AVCOMM®

INDUSTRIAL AI

AVCOMM G3-8000

The 3rd Generation of 8000 series

User Manual

Graphical User Interface

Reference Products:

Product Name: The 3rd Generation of 8000 Series, Industrial Ethernet Switch, Fully Managed, PTP/TSN
Model Number: 8008TX, 8010GX2, 8012GX4, 8014GX4
Document Title: RM_GUI_EN, G3 8000_GUI_EN
Document Version: 3.2
Release Date: July, 2025

Company Information

Company Name: Avcomm Technologies, Inc.
Address: 1300 Bay Area, B229, Houston, TX 77058, United States of America
Phone: +1 713-933-4534
Email: info@avcomm.us
Website: www.avcomm.us

Technical Support

If you encounter any problems during installation or operation of this product, please contact our technical support team.
Technical Support Email: support@avcomm.us
Technical Support Phone: +1 713-933-4534
Business Hours: Monday – Friday, 08:00 – 18:00 US. Central Time

Sales Information

For product purchasing, pricing, or distributor information, please contact our sales team.
Sales Email: sales@avcomm.us
Sales Phone: +1 713-933-4534

AVCOMM®

INDUSTRIAL AI

Copyright Notice

Disclaimer

The information in this document is subject to change without notice and does not represent a commitment on the part of Avcomm Technologies, Inc.

Avcomm Technolgoies, Inc. assumes no responsibility for any errors that may appear in this document. In no event shall Avcomm Technolgoies, Inc. be liable for direct, indirect, special, incidental, or consequential damages resulting from the use of this product or the information contained in this document.

Trademarks

All trademarks, registered trademarks, and product names mentioned in this document are the property of their respective owners.

Compliance and Certifications

This product complies with applicable standards and regulations.
Certifications may include but are not limited to:
CE
FCC
RoHS
Other applicable certifications

Content

Safety Instructions

⚠ **WARNING**

UNCONTROLLED MACHINE ACTIONS

To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.

Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

About This Manual

The "RM GUI EN" reference manual contains detailed information on using the graphical user interface (web-based interface) to operate the individual functions of the device.
The manual is designed to describe configuration steps, and support for features should be based on the specific device.

Accessing Switch

Accessing the Switch Through Web

When accessing the switch through Web browser, please make sure that the applied browser complies with the following requirements:

HTML of version 4.0

HTTP of version 1.1

JavaScript^{TM} of version 1.5

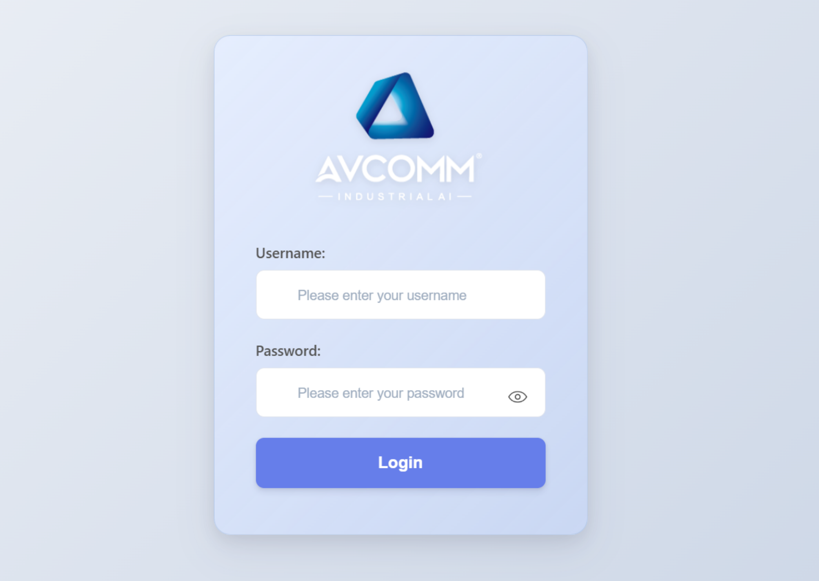
What's more, please ensure that the main program file, which is running on the switch, supports Web access and your computer has already connected to the network which the switch is located.

Note: The device webpage is only compatible with Chrome and Microsoft Edge.

Initially Accessing the Switch

When the switch is initially used, you can use the Web access without any extra settings:

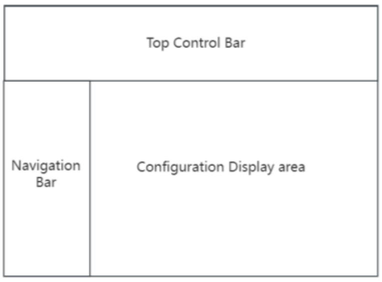
1. Modify the IP address of the network adapter and subnet mask of your computer to 192.168.2.2 and 255.255.255.0 respectively.
2. Open the Web browser and enter 192.168.2.1 in the address bar. It is noted that 192.168.2.1 is the default management address of the switch.
3. If the IE browser is used, you can see a dialog box similar to the following figure. please enter the username and the password in the ID authentication dialog box. Both the original username and the password are "admin", which is capital sensitive.



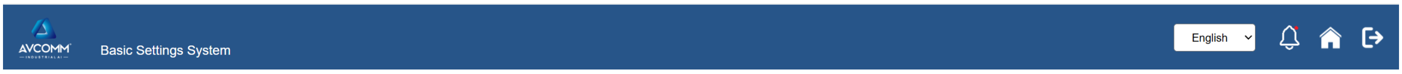
4. After successful authentication, the port status information about the switch will appear on the IE browser.

Introduction of Web Interface

The Web homepage appears after login, the whole homepage consists of the **top control bar**, the **navigation bar**, the **configuration display area**.



Top Control Bar



Home

By default, the list is located at "Basic Settings > System",shows "System Information".

English

The interface will turn into the English version.

Chinese

The interface will turn into the Chinese version.

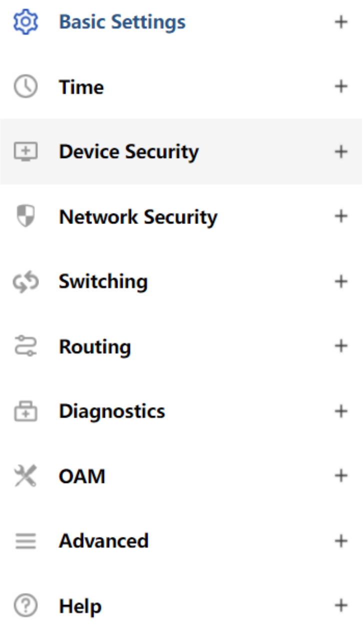
Logout

Exit.

Status Management Information

Displays four status management options and the number of status anomaly alerts in each option. If the number of alerts in all options is zero, the red dot will be removed.

Navigation Bar

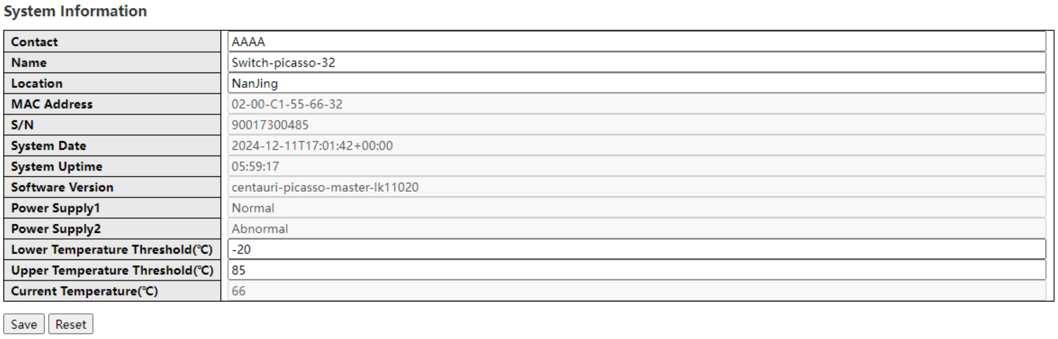


The contents in the navigation bar are shown in a form of list and classified according to types. By default, the list is located at "Diagnostics--Ports--State". If a certain item need be configured, please click the group name and then the sub-item. For example, to browse the system configuration, you have to click "Basic Settings" and then "System ", "information", "Status".

Note :

Different levels of user restrictions result in different web page displays. The lower the user level, the less web page display functionality.

Configuration Display Area



System Information

Contact	AAAA
Name	Switch-picasso-32
Location	NanJing
MAC Address	02-00-C1-55-66-32
S/N	90017300485
System Date	2024-12-11T17:01:42+00:00
System Uptime	05:59:17
Software Version	centauri-picasso-master-lk11020
Power Supply1	Normal
Power Supply2	Abnormal
Lower Temperature Threshold(℃)	-20
Upper Temperature Threshold(℃)	85
Current Temperature(℃)	66

The configuration display area shows the state and configuration of the device. The contents of this area can be modified by the clicking of the items in the navigation bar.

You can save the page configuration by clicking on "Save" on the page. By clicking on "Reset" on the page, any changes made locally can be undone and restored to the previously saved values.

Button

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.

Clear All

Clear all current entries.

Clear This

Clear the currently selected entries.

Save

Click to save the changes made to the current page.

Reset

Click to restore this page to its configuration before the changes.

Add New Entry

Click to add a new configuration entry.

Cancel

Click Cancel to return to the previous configuration page.

Back

Click Cancel to return to the previous configuration page.

Remove All

Remove all entries on the current page.

Submit

Save the configuration of the current page and return to the previous configuration page.

1. Basic Settings

The menu contains the following dialogs:

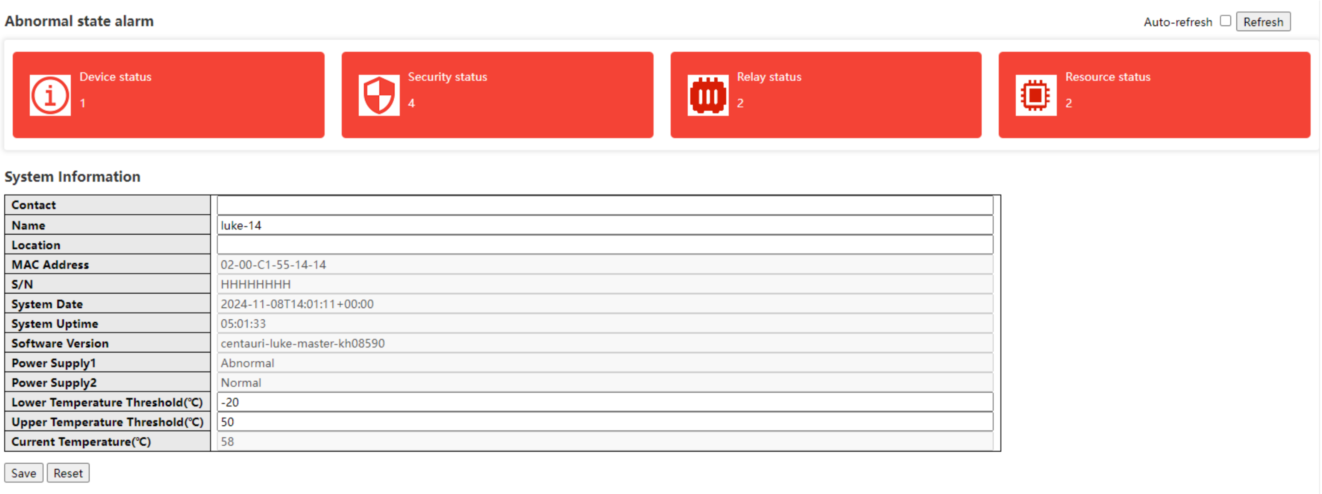
System
POE
Software
Load/Save
Restart Device
Factory Defaults

1.1. System

[Basic Settings > System]

[system information]

On this page, you can view status anomaly alerts and configure the system information of the switch.



Abnormal state alarm

System Information

Contact	
Name	luke-14
Location	
MAC Address	02-00-C1-55-14-14
S/N	HHHHHHHH
System Date	2024-11-08T14:01:11+00:00
System Uptime	05:01:33
Software Version	centauri-luke-master-kh08590
Power Supply1	Abnormal
Power Supply2	Normal
Lower Temperature Threshold(℃)	-20
Upper Temperature Threshold(℃)	50
Current Temperature(℃)	58

Status anomaly alerts

Device status

Device status Alarm information for device management, with red indicating an alert and green indicating no alert. The number of alerts at the current time will be displayed below "Device status." If the icon is red, hovering the mouse over this area will show detailed alarm information for device management.

Security status

Security status Alarm information for security management, with red indicating an alert and green indicating no alert. The number of alerts at the current time will be displayed below "Security status." If the icon is red, hovering the mouse over this area will show detailed alarm information for security management.

Relay status

Relay status Alarm information for relay management, with red indicating an alert and green indicating no alert. The number of alerts at the current time will be displayed below "Relay status." If the icon is red, hovering the mouse over this area will show detailed alarm information for relay management.

Resource status

Resource status Alarm information for resource management, with red indicating an alert and green indicating no alert. The number of alerts at the current time will be displayed below "Resource status." If the icon is red, hovering the mouse over this area will show detailed alarm information for resource management.

System Information Configuration

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.

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 (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.

Location

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

MAC Address

The MAC Address of this switch.

S/N

The serial number 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.

Code Revision

The version control identifier of the switch software.

Power Supply1

There are two power supplies, Power Supply 1 and Power Supply 2. Only one of them is in normal operating condition, while the other is in an abnormal state.

Power Supply2

There are two power supplies, Power Supply 1 and Power Supply 2. Only one of them is in normal operating condition, while the other is in an abnormal state.

Lower Temperature Threshold

The minimum temperature at which the CPU can operate normally.

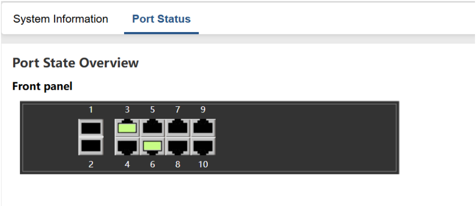
Upper Temperature Threshold

The maximum temperature at which the CPU can operate normally.

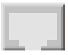
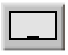
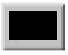
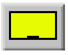
Current Temperature

Current temperature of the CPU.

[Port Status]



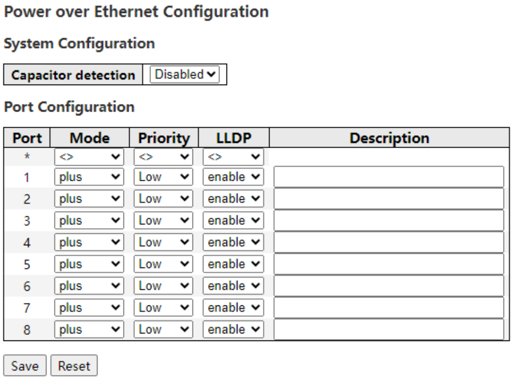
This option provides an overview of the current switch port states.

RJ45 ports			
SFP ports			
State	Disabled	Down	Link

1.2. PoE

[Basic Settings > PoE]

[Configuration]



Power over Ethernet Configuration

System Configuration

Capacitor detection	Disabled

Port Configuration

Port	Mode	Priority	LLDP	Description
*	<>	<>	<>	
1	plus	Low	enable	
2	plus	Low	enable	
3	plus	Low	enable	
4	plus	Low	enable	
5	plus	Low	enable	
6	plus	Low	enable	
7	plus	Low	enable	
8	plus	Low	enable	

Power over Ethernet Configuration

System Configuration

Capacitor detection

Indicates whether the PD (Powered Device) capacitor detection feature is enabled or not.

Port Configuration

Port

This is the physical port number for this row.

Mode

Set PoE mode or disable PoE feature, two PoE modes are supported. Standard：Power only IEEE compliant PDs. Plus: Power IEEE compliant and legacy PDs.

Priority

Set port power priority. Priority determines the order in which the interfaces will receive power. Interfaces with a higher priority will receive power before interfaces with a lower priority. Low means lowest priority. High means medium priority. Critical means highest priority.

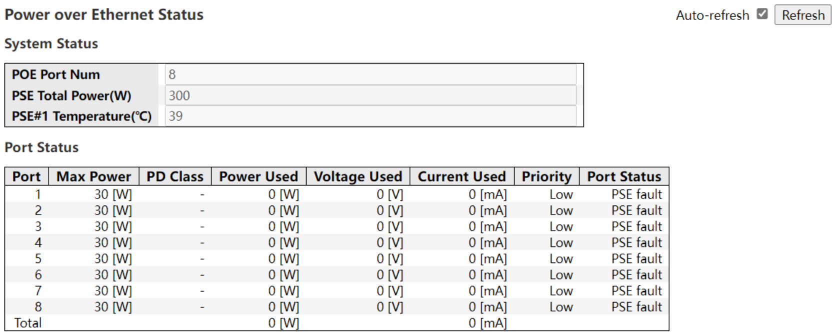
LLDP

Set port lldp awareness. If this value is disable, the PSE will ignore PoE related parts of received LLDP frames.

Description

Textual description for each PoE-PD device connected to the port.

[Status]



Power over Ethernet Status

System Status

POE Port Num	8
PSE Total Power(W)	300
PSE#1 Temperature(℃)	39

Port Status

Port	Max Power	PD Class	Power Used	Voltage Used	Current Used	Priority	Port Status
1	30 [W]	-	0 [W]	0 [V]	0 [mA]	Low	PSE fault
2	30 [W]	-	0 [W]	0 [V]	0 [mA]	Low	PSE fault
3	30 [W]	-	0 [W]	0 [V]	0 [mA]	Low	PSE fault
4	30 [W]	-	0 [W]	0 [V]	0 [mA]	Low	PSE fault
5	30 [W]	-	0 [W]	0 [V]	0 [mA]	Low	PSE fault
6	30 [W]	-	0 [W]	0 [V]	0 [mA]	Low	PSE fault
7	30 [W]	-	0 [W]	0 [V]	0 [mA]	Low	PSE fault
8	30 [W]	-	0 [W]	0 [V]	0 [mA]	Low	PSE fault
Total			0 [W]		0 [mA]		

Power over Ethernet Status

System Status

POE Port Num

Indicates the max number of poe ports.

PSE Total Power(W)

Indicates the max power of power supply.

PSE#1 Temperature(℃)

Indicates the pse temperature.

Port Status

Port

This is the physical port number for this row.

Max Power

Indicates the maximum power (in milliwatt) that the PD device may consume. This value is derived from PD class 0-8.

PD Class

Displays the PoE PD class that the PD device is signaling to the Switch PoE port. Possible values range from class 1-8 (class 0 is same as class 3). In case the PD hardware has double independent class signature hardware (independent class over each two out of four pairs) then two class numbers will be reported as '4,4'.

Power Used

Indicates the power(in milliwatt) that the PD is consuming right now.

Voltage Used

Indicates the voltage (in mV) that the PD is consuming right now.

Current Used

Indicates the current(in mA) that the PD is consuming right now.

Priority

Indicates the port power priority.

Port Status

Indicate port status. unknownState: PD state unknown. budgetExceeded: PoE is turned OFF due to power budget exceeded on PSE. noPoweredDeviceDetected: No PD detected. poweredDeviceOn: PSE supplying power to PD through PoE. poweredDeviceOverloaded: PD consumes more power than the maximum limit configured on the PSE port. notSupported: PoE not supported. disabled: PoE is disabled for the interface. disabledInterfaceShutdown: PD is powered down due to interface shut-down. pdFault: pd fault. pseFault: pse fault.

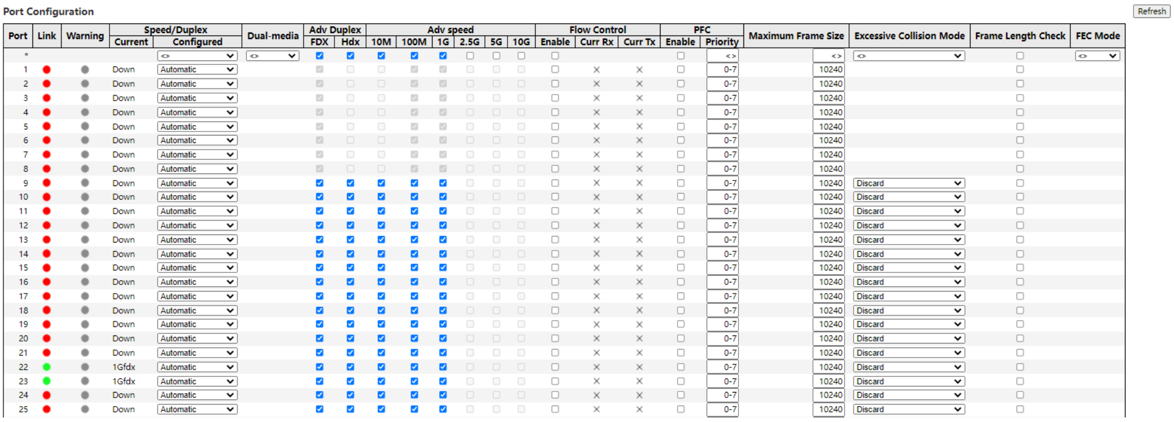
1.3. Port

1.3.1. Ports Configuration

[Basic Settings > Port > Ports Configuration]

Configuration

On this page, you can configure ports.



