non-master station structure.

Port1

The network port 1 on the switch device used to form the ring network.

Port1 Status

The status of network port 1 on the switch device used to form the ring network.

Port2

The network port 2 on the switch device used to form the ring network.

Port2 Status

The status of network port 2 on the switch device used to form the ring network.

6.14 MEP

6.14.1 Maintenance Entity Point

The Maintenance Entity Point instances are configured here.

Maintenance Entity Point										Refresh
Delete	Instance	Domain	Mode	Direction	Residence Port	Level	Flow Instance	Tagged VID	This MAC	Alarm
☐	1	Port	Mep	Down	1	0		0	00-22-6F-00-66-34	🔴
☐	2	Port	Mep	Down	1	0		0	00-22-6F-00-66-34	🔴
Add New MEP	Save	Reset								

Delete

This box is used to mark a MEP for deletion in next Save operation.

Inst

The ID of the MEP. Click on the ID of a MEP to enter the configuration page. The range is from 1 through 100.

Domain

- Port: This is a MEP in the Port Domain.
- EVC: This is a MEP in the EVC Domain. 'Flow Instance' is an EVC. The EVC must be created
- VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In case of Up-MEP the VLAN must be created

Mode

- MEP: This is a Maintenance Entity End Point.
- MIP: This is a Maintenance Entity Intermediate Point.

Direction

- Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.
- Up: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'. Residence Port monitoring port

Residence Port

The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.

Level

See help on MEP create WEB.

Flow Instance

The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.

Tagged VID

- Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.
- EVC MEP: This is not used.
- VLAN MEP: This is not used.
- EVC MIP: On Serval, this is the Subscriber VID that identifies the subscriber flow in this EVC where the MIP is active.

This MAC

The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

Alarm

There is an active alarm on the MEP.

Buttons

Add new MEP: Click to add a new MEP entry.

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.14.2 MEP Configuration

This page allows the user to inspect and configure the current MEP Instance.

6.14.2.1 Instance Data

MEP Instance

The ID of the MEP.

Domain

- Port: This is a MEP in the Port Domain.
- EVC: This is a MEP in the EVC Domain. 'Flow Instance' is an EVC. The EVC must be created
- VLAN: This is a MEP in the VLAN Domain. 'Flow Instance' is a VLAN. In case of Up-MEP the VLAN must be created

Mode

- MEP: This is a Maintenance Entity End Point.
- MIP: This is a Maintenance Entity Intermediate Point.

Direction

- Down: This is a Down MEP - monitoring ingress OAM and traffic on 'Residence Port'.
- Up: This is a Up MEP - monitoring egress OAM and traffic on 'Residence Port'.

Residence Port

The port where MEP is monitoring - see 'Direction'. For a EVC MEP the port must be a port in the EVC. For a VLAN MEP the port must be a VLAN member.

Flow Instance

The MEP is related to this flow - See 'Domain'. This is not relevant and not shown in case of Port MEP.

Tagged VID

- Port MEP: An outer C/S-tag (depending on VLAN Port Type) is added with this VID. Entering '0' means no TAG added.
- EVC MEP: This is not used.
- VLAN MEP: This is not used.
- EVC MIP: On Serval, this is the Subscriber VID that identifies the subscriber flow in this EVC where the MIP is active.

This MAC

The MAC of this MEP - can be used by other MEP when unicast is selected (Info only).

6.14.2.2 Instance Configuration

EVC QoS

This is only relevant for a EVC MEP. This is the Qos of the EVC and used for getting QoS counters for Loss Measurement.

Level

See help on MEP create WEB.

Format

This is the configuration of the two possible Maintenance Association Identifier formats.
ITU ICC: Defined by ITU (Y1731 Fig. A3). 'Domain Name' is not used. 'MEG id' must be max. 13 char.
IEEE String: Defined by IEEE (802.1ag Section 21.6.5). 'Domain Name' can be max. 16 char. 'MEG id' (Short MA Name) can be max. 16 char.

ITU CC ICC: This is defined by ITU (Y1731 Fig. A5). 'Domain Name' is not used. 'MEG id' must be max. 15 char.

Domain Name

This is the IEEE Maintenance Domain Name and is only used in case of 'IEEE String' format. This string can be empty giving Maintenance Domain Name Format 1 - Not present. This can be max 16 char.

MEG Id

This is either ITU MEG ID or IEEE Short MA Name - depending on 'Format'. See 'Format'. In case of ITU ICC format this must be 13 char. In case of ITU CC ICC format this must be 15 char. In case of IEEE String format this can be max 16 char.

MEP Id

This value will become the transmitted two byte CCM MEP ID.

Tagged VID

This value will be the VID of a TAG added to the OAM PDU.

VOE

This will attempt to utilize VOE HW for MEP implementation. Not all platforms support VOE.

cLevel

Fault Cause indicating that a CCM is received with a lower level than the configured for this MEP.

cMEG

Fault Cause indicating that a CCM is received with a MEG ID different from configured for this MEP.

cMEP

Fault Cause indicating that a CCM is received with a MEP ID different from all 'Peer MEP ID' configured for this MEP.

cAIS

Fault Cause indicating that AIS PDU is received.

cLCK

Fault Cause indicating that LCK PDU is received.

cDEG

Fault Cause indicating that server layer is indicating Signal Degraded.

cSSF

Fault Cause indicating that server layer is indicating Signal Fail.

aBLK

The consequent action of blocking service frames in this flow is active.

aTSD

The consequent action of indicating Trail Signal Degrade is calculated.

aTSF

The consequent action of indicating Trail Signal Fail to-wards protection is active.

Delete

This box is used to mark a Peer MEP for deletion in next Save operation.

6.14.2.3 Peer MEP ID

This value will become an expected MEP ID in a received CCM - see 'cMEP'.

Unicast Peer MAC

This MAC will be used when unicast is selected with this peer MEP. Also this MAC is used to create HW checking of receiving CCM PDU (LOC detection) from this MEP.

cLOC

Fault Cause indicating that no CCM has been received (in 3,5 periods) - from this peer MEP.

cRDI

Fault Cause indicating that a CCM is received with Remote Defect Indication - from this peer MEP.

cPeriod

Fault Cause indicating that a CCM is received with a period different what is configured for this MEP - from this peer MEP.

cPriority

Fault Cause indicating that a CCM is received with a priority different what is configured for this MEP - from this peer MEP.

Buttons

Add new peer MEP: Click to add a new peer MEP.

6.14.2.4   Function Configuration

Continuity Check

Enable

Continuity Check based on transmitting/receiving CCM PDU can be enabled/disabled. The CCM PDU is always transmitted as Multi-cast Class 1.

Priority

The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.

Frame rate

Selecting the frame rate of CCM PDU. This is the inverse of transmission period as described in Y.1731.: This value has the following uses:

* The transmission rate of the CCM PDU.

* Fault Cause cLOC is declared if no CCM PDU has been received within 3.5 periods - see 'cLOC'.

* Fault Cause cPeriod is declared if a CCM PDU has been received with different period - see 'cPeriod'.

Selecting 300f/sec or 100f/sec will configure HW based CCM (if possible). Selecting other frame rates will configure SW based CCM. In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

TLV

Enable/disable of TLV insertion in the CCM PDU.

APS Protocol

Enable

Automatic Protection Switching protocol information transportation based on transmitting/receiving R-APS/L-APS PDU can be enabled/disabled. Must be enabled to support ERPS/ELPS implementing APS. This is only valid with one Peer MEP configured.

Priority

The priority to be inserted as PCP bits in TAG (if any).

Cast

Selection of APS PDU transmitted unicast or multi-cast. The unicast MAC will be taken from the 'Unicast Peer MAC' configuration. Unicast is only valid for L-APS - see 'Type'. The R-APS PDU is always transmitted with multi-cast MAC described in G.8032.

Type

R-APS: APS PDU is transmitted as R-APS - this is for ERPS.

L-APS: APS PDU is transmitted as L-APS - this is for ELPS.

Last Octet

This is the last octet of the transmitted and expected RAPS multi-cast MAC. In G.8031 （03/2010） a RAPS multi-cast MAC is defined as 01-19-A7-00-00-XX. In current standard the value for this last octet is '01' and the usage of other values is for further study.

6.14.2.5 TLV Configuration

Configuration of the OAM PDU TLV. Currently only TLV in the CCM is supported.

Organization Specific - OUI First

The transmitted first value in the OS TLV OUI field.

Organization Specific - OUI Second

The transmitted second value in the OS TLV OUI field.

Organization Specific - OUI Third

The transmitted third value in the OS TLV OUI field.

Organization Specific - Sub-Type

The transmitted value in the OS TLV Sub-Type field.

Organization Specific - Value

The transmitted value in the OS TLV Value field.

6.14.2.6 TLV Status

Display of the last received TLV. Currently only TLV in the CCM is supported.

CC Organization Specific - OUI First

The last received first value in the OUI field.

CC Organization Specific - OUI Second

The last received second value in the OS TLV OUI field.

CC Organization Specific - OUI Third

The last received third value in the OS TLV OUI field.

CC Organization Specific - Sub-Type

The last received value in the OS TLV Sub-Type field.

CC Organization Specific - Value

The last received value in the OS TLV Value field.

CC Organization Specific - Last RX

OS TLV was received in the last received CCM PDU.

CC Port Status - Value

The last received value in the PS TLV Value field.

CC Port Status - Last RX

PS TLV was received in the last received CCM PDU.

CC Interface Status - Value

The last received value in the IS TLV Value field.

CC Interface Status - Last RX

IS TLV was received in the last received CCM PDU.