Port Configuration

Port	Link	Warning	Speed/Duplex		Dual-media	Adv Duplex		Adv speed						Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check	FEC Mode
			Current	Configured		FDX	Hdx	10M	100M	1G	2.5G	5G	10G	Enable	Curr Rx	Curr Tx	Enable	Priority				
*				<>	<>	☑	☑	☑	☑	☑	☐	☐	☐	☐			☐	<>	<>	<>	☐	<>
1	🔴	●	Down	Automatic		☑	☐	☐	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240		☐	
2	🔴	●	Down	Automatic		☑	☐	☐	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240		☐	
3	🔴	●	Down	Automatic		☑	☐	☐	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240		☐	
4	🔴	●	Down	Automatic		☑	☐	☐	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240		☐	
5	🔴	●	Down	Automatic		☑	☐	☐	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240		☐	
6	🔴	●	Down	Automatic		☑	☐	☐	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240		☐	
7	🔴	●	Down	Automatic		☑	☐	☐	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240		☐	
8	🔴	●	Down	Automatic		☑	☐	☐	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240		☐	
9	🔴	●	Down	Automatic		☑	☑	☑	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240	Discard	☐	
10	🔴	●	Down	Automatic		☑	☑	☑	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240	Discard	☐	
11	🔴	●	Down	Automatic		☑	☑	☑	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240	Discard	☐	
12	🔴	●	Down	Automatic		☑	☑	☑	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240	Discard	☐	
13	🔴	●	Down	Automatic		☑	☑	☑	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240	Discard	☐	
14	🔴	●	Down	Automatic		☑	☑	☑	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240	Discard	☐	
15	🔴	●	Down	Automatic		☑	☑	☑	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240	Discard	☐	
16	🔴	●	Down	Automatic		☑	☑	☑	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240	Discard	☐	
17	🔴	●	Down	Automatic		☑	☑	☑	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240	Discard	☐	
18	🔴	●	Down	Automatic		☑	☑	☑	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240	Discard	☐	
19	🔴	●	Down	Automatic		☑	☑	☑	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240	Discard	☐	
20	🔴	●	Down	Automatic		☑	☑	☑	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240	Discard	☐	
21	🔴	●	Down	Automatic		☑	☑	☑	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240	Discard	☐	
22	🟢	●	1Gfdx	Automatic		☑	☑	☑	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240	Discard	☐	
23	🟢	●	1Gfdx	Automatic		☑	☑	☑	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240	Discard	☐	
24	🔴	●	Down	Automatic		☑	☑	☑	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240	Discard	☐	
25	🔴	●	Down	Automatic		☑	☑	☑	☑	☑	☐	☐	☐	☐	×	×	☐	0-7	10240	Discard	☐	

Port Configuration

*

Select all items corresponding to all ports.

Port

This is the physical port number for this row.

Link

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

Warning

Operational warnings of the port.

●: No warnings.

🟡: There are warnings.

Current Link Speed

Provides the current link speed of the 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:

Disabled : Disables the switch port operation.

Automatic : Port auto negotiating speed and duplex with the link partner and selects the highest speed that is compatible with the link partner.

10Mbps HDX : Forces the port in 10Mbps half duplex mode.

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

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

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

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

2.5Gbps FDX : Forces the port in 2.5Gbps full duplex mode.

10Gbps FDX : Forces the port in 10Gbps full duplex mode.

Dual-media

If a port is Dual-media, this field selects which of the ports to use. If Dual is selected, both ports can be used, and if both ports has link, the SFP port will be preferred.

Advertise Duplex

When duplex is set as auto i.e auto negotiation, 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 i.e auto negotiation, the port will only advertise the specified speeds (10M 100M 1G 2.5G 5G 10G) 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.

Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.

NOTICE: The 100FX standard does not support Auto Negotiation, so when in 100FX mode the flow control capabilities will always be shown as "disabled".

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, e.g. '0-3,7' which equals '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 does not 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.

FEC Mode

FEC is short for Forward Error Correction. It is a technique for controlling errors over an unreliable link. The idea is that the sender adds some extra bits to the frame that allows a receiver to correct bit errors in the received frame.

R-FEC (IEEE802.3 clause 74 - sometimes called Firecode). This is meant for 10G. The parameter affects both what is requested during clause 73 aneg and what the port is configured to use if not running clause 73 aneg. If running clause 73 aneg on 10G ports we always tell the link partner that we support R-FEC. What the end user can control with the fec command is whether we request R-FEC. If either us or the link partner requests R-FEC, the port will end up using R-FEC.

auto: This is the default and means the following:

If a 10G port runs clause 73, R-FEC will be requested.

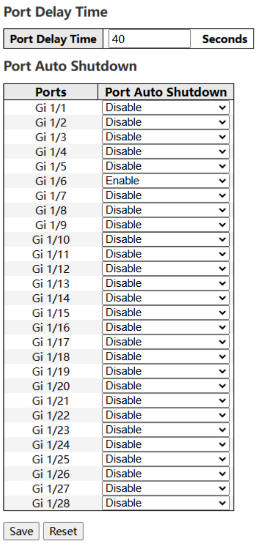
Otherwise, no FEC will be enabled.

r-fec: If a 10G port runs clause 73, only R-FEC will be requested. If a 10G port does not run clause 73, but is loaded with at least a 10G SFP and the speed is at least 5G, only R-FEC will be enabled. Otherwise, no FEC will be enabled.

none: If the port is running clause 73, R-FEC will not be requested (but remember that this does not mean that the clause 73 aneg will not result in the port running FEC). Otherwise, the port will not run any FEC.

PORT AUTO SHUTDOWN

This page allows configuration of automatic port closure.



Port Delay Time

Port Delay Time	40	Seconds

Port Auto Shutdown

Ports	Port Auto Shutdown
Gi 1/1	Disable
Gi 1/2	Disable
Gi 1/3	Disable
Gi 1/4	Disable
Gi 1/5	Disable
Gi 1/6	Enable
Gi 1/7	Disable
Gi 1/8	Disable
Gi 1/9	Disable
Gi 1/10	Disable
Gi 1/11	Disable
Gi 1/12	Disable
Gi 1/13	Disable
Gi 1/14	Disable
Gi 1/15	Disable
Gi 1/16	Disable
Gi 1/17	Disable
Gi 1/18	Disable
Gi 1/19	Disable
Gi 1/20	Disable
Gi 1/21	Disable
Gi 1/22	Disable
Gi 1/23	Disable
Gi 1/24	Disable
Gi 1/25	Disable
Gi 1/26	Disable
Gi 1/27	Disable
Gi 1/28	Disable

PORT DELAY TIME

PORT DELAY TIME

Set the time range for device port auto-close: 30 Seconds-600 Seconds.

PORT AUTO SHUTDOWN

Ports

Indicates the maximum number of ports for the current device.

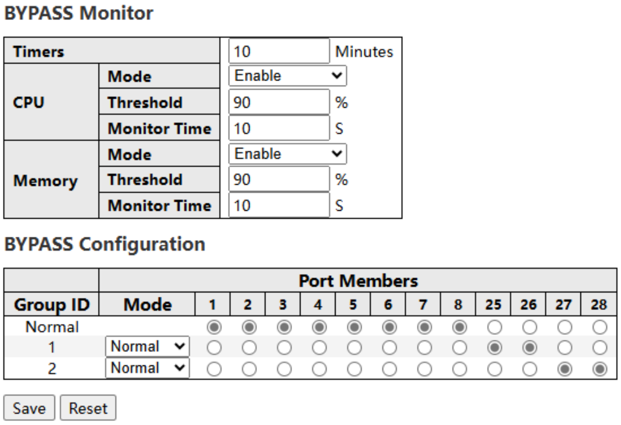
PORT AUTO SHUTDOWN

Set device port auto-close to Enabled or Disabled.

1.3.2. BYPASS

[Basic Settings > Port > BYPASS]

On this page, you can configure the port BYPASS group.



BYPASS Monitor

Timers		10	Minutes
CPU	**Mode**	Enable	
	Threshold	90	%
	Monitor Time	10	S
Memory	**Mode**	Enable	
	Threshold	90	%
	Monitor Time	10	S

BYPASS Configuration

	Port Members												
Group ID	**Mode**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**25**	**26**	**27**	**28**
Normal		●	●	●	●	●	●	●	●	○	○	○	○
1	Normal	○	○	○	○	○	○	○	○	●	●	○	○
2	Normal	○	○	○	○	○	○	○	○	○	○	●	●

[Configuration]

BYPASS monitor

Timers

Display timer monitoring information. The default value is 10 minutes, and the timer's allowed range is from 3 to 60 minutes.

CPU

Display CPU monitoring information. The mode is enabled by default, with a threshold range of 50-100 and a default value of 90%. The monitoring duration range is 5-50 seconds with a default value of 10 s. When configured to disable, the CPU monitoring function is turned off.

Memory

Display memory monitoring information. The mode is enabled by default, with a threshold range of 50-100 and a default value of 90%. The monitoring duration range is 5-50 seconds with a default value of 10 s. When configured to disable, the memory monitoring function is turned off.

BYPASS Configuration

*

Select all items corresponding to all ports.

Port Members

Shows the port members that use the BYPASS function.

Group ID

Select the available BYPASS group for the given switch port. The possible group IDs are:

Normal : The port has not been added to the BYPASS group.

1 : Add the port to BYPASS group 1.

2 : Add the port to BYPASS group 2.

Mode

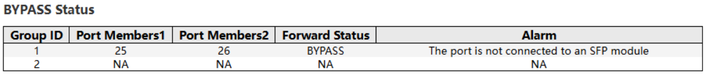
Select the corresponding mode for the given BYPASS group. The available modes are:

Enable : Activates the bypass function for the group.

Normal : Sets the BYPASS group mode to Normal Mode.

Enhanced : Sets the BYPASS group mode to Enhanced Mode.

[Status]



BYPASS Status

Group ID	Port Members1	Port Members2	Forward Status	Alarm
1	25	26	BYPASS	The port is not connected to an SFP module
2	NA	NA	NA	NA

BYPASS Status

Alarm

Display the open status of ports for BYPASS group members. If not opened, display NA.

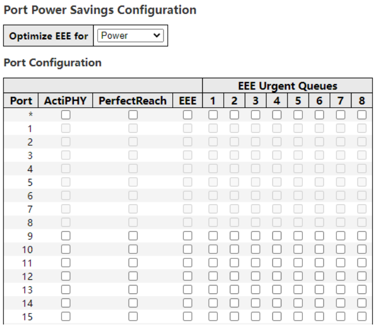
1.3.3. Green Ethernet

Port Power Savings

[Basic Settings > Port > Green Ethernet > Port Power Savings]

[configuration]

On this page, you can configure the port power savings features.



Port Power Savings Configuration

Optimize EEE for: Power

Port Configuration

				EEE Urgent Queues							
Port	ActiPHY	PerfectReach	EEE	1	2	3	4	5	6	7	8
*	□	□	□	□	□	□	□	□	□	□	□
1	□	□	□	□	□	□	□	□	□	□	□
2	□	□	□	□	□	□	□	□	□	□	□
3	□	□	□	□	□	□	□	□	□	□	□
4	□	□	□	□	□	□	□	□	□	□	□
5	□	□	□	□	□	□	□	□	□	□	□
6	□	□	□	□	□	□	□	□	□	□	□
7	□	□	□	□	□	□	□	□	□	□	□
8	□	□	□	□	□	□	□	□	□	□	□
9	□	□	□	□	□	□	□	□	□	□	□
10	□	□	□	□	□	□	□	□	□	□	□
11	□	□	□	□	□	□	□	□	□	□	□
12	□	□	□	□	□	□	□	□	□	□	□
13	□	□	□	□	□	□	□	□	□	□	□
14	□	□	□	□	□	□	□	□	□	□	□
15	□	□	□	□	□	□	□	□	□	□	□

Port Power Savings Configuration

Optimize EEE for

Sets if EEE should be optimized for least traffic latency or least power comsumption.

Port Configuration

Port

The switch port number of the physical port.

ActiPHY

Link down power savings enabled. ActiPHY works by lowering the power for a port when there is no link. The port is powered up for short moment in order to determine if cable is inserted.

PerfectReach

Cable length power savings enabled. PerfectReach works by determining the cable length and lowering the power for ports with short cables.

EEE

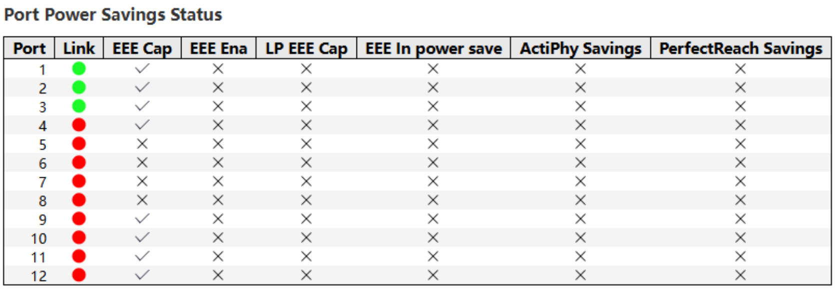
Controls whether EEE is enabled for this switch port. For maximizing power savings, the circuit isn't started at once transmit data is ready for a port, but is instead queued until a burst of data is ready to be transmitted. This will give some traffic latency.If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.

EEE Urgent Queues

Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

[Status]

This page provides the current status for EEE.



Port Power Savings Status

Port	Link	EEE Cap	EEE Ena	LP EEE Cap	EEE In power save	ActiPhy Savings	PerfectReach Savings
1	🟢	✓	✕	✕	✕	✕	✕
2	🟢	✓	✕	✕	✕	✕	✕
3	🟢	✓	✕	✕	✕	✕	✕
4	🔴	✓	✕	✕	✕	✕	✕
5	🔴	✕	✕	✕	✕	✕	✕
6	🔴	✕	✕	✕	✕	✕	✕
7	🔴	✕	✕	✕	✕	✕	✕
8	🔴	✕	✕	✕	✕	✕	✕
9	🔴	✓	✕	✕	✕	✕	✕
10	🔴	✓	✕	✕	✕	✕	✕
11	🔴	✓	✕	✕	✕	✕	✕
12	🔴	✓	✕	✕	✕	✕	✕

Port Power Savings Status

Port

This is the physical port number for this row.

Link

Shows if the EEE link is up for the port (green = link up, red = link down).

EEE cap

Shows if the port is EEE capable.

EEE Ena

Shows if EEE is enabled for the port (reflects the settings at the Port Power Savings configuration page).

LP EEE cap

Shows if the link partner is EEE capable.

EEE In power save

Shows if the system is currently saving power due to EEE. When EEE is enabled, the system will powered down if no frame has been received or transmitted in 5 uSec.

Actiphy Savings

Shows if the system is currently saving power due to ActiPhy.

PerfectReach Savings

Shows if the system is currently saving power due to PerfectReach.

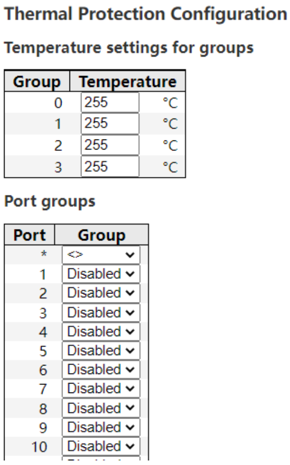
1.3.4. Thermal Protection

[Basic Settings > Port > Thermal Protection]

[configuration]

This page allows the user to inspect and configure the current settings for controlling thermal protection. Thermal protection is used to protect the chip from getting overheated.

When the temperature exceeds the configured thermal protection temperature, ports will be turned off in order to decrease the power consumption. It is possible to arrange the ports with different groups. Each group can be given a temperature at which the corresponding ports shall be turned off.



Thermal Protection Configuration

Temperature settings for groups

Group	Temperature	
0	255	°C
1	255	°C
2	255	°C
3	255	°C

Port groups

Port	Group
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled

Temperature settings for groups

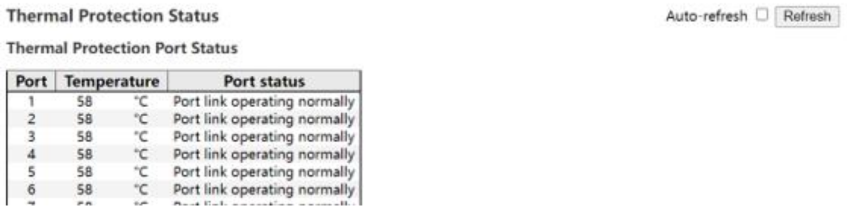
The temperature at which the ports in the corresponding group will be turned off. The supported temperature range is from 0 to 255 ℃.

Port groups

The group to which the port belongs. 4 groups are supported.

[Status]

This page allows the user to inspect status information related to thermal protection.



Thermal Protection Status

Thermal Protection Port Status

Port	Temperature		Port status
1	58	°C	Port link operating normally
2	58	°C	Port link operating normally
3	58	°C	Port link operating normally
4	58	°C	Port link operating normally
5	58	°C	Port link operating normally
6	58	°C	Port link operating normally

Thermal Protection Port Status

Port

The switch port number.

Temperature

Shows the current chip temperature in degrees Celsius.

Port Status

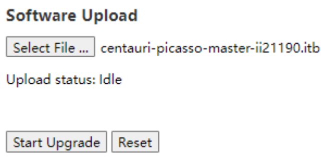
Shows if the port is thermally protected (link is down) or if the port is operating normally.

1.4. Software

1.4.1. Upload

[Basic Settings > Software > Upload]

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



Software Upload

centauri-picasso-master-ii21190.itb

Upload status: Idle

Software Upload

Browse to the location of a software image and click **Upload**.

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.

If an upload failure occurs, you can click Reset, then select the file again to upload.

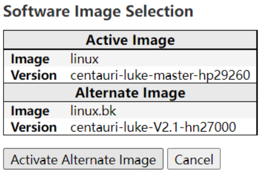
Warning: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

1.4.2. Image Select

[Basic Settings > Software > Image 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.



Software Image Selection

Active Image	
Image	linux
Version	centauri-luke-master-hp29260
Alternate Image	
Image	linux.bk
Version	centauri-luke-V2.1-hn27000

Software Image Selection

Note:

1. 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.

2. 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.

3. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

Image

The file name of the firmware image, from when the image was last updated.

Version

The version of the firmware image.

1.5. Load/Save

[Basic Settings > Load/Save]

Maintaining Configuration Files

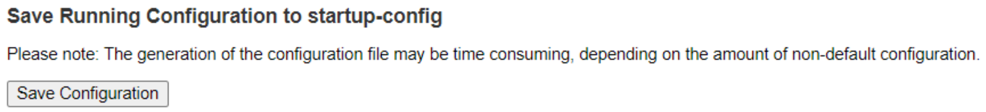
The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.

The available files are:

- *running-config*: A virtual file that represents the currently active configuration 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.

1.5.1. Save startup-config

[Basic Settings > Load/Save > Save startup-config]



Save Running Configuration to startup-config

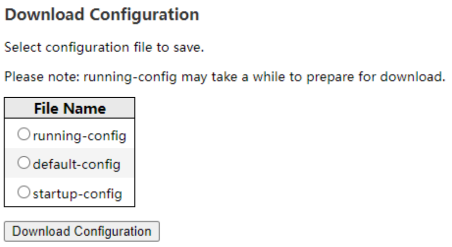
Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

Save Running Configuration to startup-config

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

1.5.2. Download

[Basic Settings > Load/Save > Download]



Download Configuration

Select configuration file to save.

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

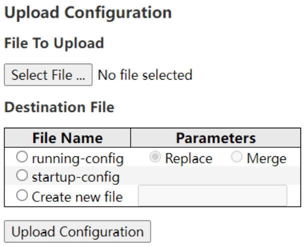
File Name
○ running-config
○ default-config
○ startup-config

Download Configuration

It is possible to download any of the files on the switch to the web browser. Select the file and click **Download Configuration**. Download of running-config may take a little while to complete, as the file must be prepared for download.

1.5.3. Upload

[Basic Settings > Load/Save > Upload]



Upload Configuration

File To Upload

Select File ... No file selected

Destination File

File Name	Parameters
○ running-config	● Replace ○ Merge
○ startup-config	
○ Create new file	

Upload Configuration

Upload Configuration

It is possible to upload a file from the web browser to all the files on the switch, except *default-config* which is read-only. Select the file to upload, select the destination file on the target, then click 'upload configuration'.

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

Replace mode

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

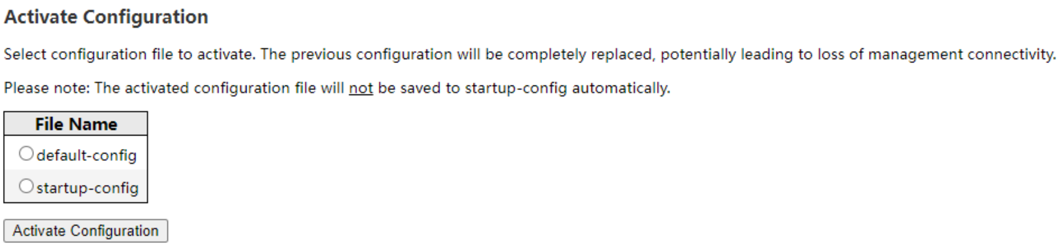
Merge mode

The uploaded file is merged into *running-config*.

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

1.5.4. Activate

[Basic Settings > Load/Save > Activate]



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

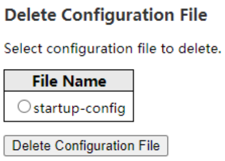
It is possible to activate any of the configuration files present on the switch, except for running-config which represents the currently active configuration.

Select the file to activate and click Activate Configuration.

This will initiate the process of completely replacing the existing configuration with that of the selected file.

1.5.5. Delete

[Basic Settings > Load/Save > Delete]



Delete Configuration File

Select configuration file to delete.

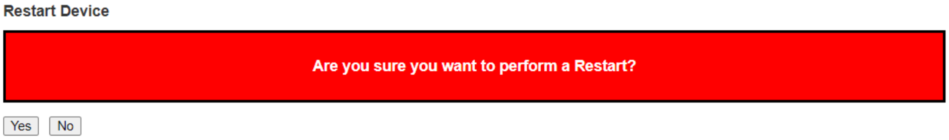
File Name
○ startup-config

Delete Configuration File

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.

1.6. Restart Device

[Basic Settings > Restart Device]



Restart Device

Are you sure you want to perform a Restart?

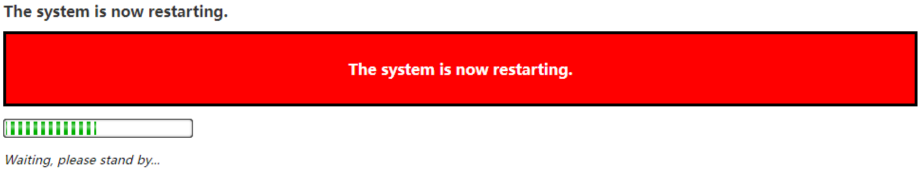
Restart Device

You can restart the switch with this page. After restart, the switch will boot normally.

Click **Yes** to restart device.

Click **No** to return to the Port State page without restarting.

If click **Yes**, You can see the following page display.



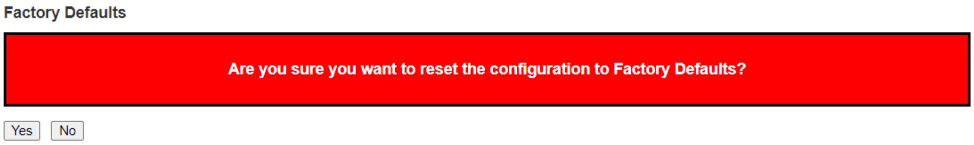
The system is now restarting.

The system is now restarting.

Waiting, please stand by...

1.7. Factory Defaults

[Basic Settings > Factory Defaults]



Factory Defaults

Are you sure you want to reset the configuration to Factory Defaults?

Factory Defaults

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

The new configuration is available immediately, which means that no restart is necessary.

Click **Yes** to reset the configuration to Factory Defaults.

Click **No** to return to the Port State page without resetting the configuration.

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

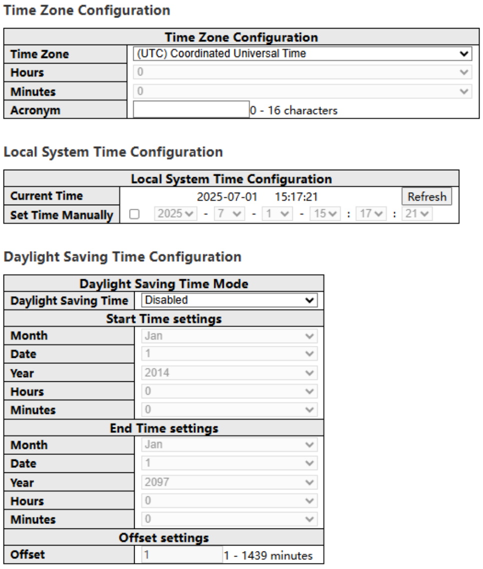
2. Time

The menu contains the following dialogs:
Basic Settings
NTP
PTP
SyncE
TSN

2.1. Basic Settings

[Time > Basic Settings]

On this page, you can configure the time Zone.



Time Zone Configuration

Time Zone Configuration	
Time Zone	(UTC) Coordinated Universal Time
Hours	0
Minutes	0
Acronym	0 - 16 characters

Local System Time Configuration

Local System Time Configuration	
Current Time	2025-07-01 15:17:21 Refresh
Set Time Manually	□ 2025 - 7 - 1 - 15 : 17 : 21

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled
Start Time settings	
Month	Jan
Date	1
Year	2014
Hours	0
Minutes	0
End Time settings	
Month	Jan
Date	1
Year	2097
Hours	0
Minutes	0
Offset settings	
Offset	1 1 - 1439 minutes

Time Zone Configuration

Time Zone

Lists various Time Zones world wide. Select appropriate Time Zone from the drop down and click Save to set. The 'Manual Setting' options is used for the specific time zone which is excluded from the options list.

Hours

Number of hours offset from UTC. The field is only available when time zone manual setting.

Minutes

Number of minutes offset from UTC. The field is only available when time zone manual setting.

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) Notice the string '' is a special syntax that is reserved for null input.

Local System Time Configuration

Current Time

Show the current time; users cannot change it. Refreshing will update the displayed current time to the most recent refresh point.

Set Time Manually

You can select the check box and set the current system time by selecting the drop-down box.

The current time is displayed when the user sets the time. The current time is offset by district time and daylight saving time.

When the NTP service is enabled, the time cannot be configured.

The years are limited to 1970-2037.

In leap years, February 29 can be configured, and illegal dates such as February 31 cannot be configured.

Here is an example of offset logic in a normal usage scenario: The daylight saving time (DST) mode is set to non-repeating, the UTC offset is set to 0, the DST start time is set to 00:00 on January 1, 2008, the DST end time is set to 02:02 on January 1, 2008, and the DST offset is set to 2 hours.If the current time is set to 00:58:36 on January 1, 2008 (which is before DST starts), once the time reaches the DST start time, the current time will instantly shift from 1:00 to 2:00. After 2 minutes, when the time reaches the DST end time, it will shift back from 2:02 to 1:02.

Abnormal scenario: It is important to note that you should not set the current system time within the interval between the DST start time and the DST start time plus the offset. If you do, the current time will lose the amount of the DST offset.

Example of an abnormal scenario: The DST start time is 08:00 on August 8, 2024, and the DST end time is 12:00 on August 8, 2024. The DST offset is set to 60 minutes. If the current time is set to 08:30:00 on August 8, 2024, the displayed current time will be 07:30 on August 8, 2024.

Daylight Saving Time Configuration

Daylight Saving Time

This option is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration.

Select **Disable** to disable the Daylight Saving Time configuration.

Select **Recurring** and configure the Daylight Saving Time duration to repeat the configuration every year.

Select **Nonrecurring** and configure the Daylight Saving Time duration for single time configuration. (Default : Disabled).

Recurring Configurations

Start time settings

Week - Select the starting week number.

Day - Select the starting day.

Month - Select the starting month.

Hours - Select the starting hour.

Minutes - Select the starting minute.

End time settings

Week - Select the ending week number.

Day - Select the ending day.

Month - Select the ending month.

Hours - Select the ending hour.

Minutes - Select the ending minute.

Offset settings

Offset - Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1439).

Non-Recurring Configurations

Start time settings

Month - Select the starting month.

Date - Select the starting date.

Year - Select the starting year.

Hours - Select the starting hour.

Minutes - Select the starting minute.

End time settings

Month - Select the ending month.

Date - Select the ending date.

Year - Select the ending year.

Hours - Select the ending hour.

Minutes - Select the ending minute.

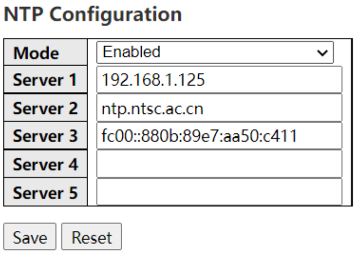
Offset settings

Offset - Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1439).

2.2. NTP

[Time > NTP]

On this page, you can configure NTP.



NTP Configuration

Mode	Enabled
Server 1	192.168.1.125
Server 2	ntp.ntsc.ac.cn
Server 3	fc00::880b:89e7:aa50:c411
Server 4	
Server 5	

NTP Configuration

Mode

Indicates the NTP mode operation. Possible modes are:

Enabled: Enable NTP client mode operation.

Disabled: Disable NTP client mode operation.

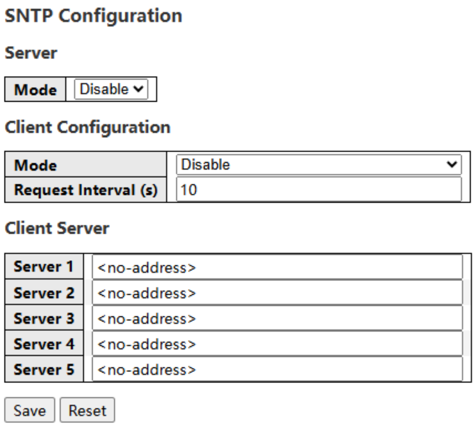
Server#

Provide the domain names and IPv4 or IPv6 addresses of NTP servers. A domain name is a sequence of strings separated by dots, with the rightmost part being the top-level domain (TLD), such as www.example.com. An IPv4 address is a 32-bit binary number typically represented in dotted decimal notation, with each segment ranging from 0 to 255, such as 192.168.1.1. An IPv6 address is a 128-bit binary number usually represented in hexadecimal separated by colons, with each group containing four hexadecimal digits, making eight groups in total, such as 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

2.3. SNTP

[Time > SNTP]

On this page, you can configure SNTP.



SNTP Configuration

Server

Mode	Disable

Client Configuration

Mode	Disable
Request Interval (s)	10

Client Server

Server 1	<no-address>
Server 2	<no-address>
Server 3	<no-address>
Server 4	<no-address>
Server 5	<no-address>

SNTP Configuration

Server Mode

Indicates the SNTP mode operation. Possible modes are:

Enabled: Enable SNTP client mode operation.

Disabled: Disable SNTP client mode operation.

Client Configuration

Indicates the SNTP mode operation. Possible modes are:

Enabled: Enable SNTP client mode operation.

Disabled: Disable SNTP client mode operation.

Request interval(s): Indicates the SNTP synchronization time interval, specifying how often synchronization occurs (in seconds).

Client Server

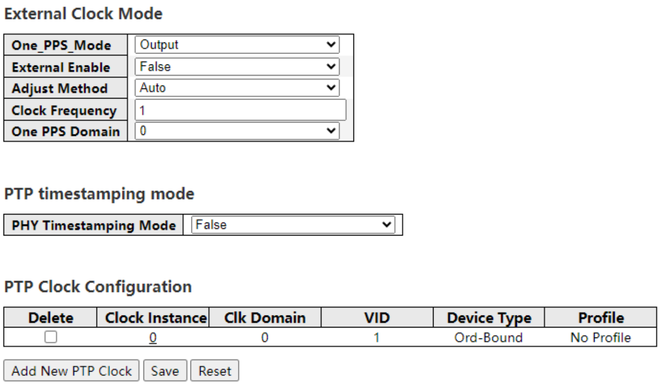
Provide the domain names and IPv4 or IPv6 addresses of SNTP servers. A domain name is a sequence of strings separated by dots, with the rightmost part being the top-level domain (TLD), such as www.example.com. An IPv4 address is a 32-bit binary number typically represented in dotted decimal notation, with each segment ranging from 0 to 255, such as 192.168.1.1. An IPv6 address is a 128-bit binary number usually represented in hexadecimal separated by colons, with each group containing four hexadecimal digits, making eight groups in total, such as 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

2.4. PTP

[Time > PTP]

[Configuration]

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



External Clock Mode

One_PPS_Mode	Output
External Enable	False
Adjust Method	Auto
Clock Frequency	1
One PPS Domain	0

PTP timestamping mode

PHY Timestamping Mode	False

PTP Clock Configuration

Delete	Clock Instance	Clk Domain	VID	Device Type	Profile
□	0	0	1	Ord-Bound	No Profile

External Clock Mode

One_PPS_Mode

This Selection box will allow you to select the One_pps_mode configuration.

The following values are possible:

1. Output : Enable the 1 pps clock output.

2. Input : Enable the 1 pps clock input.

3. Disable : Disable the 1 pps clock in/out-put.

External Enable

This Selection box will allow you to configure the External Clock output.

The following values are possible:

1. True : Enable the external clock output.

2. False : Disable the external clock output.

Adjust Method

This Selection box will allow you to configure the Frequency adjustment configuration.

1. LTC : Select Local Time Counter (LTC) frequency control.

2. Auto : AUTO Select clock control, based on PTP profile and available HW resources.

Clock Frequency

This will allow to set the Clock Frequency.

The possible range of values are 1 - 25000000 (1 - 25MHz).

One PPS Domain

Hardware-captured timestamps support multiple clock domains and offer configurable options.

PTP timestamping mode

PHY Timestamping Mode

When the device supports PHY timestamping, it is used to determine whether to enable PHY timestamping.

PTP Clock Configuration

Delete

Check this checkbox and click on 'Save' to delete the clock instance.

Clock Instance

Indicates the instance number of a particular Clock Instance [0..3].

Click on the Clock Instance number to edit the Clock details.

Clk Domain

Indicates the HW clock domain used by the clock.

VID

VLAN Identifier used for tagging the VLAN packets.

Device Type

Indicates the Type of the Clock Instance. There are five Device Types.

1. Ord-Bound - clock's Device Type is Ordinary-Boundary Clock.
2. P2p Transp - clock's Device Type is Peer to Peer Transparent Clock.
3. E2e Transp - clock's Device Type is End to End Transparent Clock.
4. Master Only - clock's Device Type is Master Only.
5. Slave Only - clock's Device Type is Slave Only.
6. BC-fronted - boundary Clock front end.
7. AED-GM - AED Grandmaster.
8. internal Clock.

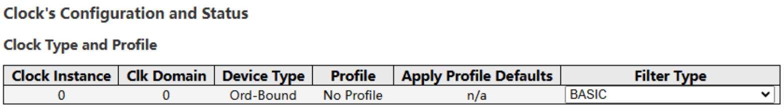
Profile

Indicates the profile used by the clock.

1. No Profile.
2. 1588 - IEEE 1588 profile.
3. G8265.1 - G8265.1 profile.
4. G8275.1 - G8275.1 profile.
5. G8275.2 - G8275.2 profile.

Click on the clock instance to enter the specific clock instance configuration page.

Clock Type and Profile



Clock's Configuration and Status

Clock Type and Profile

Clock Instance	Clk Domain	Device Type	Profile	Apply Profile Defaults	Filter Type
0	0	Ord-Bound	No Profile	n/a	BASIC

Clock Instance

The instance number of a specific clock instance [0..3].

Clk Domain

The CLK clock domain used by the clock.

Device Type

The type of clock instance. There are eight device types:

Ord-Bound - The device type of the clock is ordinary boundary clock.

P2p Transp - The device type of the clock is peer-to-peer transparent clock.

E2e Transp - The device type of the clock is end-to-end transparent clock.

Master Only - The device type of the clock is master clock.

Slave Only - The device type of the clock is slave clock.

BC-fronted - The device type of the clock is boundary clock front-end.

AED-GM - The device type of the clock is AED grandmaster clock.

Internal clock.

Profile

The configuration profile used by the clock:

1. None - The default 1588 profile is used.

2. 1588 - IEEE 1588 profile.

3. G8265.1 - G8265.1 profile.

4. G8275.1 - G8275.1 profile.

5. G8275.2 - G8275.2 profile.

Apply Profile Defaults

Click to apply attributes.

Filter Type

There are four filtering types:

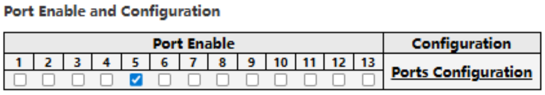
1. ACL_BASIC_PHASE.

2. ACL_BASIC_PHASE_LOW.

3. ACL_BC_FULL_ON_PATH_FREQ.

4. BASIC. The default is the BASIC algorithm.

Port Enable and Configuration



Port Enable and Configuration

Port Enable													Configuration
1	2	3	4	5	6	7	8	9	10	11	12	13	Ports Configuration
□	□	□	□	☑	□	□	□	□	□	□	□	□	

Port Enable

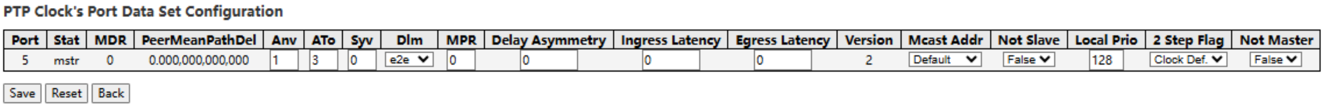
Check the corresponding port to indicate that the PTP instance completes clock synchronization on this port.

Configuration

Ports Configuration.

Click Ports Configuration.

PTP Clock's Port Data Set Configuration



PTP Clock's Port Data Set Configuration

Port	Stat	MDR	PeerMeanPathDel	Anv	ATo	Syv	Dlm	MPR	Delay Asymmetry	Ingress Latency	Egress Latency	Version	Mcast Addr	Not Slave	Local Prio	2 Step Flag	Not Master
5	mstr	0	0.000,000,000,000	1	3	0	e2e	0	0	0	0	2	Default	False	128	Clock Def.	False

Port

Enable the clock port.

Stat

PTP port states are divided into: init, lstn, uncl, slve, mstr, dsbl, p2pt, et2t, flty, frnd.

MDR

This value indicates the configuration value for the delay request message interval currently in use. The value is a positive integer n, representing 2 to the power of n, where the actual time interval is 2^n seconds. This interval denotes the time between sending delay request messages from a Slave device to a Master device.

PeerMeanPathDel

This value represents the delay information measured and calculated from the peer_delay_req and resp response messages. The format is as follows: AA.BBB,CCC,DDD where AA is in seconds, BBB is in milliseconds, CCC is in microseconds, and DDD is in nanoseconds.

Anv

This value represents the number of times an announce request message is sent. It is calculated as a power of 2, with the unit in seconds.

ATo

This value, together with the frequency of announce message sending, determines the announce message sending timeout.

Syv

This value represents the sync request message transmission period, calculated as a power of 2, with the unit in seconds.

Dlm

This value represents the link measurement method and can be one of three types: e2e, p2p, or cp2p. The choice depends on the clock type of the peer device. If the peer is a p2p transparent clock, select either p2p or cp2p, noting that the header formats for p2p and cp2p are different.

MPR

This value represents the delay request message transmission period, calculated as a power of 2, with the unit in seconds.

Delay Asymmetry

When the receive path delay is greater than the send path delay or when the receive path delay is less than the send path delay, it indicates that the delay compensation amount needs to be set. This parameter needs to be configured.

Ingress Latency

This parameter is used to configure the ingress delay of the device. Ingress delay refers to the time delay between receiving the data packet at the network interface and the actual processing of the data packet within the device.

Egress Latency

This parameter is used to configure the egress delay of the device. Egress delay refers to the time delay from when a data packet is processed internally within the device and ready to be sent to the network interface, to when the data packet is actually transmitted from the network interface.

Version

Protocol version number, currently by default is 1588 2019 2.0 version.

Mcast Addr

The default value is 'default'.

When set to 'default',

the layer 2 multicast destination address is: 0x01, 0x1b, 0x19, 0x00, 0x00, 0x00 (syn announce), the layer 3 multicast IP address is: 0x01, 0x00, 0x5e, 0x00, 0x01, 0x81.

When set to 'Link_local',

the layer 2 multicast destination address is: 0x01, 0x80, 0xC2, 0x00, 0x00, 0x0E (syn announce), d the layer 3 multicast IP address is: 0x01, 0x00, 0x5e, 0x00, 0x00, 0x6B.

Not Slave

When this value is set to true, the port defaults to being the master clock.

Local Prio

Local priority setting is used in the ITU-T G.8275.1 and G.8275.2 standards, where the local priority is involved in the master clock selection process through the BMCA algorithm.

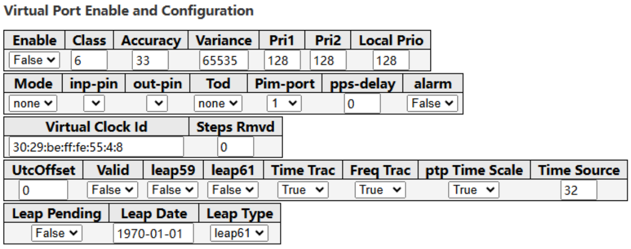
2 Step Flag

This value determines whether to use a two-step clock, where a follow-up message carries timestamp information following a sync message. The default is 'default', following the global PTP clock configuration settings.

Not Master

When this value is set to true, the port defaults to being the slave clock.