6.14.2.7 Link State Tracking

Enable

When LST is enabled in an instance, Local SF or received 'isDown' in CCM Interface Status TLV, will bring down the residence port. Only valid in Up-MEP. The CCM rate must be 1 f/s or faster.

Buttons

Fault management: Click to enter Fault Management page.

Performance Monitoring: Click to go to Performance Monitor page.

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.14.2.8 Fault Management

This page allows the user to inspect and configure the Fault Management of the current MEP Instance.

Loop Back

Enable

Loop Back based on transmitting/receiving LBM/LBR PDU can be enabled/disabled. Loop Back is automatically disabled when all 'To Send' LBM PDU has been transmitted - waiting 5 sec. for all LBR from the end.

DEI

The DEI to be inserted as PCP bits in TAG (if any).

Priority

The priority to be inserted as PCP bits in TAG (if any).

Cast

Selection of LBM PDU transmitted unicast or multi-cast. The unicast MAC will be configured through 'Peer MEP' or 'Unicast Peer MAC'. To-wards MIP only unicast Loop Back is possible.

Peer MEP

This is only used if the 'Unicast MAC' is configured to all zero. The LBM unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Unicast MAC

This is only used if NOT configured to all zero. This will be used as the LBM PDU unicast MAC. This is the only way to configure Loop Back to-wards a MIP.

Transmitted

The number of LBM PDU to send in one loop test. The value 0 indicate infinite transmission (test behaviour). This is HW based LBM/LBR and Requires VOE.

Size

The LBM frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing LBM OAM PDU - including CRC (four bytes).

Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes

The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.

There are two frame MAX sizes to consider.

Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 9600 Bytes

CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 1526 Bytes

Consider that the Peer MEP must be able to handle the selected frame size. Consider that In case of SW based MEP, the received LBR PDU must be copied to CPU

Warning will be given if selected frame size exceeds the CPU RX frame MAX size

Frame MIN Size is 64 Bytes.

Interval

The interval between transmitting LBM PDU. In 10 ms. If   'To Send' != 0 (max 100 - '0' is as fast as possible) in 1us. If 'To Send' == 0 (max 10.000)",

Loop Back State

Transaction ID

The transaction id of the first LBM transmitted. For each LBM transmitted the transaction id in the PDU is incremented.

Transmitted

The total number of LBM PDU transmitted.

Reply MAC

The MAC of the replying MEP/MIP. In case of multicast LBM, replies from all peer MEP in the group can be received. This MAC is not shown in case of 'To Send' == 0.

Received

The total number of LBR PDU received from this 'Reply MAC'.

Out Of Order

The number of LBR PDU received from this 'Reply MAC' with incorrect 'Transaction ID'.

Link Trace

Enable

Link Trace based on transmitting/receiving LTM/LTR PDU can be enabled/disabled. Link Trace is automatically disabled when all 5 transactions are done with 5 sec. interval - waiting 5 sec. for all LTR in the end. The LTM PDU is always transmitted as Multi-cast Class 2.

Priority

The priority to be inserted as PCP bits in TAG (if any).

Peer MEP

This is only used if the 'Unicast MAC' is configured to all zero. The Link Trace Target MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Unicast MAC

This is only used if NOT configured to all zero. This will be used as the Link Trace Target MAC. This is the only way to configure a MIP as Target MAC.

Time To Live

This is the LTM PDU TTL value as described in Y.1731. This value is decremented each time forwarded by a MIP. Will not be forwarded reaching zero.

Link Trace State

Transaction ID

The transaction id is incremented for each LTM send. This value is inserted the transmitted LTM PDU and is expected to be received in the LTR PDU. Received LTR with wrong transaction id is ignored. There are five transactions in one Link Trace activated.

Time To Live

This is the TTL value taken from the LTM received by the MIP/MEP sending this LTR - decremented as if forwarded.

Mode

Indicating if is was a MEP/MIP sending this LTR.

Direction

Indicating if MEP/MIP sending this LTR is ingress/egress.

Forwarded

Indicating if MEP/MIP sending this LTR has forwarded the LTM.

Relay

The Relay action can be one of the following

MAC: The was a hit on the LT Target MAC

FDB: LTM is forwarded based on data in the Filtering DB.

MFDB: LTM is forwarded based on data in the MIP CCM DB

Last MAC

The MAC identifying the last sender of the LBM causing this LTR - initiating MEP or previous MIP forwarding.

Next MAC

The MAC identifying the next sender of the LBM causing this LTR - MIP forwarding or terminating MEP.

Test Signal

Enable

Test Signal based on transmitting TST PDU can be enabled/disabled.

DEI

The DEI to be inserted as PCP bits in TAG (if any).

Priority

The priority to be inserted as PCP bits in TAG (if any).

Peer MEP

The TST frame destination MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Rate

The TST frame transmission bit rate - in Mega bits pr. second. Limit is 400 Mbps. This is the bit rate of a standard frame without any encapsulation. If 1 Mbps rate is selected in a EVC MEP, the added tag will give a higher bitrate on the wire.

Size

The TST frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing TST OAM PDU - including CRC (four bytes).

Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes

The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.

There are two frame MAX sizes to consider.

Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of 9600 Bytes

CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of 1526 Bytes

Consider that the Peer MEP must be able to handle the selected frame size. Consider that in order to calculate the 'RX rate' a received TST PDU must be copied to CPU

Warning will be given if selected frame size exceeds the CPU RX frame MAX size

Frame MIN Size is 64 Bytes.

Pattern

The 'empty' TST PDU has the size of 12 bytes. In order to achieve the configured frame size a data TLV will be added with a pattern.

Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + TST PDU LENGTH(46) + CRC(4) = 64 bytes

The TST PDU needs to be 46 bytes so a pattern of 46-12=34 bytes will be added.

All 0: Pattern will be '00000000'

All one: Pattern will be '11111111'

10101010: Pattern will be '10101010'

184

Test Signal State

TX frame count

The number of transmitted TST frames since last 'Clear'.

RX frame count

The number of received TST frames since last 'Clear'.

RX rate

The current received TST frame bit rate in Kbps. This is calculated on a 1 s. basis, starting when first TST frame is received after 'Clear'. The frame size used for this calculation is the first received after 'Clear'

Test time

The number of seconds passed since first TST frame received after last 'Clear'.

Clear

This will clear all Test Signal State. Transmission of TST frame will be restarted. Calculation of 'Rx frame count', 'RX rate' and 'Test time' will be started when receiving first TST frame.

Client Configuration

Only a Port MEP is able to be a server MEP with flow configuration. The Priority in the client flow is always the highest priority configured in the EVC.

Domain

The domain of the client layer flow.

Inst

Client layer flow instance numbers.

Level

Client layer level - AIS and LCK PDU transmitted in this client layer flow will be on this level.

AIS Prio

The priority to be used when transmitting AIS in each client flow. Priority resulting in highest possible PCP can be selected.

LCK Prio

The priority to be used when transmitting LCK in each client flow. Priority resulting in highest possible PCP can be selected.

AIS

Enable

Insertion of AIS signal (AIS PDU transmission) in client layer flows, can be enable/disabled.

Frame Rate

Selecting the frame rate of AIS PDU. This is the inverse of transmission period as described in Y.1731.:

Protection

Selecting this means that the first 3 AIS PDU is transmitted as fast as possible - in case of using this for protection in the end point.

LOCK

Enable

Insertion of LOCK signal (LCK PDU transmission) in client layer flows, can be enable/disabled.

Frame Rate

Selecting the frame rate of LCK PDU. This is the inverse of transmission period as described in Y.1731.:

Buttons

Refresh: Click to refresh the page immediately.

Back: Click to go back to this MEP instance main page.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.14.2.9 Performance Monitoring

This page allows the user to inspect and configure the performance monitor of the current MEP Instance.

MEP Instance	Domain	Mode	Direction	Residence Port	Flow Instance	Tagged VID	EPS Instance	This MAC
2	Port	Mep	Down	1		0	0	00-22-6F-00-66-34

Instance Configuration

Level	Format	Domain Name	MEG id	MEP id	Tagged VID	Syslog	cLevel	cMEG	cMEP	cAIS	cLCK	cLoop	cConfig	cSSF	aBLK	aTSD	aTSF
0	ITU ICC		ICC000MEG0000	1	0												

Peer MEP Configuration

Delete	Peer MEP ID	Unicast Peer MAC	cLOC	cRDI	cPeriod	cPriority	cDEG

No Peer MEP Added

Add New Peer MEP

Functional Configuration

Continuity Check

Enable	Priority	Frame rate	TLV
	0	1 f/sec	

APS Protocol

Enable	Priority	Cast	Type	Last Octet
	0	Multi	L-APS	1

Fault Management   Performance Monitoring

TLV Configuratio

Organization Specific TLV (Global)

OUI First	OUI Second	OUI Third	Sub-Type	Value
0	0	12	1	2

TLV Status

Peer MEP ID	CC Organization Specific						CC Port Status		CC Interface Status	
	OUI First	OUI Second	OUI Third	Sub-Type	Value	Last RX	Value	Last RX	Value	Last RX

No Peer MEP Added

Link State Tracking

Enable

Save   Reset

Performance Monitoring Data Set
Enable

When enabled this MEP instance will contribute to the 'PM Data Set' gathered by the PM Session.

Loss Measurement
Tx

Loss Measurement initiator is enabled/disabled. Initiator is transmitting/receiving CCM or LMM/LMR or SLM/SLR/1SL PDUs - see 'Synthetic' and 'Ended'.
Service frame LM (not 'Synthetic') is only allowed with one Peer MEP configured.
Synthetic frame LM is allowed with multiple Peer MEPs configured.