Virtual Port Enable and Configuration



Virtual Port Enable and Configuration

Enable	Class	Accuracy	Variance	Pri1	Pri2	Local Prio
False	6	33	65535	128	128	128

Mode	inp-pin	out-pin	Tod	Pim-port	pps-delay	alarm
none			none	1	0	False

Virtual Clock Id	Steps Rmvd
30:29:be:ff:fe:55:4:8	0

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	ptp Time Scale	Time Source
0	False	False	False	True	True	True	32

Leap Pending	Leap Date	Leap Type
False	1970-01-01	leap61

Enable

Enable virtual port.

Class

This is the clock class field within the clock quality structure. According to the 1588 protocol standard:

1. 6 (GM locked to 1pps output)

2. 7 (GM in holdover state after 1pps output)

3. 135 (boundary clock in holdover state)

4. 165 (boundary clock out of holdover state)

5. 140 (CAT 1 GM out of holdover state)

6. 150 (CAT 2 GM out of holdover state)

7. 160 (CAT 3 GM out of holdover state)

8. 248 (default)

9. 255 (time from clock)

Accuracy

This is the clock accuracy field within the clock quality structure. The values represent:

1. 32 (25 nanoseconds)
2. 33 (100 nanoseconds)
3. 34 (250 nanoseconds)
4. 35 (1 microsecond)
5. 36 (2.5 microseconds)
6. 37 (10 microseconds)
7. 38 (25 microseconds)
8. 39 (100 microseconds)
9. 40 (250 microseconds)
10. 41 (1 millisecond)
11. 42 (2.5 milliseconds)
12. 43 (10 milliseconds)
13. 44 (25 milliseconds)
14. 45 (100 milliseconds)
15. 46 (250 milliseconds)
16. 47 (1 second)
17. 48 (10 seconds)
18. 49 (greater than 10 seconds)
19. 254 (unknown)

Variance

This parameter is used in the IEEE 1588 protocol to evaluate the stability and quality of the time offset of the master clock. It provides a measure of the master clock's stability for the slave clocks, aiding in the optimization of the time synchronization process to ensure precision and reliability in the network. A smaller variance indicates that the time offset between the master clock and the slave clocks is more stable and consistent.

Pri#

The priority1 and priority2 parameters in the protocol message are used to determine the selection order of the Grandmaster Clock in the Precision Time Protocol (PTP).

Local Prio

Local priority setting is used in the ITU-T G.8275.1 and G.8275.2 standards, where the local priority is involved in the master clock selection process through the BMCA algorithm.

Mode

There are four modes:

1. None.

2. pps-in.

3. pps-out.

4. freq-out.

Inp-pin

Indicates configuring an input/output pin as PPS input mode to receive the per-second pulse signal sent by an external device.

Out-pin

Indicates configuring an input/output pin as PPS output mode to send the per-second pulse signal.

Tod

Indicates the protocol used for transmitting astronomical time (date and time information). The specific options are as follows:

ZDA is the most commonly used standard protocol, specifically used for transmitting date and time information.

GGA and RMC provide positional data as well as time information.

POLYT and PIM may be custom protocols for specific systems or applications.

NONE indicates that no protocol is used for transmitting time information.

Pim-port

The port number for transmitting TOD using the PIM protocol.

pps-delay

Estimated delay time for the PPS signal from the source to the receiver.

alarm

Whether to alarm.

Virtual Clock Id

When using a virtual clock port, configure the clock identifier. This value can be modified.

Steps Rmvd

This parameter represents the number of intermediate clocks that the sync message has passed through from the Master Clock to the current device. Specifically, it records how many steps (Steps) it has taken from the Master Clock to the current device. This value can be configured.

UtcOffset

Set the UTC offset.

Valid

Valid This field indicates whether the leap second fields leap59 and leap61 are valid.

leap59

When set to valid, this indicates that the current UTC will decrease by 1 second (i.e., a leap second minus 1 second) for the purpose of global time synchronization adjustment.

leap61

When set to valid, this indicates that the current UTC will increase by 1 second (i.e., a leap second plus 1 second) for the purpose of global time synchronization adjustment.

Time Trac

Time Traceable Indicates the timeTraceable field in the announce message header. This flag is used to indicate whether the device's time is traceable. If the device’ s time can be traced back to a known standard, this flag will be set to TRUE. This confirms that the device can ensure its time is synchronized with a reference time source, further enhancing the precision and reliability of clock synchronization.

Freq Trac

Frequency Traceable Indicates the frequencyTraceable field in the announce message header. This flag is used to indicate whether the device's frequency is traceable. If the device’ s frequency can be traced back to a known standard, this flag will be set to TRUE. This confirms that the device can ensure its clock frequency is synchronized with a reference standard, providing more accurate clock synchronization services.

ptp Time Scale

The ptpTimescale field in the announce message header determines the accuracy and scope of the timestamps. This field can be set to TRUE or FALSE, indicating whether the timestamps follow the time scale defined by the IEEE 1588 standard. Specifically, when ptpTimescale is set to TRUE, it means that the timestamps adhere to the IEEE 1588 standard's time scale, defining the accuracy and scope according to the standard. Conversely, if ptpTimescale is set to FALSE, it means that the timestamps do not follow the IEEE 1588 standard's time scale and may use other time scales or precision.

Time Source

This field represents the timeSource field in the announce message. Specifically, the value of the timeSource field represents the type and origin of the clock. Common values include:

Local Clock: Refers to the device's own clock.

GPS: Receives time information through the GPS system.

Other Time Sources: May come from other network devices or synchronization protocols.

Leap Pending

Compensates for the timestamp handling delays of various nodes, ensuring accuracy and consistency in time synchronization.

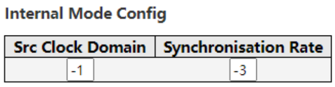
Leap Date

Select the starting point of the leap time.

Leap Type

Leap types are divided into two kinds, leap59 and leap61.

Internal Mode Config



Internal Mode Config

Src Clock Domain	Synchronisation Rate
-1	-3

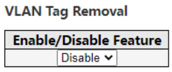
Src Clock Domain

This parameter corresponds to the clock instance number when the clock type is set to Internal.

Synchronisation Rate

This parameter represents the time interval, indicating how often the software clock synchronizes with hardware domain 0.

VLAN Tag Removal



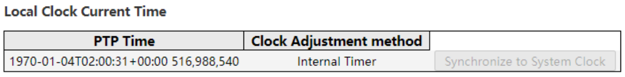
VLAN Tag Removal

Enable/Disable Feature
Disable

Enable/Disable Feature

The purpose of this command is to modify the handling of PTP packets at startup, so that VLAN tags are ignored during reception and transmission.

Local Clock Current Time



Local Clock Current Time

PTP Time	Clock Adjustment method	
1970-01-04T02:00:31+00:00 516,988,540	Internal Timer	Synchronize to System Clock

PTP Time

Current time information of the hardware clock domain.

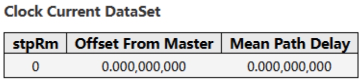
Clock Adjustment method

The clock adjustment mode for the hardware clock domain. The default is the Internal Timer mode.

Synchronize to System Clock

This operation is only applicable to instances where the clock type is 'Masteronly'. Through this operation, the system time of the device can be periodically synchronized to the hardware clock domain of the specified PTP instance (<0-3>).

Clock Current DataSet



Clock Current DataSet

stpRm	Offset From Master	Mean Path Delay
0	0.000,000,000	0.000,000,000

stpRm

This field indicates the number of hops (steps) that time synchronization information has traveled from the master clock to the current device.

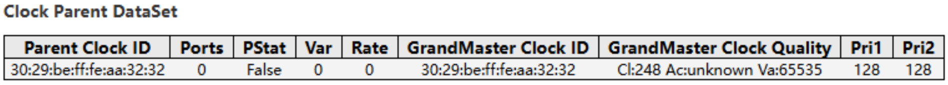
Offset From Master

It indicates the time difference between the device's local clock and the master clock.

Mean Path Delay

It indicates the average signal transmission delay between the master clock and the slave device.

Clock Parent DataSet



Clock Parent DataSet

Parent Clock ID	Ports	PStat	Var	Rate	GrandMaster Clock ID	GrandMaster Clock Quality	Pri1	Pri2
30:29:be:ff:fe:aa:32:32	0	False	0	0	30:29:be:ff:fe:aa:32:32	Cl:248 Ac:unknown Va:65535	128	128

Parent Port ID

The identifier of the parent clock in the network.

Port1

The port number of the parent clock device.

PStat

Indicates whether statistics are enabled for the parent clock.

Var

This field represents the scaled logarithmic variance of the observed relative offset of the parent clock, used for quality assessment of time synchronization.

Rate

This field represents the rate of change of clock frequency, used for quality assessment of time synchronization.

GrandMaster Clock ID

The identifier of the grandmaster clock in the network.

GrandMaster Clock Quality

1.CI (Clock Class)

Meaning: The clockClass field indicates the type or classification of the clock, with values ranging from 0 to 255. Different values represent different clock levels or qualities.

Category Description:

0-127: Indicates the category of ordinary clocks. Among them, 0 indicates the primary clock, and 127 indicates the highest quality.

128-255: Indicates different types of subordinate clocks with lower priority.

Function: Upstream clocks can select the best master clock for synchronization based on the clockClass. This is an important indicator in the clock selection process.

2. Ac (Clock Accuracy)

Meaning: clockAccuracy indicates the accuracy of the clock, usually expressed as a negative power of 2 (for example, -6 represents an accuracy of 1/64 second).

Value Description:

Smaller values (e.g., -6) indicate high accuracy; larger values (e.g., -18) indicate lower accuracy.

Based on this field, clock users can determine the time accuracy of a specific clock and make further choices.

3. (Va) Offset Scaled Log Variance

Meaning: offsetScaledLogVariance measures the fluctuation of clock offset and represents the stability of the clock frequency. It is usually expressed as a normalized logarithmic variance.

Value Description:

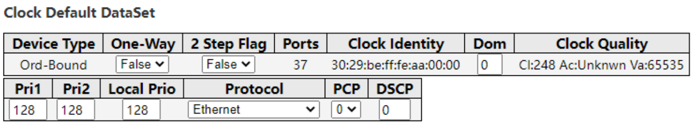
Smaller values indicate that the clock offset is relatively stable, making it suitable for use as a master clock.

Larger values indicate that the clock stability is poor and may not be suitable for synchronization.

Pri#

Parent Priority1 and Parent Priority2 Attributes.

Clock Default DataSet



Clock Default DataSet

Device Type	One-Way	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality
Ord-Bound	False	False	37	30:29:be:ff:fe:aa:00:00	0	Cl:248 Ac:Unknwn Va:65535

Pri1	Pri2	Local Prio	Protocol	PCP	DSCP
128	128	128	Ethernet	0	0

Device Type

There are eight types of clock instances in terms of devices:

Ord-Bound - The clock's device type is an Ordinary Boundary Clock.

P2p Transp - The clock's device type is a Peer-to-Peer Transparent Clock.

E2e Transp - The clock's device type is an End-to-End Transparent Clock.

Master Only - The clock's device type is a Master Clock.

Slave Only - The clock's device type is a Slave Clock.

BC-fronted - The clock's device type is a Boundary Clock Fronted.

AED-GM - The clock's device type is an AED Grandmaster Clock.

internal - The clock's device type is an Internal Clock.

One-Way

Indicates whether a DelayReq message is sent after a Sync message. By default, the DelayReq message is sent. If set to 'Yes', the DelayReq message will not be sent.

2 step flag

Indicates whether the two-step clock mode is used. If the two-step clock is enabled, a Follow Up message will follow the Sync message to carry timestamp information.

Ports

Indicates the maximum number of ports for the current device.

Clock Identity

This value is derived from the device's MAC address (e.g., 30-29-BE-52-26-26) and serves as a unique identifier for the clock device.

Dom

This configuration value specifies the domainNumber parameter value carried in protocol messages. The domainNumber is used to distinguish different PTP clock domains to ensure independent operation between different PTP instances in the same network.

Clock Quality

This value is derived from the device's MAC address, for example: 30-29-BE-52-26-26, used as a unique identifier for the clock device.

Pri#

Corresponds to the priority1 and priority2 parameters in protocol messages. These two parameters are used in PTP (Precision Time Protocol) to determine the selection order of the Grandmaster Clock.

Local Prio

Local priority settings are used in the ITU-T G.8275.1 and G.8275.2 standard specifications. Local priority participates in the Grandmaster Clock selection process through the BMCA algorithm.

Protocol

1. Ethernet: Indicates the use of standard Ethernet for PTP, which is usually the most common transmission method.

2. EthernetMixed: Refers to the implementation of PTP in an Ethernet environment, where multiple protocols are used in a mixed manner, possibly including support for traditional Ethernet and other network protocols.

3. IPv4Multi: Refers to the PTP protocol operating in an IPv4 multicast environment. This may mean that PTP messages are sent to multiple destinations.

4. IPv4Mixed: Refers to using multiple transmission methods for PTP in an IPv4 environment, such as supporting both unicast and multicast simultaneously.

5. IPv4Uni: Refers to the PTP protocol running in an IPv4 unicast environment, where each PTP message is sent directly to a specific receiver.

6. OnePPS: Sends one pulse signal per second. The OnePPS signal provides the receiving device with an absolute time reference point once per second, allowing the receiving device to adjust its local clock more accurately according to this pulse signal, thus reducing time error.

7. EthIPv4IPv6Combo: Similar PTP implementation in an IPv6 environment, indicating the mixed use of multiple protocols in an IPv6 network.

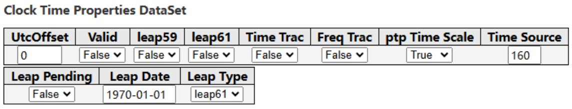
PCP

The PCP parameter is used to specify the priority of PTP messages in Ethernet, ensuring that critical time synchronization messages receive priority processing during network transmission, thereby reducing latency and improving synchronization accuracy.

DSCP

The DSCP parameter is used to mark the quality of service for PTP messages in an IP network, ensuring that these messages enjoy higher transmission priority during routing and switching, thereby enhancing the reliability and responsiveness of time synchronization.

Clock Time Properties DataSet



Clock Time Properties DataSet

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	ptp Time Scale	Time Source
0	False	False	False	False	False	True	160

Leap Pending	Leap Date	Leap Type
False	1970-01-01	leap61

UtcOffset

Set the UTC offset.

Valid

Valid This field indicates whether the leap second fields leap59 and leap61 are valid.

leap59

When set to valid, this indicates that the current UTC will decrease by 1 second (i.e., a leap second minus 1 second) for the purpose of global time synchronization adjustment.

leap61

When set to valid, this indicates that the current UTC will increase by 1 second (i.e., a leap second plus 1 second) for the purpose of global time synchronization adjustment.

Time Trac

Time Traceable Indicates the timeTraceable field in the announce message header. This flag is used to indicate whether the device's time is traceable. If the device’ s time can be traced back to a known standard, this flag will be set to TRUE. This confirms that the device can ensure its time is synchronized with a reference time source, further enhancing the precision and reliability of clock synchronization.

Freq Trac

Frequency Traceable Indicates the frequencyTraceable field in the announce message header. This flag is used to indicate whether the device's frequency is traceable. If the device’ s frequency can be traced back to a known standard, this flag will be set to TRUE. This confirms that the device can ensure its clock frequency is synchronized with a reference standard, providing more accurate clock synchronization services.

ptp Time Scale

The ptpTimescale field in the announce message header determines the accuracy and scope of the timestamps. This field can be set to TRUE or FALSE, indicating whether the timestamps follow the time scale defined by the IEEE 1588 standard. Specifically, when ptpTimescale is set to TRUE, it means that the timestamps adhere to the IEEE 1588 standard's time scale, defining the accuracy and scope according to the standard. Conversely, if ptpTimescale is set to FALSE, it means that the timestamps do not follow the IEEE 1588 standard's time scale and may use other time scales or precision.

Time Source

This field represents the timeSource field in the announce message. Specifically, the value of the timeSource field represents the type and origin of the clock. Common values include:

Local Clock: Refers to the device's own clock.

GPS: Receives time information through the GPS system.

Other Time Sources: May come from other network devices or synchronization protocols.

Leap Pending

Compensates for the timestamp handling delays of various nodes, ensuring accuracy and consistency in time synchronization.

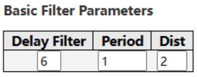
Leap Date

Select the starting point of the leap time.

Leap Type

Leap types are divided into two kinds, leap59 and leap61.

Basic Filter Parameters



Basic Filter Parameters

Delay Filter	Period	Dist
6	1	2

Delay Filter

In the basic convergence algorithm, the delay parameter is used to measure the propagation and processing delay of synchronization messages as they traverse the network. This parameter helps the algorithm accurately compute synchronization offset, thereby correctly adjusting the clocks.

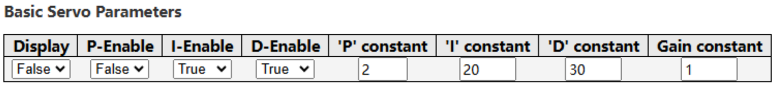
Period

In the basic convergence algorithm, the period parameter defines the interval at which synchronization messages are sent. By adjusting this parameter, you can control the frequency of synchronization messages to ensure that device clocks stay synchronized.

Dist

The dist parameter represents the relative distance or network hops between devices. This parameter helps the basic convergence algorithm to more accurately calculate the total delay, thereby better adjusting the device clocks.

Basic Servo Parameters



Basic Servo Parameters

Display	P-Enable	I-Enable	D-Enable	'P' constant	'I' constant	'D' constant	Gain constant
False	False	True	True	2	20	30	1

Display

This parameter is used to display the calculated parameter information in the base convergence algorithm of a PTP instance.

P-Enable

This parameter is used to disable the P parameter in the base convergence algorithm of a PTP instance.

I-Enable

This parameter is used to disable the I parameter in the base convergence algorithm of a PTP instance.

D-Enable

This parameter is used to disable the D parameter in the base convergence algorithm of a PTP instance.

'P' constant

This parameter is used to set the value of the P parameter in the base convergence algorithm for a specific PTP instance. The parameter is mainly used to adjust the performance of the servo convergence algorithm to improve the accuracy and stability of clock synchronization.

'I' constant

This parameter is used to set the value of the I parameter in the base convergence algorithm for a specific PTP instance. The parameter is mainly used to adjust the performance of the servo convergence algorithm to improve the accuracy and stability of clock synchronization.

'D' constant

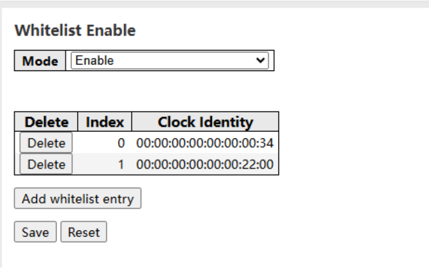
This parameter is used to set the value of the D parameter in the base convergence algorithm for a specific PTP instance. The parameter is mainly used to adjust the performance of the servo convergence algorithm to improve the accuracy and stability of clock synchronization.

Gain constant

This parameter is used to set the value of the Gain parameter in the base convergence algorithm for a specific PTP instance. The parameter is mainly used to adjust the performance of the servo convergence algorithm to improve the accuracy and stability of clock synchronization.

[Whitelist]

This page allows users to configure the PTP service whitelist.



Whitelist Enable

Mode	Enable

Delete	Index	Clock Identity
Delete	0	00:00:00:00:00:00:00:34
Delete	1	00:00:00:00:00:00:22:00

Whitelist Enable

Mode

Whitelist Enable Switch: When turned on, the whitelist functionality will be activated.

Delete

Delete Button: Click to remove the specified entry from the whitelist.

Index

Whitelist Index Value: Select through the dropdown menu. This value varies for different lists.

Clock Identity

Whitelist List Value.

Add Whitelist Entry

Use this button to add a new entry to the whitelist.

Save

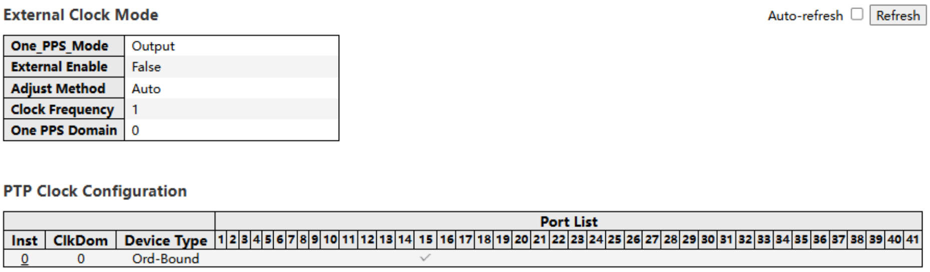
Use this button to save the newly added whitelist entry to the page.

Reset

You can undo any local changes made and revert to the previously saved values.

[Status]

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



External Clock Mode

One_PPS_Mode	Output
External Enable	False
Adjust Method	Auto
Clock Frequency	1
One PPS Domain	0

PTP Clock Configuration

			Port List																																						
Inst	ClkDom	Device Type	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
0	0	Ord-Bound															✓																										

External Clock Mode

One_PPS_Mode

Shows the current One_pps_mode configured.

1. Output : Enable the 1 pps clock output.

2. Input : Enable the 1 pps clock input.

3. Disable : Disable the 1 pps clock in/out-put.

External Enable

Shows the current External clock output configuration.

1. True : Enable the external clock output.

2. False : Disable the external clock output.

Adjust Method

Shows the current Frequency adjustment configuration.

1. LTC : Use Local Time Counter (LTC) frequency control.

2. Single : Use SyncE DPLL frequency control, if allowed by SyncE.

3. Independent : Use an oscillator independent of SyncE for frequency control, if supported by the HW.

4. Common : Use second DPLL for PTP, Both DPLL have the same (SyncE recovered) clock.

5. Auto : AUTO Select clock control, based on PTP profile and available HW resources.

Clock Frequency

Shows the current clock frequency used by the External Clock.

The possible range of values are 1 - 25000000 (1 - 25MHz).

One PPS Domain

Hardware-captured timestamps support multiple clock domains and offer configurable options.

PTP Clock Configuration

Inst

Indicates the Instance of a particular Clock Instance [0..3].

Click on the Clock Instance number to monitor the Clock details.

ClkDom

Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3].

Device Type

Indicates the Type of the Clock Instance. There are five Device Types.

1. Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock.

2. P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock.

3. E2e Transp - Clock's Device Type is End to End Transparent Clock.

4. Master Only - Clock's Device Type is Master Only.

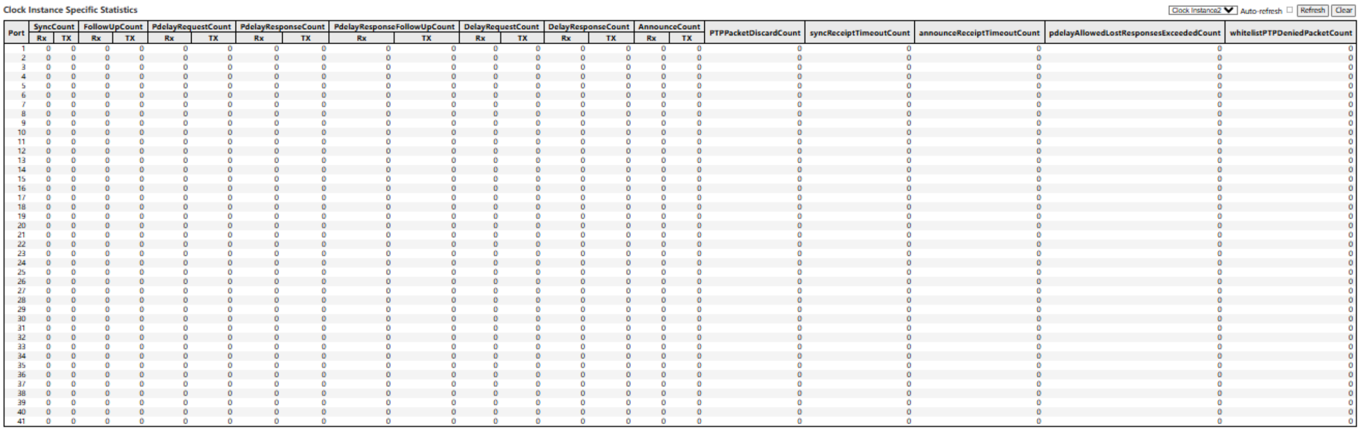
5. Slave Only - Clock's Device Type is Slave Only.

Port List

Shows the ports configured for that Clock Instance.

[Statistics]

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



Clock Instance Specific Statistics

Port	SyncCount		FollowUpCount		PdelayRequestCount		PdelayResponseCount		PdelayResponseFollowUpCount		DelayRequestCount		DelayResponseCount		AnnounceCount		PTPPacketDiscardCount	syncReceiptTimeoutCount	announceReceiptTimeoutCount	pdelayAllowedLostResponsesExceededCount	whitelistPTPDeniedPacketCount
	Rx	TX	Rx	TX	Rx	TX	Rx	TX	Rx	TX	Rx	TX	Rx	TX	Rx	TX					
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
37	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
38	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
39	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
40	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
41	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Recieved counters

Port

This is displayed as the physical port number of the device.

SyncCount

A counter that increments every time when synchronization information is received or transmit.

FollowUpCount

A counter that increments every time when a Follow Up message is received or transmit.

PdelayRequestCount

A counter that increments every time when a Pdelay_Req message is received or transmit.

PdelayResponseCount

A counter that increments every time when a Pdelay_Resp message is received or transmit.

PdelayResponseFollowUpCount

A counter that increments every time when a Pdelay_Resp_Follow_Up message is received or transmit.

DelayRequestCount

A counter that increments every time a Delay_Req message is received or transmission.

DelayResponseCount

A counter that increments every time a Delay_Resp message is received or transmitted.

AnnounceCount

A counter that increments every time when an Announce message is received or transmit.

PTPPacketDiscardCount

A counter that increments every time when a PTP message is discarded.

syncReceiptTimeoutCount

A counter that increments every time when sync receipt timeout occurs.

announceReceiptTimeoutCount

A counter that increments every time when announce receipt timeout occurs.

pdelayAllowedLostResponsesExceededCount

A counter that increments everytime the value of the variable lostResponses exceeds the value of the variable allowedLostResponses.

whitelistPTPDeniedPacketCount

After enabling the PTP whitelist function, the number of message packets rejected (due to not being on the whitelist) will be counted upon receiving PTP messages.

Transmit Counters

SyncCount

A counter that increments every time synchronization information is transmitted.

FollowUpCount

A counter that increments every time a Follow_Up message is transmitted.

PdelayRequestCount

A counter that increments every time a Pdelay_Req message is transmitted.

PdelayResponseCount

A counter that increments every time a Pdelay_Resp message is transmitted.

PdelayResponseFollowUpCount

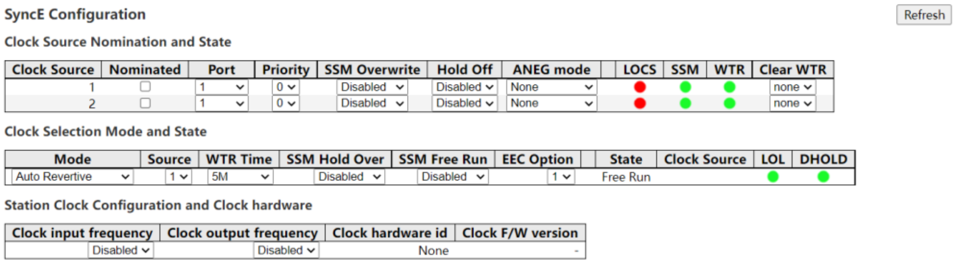
A counter that increments every time a Pdelay_Resp_Follow_Up message is transmitted.

AnnounceCount

A counter that increments every time an Announce message is transmitted.

2.5. SyncE

[Time > SyncE]



SyncE Configuration

Refresh

Clock Source Nomination and State

Clock Source	Nominated	Port	Priority	SSM Overwrite	Hold Off	ANEG mode		LOCS	SSM	WTR	Clear WTR
1	□	1	0	Disabled	Disabled	None		🔴	🟢	🟢	none
2	□	1	0	Disabled	Disabled	None		🔴	🟢	🟢	none

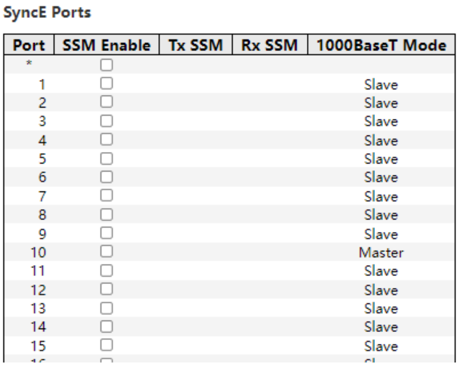
Clock Selection Mode and State

Mode	Source	WTR Time	SSM Hold Over	SSM Free Run	EEC Option		State	Clock Source	LOL	DHOLD
Auto Revertive	1	5M	Disabled	Disabled	1		Free Run		🟢	🟢

Station Clock Configuration and Clock hardware

Clock input frequency	Clock output frequency	Clock hardware id	Clock F/W version
Disabled	Disabled	None	-

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



SyncE Ports

Port	SSM Enable	Tx SSM	Rx SSM	1000BaseT Mode
*	□			
1	□			Slave
2	□			Slave
3	□			Slave
4	□			Slave
5	□			Slave
6	□			Slave
7	□			Slave
8	□			Slave
9	□			Slave
10	□			Master
11	□			Slave
12	□			Slave
13	□			Slave
14	□			Slave
15	□			Slave

Clock Source Nomination and State

For each possible clock source the following can be configured.

Clock Source

This is the instance number of the clock source. This has to be referenced when selecting 'Manual' Mode.

Nominated

When a clock source is nominated, the clock output from the related PHY (Port) is enabled against the clock controller. This makes it available as a possible source in the clock selection process. If it is supported by the actual HW configuration, The Station clock input can be nominated as a Clock Source.

Port

In this drop down box, the ports that are possible to select for this clock source, is presented. The PCB104 Synce module supports 10MHz station clock input. The station clock input is indicated by a port name = 'S-CLK'. The serval1 has a limitation that chip port 1 cannot be nominated as source 1. On the Vitesse boards this is port 7 (interface gi 1/7).

Serval2 NID board limitations: Port 5-12 can be configured for 100M, 1G or 2.5G speed. In 2.5G speed mode the SyncE hardware is not able to lock, because the recovered clock output frequency does not match the SyncE hardware's frequency options.

Priority

The priority for this clock source. Lowest number (0) is the highest priority. If two clock sources has the same priority, the lowest clock source number gets the highest priority in the clock selection process.

SSM Overwrite

A selectable clock source Quality Level (QL) to overwrite any QL received in a SSM. If QL is not Received in a SSM (SSM is not enabled on this port), the SSM Overwrite QL is used as if received. The SSM Overwrite can be set to QL_NONE, indicating that the clock source is without any known quality (Lowest compared to clock source with known quality).

1. Disabled.

2. QL PRC - Precision Reference Clock.

3. QL SSUA - Synchronous Signal Under Algorithm.

4. QL SSUB - Synchronous Signal Under Bus.

5. QL EECE1 - Error Event Condition 1.

6. QL DNU - Do Not Use.

Hold Off

The Hold Off timer value. Active loss of clock Source will be delayed the selected amount of time. The clock selector will not change clock source if the loss of clock condition is cleared within this time. Test represents 100ms.

ANEG Mode

This is relevant for 1000BaseT ports only. In order to recover clock from port it must be negotiated to 'Slave' mode. In order to distribute clock the port must be negotiated to 'Master' mode.
This different ANEG modes can be activated on a Clock Source port:
Prefer Slave: The Port will be negotiated to 'Slave' mode if possible.
Prefer Master: The Port will be negotiated to 'Master' mode if possible.
Forced Slave: The Port will be forced to 'Slave' mode.

The selected port in 'Locked' state will always be negotiated to 'Slave' if possible.

LOCS

Signal is lost on this clock source.

SSM

If SSM(System Synchronization Message) is enabled and not received properly. Type of SSM fail will be indicated in the 'Rx SSM' field.

WTR

Wait To Restore timer is active.

Clear WTR

Clears the WTR timer and makes this clock source available to the clock selection process.

Clock Selection Mode and State

The Clock Selector is only in one instance - the one who selects between the nominated clock sources.

Mode

The definition of the 'best' clock source is firstly the one with the highest (QL) and secondly (the ones with equal QL) the highest priority.

Clock Selector can be in different modes:

Manual: Clock selector will select the clock source stated in Source (see below). If this manually selected clock source is failing, the clock selector will go into holdover state.

Manual To Selected: Same as Manual mode where the port. selected clock source will become Source.

Auto NonRevertive: Clock Selection of the best clock source is only done when the selected clock fails.

Auto Revertive: Clock Selection of the best clock source is constantly done.

Force Hold Over: Clock Selector is forced to Hold Over State.

Force Free Run: Clock Selector is forced to Free Run State.

Source

Only relevant if Manual mode is selected (see above).

WTR Time

WTR is the Wait To Restore timer value in minutes. The WTR time is activated on the falling edge of a clock source failure (in Revertive mode). This means that the clock source is first available for clock selection after WTR Time (can be cleared).

SSM Hold Over

This is the transmitted SSM QL value when clock selector is in Hold Over State.

SSM Free Run

This is the transmitted SSM QL value when clock selector is in Free Run State.

EEC Option

The ZL30xxx based Synce modules support both EEC1 and EEC2 option. The difference is: EEC1=> DPLL bandwidth=3,5 Hz, EEC2=> DPLL bandwidth = 0,1 Hz.

State

This is indicating the state of the clock selector. Possible states are:
Free Run: There is no external clock sources to lock to (unlocked state). The Clock Selector has never been locked to a clock source long enough to calculate the hold over frequency offset to local oscillator. The frequency of this node is the frequency of the local oscillator.
Hold Over: There is no external clock sources to lock to (unlocked state). The Clock Selector has calculate the holdover frequency offset to local oscillator. The frequency of this node is hold to the frequency of the clock source previous locked to.
Locked: Clock selector is locked to the clock source indicated (See next).

Top: Clock selector is locked to Time over packets, e.g. PTP (See next).

Clock Source

The clock source locked to when clock selector is in locked state.

LOL

Clock selector has raised the Los Of Lock alarm.

DHOLD

Clock selector has not yet calculated the holdover frequency offset to local oscillator. This becomes active for about 10 s. when a new clock source is selected.

Station Clock Configuration and Clock hardware

The Synce module may have a Station clock input and/or a Station clock output.

Clock input frequency

If supported by the Synce HW, the station clock input frequency can be configured, the possible frequencies are:

1,544 MHz, 2,048 MHz or 10 MHz

Clock Output frequency

If supported by the Synce HW, the station clock output frequency can be configured, the possible frequencies are:

1,544 MHz, 2,048 MHz or 10 MHz

Clock hardware id

It corresponds to a dedicated clock synchronization chip.

Clock F/W version

The version information corresponding to the synchronization chip, with the Party and Masses Department having only this chip, hwZL30772, for which version information is provided.

SyncE Ports

For each possible port on switch.

Port

The port number to configure.

SSM Enable

Enable and disable of SSM functionality on this port.

Tx SSM

Monitoring of the transmitted SSM QL on this port. Transmitted QL should be the Quality Level of the clock generated by this node. This means the QL of the clock source this node is locked to.

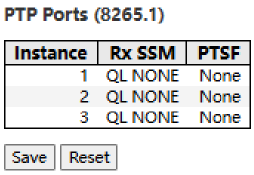
Rx SSM

Monitoring of the received SSM QL on this port. If link is down on port, QL_LINK is indicated. If no SSM is received, QL_FAIL is indicated.

1000BaseT Mode

If PHY is in 1000BaseT Mode then this is monitoring the master/slave mode. In order to receive clock on a port, it has to be in slave mode. In order to transmit clock on a port, it has to be in master mode.

PTP Ports



PTP Ports (8265.1)

Instance	Rx SSM	PTSF
1	QL NONE	None
2	QL NONE	None
3	QL NONE	None

Instance

Monitor the instance values received at this port.

Rx SSM

Monitoring of the received SSM QL on this port. If link is down on port, QL_LINK is indicated. If no SSM is received, QL_FAIL is indicated.

PTSF

Monitor the PTSF status received at this port.

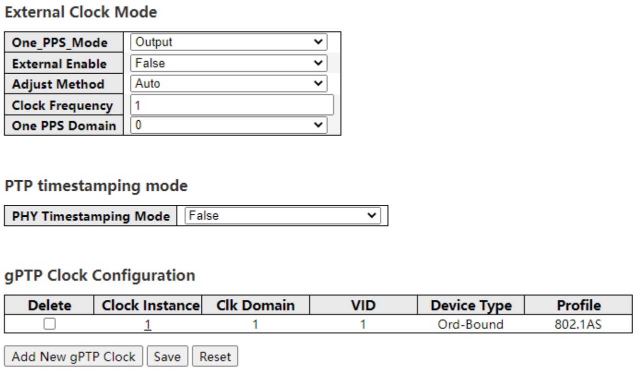
2.6. TSN

2.6.1. gPTP

[Time > TSN > gPTP]

[Configuration]

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



External Clock Mode

One_PPS_Mode	Output
External Enable	False
Adjust Method	Auto
Clock Frequency	1
One PPS Domain	0

PTP timestamping mode

PHY Timestamping Mode	False

gPTP Clock Configuration

Delete	Clock Instance	Clk Domain	VID	Device Type	Profile
□	1	1	1	Ord-Bound	802.1AS

External Clock Mode

One_PPS_Mode

This Selection box will allow you to select the One_pps_mode configuration.

The following values are possible:

1. Output : Enable the 1 pps clock output.

2. Input : Enable the 1 pps clock input.

3. Disable : Disable the 1 pps clock in/out-put.

External Enable

This Selection box will allow you to configure the External Clock output.

The following values are possible:

1. True : Enable the external clock output.

2. False : Disable the external clock output.

Adjust Method

This Selection box will allow you to configure the Frequency adjustment configuration.

1. LTC : Select Local Time Counter (LTC) frequency control.

2. Auto : AUTO Select clock control, based on PTP profile and available HW resources.

3. Independent : Use an oscillator independent of SyncE for frequency control, if supported by the HW.

Clock Frequency

This will allow to set the Clock Frequency.

The possible range of values are 1 - 25000000 (1 - 25MHz).

One PPS Domain

Hardware timestamp capture, supporting multiple hardware domains, offers many options.

PTP timestamping mode

PHY Timestamping Mode

Used to enable or disable PHY timestamping when the device supports it.

gPTP Clock Configuration

Delete

Check this checkbox and click on 'Save' to delete the clock instance.

Clock Instance

Indicates the instance number of a particular Clock Instance [0..3].

Clk Domain

Indicates the CLK clock domain used by the clock.

VID

VLAN Identifier used for tagging the VLAN packets.

Device Type

Indicates the Type of the Clock Instance. There are five Device Types.

1. Ord-Bound - clock's Device Type is Ordinary-Boundary Clock.

2. P2p Transp - clock's Device Type is Peer to Peer Transparent Clock.

3. E2e Transp - clock's Device Type is End to End Transparent Clock.

4. Master Only - clock's Device Type is Master Only.

5. Slave Only - clock's Device Type is Slave Only.

6. BC-fronted - boundary Clock front end.

7. AED-GM - AED Grandmaster.

Profile

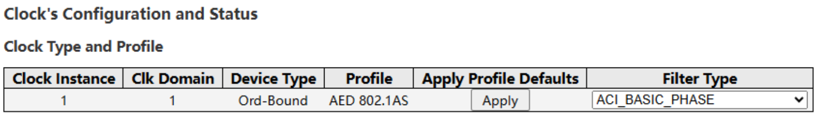
Indicates the profile used by the clock.

1. 802.1AS - 802.1AS profile.

2. AED 802.1AS - 802.1AS AED profile.

Click on the clock instance to enter the specific clock instance configuration page.

Clock Type and Profile



Clock's Configuration and Status

Clock Type and Profile

Clock Instance	Clk Domain	Device Type	Profile	Apply Profile Defaults	Filter Type
1	1	Ord-Bound	AED 802.1AS	Apply	ACI_BASIC_PHASE

Clock Instance

The instance number of a specific clock instance [0..3].

Clk Domain

The CLK clock domain used by the clock.

Device Type

The type of clock instance. There are eight device types:

Ord-Bound - The device type of the clock is ordinary boundary clock.

P2p Transp - The device type of the clock is peer-to-peer transparent clock.

E2e Transp - The device type of the clock is end-to-end transparent clock.

Master Only - The device type of the clock is master clock.

Slave Only - The device type of the clock is slave clock.

BC-fronted - The device type of the clock is boundary clock front-end.

AED-GM - The device type of the clock is AED grandmaster clock.

Internal clock.

Profile

The configuration profile used by the clock:

6. None - The default 1588 profile is used.

7. 1588 - IEEE 1588 profile.

8. G8265.1 - G8265.1 profile.

9. G8275.1 - G8275.1 profile.

10. G8275.2 - G8275.2 profile.

Apply Profile Defaults

Click to apply attributes.

Filter Type

There are four filtering types:

5. ACL_BASIC_PHASE.

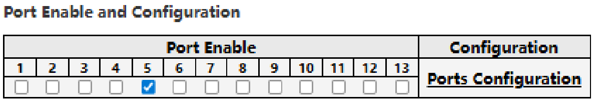
6. ACL_BASIC_PHASE_LOW.

7. ACL_BC_FULL_ON_PATH_FREQ.

8. BASIC.

The default is the BASIC algorithm.

Port Enable and Configuration



Port Enable and Configuration

Port Enable													Configuration
1	2	3	4	5	6	7	8	9	10	11	12	13	Ports Configuration
□	□	□	□	☑	□	□	□	□	□	□	□	□	

Port Enable

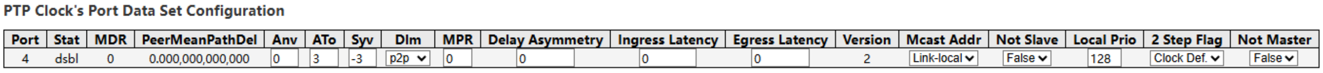
Check the corresponding port to indicate that the PTP instance completes clock synchronization on this port.