Received

Enable loss calculation when receiving LM PDUs (LMM/SLM/1SL). This is ignored when LM initiator is enabled.

Priority

The priority to be inserted as PCP bits in TAG (if any). In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Priority' has to be the same.

Cast

Selection of LM PDU transmitted unicast or multicast. The unicast MAC will be taken from the 'Unicast Peer MAC' database. In case of enable of Continuity Check and dual ended Loss Measurement both implemented on SW based CCM, 'Cast' has to be the same.

Peer MEP

Peer MEP-ID for unicast LM. The MAC is taken from the 'Unicast Peer MAC' database. Only used in case of multiple peers ('Synthetic' LM).

Rate

Selecting the frame rate of LM PDU. This is the inverse of transmission period as described in Y.1731

Selecting 100f/sec is only valid in case of 'Synthetic' LM.

Selecting 6f/min is not valid in case of dual ended 'Service frame' LM (CCM PDU based).

In case of enable of Continuity Check and Loss Measurement both implemented on SW based CCM, 'Frame Rate' has to be the same.

Size

The 'Synthetic' SLM/1SL frame size. This is entered as the wanted size (in bytes) of a un-tagged frame containing LM OAM PDU - including CRC (four bytes).

Example when 'Size' = 64 => Un-tagged frame size = DMAC(6) + SMAC(6) + TYPE(2) + LBM PDU LENGTH(46) + CRC(4) = 64 bytes

The transmitted frame will be four bytes longer for each tag added - 8 bytes in case of a tunnel EVC.

There are two frame MAX sizes to consider.

Switch RX frame MAX size: The MAX frame size (all inclusive) accepted on the switch port of Bytes

CPU RX frame MAX size: The MAX frame size (all inclusive) possible to copy to CPU of Bytes

Consider that the Peer MEP must be able to handle the selected frame size. Consider that the received SLR PDU must be copied to CPU

Warning will be given if selected frame size exceeds the CPU RX frame MAX size

3onedata

Frame MIN Size is 64 Bytes.

Synthetic

Synthetic frame LM is enable. This is SLM/SLR/1SL PDU based LM.

Ended

Single: Single ended Loss Measurement implemented on LMM/LMR or SLM/SLR.

Dual: Dual ended Loss Measurement implemented on SW based CCM or 1SL.

FLR Interval

This is the interval in number of measurement intervals where the interval Frame Loss Ratio is calculated.

Meas Interval

This is the 'synthetic' LM measurement interval in milliseconds. This must be a whole number of the LM PDU transmission interval (inverse 'Rate'). This is the interval in time where the loss and FLR is calculated based on the counted number of SL OAM PDUs. It is in this interval that the calculated FLR is checked against availability, high loss and degraded FLR threshold.

For example: 'Rate' = 100f/sec => 'Meas Interval' = N*10 milliseconds.

For example: 'Rate' = 10f/sec => 'Meas Interval' = N*100 milliseconds.

In case of service frame based LM this attribute is not used and the measurement interval is always the LM PDU transmission interval.

Loss Threshold

Far end loss threshold count is incremented if a loss measurement is above this threshold.

SLM Test ID

The Test ID value to use in SLM PDUs (see G.8013, section 9.22.1). The default value is 0.

Loss Measurement State

Peer MEP

The Peer MEP ID that the following state relates to.

Tx

The accumulated transmitted LM PDUs - since last 'clear'.

Received

The accumulated received LM PDUs - since last 'clear'.

Near End Loss Count

The accumulated near end frame loss count - since last 'clear'.

Far End Loss Count

The accumulated far end frame loss count - since last 'clear'.

Interval Elapsed

The accumulated number of 'FLR Interval' elapsed - since last 'clear'.

Interval Near End Loss Ratio

The near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted - in the latest 'FLR Interval'. This is shown in (Loss/Tx)*10000. Same as 1/100 Percent.

Interval Far End Loss Ratio

The far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted - in the latest 'FLR Interval'. This is shown in (Loss/Tx)*10000. Same as 1/100 Percent.

Total Near End Loss Ratio

The near end frame loss ratio calculated based on the near end frame loss count and far end frame transmitted - since last 'clear'. This is shown in (Loss/Tx)*10000. Same as 1/100 Percent.

Total Far End Loss Ratio

The far end frame loss ratio calculated based on the far end frame loss count and near end frame transmitted - since last 'clear'. This is shown in (Loss/Tx)*10000. Same as 1/100 Percent.

Clear

Set of this check and save will clear the accumulated counters and restart ratio calculation.

Loss Measurement Availability

Enable

Enable/disable of loss measurement availability.

Interval

Availability interval - number of measurements with same availability in order to change availability state.

FLR Threshold

Availability frame loss ratio threshold in per mille.

Maintenance

Enable/disable of loss measurement availability maintenance.

Loss Measurement Availability Status

Near Avail Count

Near end availability count.

Far Avail Count

Far end availability count.

Near Unavail Count

Near end unavailability count.

Far Unavail Count

Far end unavailability count.

Near State

Near end availability state.

Far State

Far end availability state.

Loss Measurement High Loss Interval

Enable

Enable/disable of loss measurement high loss interval.

FLR Threshold

High Loss Interval frame loss ratio threshold in per mille.

Consecutive Interval

High Loss Interval consecutive interval (number of measurements).

Loss Measurement High Loss Interval Status

Near Count

Near end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold.

Far Count

Far end high loss interval count (number of measurements where availability state is available and FLR is above high loss interval FLR threshold.

Near Consecutive Count

Near end high loss interval consecutive count.

Far Consecutive Count

Far end high loss interval consecutive count.

Loss Measurement Signal Degrade

Enable

Enable/disable of loss measurement signal degrade.

TX Minimum

Minimum number of frames that must be transmitted in a measurement before frame loss ratio is tested against loss ratio threshold.

FLR Threshold

Signal Degraded frame loss ratio threshold in per mille.

Bad Threshold

Number of consecutive bad interval measurements required to set degrade state.

Good Threshold

Number of consecutive good interval measurements required to clear degrade state.

Delay Measurement

Enable

Delay Measurement based on transmitting 1DM/DMM PDU can be enabled/disabled. Delay Measurement based on receiving and handling 1DM/DMR PDU is always enabled.

Priority

The priority to be inserted as PCP bits in TAG (if any).

Cast

Selection of 1DM/DMM PDU transmitted unicast or multicast. The unicast MAC will be configured through 'Peer MEP'.

Peer MEP

This is only used if the 'Cast' is configured to Uni. The 1DM/DMR unicast MAC will be taken from the 'Unicast Peer MAC' configuration of this peer.

Ended

Single: Single ended Delay Measurement implemented on DMM/DMR.

Dual: Dual ended Delay Measurement implemented on 1DM.

Tx Mode

Standardize: Y.1731 standardize way to transmit 1DM/DMR.

Proprietary: Proprietary way with follow-up packets to transmit 1DM/DMR.

Counter

This is only used if the 'Ended' is configured to single ended.

Round trip: The frame delay calculated by the transmitting and receiving timestamps of initiators. Frame Delay = RxTimeb-TxTimeStampf

Flow: The frame delay calculated by the transmitting and receiving timestamps of initiators and remotes. Frame Delay = (RxTimeb-TxTimeStampf)-(TxTimeStampb-RxTimeStampf)

Gap

The gap between transmitting 1DM/DMM PDU in 10ms. The range is 10 to 65535.

Count

The number of last records to calculate. The range is 10 to 2000.

Unit

The time resolution.

Synchronized

Enable to use DMM/DMR packet to calculate dual ended DM. If the option is enabled, the following action will be taken. When DMR is received, two-way delay (roundtrip or flow) and both near-end-to-far-end and far-end-to-near-end one-way delay are calculated. When DMM or 1DM is received, only far-end-to-near-end one-way delay is calculated.

Counter Overflow Action

The action to counter when overflow happens.

Delay Measurement State

Tx

The accumulated transmit count - since last 'clear'.

Rx

The accumulated receive count - since last 'clear'.

Rx Timeout

The accumulated receive timeout count for two-way only - since last 'clear'.

Rx Error

The accumulated receive error count - since last 'clear'. This is counting if the frame delay is larger than 1 second or if far end residence time is larger than the round trip time.

Av Delay Tot

The average total delay - since last 'clear'.

Av Delay last N

The average delay of the last n packets - since last 'clear'.

Delay Min.

The minimum delay - since last 'clear'.

Delay Max.

The maximum delay - since last 'clear'.

Av Delay-Var Tot

The average total delay variation - since last 'clear'.

Av Delay-Var last N

The average delay variation of the last n packets - since last 'clear'.

Delay-Var Min.

The minimum delay variation - since last 'clear'.

Delay-Var Max.

The maximum delay variation - since last 'clear'.

Overflow

The number of counter overflow - since last 'clear'.

Clear

Set of this check and save will clear the accumulated counters.

Far-end-to-near-end one-way delay

The one-way delay is from remote devices to the local devices. Here are the conditions to calculate this delay. DM received by 1. 2DMM received with Synchronized enabled. 3DMR received with Synchronized enabled.

Near-end-to-far-end one-way delay

The one-way delay is from the local devices to remote devices. The only case to calculate this delay is below. DMR received with Synchronized enabled.

Delay Measurement Bins

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

Measurement Bins for FD

Configurable number of Frame Delay Measurement Bins per Measurement Interval.

The minimum number of FD Measurement Bins per Measurement Interval supported is 2.

The maximum number of FD Measurement Bins per Measurement Interval supported is 10.

The default number of FD Measurement Bins per Measurement Interval supported is 3.

Measurement Bins for IFDV

Configurable number of Inter-Frame Delay Variation Measurement Bins per Measurement Interval.