Configuration

Ports Configuration.

Click Port Configuration.

PTP Clock's Port Data Set Configuration



PTP Clock's Port Data Set Configuration

Port	Stat	MDR	PeerMeanPathDel	Anv	ATo	Syv	Dlm	MPR	Delay Asymmetry	Ingress Latency	Egress Latency	Version	Mcast Addr	Not Slave	Local Prio	2 Step Flag	Not Master
4	dsbl	0	0.000,000,000,000	0	3	-3	p2p	0	0	0	0	2	Link-local	False	128	Clock Def.	False

Port

Enable the clock port.

Stat

PTP port states are divided into: init, lstn, uncl, slve, mstr, dsbl, p2pt, et2t, flty, frnd.

MDR

This value indicates the configuration value for the delay request message interval currently in use. The value is a positive integer n, representing 2 to the power of n, where the actual time interval is 2^n seconds. This interval denotes the time between sending delay request messages from a Slave device to a Master device.

PeerMeanPathDel

This value represents the delay information measured and calculated from the peer_delay_req and resp response messages. The format is as follows: AA.BBB,CCC,DDD where AA is in seconds, BBB is in milliseconds, CCC is in microseconds, and DDD is in nanoseconds.

Anv

This value represents the number of times an announce request message is sent. It is calculated as a power of 2, with the unit in seconds.

ATo

This value, together with the frequency of announce message sending, determines the announce message sending timeout.

Syv

This value represents the sync request message transmission period, calculated as a power of 2, with the unit in seconds.

Dlm

This value represents the link measurement method and can be one of three types: e2e, p2p, or cp2p. The choice depends on the clock type of the peer device. If the peer is a p2p transparent clock, select either p2p or cp2p, noting that the header formats for p2p and cp2p are different.

MPR

This value represents the delay request message transmission period, calculated as a power of 2, with the unit in seconds.

Delay Asymmetry

When the receive path delay is greater than the send path delay or when the receive path delay is less than the send path delay, it indicates that the delay compensation amount needs to be set. This parameter needs to be configured.

Ingress Latency

This parameter is used to configure the ingress delay of the device. Ingress delay refers to the time delay between receiving the data packet at the network interface and the actual processing of the data packet within the device.

Egress Latency

This parameter is used to configure the egress delay of the device. Egress delay refers to the time delay from when a data packet is processed internally within the device and ready to be sent to the network interface, to when the data packet is actually transmitted from the network interface.

Version

Protocol version number, currently by default is 1588 2019 2.0 version.

Mcast Addr

The default value is 'default'.

When set to 'default',

the layer 2 multicast destination address is: 0x01, 0x1b, 0x19, 0x00, 0x00, 0x00 (syn announce), the layer 3 multicast IP address is: 0x01, 0x00, 0x5e, 0x00, 0x01, 0x81.

When set to 'Link_local',

the layer 2 multicast destination address is: 0x01, 0x80, 0xC2, 0x00, 0x00, 0x0E (syn announce), d the layer 3 multicast IP address is: 0x01, 0x00, 0x5e, 0x00, 0x00, 0x6B.

Not Slave

When this value is set to true, the port defaults to being the master clock.

Local Prio

Local priority setting is used in the ITU-T G.8275.1 and G.8275.2 standards, where the local priority is involved in the master clock selection process through the BMCA algorithm.

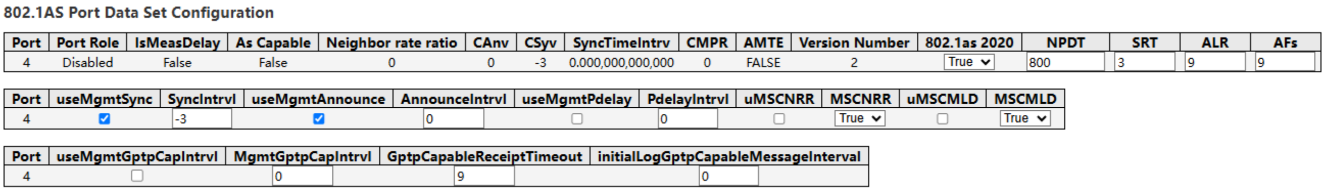
2 Step Flag

This value determines whether to use a two-step clock, where a follow-up message carries timestamp information following a sync message. The default is 'default', following the global PTP clock configuration settings.

Not Master

When this value is set to true, the port becomes the default slave clock.

802.1AS Port Data Set Configuration



802.1AS Port Data Set Configuration

Port	Port Role	IsMeasDelay	As Capable	Neighbor rate ratio	CAnv	CSyv	SyncTimeIntrv	CMPR	AMTE	Version Number	802.1as 2020	NPDT	SRT	ALR	AFs
4	Disabled	False	False	0	0	-3	0.000,000,000,000	0	FALSE	2	True ⌄	800	3	9	9

Port	useMgmtSync	SyncIntrvl	useMgmtAnnounce	AnnounceIntrvl	useMgmtPdelay	PdelayIntrvl	uMSCNRR	MSCNRR	uMSCMLD	MSCMLD
4	☑	-3	☑	0	□	0	□	True ⌄	□	True ⌄

Port	useMgmtGptpCapIntrvl	MgmtGptpCapIntrvl	GptpCapableReceiptTimeout	initialLogGptpCapableMessageInterval
4	□	0	9	0

Port

Enable the clock port.

Port role

gPTP Port States are classified as Disabled, Master, Passive, Slave.

IsMeasDelay

The value (isMeasuringDelay) indicates whether the port has completed the propagation delay measurement of the PTP link.

As Capable

The value (asCapable) indicates whether the link between two PTP instances on a network can achieve time synchronization according to the IEEE 802.1AS protocol.

Neighbor rate ratio

The value denotes the frequency ratio between adjacent nodes, which is calculated.

CAnv

The value indicates the current announce message transmission interval.

CSyv

The value indicates the current sync message transmission interval.

SyncTimeIntrv

The value represents the time interval for forwarding sync messages.

CMPR

The value indicates the current peer delay request message transmission period.

AMTE

The value specifies whether to enable or disable the acceptance of the main clock table.

Version Number

Protocol version number, currently the default is 1588 2019 version 2.0.

802.1as 2020

802.1AS 2020 profile.

NPDT

The value indicates the minimum delay threshold for peer_delay_req and resp response messages. If the actual delay value exceeds this value, it triggers time synchronization messages.

SRT

The value represents the timeout period, measured in units of syncTimeInterval.

ALR

This value represents the maximum number of times a peer_delay_req request message can be sent without receiving a response. If the number of unresponded peer_delay_req request messages exceeds this setting, the Pdelay counter that allows for missed responses will start to be counted.

AFs

This value represents the maximum number of consecutive failures allowed in the peer_delay_req request process. If the specified maximum allowed failure count is exceeded, the device will not trigger gPTP clock synchronization to avoid inaccurate time synchronization states.

useMgmtSync

Check the box to confirm whether the sync message transmission interval follows the SyncIntrvl setting.

SyncIntrvl

When checked, the sync transmission interval will be the value set here.

useMgmtAnnounce

Check the box to confirm whether the Announce message transmission interval follows the AnnounceIntrvl setting.

AnnounceIntrvl

When checked, the Announce message transmission interval will be the value set here.

useMgmtPdelay

Check the box to confirm whether the Peer_delay_req message transmission interval follows the PdelayIntrvl setting.

PdelayIntrvl

When checked, the Peer_delay_req message transmission interval will be the value set here.

uMSCNRR

When checked, the MSCNRR value is valid.

MSCNRR

Whether to calculate the neighbor_rate_ratio (frequency ratio between adjacent nodes).

uMSCMLD

When checked, the MSCMLD value is valid.

MSCMLD

Whether to update the link delay value results.

useMgmtGptpCapIntrvl

Check the box to confirm whether the signal message transmission interval follows the MgmtGptpCapIntrvl setting.

MgmtGptpCapIntrvl

When checked, the signal message transmission interval will be the value set here.

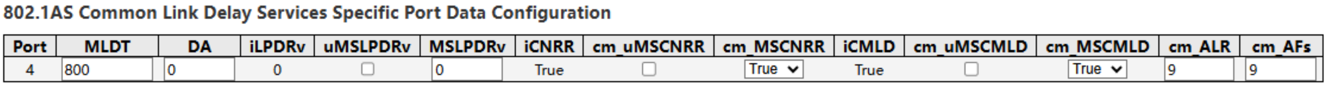
GptpCapableReceiptTimeout

This value is used to set the timeout value for Signal messages in the gPTP messages for the port, representing the timeout interval for signal messages.

initialLogGptpCapableMessageInterval

The initial signal message transmission interval will be the value set here.

802.1AS Common Link Delay Services Specific Port Data Configuration



802.1AS Common Link Delay Services Specific Port Data Configuration

Port	MLDT	DA	iLPDRv	uMSLPDRv	MSLPDRv	iCNRR	cm_uMSCNRR	cm_MSCNRR	iCMLD	cm_uMSCMLD	cm_MSCMLD	cm_ALR	cm_AFs
4	800	0	0	□	0	True	□	True	True	□	True	9	9

Port

Enable the clock port.

MLDT

In common link delay measurement mode, this value represents the minimum delay threshold for peer_delay_req and resp response messages. If the actual delay value exceeds this threshold, time synchronization messages will be triggered.

DA

In common link delay measurement mode, this parameter represents the delay asymmetry. It can be set if the uplink and downlink delays are different in the current network.

iLPDRv

In common link delay measurement mode, this value represents the current transmission interval for peer delay request messages.

uMSLPDRv

Check the box to confirm if the MSLPDRv message transmission interval follows the PdelayIntrvl setting.

MSLPDRv

When checked, in common link delay measurement mode, the transmission interval for Peer_delay_req messages will be the value set here.

iCNRR

Whether to currently calculate the neighbor_rate_ratio (frequency ratio between adjacent nodes).

cm_uMSCNRR

When this value is checked, the cm_MSCNRR value is valid.

cm_MSCNRR

Whether to currently calculate the neighbor_rate_ratio (frequency ratio between adjacent nodes).

iCMLD

Whether to currently update the link delay value results.

cm_uMSCMLD

When this value is checked, the cm_MSCMLD value is valid.

cm_MSCMLD

Whether to currently update the link delay value results.

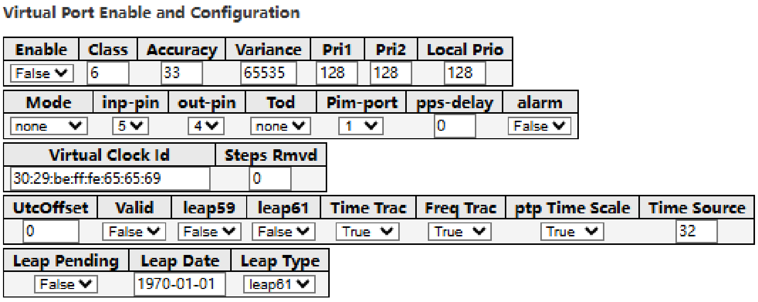
cm_ALR

In common link delay measurement mode, this value represents the maximum number of times a peer_delay_req request message can be sent without receiving a response. If the number of unresponded peer_delay_req request messages exceeds this setting, the Pdelay counter that allows for missed responses will start to be counted.

cm_AFs

In common link delay measurement mode, this value represents the maximum number of consecutive failures allowed in the peer_delay_req request process. If the specified maximum allowed failure count is exceeded, the device will not trigger gPTP clock synchronization to avoid inaccurate time synchronization states.

Virtual Port Enable and Configuration



Virtual Port Enable and Configuration

Enable	Class	Accuracy	Variance	Pri1	Pri2	Local Prio
False	6	33	65535	128	128	128

Mode	inp-pin	out-pin	Tod	Pim-port	pps-delay	alarm
none	5	4	none	1	0	False

Virtual Clock Id	Steps Rmvd
30:29:be:ff:fe:65:65:69	0

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	ptp Time Scale	Time Source
0	False	False	False	True	True	True	32

Leap Pending	Leap Date	Leap Type
False	1970-01-01	leap61

Enable

Enable virtual port.

Class

This is the clock class field within the clock quality structure. According to the 1588 protocol standard:

6 (GM locked to 1pps output)

7 (GM in holdover state after 1pps output)

135 (boundary clock in holdover state)

165 (boundary clock out of holdover state)

140 (CAT 1 GM out of holdover state)

150 (CAT 2 GM out of holdover state)

160 (CAT 3 GM out of holdover state)

248 (default)

255 (time from clock)

Accuracy

This is the clock accuracy field within the clock quality structure. The values represent:

32 (25 nanoseconds)

33 (100 nanoseconds)

34 (250 nanoseconds)

35 (1 microsecond)

36 (2.5 microseconds)

37 (10 microseconds)

38 (25 microseconds)

39 (100 microseconds)

40 (250 microseconds)

41 (1 millisecond)

42 (2.5 milliseconds)

43 (10 milliseconds)

44 (25 milliseconds)

45 (100 milliseconds)

46 (250 milliseconds)

47 (1 second)

48 (10 seconds)

49 (greater than 10 seconds)

254 (unknown)

Variance

This parameter is used in the IEEE 1588 protocol to evaluate the stability and quality of the time offset of the master clock. It provides a measure of the master clock's stability for the slave clocks, aiding in the optimization of the time synchronization process to ensure precision and reliability in the network. A smaller variance indicates that the time offset between the master clock and the slave clocks is more stable and consistent.

Pri#

The priority1 and priority2 parameters in the protocol message are used to determine the selection order of the Grandmaster Clock in the Precision Time Protocol (PTP).

Local Prio

Local priority setting is used in the ITU-T G.8275.1 and G.8275.2 standards, where the local priority is involved in the master clock selection process through the BMCA algorithm.

Mode

There are four modes:

5. none.

6. pps-in.

7. pps-out.

8. freq-out.

Inp-pin

Indicates configuring an input/output pin as PPS input mode to receive the per-second pulse signal sent by an external device.

Out-pin

Indicates configuring an input/output pin as PPS output mode to send the per-second pulse signal.

Tod

Indicates the protocol used for transmitting astronomical time (date and time information). The specific options are as follows:

ZDA is the most commonly used standard protocol, specifically used for transmitting date and time information.

GGA and RMC provide positional data as well as time information.

POLYT and PIM may be custom protocols for specific systems or applications.

NONE indicates that no protocol is used for transmitting time information.

Pim-port

The port number for transmitting TOD using the PIM protocol.

pps-delay

Estimated delay time for the PPS signal from the source to the receiver.

alarm

Whether to alarm.

Virtual Clock Id

When using a virtual clock port, configure the clock identifier. This value can be modified.

Steps Rmvd

This parameter represents the number of intermediate clocks that the sync message has passed through from the Master Clock to the current device. Specifically, it records how many steps (Steps) it has taken from the Master Clock to the current device. This value can be configured.

UtcOffset

Set the UTC offset.

Valid

Valid This field indicates whether the leap second fields leap59 and leap61 are valid.

leap59

When set to valid, this indicates that the current UTC will decrease by 1 second (i.e., a leap second minus 1 second) for the purpose of global time synchronization adjustment.

leap61

When set to valid, this indicates that the current UTC will increase by 1 second (i.e., a leap second plus 1 second) for the purpose of global time synchronization adjustment.

Time Trac

Time Traceable Indicates the timeTraceable field in the announce message header. This flag is used to indicate whether the device's time is traceable. If the device’ s time can be traced back to a known standard, this flag will be set to TRUE. This confirms that the device can ensure its time is synchronized with a reference time source, further enhancing the precision and reliability of clock synchronization.

Freq Trac

Frequency Traceable Indicates the frequencyTraceable field in the announce message header. This flag is used to indicate whether the device's frequency is traceable. If the device’ s frequency can be traced back to a known standard, this flag will be set to TRUE. This confirms that the device can ensure its clock frequency is synchronized with a reference standard, providing more accurate clock synchronization services.

ptp Time Scale

The ptpTimescale field in the announce message header determines the accuracy and scope of the timestamps. This field can be set to TRUE or FALSE, indicating whether the timestamps follow the time scale defined by the IEEE 1588 standard. Specifically, when ptpTimescale is set to TRUE, it means that the timestamps adhere to the IEEE 1588 standard's time scale, defining the accuracy and scope according to the standard. Conversely, if ptpTimescale is set to FALSE, it means that the timestamps do not follow the IEEE 1588 standard's time scale and may use other time scales or precision.

Time Source

This field represents the timeSource field in the announce message. Specifically, the value of the timeSource field represents the type and origin of the clock. Common values include:

Local Clock: Refers to the device's own clock.

GPS: Receives time information through the GPS system.

Other Time Sources: May come from other network devices or synchronization protocols.

Leap Pending

Compensates for the timestamp handling delays of various nodes, ensuring accuracy and consistency in time synchronization.

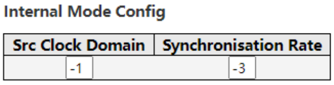
Leap Date

Select the starting point of the leap time.

Leap Type

Leap types are divided into two kinds, leap59 and leap61.

Internal Mode Config



Internal Mode Config

Src Clock Domain	Synchronisation Rate
-1	-3

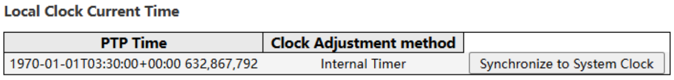
Src Clock Domain

This parameter corresponds to the clock instance number when the clock type is set to Internal.

Synchronisation Rate

This parameter represents the time interval, indicating how often the software clock synchronizes with hardware domain 0.

Local Clock Current Time



Local Clock Current Time

PTP Time	Clock Adjustment method	
1970-01-01T03:30:00+00:00 632,867,792	Internal Timer	Synchronize to System Clock

PTP Time

Current time information of the hardware clock domain.

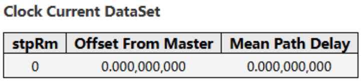
Clock Adjustment method

The clock adjustment mode for the hardware clock domain. The default is the Internal Timer mode.

Synchronize to System Clock

This operation is only applicable to instances where the clock type is 'Masteronly'. Through this operation, the system time of the device can be periodically synchronized to the hardware clock domain of the specified PTP instance (<0-3>).

Clock Current DataSet



Clock Current DataSet

stpRm	Offset From Master	Mean Path Delay
0	0.000,000,000	0.000,000,000

stpRm

This field indicates the number of hops (steps) that time synchronization information has traveled from the master clock to the current device.

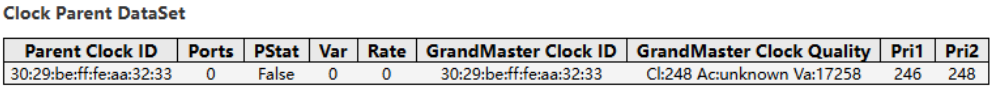
Offset From Master

It indicates the time difference between the device's local clock and the master clock.

Mean Path Delay

It indicates the average signal transmission delay between the master clock and the slave device.

Clock Parent DataSet



Clock Parent DataSet

Parent Clock ID	Ports	PStat	Var	Rate	GrandMaster Clock ID	GrandMaster Clock Quality	Pri1	Pri2
30:29:be:ff:fe:aa:32:33	0	False	0	0	30:29:be:ff:fe:aa:32:33	Cl:248 Ac:unknown Va:17258	246	248

Parent Clock ID

The identifier of the parent clock in the network.

Ports

The ports number of the parent clock device.

PStat

Indicates whether statistics are enabled for the parent clock.

Var

This field represents the scaled logarithmic variance of the observed relative offset of the parent clock, used for quality assessment of time synchronization.

Rate

This field represents the rate of change of clock frequency, used for quality assessment of time synchronization.

GrandMaster Clock ID

The identifier of the grandmaster clock in the network.

GrandMaster Clock Quality

1.CI (Clock Class)

Meaning: The clockClass field indicates the type or classification of the clock, with values ranging from 0 to 255. Different values represent different clock levels or qualities.

Category Description:

0-127: Indicates the category of ordinary clocks. Among them, 0 indicates the primary clock, and 127 indicates the highest quality.

128-255: Indicates different types of subordinate clocks with lower priority.

Function: Upstream clocks can select the best master clock for synchronization based on the clockClass. This is an important indicator in the clock selection process.

2. Ac (Clock Accuracy)

Meaning: clockAccuracy indicates the accuracy of the clock, usually expressed as a negative power of 2 (for example, -6 represents an accuracy of 1/64 second).

Value Description:

Smaller values (e.g., -6) indicate high accuracy; larger values (e.g., -18) indicate lower accuracy.

Based on this field, clock users can determine the time accuracy of a specific clock and make further choices.

3. (Va) Offset Scaled Log Variance

Meaning: offsetScaledLogVariance measures the fluctuation of clock offset and represents the stability of the clock frequency. It is usually expressed as a normalized logarithmic variance.

Value Description:

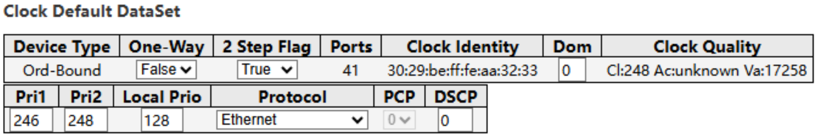
Smaller values indicate that the clock offset is relatively stable, making it suitable for use as a master clock.

Larger values indicate that the clock stability is poor and may not be suitable for synchronization.

Pri#

Parent Priority1 and Parent Priority2 Attributes.

Clock Default DataSet



Clock Default DataSet

Device Type	One-Way	2 Step Flag	Ports	Clock Identity	Dom	Clock Quality
Ord-Bound	False	True	41	30:29:be:ff:fe:aa:32:33	0	Cl:248 Ac:unknown Va:17258

Pri1	Pri2	Local Prio	Protocol	PCP	DSCP
246	248	128	Ethernet	0	0

Device Type

There are eight types of clock instances in terms of devices:

Ord-Bound - The clock's device type is an Ordinary Boundary Clock.

P2p Transp - The clock's device type is a Peer-to-Peer Transparent Clock.

E2e Transp - The clock's device type is an End-to-End Transparent Clock.

Master Only - The clock's device type is a Master Clock.

Slave Only - The clock's device type is a Slave Clock.

BC-fronted - The clock's device type is a Boundary Clock Fronted.

AED-GM - The clock's device type is an AED Grandmaster Clock.

internal - The clock's device type is an Internal Clock.

One-Way

Indicates whether a DelayReq message is sent after a Sync message. By default, the DelayReq message is sent. If set to 'Yes', the DelayReq message will not be sent.

2 step flag

Indicates whether the two-step clock mode is used. If the two-step clock is enabled, a Follow Up message will follow the Sync message to carry timestamp information.

Ports

Indicates the maximum number of ports for the current device.

Clock Identity

This value is derived from the device's MAC address (e.g., 30-29-BE-52-26-26) and serves as a unique identifier for the clock device.

Dom

This configuration value specifies the domainNumber parameter value carried in protocol messages. The domainNumber is used to distinguish different PTP clock domains to ensure independent operation between different PTP instances in the same network.

Clock Quality

This value is derived from the device's MAC address, for example: 30-29-BE-52-26-26, used as a unique identifier for the clock device.

Pri#

Corresponds to the priority1 and priority2 parameters in protocol messages. These two parameters are used in PTP (Precision Time Protocol) to determine the selection order of the Grandmaster Clock.

Local Prio

Local priority settings are used in the ITU-T G.8275.1 and G.8275.2 standard specifications. Local priority participates in the Grandmaster Clock selection process through the BMCA algorithm.

Protocol

8. Ethernet: Indicates the use of standard Ethernet for PTP, which is usually the most common transmission method.

9. EthernetMixed: Refers to the implementation of PTP in an Ethernet environment, where multiple protocols are used in a mixed manner, possibly including support for traditional Ethernet and other network protocols.

10. IPv4Multi: Refers to the PTP protocol operating in an IPv4 multicast environment. This may mean that PTP messages are sent to multiple destinations.

11. IPv4Mixed: Refers to using multiple transmission methods for PTP in an IPv4 environment, such as supporting both unicast and multicast simultaneously.

12. IPv4Uni: Refers to the PTP protocol running in an IPv4 unicast environment, where each PTP message is sent directly to a specific receiver.

13. OnePPS: Sends one pulse signal per second. The OnePPS signal provides the receiving device with an absolute time reference point once per second, allowing the receiving device to adjust its local clock more accurately according to this pulse signal, thus reducing time error.

14. EthIPv4IPv6Combo: Similar PTP implementation in an IPv6 environment, indicating the mixed use of multiple protocols in an IPv6 network.

PCP

The PCP parameter is used to specify the priority of PTP messages in Ethernet, ensuring that critical time synchronization messages receive priority processing during network transmission, thereby reducing latency and improving synchronization accuracy.

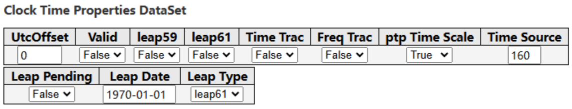
DSCP

The DSCP parameter is used to mark the quality of service for PTP messages in an IP network, ensuring that these messages enjoy higher transmission priority during routing and switching, thereby enhancing the reliability and responsiveness of time synchronization.

isGM

When the profile uses the AED 802.1 AS attribute, this field indicates whether the device type is AED-GM. If the device is AED-GM, the value is true; otherwise, it is false.

Clock Time Properties DataSet



Clock Time Properties DataSet

UtcOffset	Valid	leap59	leap61	Time Trac	Freq Trac	ptp Time Scale	Time Source
0	False	False	False	False	False	True	160

Leap Pending	Leap Date	Leap Type
False	1970-01-01	leap61

UtcOffset

Set the UTC offset.

Valid

Valid This field indicates whether the leap second fields leap59 and leap61 are valid.

leap59

When set to valid, this indicates that the current UTC will decrease by 1 second (i.e., a leap second minus 1 second) for the purpose of global time synchronization adjustment.

leap61

When set to valid, this indicates that the current UTC will increase by 1 second (i.e., a leap second plus 1 second) for the purpose of global time synchronization adjustment.

Time Trac

Time Traceable Indicates the timeTraceable field in the announce message header. This flag is used to indicate whether the device's time is traceable. If the device’ s time can be traced back to a known standard, this flag will be set to TRUE. This confirms that the device can ensure its time is synchronized with a reference time source, further enhancing the precision and reliability of clock synchronization.

Freq Trac

Frequency Traceable Indicates the frequencyTraceable field in the announce message header. This flag is used to indicate whether the device's frequency is traceable. If the device’s frequency can be traced back to a known standard, this flag will be set to TRUE. This confirms that the device can ensure its clock frequency is synchronized with a reference standard, providing more accurate clock synchronization services.

ptp Time Scale

The ptpTimescale field in the announce message header determines the accuracy and scope of the timestamps. This field can be set to TRUE or FALSE, indicating whether the timestamps follow the time scale defined by the IEEE 1588 standard. Specifically, when ptpTimescale is set to TRUE, it means that the timestamps adhere to the IEEE 1588 standard's time scale, defining the accuracy and scope according to the standard. Conversely, if ptpTimescale is set to FALSE, it means that the timestamps do not follow the IEEE 1588 standard's time scale and may use other time scales or precision.

Time Source

This field represents the timeSource field in the announce message. Specifically, the value of the timeSource field represents the type and origin of the clock. Common values include:

Local Clock: Refers to the device's own clock.

GPS: Receives time information through the GPS system.

Other Time Sources: May come from other network devices or synchronization protocols.

Leap Pending

Compensates for the timestamp handling delays of various nodes, ensuring accuracy and consistency in time synchronization.

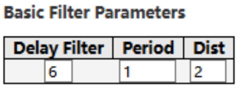
Leap Date

Select the starting point of the leap time.

Leap Type

Leap types are divided into two kinds, leap59 and leap61.

Basic Filter Parameters



Basic Filter Parameters

Delay Filter	Period	Dist
6	1	2

Delay Filter

In the basic convergence algorithm, the delay parameter is used to measure the propagation and processing delay of synchronization messages as they traverse the network. This parameter helps the algorithm accurately compute synchronization offset, thereby correctly adjusting the clocks.

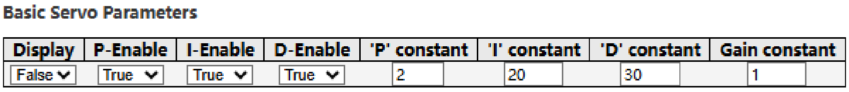
Period

In the basic convergence algorithm, the period parameter defines the interval at which synchronization messages are sent. By adjusting this parameter, you can control the frequency of synchronization messages to ensure that device clocks stay synchronized.

Dist

The dist parameter represents the relative distance or network hops between devices. This parameter helps the basic convergence algorithm to more accurately calculate the total delay, thereby better adjusting the device clocks.

Basic Servo Parameters



Basic Servo Parameters

Display	P-Enable	I-Enable	D-Enable	'P' constant	'I' constant	'D' constant	Gain constant
False	True	True	True	2	20	30	1

Display

This parameter is used to display the calculated parameter information in the base convergence algorithm of a PTP instance.

P-Enable

This parameter is used to disable the P parameter in the base convergence algorithm of a PTP instance.

I-Enable

This parameter is used to disable the I parameter in the base convergence algorithm of a PTP instance.

D-Enable

This parameter is used to disable the D parameter in the base convergence algorithm of a PTP instance.

'P' constant

This parameter is used to set the value of the P parameter in the base convergence algorithm for a specific PTP instance. The parameter is mainly used to adjust the performance of the servo convergence algorithm to improve the accuracy and stability of clock synchronization.

'I' constant

This parameter is used to set the value of the I parameter in the base convergence algorithm for a specific PTP instance. The parameter is mainly used to adjust the performance of the servo convergence algorithm to improve the accuracy and stability of clock synchronization.

'D' constant

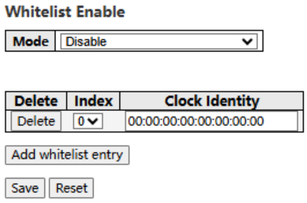
This parameter is used to set the value of the D parameter in the base convergence algorithm for a specific PTP instance. The parameter is mainly used to adjust the performance of the servo convergence algorithm to improve the accuracy and stability of clock synchronization.

Gain constant

This parameter is used to set the value of the Gain parameter in the base convergence algorithm for a specific PTP instance. The parameter is mainly used to adjust the performance of the servo convergence algorithm to improve the accuracy and stability of clock synchronization.

[Whitelist]

This page allows users to configure the PTP service whitelist.



Whitelist Enable

Mode	Disable

Delete	**Index**	**Clock Identity**
Delete	0	00:00:00:00:00:00:00:00

Whitelist Enable

Mode

Whitelist Enable Switch: When turned on, the whitelist functionality will be activated.

Delete

Delete Button: Click to remove the specified entry from the whitelist.

Index

Whitelist Index Value: Select through the dropdown menu. This value varies for different lists.

Clock Identity

Whitelist List Value.

Add Whitelist Entry

Use this button to add a new entry to the whitelist.

Save

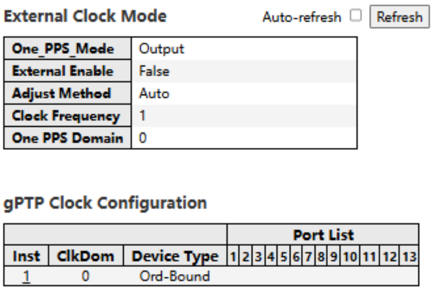
Use this button to save the newly added whitelist entry to the page.

Reset

You can undo any local changes made and revert to the previously saved values.

[Status]

This page allows the user to inspect the current gPTP clock settings.



External Clock Mode

One_PPS_Mode	Output
External Enable	False
Adjust Method	Auto
Clock Frequency	1
One PPS Domain	0

gPTP Clock Configuration

			Port List												
Inst	ClkDom	Device Type	1	2	3	4	5	6	7	8	9	10	11	12	13
1	0	Ord-Bound													

External Clock Mode

One_PPS_Mode

Shows the current One_pps_mode configured.

1. Output : Enable the 1 pps clock output.

2. Input : Enable the 1 pps clock input.

3. Disable : Disable the 1 pps clock in/out-put.

External Enable

Shows the current External clock output configuration.

1. True : Enable the external clock output.

2. False : Disable the external clock output.

Adjust Method

Shows the current Frequency adjustment configuration.

1. LTC : Use Local Time Counter (LTC) frequency control.

2. Single : Use SyncE DPLL frequency control, if allowed by SyncE.

3. Independent : Use an oscillator independent of SyncE for frequency control, if supported by the HW.

4. Common : Use second DPLL for PTP, Both DPLL have the same (SyncE recovered) clock.

5. Auto : AUTO Select clock control, based on PTP profile and available HW resources.

Clock Frequency

Shows the current clock frequency used by the External Clock.

The possible range of values are 1 - 25000000 (1 - 25MHz).

One PPS Domain

Hardware timestamp capture, supporting multiple hardware domains, offers many options.

gPTP Clock Configuration

Inst

Indicates the Instance of a particular Clock Instance [0..3].

Click on the Clock Instance number to monitor the Clock details.

ClkDom

Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3].

Device Type

Indicates the Type of the Clock Instance. There are five Device Types.

1. Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock.

2. P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock.

3. E2e Transp - Clock's Device Type is End to End Transparent Clock.

4. Master Only - Clock's Device Type is Master Only.

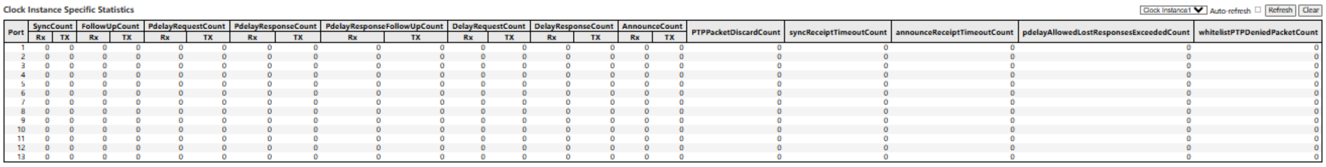
5. Slave Only - Clock's Device Type is Slave Only.

Port List

Shows the ports configured for that Clock Instance.

[Statistics]

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

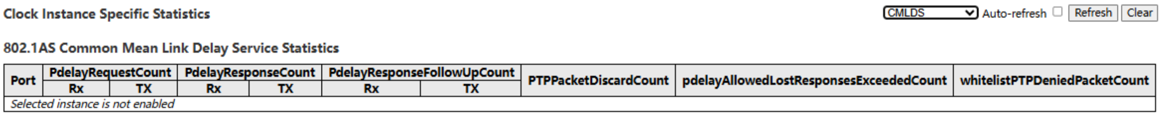


Clock Instance Specific Statistics

Port	SyncCount		FollowUpCount		PdelayRequestCount		PdelayResponseCount		PdelayResponseFollowUpCount		DelayRequestCount		DelayResponseCount		AnnounceCount		PTPPacketDiscardCount	syncReceiptTimeoutCount	announceReceiptTimeoutCount	pdelayAllowedLostResponsesExceededCount	whitelistPTPDeniedPacketCount
	Rx	TX	Rx	TX	Rx	TX	Rx	TX	Rx	TX	Rx	TX	Rx	TX	Rx	TX					
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

802.1AS Clock Instance Specific Statistics

Click on the upper right corner to switch to CMDLS mode, as shown in the following figure.



Clock Instance Specific Statistics

802.1AS Common Mean Link Delay Service Statistics

Port	PdelayRequestCount		PdelayResponseCount		PdelayResponseFollowUpCount		PTPPacketDiscardCount	pdelayAllowedLostResponsesExceededCount	whitelistPTPDeniedPacketCount
	Rx	TX	Rx	TX	Rx	TX			
Selected instance is not enabled									

Recieved counters

Port

Displays the sequence configured for this clock instance.

SyncCount

A counter that increments every time when synchronization information is received or transmit.

FollowUpCount

A counter that increments every time when a Follow Up message is received or transmit.

PdelayRequestCount

A counter that increments every time when a Pdelay_Req message is received or transmit.

PdelayResponseCount

A counter that increments every time when a Pdelay_Resp message is received or transmit.

PdelayResponseFollowUpCount

A counter that increments every time when a Pdelay_Resp_Follow_Up message is received or transmit.

DelayRequestCount

A counter that increments every time when a Dlay_Req message is received or transmit.

DelayResponseCount

A counter that increments every time when a Dlay_Resp message is received or transmit.

AnnounceCount

A counter that increments every time when an Announce message is received or transmit.

PTPPacketDiscardCount

A counter that increments every time when a PTP message is discarded.

syncReceiptTimeoutCount

A counter that increments every time when sync receipt timeout occurs.

announceReceiptTimeoutCount

A counter that increments every time when announce receipt timeout occurs.

pdelayAllowedLostResponsesExceededCount

A counter that increments everytime the value of the variable lostResponses exceeds the value of the variable allowedLostResponses.

whitelistPTPDeniedPacketCount

After enabling the PTP whitelist function, the number of message packets rejected (due to not being on the whitelist) will be counted upon receiving PTP messages.

Transmit Counters

SyncCount

A counter that increments every time synchronization information is transmitted.

FollowUpCount

A counter that increments every time a Follow_Up message is transmitted.

PdelayRequestCount

A counter that increments every time a Pdelay_Req message is transmitted.

PdelayResponseCount

A counter that increments every time a Pdelay_Resp message is transmitted.

PdelayResponseFollowUpCount

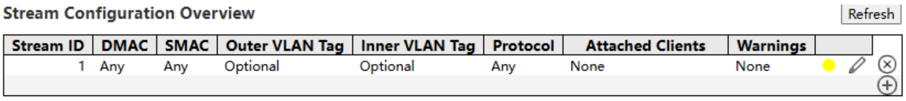
A counter that increments every time a Pdelay_Resp_Follow_Up message is transmitted.

AnnounceCount

A counter that increments every time an Announce message is transmitted.

2.6.2. Stream

[Time > TSN > Stream]



Stream Configuration Overview

Refresh

Stream ID	DMAC	SMAC	Outer VLAN Tag	Inner VLAN Tag	Protocol	Attached Clients	Warnings	
1	Any	Any	Optional	Optional	Any	None	None	●

Stream Configuration Overview

Configuration Buttons

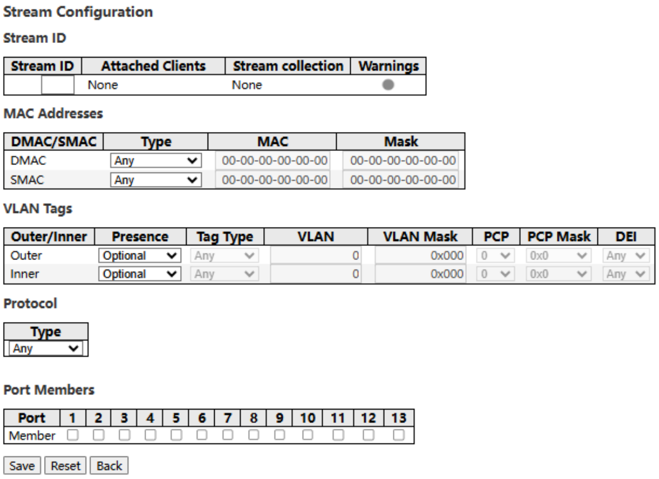
You can modify each Stream in the table using the following buttons:

✎: Edits the Stream row.

⊗: Deletes the Stream.

⊕: Adds new Stream.

Click on ⊕ add Stream configuration.



Stream Configuration

Stream ID

Stream ID	Attached Clients	Stream collection	Warnings
	None	None	●

MAC Addresses

DMAC/SMAC	Type	MAC	Mask
DMAC	Any	00-00-00-00-00-00	00-00-00-00-00-00
SMAC	Any	00-00-00-00-00-00	00-00-00-00-00-00

VLAN Tags

Outer/Inner	Presence	Tag Type	VLAN	VLAN Mask	PCP	PCP Mask	DEI
Outer	Optional	Any	0	0x000	0	0x0	Any
Inner	Optional	Any	0	0x000	0	0x0	Any

Protocol

Type
Any

Port Members

Port	1	2	3	4	5	6	7	8	9	10	11	12	13
Member	□	□	□	□	□	□	□	□	□	□	□	□	□

Stream Configuration

Stream ID

Stream ID

The ID of the stream. The lower the ID, the higher precedence when matching.

For example, if Stream #1 matches all frames with a multicast DMAC and

Stream #2 matches a particular multicast DMAC, Stream #2 will never be hit.

If editing an existing stream, this field is not editable, but it is if

adding a new.

If attempting to save a new stream with an ID already in use, a confirmation

box will be shown.

Attached Clients

Streams don't do anything by themselves. They are utilized by PSFP and FRER.

for matching particular flows. This field indicates which of those two protocols - if any - are utilizing a particular stream. The number in parenthesis shows the PSFP or FRER instance the stream is used on.

A stream may be part of a stream collection, in which case no clients can be attached directly to the stream itself. They must attach to the stream collection. In this case, this fields shows a dash ("-"). See also next help topic.

If no clients are attached to a stream, the stream will be installed into hardware anyway. This allows the user to create two streams, where the first e.g. matches a particular range of MAC address and the second matches the same range of MAC addresses plus some more. The second stream can them be used in FRER or PSFP to match all the MAC addresses of the second stream, except that from the first.

Stream collection

If a stream is part of a stream collection, this shows the ID of the stream collection. The ID is a hyperlink to the stream collection configuration page. If the stream is not part of a stream collection, the field just shows "None".

Warnings

Configuration of a stream may result in configurational warnings.For instance, if a stream is not instantiated on any ports, it is not of any use, and a warning will appear.A color indicates the warning state as follows:

●:The stream is not yet created.

🟢:The stream has no configurational warnings.

🟡:The stream has configurational warnings.

MAC Address

DMAC

Destination mac address to be used with Dest Mask

SMAC

Source Mac address to be used with Src Mask

Type

The drop-down list for the DMAC offers the following options:

- Any: Match on any DMAC (default).
- Multicast: Match on multicast (but not broadcast) frames.
- Broadcast: Match on broadcast frames.
- Unicast: Match on unicast frames.
- Not Broadcast: Match on unicast and multicast frames.
- Not Unicast: Match on multicast and broadcast frames.
- MAC/Mask: Match on a particular DMAC address with mask. The 'MAC' and 'Mask' fields will become available for editing when this is selected.