The minimum number of FD Measurement Bins per Measurement Interval supported is 2.

The maximum number of FD Measurement Bins per Measurement Interval supported is 10.

The default number of FD Measurement Bins per Measurement Interval supported is 2.

Measurement Threshold

Configurable the Measurement Threshold for each Measurement Bin.

The unit for a measurement threshold is in microseconds (us).

The default configured measurement threshold for a Measurement Bin is an increment of 5000 us.

Delay Measurement Bins for FD

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

Bin   Threshold   Range

bin0   0 us 0 us <= measurement < 5,000 us

bin1   5,000 us 5,000 us <= measurement < 10,000 us

bin2   10,000 us   10,000 us <= measurement < 15,000 us

bin3   15,000 us   15,000 us <= measurement < infinite us

Delay Measurement Bins for IFDV

A Measurement Bin is a counter that stores the number of delay measurements falling within a specified range, during a Measurement Interval.

If the measurement threshold is 5000 us and the total number of Measurement Bins is four, we can give an example as follows.

Bin	Threshold	Range
bin0	0 us	0 us <= measurement < 5,000 us
bin1	5,000 us	5,000 us <= measurement < 10,000 us
bin2	10,000 us	10,000 us <= measurement < 15,000 us
bin3	15,000 us	15,000 us <= measurement < infinite us

Buttons

Refresh: Click to refresh the page immediately.

Back: Click to go back to this MEP instance main page.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.15 ERPS

6.15.1 ERPS

The ERPS instances are configured here.

Delete

This box is used to mark an ERPS for deletion in next save operation.

ERPS ID

The ID of the created Protection group, It must be an integer value between 1 and 64. The maximum numbers of ERPS Protection Groups that can be created are 64. Click on the ID of a Protection group to enter the configuration page.

Port 0

This will create a Port 0 of the switch in the ring.

Port 1

This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance

Port 0 SF MEP

The Port 0 Signal Fail reporting MEP.

Port 1 SF MEP

The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Port 0 APS MEP

The Port 0 APS PDU handling MEP.

Port 1 APS MEP

The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Ring Type

Type of Protecting ring. It can be either major ring or sub-ring.

Interconnected Node

Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.

Virtual Channel

Sub-rings can either have virtual channel or not on the interconnected node. This is configured using "Virtual Channel" checkbox. "Yes" indicates it is a sub-ring with virtual channel. "No" indicates, sub-ring doesn't have virtual channel.

Major Ring ID

Major ring group ID for the interconnected sub-ring. It is used to send topology change updates on major ring. If ring is major, this value is same as the protection group ID of this ring.

Alarm

There is an active alarm on the ERPS.

Buttons

Add new protection group: Click to add a new protection group entry.

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

6.15.2 ERPS Configuration

The ERPS instances are configured here.

Delete

This box is used to mark an ERPS for deletion in next save operation.

ERPS ID

The ID of the created Protection group, It must be an integer value between 1 and 64. The maximum numbers of ERPS Protection Groups that can be created are 64. Click on the ID of a Protection group to enter the configuration page.

Port 0

This will create a Port 0 of the switch in the ring.

Port 1

This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance

Port 0 SF MEP

The Port 0 Signal Fail reporting MEP.

Port 1 SF MEP

The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring

instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Port 0 APS MEP

The Port 0 APS PDU handling MEP.

Port 1 APS MEP

The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Ring Type

Type of Protecting ring. It can be either major ring or sub-ring.

Interconnected Node

Interconnected Node indicates that the ring instance is interconnected. Click on the checkbox to configure this. "Yes" indicates it is an interconnected node for this instance. "No" indicates that the configured instance is not interconnected.

Buttons

Add new protection group: Click to add a new protection group entry.

Refresh: Click to refresh the page immediately.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

This page allows the user to inspect and configure the current ERPS Instance.

Instance Data

ERPS ID

The ID of the Protection group.

Port 0

This will create a Port 0 of the switch in the ring.

Port 1

This will create "Port 1" of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance

Port 0 SF MEP

The Port 0 Signal Fail reporting MEP.

Port 1 SF MEP

The Port 1 Signal Fail reporting MEP. As only one SF MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Port 0 APS MEP

The Port 0 APS PDU handling MEP.

Port 1 APS MEP

The Port 1 APS PDU handling MEP. As only one APS MEP is associated with interconnected sub-ring without virtual channel, it is configured as "0" for such ring instances. "0" in this field indicates that no Port 1 APS MEP is associated with this instance.

Ring Type

Type of Protecting ring. It can be either major ring or sub-ring.

Instance Configuration

Configured

Red: This ERPS is only created and has not yet been configured - is not active.

Green: This ERPS is configured - is active.

Guard Time

Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages.

The period of the guard timer can be configured in 10 ms steps between 10 ms and 2 seconds. The default value is 500 ms.

WTR Time

The Wait To Restore timing value to be used in revertive switching.

The period of the WTR time can be configured by the operator in 1 minute steps between 5 and 12 minutes. The default value is 5 minutes.

Hold Time

The timing value to be used to make persistent check on Signal Fail before switching.

The range of the hold off timer is 0 to 10 seconds in steps of 100 ms

Version

ERPS Protocol Version - v1 or v2

Revertive

In Revertive mode, after the conditions causing a protection switch has cleared, the traffic channel is restored to the working transport entity, i.e., blocked on the RPL.

In Non-Revertive mode, the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared.

VLAN config

VLAN configuration of the Protection Group. Click on the "VLAN Config" link to configure VLANs for this protection group.

RPL Configuration

RPL Role

It can be either RPL owner or RPL Neighbor.

RPL Port

This allows to select the east port or west port as the RPL block.

Clear

If the owner has to be changed, then the clear check box allows to clear the RPL owner for that ERPS ring.

Sub-Ring Configuration

Topology Change

Clicking this checkbox indicates that the topology changes in the sub-ring are propagated in the major ring.

Instance Command

Command

Administrative command. A port can be administratively configured to be in either manual switch or forced switch state.

Forced Switch

Forced Switch command forces a block on the ring port where the command is issued.

Manual Switch

In the absence of a failure or FS, Manual Switch command forces a block on the ring port where the command is issued.

Clear

The Clear command is used for clearing an active local administrative command (e.g., Forced Switch or Manual Switch).

Port

Port selection - Port0 or Port1 of the protection Group on which the command is applied.

Instance State

Protection State

ERPS state according to State Transition Tables in G.8032.

Port 0

OK: State of East port is ok

SF: State of East port is Signal Fail

Port 1

OK: State of West port is ok.

SF: State of West port is Signal Fail.

Transmit APS

The transmitted APS according to State Transition Tables in G.8032.

Port 0 Receive APS

The received APS on Port 0 according to State Transition Tables in G.8032.

Port 1 Receive APS

The received APS on Port 1 according to State Transition Tables in G.8032.

WTR Remaining

Remaining WTR timeout in milliseconds.

RPL Un-blocked

APS is received on the working flow.

No APS Received

RAPS PDU is not received from the other end.

Port 0 Block Status

Block status for Port 0 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.

Port 1 Block Status

Block status for Port 1 (Both traffic and R-APS block status). R-APS channel is never blocked on sub-rings without virtual channel.

FOP Alarm

Failure of Protocol Defect(FOP) status. If FOP is detected, red LED glows; else green LED glows.

Buttons

Save: Click to save changes.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Undo: Click to undo any changes made locally and revert to previously saved values.

```
ERPS VLAN Configuration  2          [ Refresh ]

  Delete  VLAN ID
    [ ]     5

  [ Add New Entry ]   [ Back ]

  [ Save ]   [ Reset ]
```

Delete

To delete a VLAN entry, check this box. The entry will be deleted during the next Save.

VLAN ID

Indicates the ID of this particular VLAN.

Adding a New VLAN

Click "Add New Entry" to add a new VLAN ID. Legal values for a VLAN ID are 1 through 4095.

The VLAN is enabled when you click on "Save". A VLAN without any port members will be deleted when you click "Save".

The "Delete" button can be used to undo the addition of new VLANs.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

Refresh: Refreshes the displayed table starting from the "VLAN ID" input fields.

7 Multicast

7.1 IGMP Snooping

7.1.1 Basic Configuration

This page provides IGMP Snooping related configuration.

Snooping Enabled

Enable the Global IGMP Snooping.

Unregistered IPMCv4 Flooding Enabled

Enable unregistered IPMCv4 traffic flooding.

The flooding control takes effect only when IGMP Snooping is enabled.

When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.

IGMP SSM Range

SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.

Assign valid IPv4 multicast address as prefix with a prefix length (from 4 to 32) for the range.

Leave Proxy Enabled

Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled

Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port

Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave

Enable the fast leave on the port.

Throttling

Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

7.1.2　VLAN Configuration

Navigating the IGMP Snooping VLAN Table

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

The "VLAN" input field allows the user to select the starting point in the VLAN Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next VLAN Table match. In addition, the two input fields will - upon a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The $\boxed{>>}$ will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the $\boxed{|<<}$ button to start over.

IGMP Snooping VLAN Table Columns

Delete

Check to delete the entry. The designated entry will be deleted during the next save.

VLAN ID

The VLAN ID of the entry.

Enable Listening

Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.

Querier Election

Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Querier Address

Define the IPv4 address as source address used in IP header for IGMP Querier election.

When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.

When the IPv4 management address is not set, system uses the first available IPv4 management address.

Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

IGMP Versions

Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network.

The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.

The default query interval is 125 seconds.

Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.

[|<<] : Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.

[>>] : Updates the table, starting with the entry after the last entry currently displayed.

Add new IGMP VLAN: Click to add new IGMP VLAN. Specify the VID and configure the new entry. Click "Save". The specific IGMP VLAN starts working after the corresponding static VLAN is also created.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

7.1.3 Status Monitoring

This page provides IGMP Snooping status.

VLAN ID

The VLAN ID of the entry.

Querier Version

Working Querier Version currently.

Host Version

Working Host Version currently.

Querier Status

Shows the Querier status is "ACTIVE" or "IDLE".

"DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted

The number of Transmitted Queries.

Queries Received

The number of Received Queries.

V1 Reports Received

The number of Received V1 Reports.

V2 Reports Received

The number of Received V2 Reports.

V3 Reports Received

The number of Received V3 Reports.

V2 Leaves Received

The number of Received V2 Leaves.

Router Port

Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both denote the specific port is configured or learnt to be a router port.

Port

The switch port number.

Status

Indicate whether specific port is a router port or not.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears all Statistics counters.

7.1.4 Group Information Monitoring

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

| IGMP Snooping > | Basic Configuration | VLAN Configuration | Status Monitor | Groups Information Monitor | IPV4 SFM Information Monitor | Auto-refresh ☐ | Refresh | Clear |

Statistics

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

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-

Navigating the IGMP Group Table

Each page shows up to 99 entries from the IGMP Group 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 IGMP Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP Group Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The [>>] will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the [|<<] button to start over.

IGMP Group Table Columns

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port Members

Ports under this group.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Refresh the displayed table starting from the input fields.

[|<<]: Updates the table, starting with the first entry in the IGMP Group Table.

>> : Updates the table, starting with the entry after the last entry currently displayed.

7.1.5 IPV4 SFM Information Monitoring

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

| IGMP Snooping > | Basic Configuration | VLAN Configuration | Status Monitor | Groups Information Monitor | IPV4 SFM Information Monitor | Auto-refresh ☐ | Refresh | I<< | >> |

Start from VLAN 1 and Group 224.0.0.0 with 20 entries per page.

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

Navigating the IGMP SFM Information Table

Each page shows up to 99 entris from the IGMP SFM Information 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 IGMP SFM Information Table.

The "Start from VLAN and Group" input fields allow the user to select the starting point in the IGMP SFM Information Table. Clicking the "Refresh" button will update the displayed table starting from that or the closest next IGMP SFM Information Table match. In addition, the two input fields will - upon a "Refresh" button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the I<< button to start over.

IGMP SFM Information Table Columns

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port

The switch port number.

Mode

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address

IP Address of the source.

Currently, the maximum number of IPv4 source address for filtering (per group) is 8. When there is no any source filtering address, the text "None" is shown in the Source Address field.

Type

Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch

Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.

Refresh: Refresh the displayed table starting from the input fields.

|<< : Updates the table starting from the first entry in the IGMP SFM Information Table.

>> : Updates the table, starting with the entry after the last entry currently displayed.

7.2　Multicast MAC

Static multicast MAC address could be added on this page.

Delete

Click the "Delete" button to delete the the current entry.

VLAN

The VLAN ID of the entry.

MAC address

The multicast MAC address of the entry, such as "01-00-5E-XX-XX-XX".

Configured ports

The ports that are members of the entry.

Buttons

Add new static entry: click to add a new static multicast MAC address entry.

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

8 PoE

8.1 Global Configuration

8.1.1 PoE Configuration

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

Reserved Power determined by

There are three modes for configuring how the ports/PDs may reserve power.

- Allocated mode: In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in

the Maximum Power fields.

- Class mode: In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode the Maximum Power fields have no effect.
- LLDP-MED mode: This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode. In this mode the Maximum Power fields have no effect

For all modes: If a port uses more power than the reserved power for the port, the port is shut down.

Power Management Mode

There are 2 modes for configuring when to shut down the ports:

- Actual consumption: In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down.
- Reserved Power: In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.

Capacitor Detection

Controls capacitor detection for legacy PD devices.

- Disabled: This feature is disabled.
- Enabled: This feature is enabled.

Power Supply Configuration

Power Source

For being able to determine the amount of power the PD may use, it must be defined what amount of power a power source can deliver.

Valid values are in the range 0 to 120 Watts.

Port Configuration

Port

This is the logical port number for this row.

Ports that are not PoE-capable are grayed out and thus impossible to configure PoE for.

PoE Mode

The PoE Mode represents the PoE operating mode for the port.

- Disable: PoE disabled for the port.
- PoE: Enables PoE IEEE 802.3af (Class 4 PDs limited to 15.4W)
- PoE+: Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 30W)

Prio

The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical.

The priority is used in the case where the remote device requires more power than the power supply can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.

Maximum Power

The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.

The maximum allowed value is 30 W.

Buttons

Save: Click to save changes.

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

8.1.2　Power Over Ethernet Status

This page allows the user to inspect the current status for all PoE ports.

Global Configuration >	POE Configuration	POE Status Monitor					Auto-refresh ☐	Refresh

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
3	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
6	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE not available - No PoE chip found
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

Local Port

This is the logical port number for this row.

PD Class

Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the PDs class.

Five Classes are defined:

- Class 0: Max. power 15.4 W
- Class 1: Max. power 4.0 W
- Class 2: Max. power 7.0 W
- Class 3: Max. power 15.4 W
- Class 4: Max. power 30.0 W

Power Requirement

The Power Requested shows the requested amount of power the PD wants to be reserved.

Power Allocated

The Power Allocated shows the amount of power the switch has allocated for the PD.

Power Used

The Power Used shows how much power the PD currently is using.

Current Used

The Power Used shows how much current the PD currently is using.

Priority

The Priority shows the port's priority configured by the user.

Port Status

The Port Status shows the port's status. The status can be one of the following values:

- PoE not available - No PoE chip found - PoE not supported for the port.
- PoE turned OFF - PoE disabled : PoE is disabled by user.
- PoE turned OFF - Power budget exceeded - The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.
- No PD detected - No PD detected for the port.
- PoE turned OFF - PD overload - The PD has requested or used more power than the port can deliver, and is powered down.
- PoE turned OFF - PD is off.
- Invalid PD - PD detected, but is not working correctly.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

8.2   PoE power delay

This page is used to set PoE power supply delay time, which can prevent the instant power supply shock when the device is powered on. After the device is powered on, the PoE port first waits for Delay Time, and then powers the PD.

PoE power delay		
Port	**Delay mode**	**Delay time(5~300 sec)**
*	<> ▼	
1	Disabled ▼	5
2	Disabled ▼	5
3	Disabled ▼	5
4	Disabled ▼	5
5	Disabled ▼	5
6	Disabled ▼	5

Save   Reset

Delay Mode

Enable Delay Mode or not, options as follows:

- Enable
- Disable

Delay Time

Delay power supply of PoE port.

Buttons

Save: Click to save changes.

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

8.3 Policy Configuration

8.3.1 Policy Configuration

When PoE scheduling rule is valid only for a certain period of time, user can set time-based scheduling configuration. Therefore, first user can configure one or more time periods, and then reference the time periods in the rule, the rule will be valid only for the specified time period.

Users that adopt the same name can configure multiple time segments with different contents. After gain the union of each cycle time period and each absolute time period, the intersection of each union will become the final valid time range.

Scheduling Configuration >	Scheduling Configuration	Poe Scheduling Bind Configuration

Scheduling Profile Configuration

Delete	Name	State	Type	Time-range

Add New Name

Save   Reset

Delete

Delete one scheduling user record.

Name

Username. This is also a link to edit a name. Click username to enter Scheduling Profile Configuration page.

On the Scheduling Profile Configuration page, user can set the following several items:

- Type: the type of scheduling policy, Periodic scheduling or Abosolute scheduling.

- PStartTime: Starting time of relative time, format: HH:MM (Hour: Minute).

- PEndtime: End time of relative time, format: HH:MM (Hour: Minute).

- PWeek: Cycle date of relative time, take one week as a cycle.

- A StartTime: Starting time of absolute time, format: HH:MM (Hour: Minute).

- A StartYear: End date of absolute time, format: YYYY-MM- DD (Year-month-day).

- A EndTime: End time of absolute time, format: HH:MM (Hour: Minute).

- A EndYear: End date of absolute time, format: YYYY-MM-DD (Year-month-day).
- Buttons
  - Save: Click to save changes.
  - Reset: Click to undo any changes made locally and revert to previously saved values.

Status

User's current status, it could be Inactive or active.

Type

The type of scheduling policy, Periodic scheduling or Abosolute scheduling.

Time-range

Plan time.

Buttons

Add New Name: Click to add new name.

Save: Click to save changes.

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

8.3.2 Policy Binding

This page can configure the port to bind PoE scheduling scheme.

Pattern

Enable Mode or not, options as follows:

- Enable
- Disable

Schduling

Select an existing scheduling scheme and bind it to the port.

8.4 Auto check

This page can automatically monitor the PoE status of the port.

Port	Ping IP Address	Startup Time	Interval Time(sec)	Retry Time	Failure Log	Failure Action	Reboot Time(sec)
*					*	<>	
1	0.0.0.0	60	30	3	error=0,total=0	Reboot Remote PD	15
2	0.0.0.0	60	30	3	error=0,total=0	Reboot Remote PD	15
3	0.0.0.0	60	30	3	error=0,total=0	Reboot Remote PD	15
4	0.0.0.0	60	30	3	error=0,total=0	Reboot Remote PD	15
5	0.0.0.0	60	30	3	error=0,total=0	Reboot Remote PD	15
6	0.0.0.0	60	30	3	error=0,total=0	Reboot Remote PD	15

Ping Check: Disabled

Poe Auto Checking

Save   Reset

Ping IP Address

Ping the IP address of the remote device.

Startup Time

Startup time (reserved, not enabled).

Interval Elapsed

Test period.

Retry Time

Retry times.

Failure log

Failure log.

Failure Action

Troubleshooting.

Reboot Time

Reboot delay.

9 Service Quality

9.1 QoS Ingress Port Classification

This page allows you to configure the basic QoS Ingress Classification settings for all switch ports.

The displayed settings are:

Port

The port number for which the configuration below applies.

CoS

Controls the default class of service.

All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS.

The classified CoS can be overruled by a QCL entry.

Note:

If the default CoS has been dynamically changed, then the actual default CoS is shown in

parentheses after the configured default CoS.

DPL

Controls the default drop precedence level.

All frames are classified to a drop precedence level.

If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL.

The classified DPL can be overruled by a QCL entry.

PCP

Controls the default PCP value.

All frames are classified to a PCP value.

If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.

DEI

Controls the default DEI value.

All frames are classified to a DEI value.

If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.

Tag Class.

Display the classification mode of label frames on this port. Display the label classification of tagged frames on this port.

- Disabled: Use default CoS and DPL for tagged frames.
- Enabled: Use mapped versions of PCP and DEI for tagged frames.

Click on the mode in order to configure the mode and/or mapping.

Note:

This setting has no effect if the port can't identify VLAN. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.

DSCP Based

Click to Enable DSCP Based QoS Ingress Port Classification.

Address Mode

The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are:

- Source: Enable SMAC/SIP matching.
- Destination: Enable DMAC/DIP matching.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

9.2 QoS Ingress Port Policers

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

The displayed settings are:

Port

The port number for which the configuration below applies.

Enable

Enable or disable the port policer for this switch port.

Rate

Controls the rate for the port policer. This value is restricted to 100-3276700 when "Unit" is kbps or fps, and 1-3276 when "Unit" is Mbps or kfps. The rate is internally rounded up to the nearest value supported by the port policer.

Unit

Controls the unit of measure for the port policer rate as kbps, Mbps, fps or kfps.

Flow Control

If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

9.3 QoS Ingress Queue Policers

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

The displayed settings are:

Port

The port number for which the configuration below applies.

Enable (E)

Enable or disable the queue policer for this switch port.

Rate

Controls the rate for the queue policer. This value is restricted to 100-3276700 when "Unit" is kbps, and 1-3276 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer.

This field is only shown if at least one of the queue policers are enabled.

Unit

Controls the unit of measure for the queue policer rate as kbps or Mbps.

This field is only shown if at least one of the queue policers are enabled.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

9.4 QoS Egress Port Schedulers

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

The displayed settings are:

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-

Port

The switch port number.

Click on the port number in order to configure the schedulers.

Mode

Shows the scheduling mode for this port.

Qn

Shows the weight for this queue and port.

9.5 QoS Egress Port Shapers

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

The displayed settings are:

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port

Port

The switch port number.

Click on the port number in order to configure the shapers.

Qn

Displaying "-"indicates disabling or actual queue setting rate, for example. "800 Mbps".

Port

Displaying "-"indicates disabled or actual port setting rate-for example. "800 Mbps".

9.6 QoS Egress Port Remarking

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

The displayed settings are:

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified

Port

The switch port number.

Click on the port number in order to configure tag remarking.

Mode

Shows the tag remarking mode for this port.

- Classified: Use classified PCP/DEI values.
- Default: Use default PCP/DEI values.
- Mapped: Use mapped versions of QoS class and DP level.

9.7 Port DSCP Configuration

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

The displayed settings are:

Port

The Port column shows the list of ports for which you can configure dscp ingress and egress settings.

Ingress

In Ingress settings you can change ingress translation and classification settings for individual ports.

There are two configuration parameters available in Ingress:

1Transformation

2Class

1Transformation

To Enable the Ingress Translation click the checkbox.

2Class

Classification for a port have 4 different values.

- Disable: No Ingress DSCP Classification.
- DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.
- Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.
- All: Classify all DSCP.

Egress

Port Egress Rewriting can be one of -

- Disable: No Egress rewrite.
- Enable: Rewrite enabled without remapping.

- Remap DP Unaware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table.

- Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

9.8 DSCP based QoS Ingress Classification

This page allows you to configure basic QoS DSCP ingress classification settings based on QoS DSCP for all switches.

The displayed settings are:

DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*	☐	<> ▾	<> ▾
0 (BE)	☐	0 ▾	0 ▾
1	☐	0 ▾	0 ▾
2	☐	0 ▾	0 ▾
3	☐	0 ▾	0 ▾
4	☐	0 ▾	0 ▾
5	☐	0 ▾	0 ▾
6	☐	0 ▾	0 ▾
7	☐	0 ▾	0 ▾
8 (CS1)	☐	0 ▾	0 ▾
9	☐	0 ▾	0 ▾
10 (AF11)	☐	0 ▾	0 ▾
11	☐	0 ▾	0 ▾
12 (AF12)	☐	0 ▾	0 ▾
13	☐	0 ▾	0 ▾
14 (AF13)	☐	0 ▾	0 ▾
15	☐	0 ▾	0 ▾
16 (CS2)	☐	0 ▾	0 ▾
17	☐	0 ▾	0 ▾
18 (AF21)	☐	0 ▾	0 ▾
19	☐	0 ▾	0 ▾
20 (AF22)	☐	0 ▾	0 ▾
21	☐	0 ▾	0 ▾
22 (AF23)	☐	0 ▾	0 ▾
23	☐	0 ▾	0 ▾
24 (CS3)	☐	0 ▾	0 ▾
25	☐	0 ▾	0 ▾
26 (AF31)	☐	0 ▾	0 ▾
27	☐	0 ▾	0 ▾
28 (AF32)	☐	0 ▾	0 ▾
29	☐	0 ▾	0 ▾
30 (AF33)	☐	0 ▾	0 ▾
31	☐	0 ▾	0 ▾
32 (CS4)	☐	0 ▾	0 ▾
33	☐	0 ▾	0 ▾
34 (AF41)	☐	0 ▾	0 ▾
35	☐	0 ▾	0 ▾
36 (AF42)	☐	0 ▾	0 ▾
37	☐	0 ▾	0 ▾
38 (AF43)	☐	0 ▾	0 ▾
39	☐	0 ▾	0 ▾
40 (CS5)	☐	0 ▾	0 ▾
41	☐	0 ▾	0 ▾
42	☐	0 ▾	0 ▾
43	☐	0 ▾	0 ▾
44	☐	0 ▾	0 ▾
45	☐	0 ▾	0 ▾
46 (EF)	☐	0 ▾	0 ▾
47	☐	0 ▾	0 ▾
48 (CS6)	☐	0 ▾	0 ▾
49	☐	0 ▾	0 ▾
50	☐	0 ▾	0 ▾
51	☐	0 ▾	0 ▾
52	☐	0 ▾	0 ▾
53	☐	0 ▾	0 ▾
54	☐	0 ▾	0 ▾
55	☐	0 ▾	0 ▾
56 (CS7)	☐	0 ▾	0 ▾
57	☐	0 ▾	0 ▾
58	☐	0 ▾	0 ▾
59	☐	0 ▾	0 ▾
60	☐	0 ▾	0 ▾
61	☐	0 ▾	0 ▾
62	☐	0 ▾	0 ▾
63	☐	0 ▾	0 ▾

[Save] [Reset]

DSCP

Maximum number of supported DSCP values are 64.

Trust

Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.

QoS Classification

QoS class value can be any of (0-7).

DPL

Drop Precedence Level (0-1).

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

9.9 DSCP Translation

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

The displayed settings are:

DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<>	☐	<>	<>
0 (BE)	0 (BE)	☐	0 (BE)	0 (BE)
1	1	☐	1	1
2	2	☐	2	2
3	3	☐	3	3
4	4	☐	4	4
5	5	☐	5	5
6	6	☐	6	6
7	7	☐	7	7
8 (CS1)	8 (CS1)	☐	8 (CS1)	8 (CS1)
9	9	☐	9	9
10 (AF11)	10 (AF11)	☐	10 (AF11)	10 (AF11)
11	11	☐	11	11
12 (AF12)	12 (AF12)	☐	12 (AF12)	12 (AF12)
13	13	☐	13	13
14 (AF13)	14 (AF13)	☐	14 (AF13)	14 (AF13)
15	15	☐	15	15
16 (CS2)	16 (CS2)	☐	16 (CS2)	16 (CS2)
17	17	☐	17	17
18 (AF21)	18 (AF21)	☐	18 (AF21)	18 (AF21)
19	19	☐	19	19
20 (AF22)	20 (AF22)	☐	20 (AF22)	20 (AF22)
21	21	☐	21	21
22 (AF23)	22 (AF23)	☐	22 (AF23)	22 (AF23)
23	23	☐	23	23
24 (CS3)	24 (CS3)	☐	24 (CS3)	24 (CS3)
25	25	☐	25	25
26 (AF31)	26 (AF31)	☐	26 (AF31)	26 (AF31)
27	27	☐	27	27
28 (AF32)	28 (AF32)	☐	28 (AF32)	28 (AF32)
29	29	☐	29	29
30 (AF33)	30 (AF33)	☐	30 (AF33)	30 (AF33)
31	31	☐	31	31
32 (CS4)	32 (CS4)	☐	32 (CS4)	32 (CS4)
33	33	☐	33	33
34 (AF41)	34 (AF41)	☐	34 (AF41)	34 (AF41)
35	35	☐	35	35
36 (AF42)	36 (AF42)	☐	36 (AF42)	36 (AF42)
37	37	☐	37	37
38 (AF43)	38 (AF43)	☐	38 (AF43)	38 (AF43)
39	39	☐	39	39
40 (CS5)	40 (CS5)	☐	40 (CS5)	40 (CS5)
41	41	☐	41	41
42	42	☐	42	42
43	43	☐	43	43
44	44	☐	44	44
45	45	☐	45	45
46 (EF)	46 (EF)	☐	46 (EF)	46 (EF)
47	47	☐	47	47
48 (CS6)	48 (CS6)	☐	48 (CS6)	48 (CS6)
49	49	☐	49	49
50	50	☐	50	50
51	51	☐	51	51
52	52	☐	52	52
53	53	☐	53	53
54	54	☐	54	54
55	55	☐	55	55
56 (CS7)	56 (CS7)	☐	56 (CS7)	56 (CS7)
57	57	☐	57	57
58	58	☐	58	58
59	59	☐	59	59
60	60	☐	60	60
61	61	☐	61	61
62	62	☐	62	62
63	63	☐	63	63

Save   Reset

DSCP

Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

Ingress

Before using DSCP to realize QoS class and DPL mapping, the DSCP at the entrance can be converted into a new DSCP.

There are two configuration parameters for DSCP mapping:

1Transformation

2Class

1Transformation

DSCP at Ingress side can be translated to any of (0-63) DSCP values.

2Class

Click to enable Classification at Ingress side.

Egress

There are the following configurable parameters for Egress side:

1Remap DP0 controls remapping of frames with DP level 0.

2Remap DP1 controls the remapping of frames through DP level 1.

1Remap DP0

Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

2Remap DP1

Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

9.10 DSCP Classification

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

The displayed settings are:

QoS Classification

Actual QoS class.

DSCP DP0

Select the classified DSCP value (0-63) for Drop Precedence Level 0.

DSCP DP1

Select the classified DSCP value (0-63) for Drop Precedence Level 1.

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

9.11 QoS Control List Configuration

QoS Control List Configuration

This page shows the QoS Control List(QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch. Click on the lowest plus sign to add a new QCE to the list.

QCE

Indicates the QCE id.

Port

Indicates the list of ports configured with the QCE or 'Any'.

DMAC

Indicates the destination MAC address. Possible values are:

- Any: Match any DMAC.
- Unicast: Match unicast DMAC.
- Multicast: Match multicast DMAC.
- Broadcast: Match broadcast DMAC.

The default value is 'Any'.

SMAC

Match specific source MAC address or 'Any'.

If a port is configured to match on destination addresses, this field indicates the DMAC.

Tag Type

Indicates tag type. Possible values are:

- Any: Match tagged and untagged frames.
- Untagged: Match untagged frames.
- Tagged: Match tagged frames.

The default value is 'Any'.

VID

Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'

PCP

Priority Code Point: Valid values of PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI

Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.

Frame Type

Indicates the type of frame. Possible values are:

- Any: Match any frame type.
- Ethernet: Match EtherType frames.
- LLC: Match (LLC) frames.
- SNAP: Match (SNAP) frames.
- IPv4: Match IPv4 frames.

- IPv6: Match IPv6 frames.

ACTION

Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.

Possible actions are:

- CoS: Classify Class of Service.
- DPL: Classify Drop Precedence Level.
- DSCP: Classify DSCP value.
- PCP: Classify PCP value.
- DEI: Classify DEI value.
- Policy: Classify ACL Policy number.

Modification Buttons

You can modify each QCE (QoS Control Entry) in the table using the following buttons:

⊕: Insert a new QCE before the current row.

ⓔ: Edit QCE.

⬆: move QCE entry up.

⬇: move QCE entry down.

⊗: delete QCE.

⊕: add new QCE entries at the bottom of the QCE list.

9.12 QoS Statistics

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

The displayed counters are:

Port

The switch port number.

Qn

There are 8 QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx

The number of received and transmitted packets per queue.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page immediately.

Clear: Clears the counters for all ports.

9.13 QCL Status

QCL Status

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

User

Indicates the QCL user.

QCE

Indicates the QCE id.

Port

Indicates the list of ports configured with the QCE.

Frame Type

Indicates the type of frame. Possible values are:

- Any: Match any frame type.
- Ethernet: Match EtherType frames.
- LLC: Match (LLC) frames.
- SNAP: Match (SNAP) frames.
- IPv4: Match IPv4 frames.
- IPv6: Match IPv6 frames.

ACTION

Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content.

Possible actions are:

- CoS: Classify Class of Service.
- DPL: Classify Drop Precedence Level.
- DSCP: Classify DSCP value.
- PCP: Classify PCP value.
- DEI: Classify DEI value.
- Policy: Classify ACL Policy number.

Conflicts

Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

Buttons

Combined: Select the QCL status from this drop down list.

Auto-refresh: Check this box to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

Resolve Conflict: Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.

Refresh: Click to refresh the page.

10 System Diagnosis

10.1 Mirroring

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

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

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

Mirror Configuration

Port to mirror to	Disabled ∨

Mirror Port Configuration

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

Save Reset

From port mirroring to

This checkbox is designed for selecting destination port.

The destination port is a switched port that you receive a copy of traffic from the source port.

Notice:

- On mirror mode, the device only supports one destination port.
- The destination port needs to disable MAC Table learning.

Port

The switch port number.

Mode

Enable/disable Mirroring function.

Configuration Guideline for All Features

When the switch is running on Remote Mirroring mode, the administrator also needs to check whether or not other features are enabled or disabled.

For example, the administrator is not disabled the MSTP on reflector port. All monitor traffic will be blocked on reflector port.

All recommended settings are described as follows.

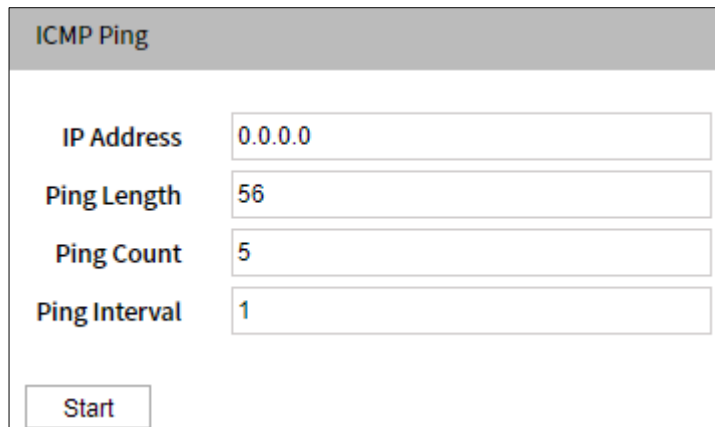|	Impact	source port	reflector port	intermediate port	destination port	Remote Mirroring VLAN
arp_inspection	High		* disabled	* disabled		
acl	Critical		* disabled	* disabled	* disabled	
dhcp_relay	High		* disabled	* disabled		
dhcp_snooping	High		* disabled	* disabled		
ip_source_guard	Critical		* disabled	* disabled	* disabled	
ipmc/igmpsnp	Critical					un-conflict
ipmc/mldsnp	Critical					un-conflict
lacp	Low				o disabled	
lldp	Low				o disabled	
mac learning	Critical		* disabled	* disabled	* disabled	
mstp	Critical		* disabled		o disabled	
mvr	Critical					un-conflict
nas	Critical		* authorized	* authorized	* authorized	
psec	Critical		* disabled	* disabled	* disabled	
qos	Critical		* unlimited	* unlimited	* unlimited	
upnp	Low				o disabled	
mac-based vlan	Critical		* disabled	* disabled		
protocol-based vlan	Critical		* disabled	* disabled		
vlan_translation	Critical		* disabled	* disabled	* disabled	
voice_vlan	Critical		* disabled	* disabled		
mrp	Low				o disabled	
mvrp	Low				o disabled	

Buttons

Save: Click to save changes.

Undo: Click to undo any changes made locally and revert to previously saved values.

10.2 Ping

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

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

After pressing "Start", ICMP packet is sent, and serial number and round trip time are displayed after receiving reply. The amount of data received in an IP packet of ICMP ECHO_REPLY type is always 8 bytes more than the requested data space (ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING server 10.10.132.20, 56 byte data.

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

Send 5 data packets, receive 5 OK, 0 bad packet

10.3 Cable Detection

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

Press "Start" to run 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. Please note that VeriPHY is only applicable to cables with a length of 7-140m.

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.

Port

The port where you are requesting VeriPHY Cable Diagnostics.

Cable Status
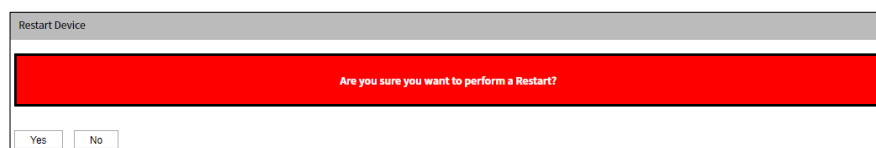
- Port:

  Switch port number.

- pair:

  The status of the cable pair.

  - OK - Correctly terminated pair

  - Open - Open pair

  - Short - Shorted pair

  - Short A - Cross-pair short to pair A

  - Short B - Cross-pair short to pair B

  - Short C - Cross-pair short to pair C

  - Short D - Cross-pair short to pair D

  - Cross A-Abnormal cross-pair coupling with pair A

- Cross B-Abnormal cross-pair coupling with pair B

- Cross C-Abnormal cross-pair coupling with pair C

- Cross D-Abnormal cross-pair coupling with pair D

- Length:

Length of cable pair (m). The resolution is 3m.

11 System Maintenance

11.1 Restart Device

You can restart the switch on this page. After restart, the switch will boot normally.

Restart Device
Are you sure you want to perform a Restart?
Yes   No
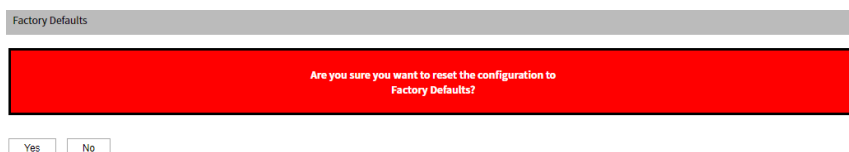
Yes: Click to restart the device.

No: Click to return to the port status page without restarting.

11.2 Factory Defaults

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

The new configuration is available immediately, which means that no restart is necessary.

Factory Defaults
Are you sure you want to reset the configuration to Factory Defaults?

Yes   No
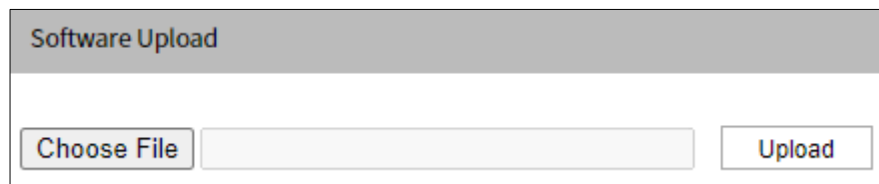
Yes: Click to reset the configuration to factory default settings.

No: Click to return to the port status page without reconfiguration.

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

11.3 Software Upload

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

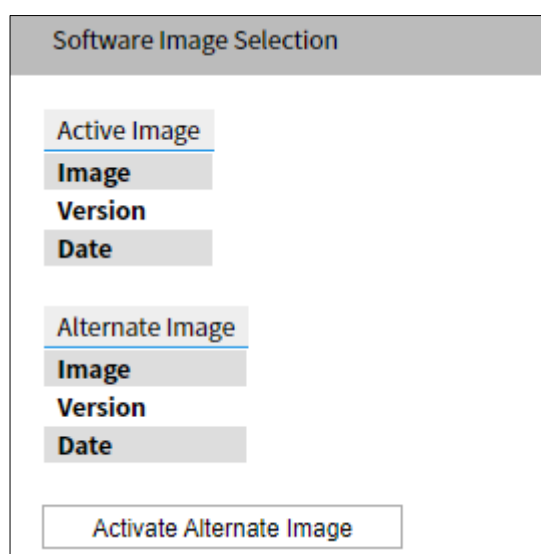Select "File" in the location of the software image, and then click "Update".

After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

Warning: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

11.4 Firmware Selection

This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

The web page displays two tables with information about the active and alternate firmware images.

Note:

- In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.
- If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
- The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

Image Information

Image

The file name of the firmware image, from when the image was last updated.

Version

The version of the firmware image.

Date

The date where the firmware was produced.

Buttons

Add alternate firmware: Click to use the alternate image. This button may be disabled depending on system state.

Cancel: Cancel activating the backup image. Navigates away from this page.

12 System Configuration

The switch stores its configuration in a number of text files in CLI format. These files are either virtual (based on ram) or stored in flash on the switch.

Available documents are:

- running-config: representing the virtual file currently configured by the activity on the switch. This file is volatile.

- startup-config: The startup configuration for the switch, read at boot time. If this file doesn't exist at boot time, the switch will start up in default configuration.

- default-config: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

- Up to 31 other files, typically used for configuration backups or alternative configurations.

12.1 Save startup-config

This will copy running-config to startup-config, thus ensuring that the currently active configuration will be used on the next restart.

Save Running Configuration to startup-config

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

Save Configuration

12.2 Download

It is possible to download any of the files on the switch to the web browser. Select the file and click "Download Configuration File".

running-config download may take some time to complete, because files must be prepared for download.

Download Configuration

Select configuration file to save.

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

File Name
◯ running-config
◯ default-config
◯ startup-config

Download Configuration

12.3 Upload

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

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

Upload Configuration

File To Upload

Choose File

Destination File

File Name	Parameters
◯ running-config	◉ Replace ◯ Merge
◯ startup-config	
◯ Create new file	

Upload Configuration

If the target is running-config, the file will be applied to the switch configuration. This can be achieved in two ways:
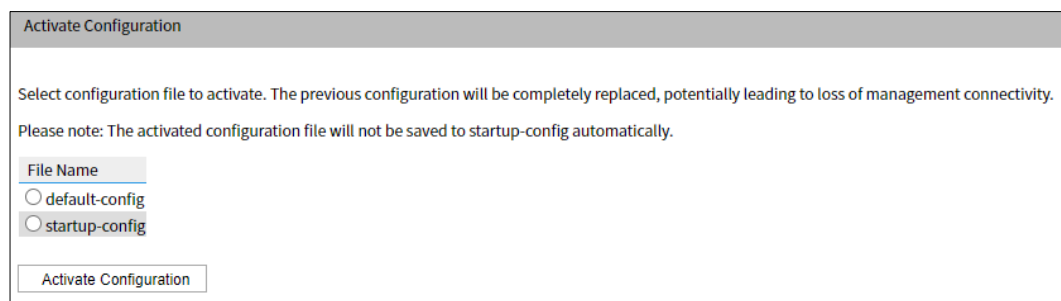
- Replace mode: the current configuration is completely replaced with the configuration in the uploaded file.

- Merge mode: the uploaded files are merged into running-config.

If the flash file system is full (that is, it contains the default configuration and 32 other files, usually including startup-config), it is impossible to create a new file. Instead an existing file must be overwritten or another file must be deleted.

12.4 Activate

You can activate any configuration file on the switch, except that running-config represents the currently active configuration.
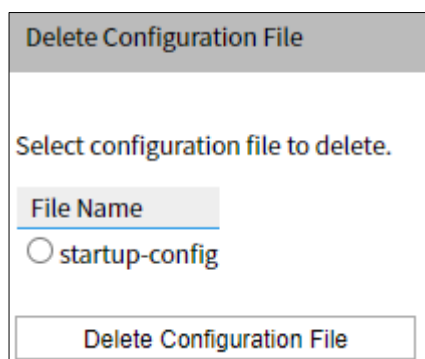
Activate Configuration

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

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

File Name
- default-config
- startup-config

[Activate Configuration]

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

12.5 Delete

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

Delete Configuration File

Select configuration file to delete.

File Name
- startup-config

[Delete Configuration File]

13 Maintenance and Service

Since the date of product delivery, our company provides 5-year product warranty. According to our company's product specification, during the warranty period, if the product exists any failure or functional operation fails, our company will repair or replace the product for users free of charge. However, the commitments above do not cover damage caused by improper usage, accident, natural disaster, incorrect operation or improper installation.

In order to ensure that consumers benefit from our company's managed switch products, consumers can get help and solutions in the following ways:

- Internet Service;
- Service Hotline;
- Product repair or replacement;

13.1 Internet Service

More useful information and tips are available via our company website.
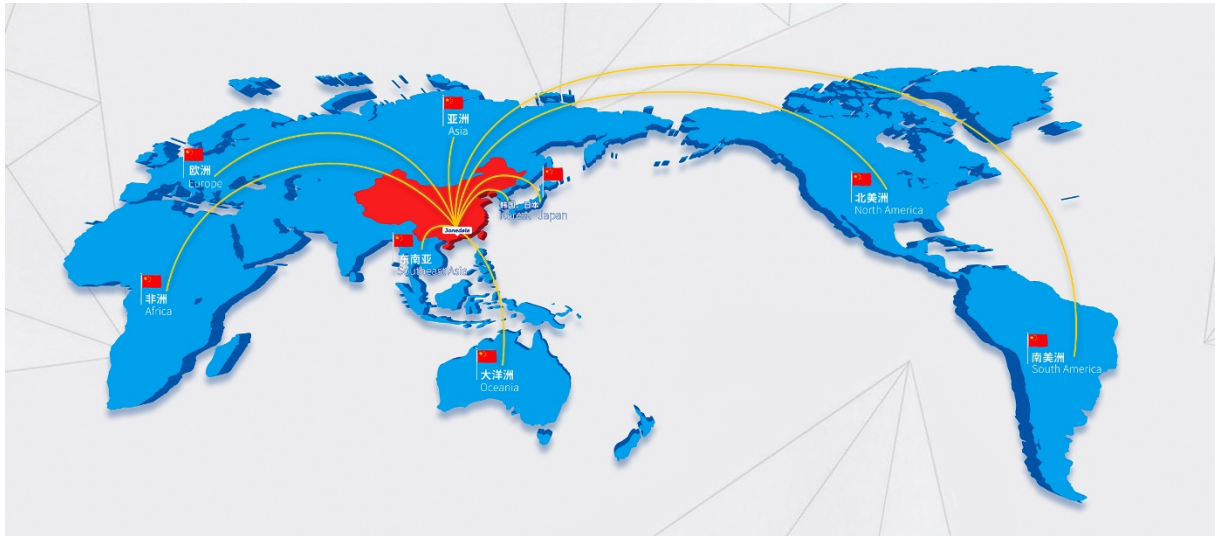Website: http://www.3onedata.com

13.2 Service Hotline

Users of our company's products could call technical support office for help. Our company has professional technical engineers to answer your questions and help you to solve the product or usage problems ASAP. Free service hotline: +86-4008804496

13.3 Product Repair or Replacement

As for the product repair, replacement or return, customers should firstly confirm with the company's technical staff, and then contact the salesmen to solve the problem. According to the company's handling procedure, customers should negotiate with our

company's technical staff and salesmen to complete the product maintenance, replacement or return.

3onedata