MAC

Device Unique Identifier.

Mask

Mask used in conjunction with the source/destination MAC.

VLAN Tags

Outer

It can be set to optional, required, or disallowed. When set to optional or disallowed, no further specifications for the outer tag are allowed.

Inner

It can be set to optional, required, or disallowed. When set to optional or disallowed, the inner tag cannot be further specified.

Presence

When this outer/inner VLAN tag is present, the packet processing state offers three configuration options:

Optional: The system can match the VLAN tag if the packet carries it. Untagged packets will continue to be processed normally.

Not Allowed: Traffic containing VLAN tags will be automatically rejected or dropped.

Required: Packets must carry a valid VLAN tag to be processed.

Tag Type

It can be set to Any, C-tag, or S-tag. This field is only applicable when the outer tag is set to required.

VLAN

VLAN number to use with VLANMASK [1-4095]. This field only applies when OuterTag is Required.

VLAN Mask

Used to mask value of VLAN [0-4095]. This field only applies when OuterTag is Required.

PCP

Pcp value to use with PcpMask. [0-7]. This field only applies when OuterTag is Required.

PCP Mask

Mask to use with Pcp. [0-7]. This field only applies when OuterTag is Required.

Dei

Can be set to Required, Optional, Not Allowed. This field only applies when OuterTag is Required.

Protocol

String describing the Protocol encapsulation. The string has two parts separated by a space. The first part specifies the encapsulation type and the output can be either ANY, ETH2, LLC, SNAP, IPV4 or IPV6. The second part specifies the encapsulation parameters and its format depends on the selected encapsulation type:

ANY

Example:

ANY

ETH2

A hex ranging from 0600 to ffff indicating the protocol type, e.g. 0800 for IP.

Example:

ETH2 0800

LLC

DSAP:xxx **SSAP**:yyy Each of these two fields can range from 0 to 255.

Example:

LLC DSAP:AA SSAP:BB

SNAP

OUI:xx-xx-xx PID:xxxx The OID can range from 00-00-00 to ff-ff-ff and the PID from 0000 to ffff. Special case is when OID is 00-00-00; then PID can only range from 0600 to ffff.

Example:

SNAP OUI:CC-CC-CC PID:111

IPV4

fragment:['yes'|'no'|'any']

options:['yes'|'no'|'any']

DSCP:[{uint6'/'uint6} | '['{uint6'-'uint6}']' | '['{uint6'-'uint6}']']

proto:uint8/uint8

sip:uint8.uint8.uint8.uint8/uint8.uint8.uint8.uint8

dip:uint8.uint8.uint8.uint8/uint8.uint8.uint8.uint8

dport:[{uint16'/'uint16} | '['{uint16'-'uint16}']' | '['{uint16'-'uint16}']']

where uint6 can range from 0-63, uint8 can range from 0-255 and uint16 can range from 0-65535.

Example:

IPV4 frag:any options:any DSCP:19/63 proto:34/255 sip:20.21.22.23/255.255.0.0 dip:10.11.12.13/255.255.255.0 dport:10/65535

IPV6

DSCP: [{uint6'/'uint6} | '['{uint6'-'uint6}']' | '['{uint6'-'uint6}']']

proto:uint8/uint8

sip: Source IP address with mask in CIDR notation.

dip: Destination IP address mask in CIDR notation.

dport: [{uint16'/'uint16} | '['{uint16'-'uint16}']' | '['{uint16'-'uint16}']']

where uint6 can range from 0-63, uint8 can range from 0-255 and uint16 can range from 0-65535.

Example:

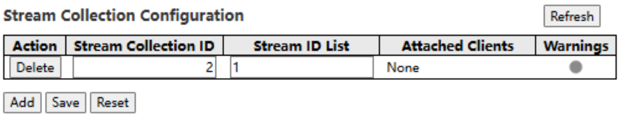
IPV6 DSCP:34/63 proto:12/255 sip:1:4001:5001::1/ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff dip:2001::1/ffff:ffff:ffff:ffff:: dport:100/65535

Port Members

Check the ports on which this filter is applied to. By default no ports are included.

2.6.3. Stream Collection

[Time > TSN > Stream Collection]



Stream Collection Configuration

Action	Stream Collection ID	Stream ID List	Attached Clients	Warnings
Delete	2	1	None	●

Stream Collection Configuration

This page allows for editing existing or add new streams collections.

A stream collection gathers one or more streams, which makes multiple streams available in functions such as FRER in generator mode, where different streams need to use the same sequence number generator.

Action

Click this button to delete the instance.

Stream Collection ID

If a stream is part of a stream collection, this shows the ID of the stream collection. The ID is a hyperlink to the stream collection configuration page. If the stream is not part of a stream collection, the field just shows "None".

Stream ID List

List of stream IDs that make up this stream collection. individual stream IDs are separated by a comma, and ranges are separated by a hyphen.
An example is 1,3,5,7-9, where Stream IDs 1, 3, 5, 7, 8, and 9 are put into the stream collection.

Attached Clients

Streams don't do anything by themselves. They are utilized by PSFP and FRER for matching particular flows. This field indicates which of those two protocols - if any - are utilizing a particular stream. The number in parenthesis shows the PSFP or FRER instance the stream is used on.
A stream may be part of a stream collection, in which case no clients can be attached directly to the stream itself. They must attach to the stream collection. In this case, this fields shows a dash ("-"). See also next help topic. If no clients are attached to a stream, the stream will be installed into hardware anyway. This allows the user to create two streams, where the first e.g. matches particular range of MAC address and the second matches the same range of MAC addresses plus some more. The second stream can them be used in FRER or PSFP to match all the MAC addresses of the second stream, except that from the first.

Warnings

Configuration of a stream may result in configurational warnings.For instance, if a stream is not instantiated on any ports, it is not of any use, and a warning will appear.A color indicates the warning state as follows:

●:The stream is not yet created.

🟢:The stream has no configurational warnings.

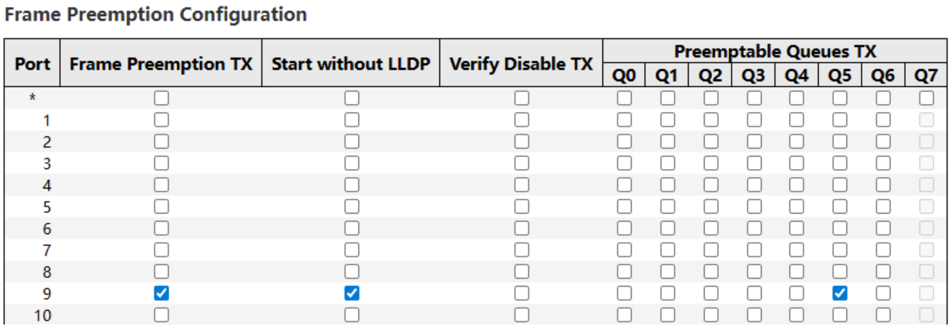
🟡:The stream has configurational warnings.

2.6.4. Frame Preemption

[Time > TSN > Frame Preemption]

[Configuration]

This page provides an overview of TSN Egress Port Frame Preemption Configuration.



Frame Preemption Configuration

Port	Frame Preemption TX	Start without LLDP	Verify Disable TX	Preemptable Queues TX							
				Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
*	□	□	□	□	□	□	□	□	□	□	□
1	□	□	□	□	□	□	□	□	□	□	□
2	□	□	□	□	□	□	□	□	□	□	□
3	□	□	□	□	□	□	□	□	□	□	□
4	□	□	□	□	□	□	□	□	□	□	□
5	□	□	□	□	□	□	□	□	□	□	□
6	□	□	□	□	□	□	□	□	□	□	□
7	□	□	□	□	□	□	□	□	□	□	□
8	□	□	□	□	□	□	□	□	□	□	□
9	☑	☑	□	□	□	□	□	□	☑	□	□
10	□	□	□	□	□	□	□	□	□	□	□

Frame Preemption Configuration

Port

The logical port for the settings contained in the same row. Please note that Frame Preemption is not supported on ports with maximum speed 25 Gigabit/sec and is also not supported on 10G Gigabit/sec Aquantia Copper port.

Frame Preemption TX

The value of the 802.3br aMACMergeEnableTx parameter for the port. This value determines whether frame preemption is enabled (TRUE) or disabled (FALSE) in the MAC Merge sublayer in the transmit direction.

Start without LLDP

When this field is checked, Frame Preemption will be active when Frame Preemption TX is checked.

Verify Disable TX

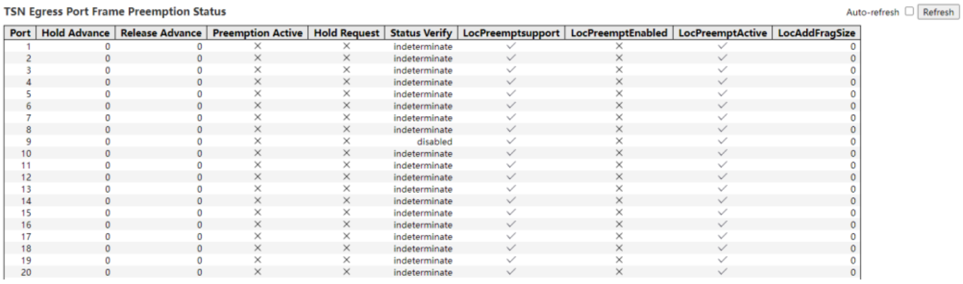
The value of the 802.3br aMACMergeVerifyDisableTx parameter for the port. This value determines whether the verify function is disabled (TRUE) or enabled (FALSE) in the MAC Merge sublayer in the transmit direction.

Preemptable Queues TX

This parameter is the administrative value of the preemption status for the priority. If checked, it takes value preemptable if frames queued for the priority are to be transmitted using the preemptable service for the Port. If not checked, it takes value express if frames queued for the priority are to be transmitted using the express service for the Port and preemption is enabled for the Port.

[Status]

This page provides an overview of TSN Egress Port Frame Preemption Status all switch ports.



TSN Egress Port Frame Preemption Status

Port	Hold Advance	Release Advance	Preemption Active	Hold Request	Status Verify	LocPreemptsupport	LocPreemptEnabled	LocPreemptActive	LocAddFragSize
1	0	0	✕	✕	indeterminate	✓	✕	✓	0
2	0	0	✕	✕	indeterminate	✓	✕	✓	0
3	0	0	✕	✕	indeterminate	✓	✕	✓	0
4	0	0	✕	✕	indeterminate	✓	✕	✓	0
5	0	0	✕	✕	indeterminate	✓	✕	✓	0
6	0	0	✕	✕	indeterminate	✓	✕	✓	0
7	0	0	✕	✕	indeterminate	✓	✕	✓	0
8	0	0	✕	✕	indeterminate	✓	✕	✓	0
9	0	0	✕	✕	disabled	✓	✕	✓	0
10	0	0	✕	✕	indeterminate	✓	✕	✓	0
11	0	0	✕	✕	indeterminate	✓	✕	✓	0
12	0	0	✕	✕	indeterminate	✓	✕	✓	0
13	0	0	✕	✕	indeterminate	✓	✕	✓	0
14	0	0	✕	✕	indeterminate	✓	✕	✓	0
15	0	0	✕	✕	indeterminate	✓	✕	✓	0
16	0	0	✕	✕	indeterminate	✓	✕	✓	0
17	0	0	✕	✕	indeterminate	✓	✕	✓	0
18	0	0	✕	✕	indeterminate	✓	✕	✓	0
19	0	0	✕	✕	indeterminate	✓	✕	✓	0
20	0	0	✕	✕	indeterminate	✓	✕	✓	0

TSN Egress Port Frame Preemption Status

Port

The logical port for the settings contained in the same row.

Hold Advance

The value of the holdAdvance parameter for the Port in nanoseconds. There is no default value; the holdAdvance is a property of the underlying MAC.

Release Advance

The value of the releaseAdvance parameter for the Port in nanoseconds. There is no default value; the releaseAdvance is a property of the underlying MAC.

Preemption Active

The value is active (TRUE) when preemption is operationally active for the Port, and idle (FALSE) otherwise.

Hold Request

The value is hold (TRUE) when the sequence of gate operations for the Port has executed a Set-And-Hold-MAC operation, and release (FALSE) when the sequence of gate operations has executed a Set-And-Release-MAC operation. The value of this object is release (FALSE) on system initialization.

Status Verify

The status of the MAC Merge sublayer verification for the given device.

LocPreemptsupport

The value is TRUE when preemption is supported on the port, and FALSE otherwise.

LocPreemptEnabled

The value is TRUE when preemption is enabled on the port, and FALSE otherwise.

LocPreemptActive

The value is TRUE when preemption is operationally active on the port, and FALSE otherwise.

LocAddFragSize

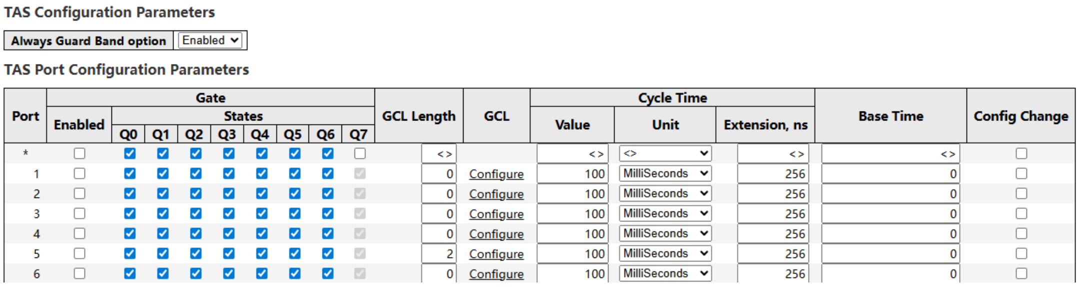
The value of the 802.3br LocAddFragSize parameter for the port. The minimum size of non-final fragments supported by the receiver on the local port. This value is expressed in units of 64 octets of additional fragment length. The minimum non-final fragment size is: (LocAddFragSize + 1) * 64 octets.

2.6.5. TAS

[Time > TSN > TAS]

[Port]

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



TAS Configuration Parameters

Always Guard Band option	Enabled

TAS Port Configuration Parameters

Port	Gate									GCL Length	GCL	Cycle Time			Base Time	Config Change
	Enabled	States										Value	Unit	Extension, ns		
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7							
*	☐	☑	☑	☑	☑	☑	☑	☑	☐	<>		<>	<>	<>	<>	☐
1	☐	☑	☑	☑	☑	☑	☑	☑	☑	0	Configure	100	MilliSeconds	256	0	☐
2	☐	☑	☑	☑	☑	☑	☑	☑	☑	0	Configure	100	MilliSeconds	256	0	☐
3	☐	☑	☑	☑	☑	☑	☑	☑	☑	0	Configure	100	MilliSeconds	256	0	☐
4	☐	☑	☑	☑	☑	☑	☑	☑	☑	0	Configure	100	MilliSeconds	256	0	☐
5	☐	☑	☑	☑	☑	☑	☑	☑	☑	2	Configure	100	MilliSeconds	256	0	☐
6	☐	☑	☑	☑	☑	☑	☑	☑	☑	0	Configure	100	MilliSeconds	256	0	☐

TAS Configuration Parameters

Always Guard Band option

The Always Guard Band option defines how the guard band values are calculated.

If a Gate Control List do not contain SetAndHold and/or SetAndRelease operations the Always Guard Band option has no effect.

If a Gate Control List do contain SetAndHold and SetAndRelease operations then:

- When Always Guard Band is Enabled, a guard band is implemented on all queues, both Express and Preemptible queues.
- When Always Guard Band is Disabled, a guard band is only implemented on Preemptible queues.

TAS Port Configuration Parameters

Port

Port number of the switch.

Gate Enabled

The Enabled parameter determines whether traffic scheduling is active (true) or inactive (false).

Gate States

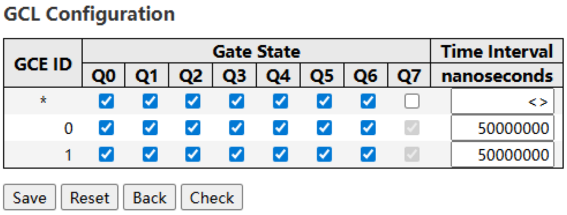
The initial value of the port open states that is used when no Gate Control List is active on the Port. the Q7 status defaults to Open and cannot be modified.

GCL Length

The Admin Gate Control List length parameter for the Port. Valid range is 0-256. The integer value indicates the number of entries Gate Control Elements in the Gate Control List. If you change the value, press the Save button before configuring the Gate Control List by pressing the GCL link.

GCL

A link to the Gate Control List parameter configuration.



GCL Configuration

GCE ID	Gate State								Time Interval
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	nanoseconds
*	☑	☑	☑	☑	☑	☑	☑	□	<>
0	☑	☑	☑	☑	☑	☑	☑	☑	50000000
1	☑	☑	☑	☑	☑	☑	☑	☑	50000000

GCL Configuration

GCL ID

Index of Gate control list.

Gate State

The GateState shows for each queue whether it is open or closed in the given time interval. the Q7 status defaults to Open and cannot be modified.

Time Interval

TimeInterval is specified in number of nanoseconds.

Cycle Time

The Admin value of the gating cycle for the Port. The Admin Cycle Time variable is a rational number of seconds, defined by value and a unit.

Cycle Time Value

The Admin Cycle Time is defined by this number of units defined in the Unit field. The Admin Cycle Time is a value in the range 1-999999999, and combined with the Cycle Time Unit the value shall be in the range 256-999999999 nanoseconds. The default value is 100 milliseconds.

Cycle Time Unit

The Admin Cycle Time unit. May be milliseconds, microseconds or nanoseconds.

Cycle Time Extension

An integer number of nanoseconds in the range 256-999999999, defining the maximum amount of time by which the gating cycle for the Port is permitted to be extended when a new cycle configuration is installed. The default value is 256 nanoseconds.

Base Time

The Admin value of base time, expressed as an IEEE 1588 precision time protocol (PTP) timescale.

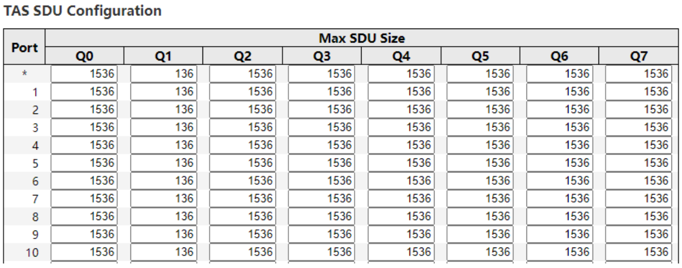
Config Change

The Configuration Change parameter signals the start of a configuration change. After a successfull configuration change, the configured Admin values will become the Oper values, which are displayed in the Time > TSN > TAS web page.

If the value of parameter Base Time is in the future, the configuration change will be executed at Base Time.

If Base Time is in the past, the configuration change will be executed as soon as possible. In practice it will be within approx 2 seconds, at a time which is an integral number of Cycle Time ahead of the configured value of Base Time. This way, the synchronisation between schedules in elements across a sceduled network can be maintained.

[Max SDU]



TAS SDU Configuration

Port	Max SDU Size							
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
*	1536	136	1536	1536	1536	1536	1536	1536
1	1536	136	1536	1536	1536	1536	1536	1536
2	1536	136	1536	1536	1536	1536	1536	1536
3	1536	136	1536	1536	1536	1536	1536	1536
4	1536	136	1536	1536	1536	1536	1536	1536
5	1536	136	1536	1536	1536	1536	1536	1536
6	1536	136	1536	1536	1536	1536	1536	1536
7	1536	136	1536	1536	1536	1536	1536	1536
8	1536	136	1536	1536	1536	1536	1536	1536
9	1536	136	1536	1536	1536	1536	1536	1536
10	1536	136	1536	1536	1536	1536	1536	1536

TAS SDU Configuration

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

Port

Port number of the switch.

Max SDU Size

The value of the Maximum SDU size parameter for the traffic class supported by the port. This value is represented as an unsigned integer in the range 0-10240. A value of 0 is interpreted as the Maximum SDU size supported by the underlying MAC: 10240. The default value of the Maximum SDU parameter is 1536.

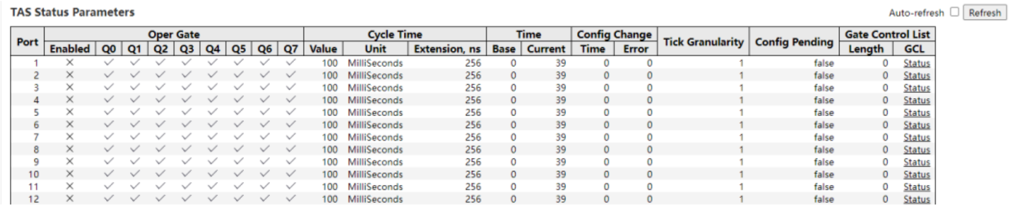
The Maximum SDU size parameter is used to calculate the guard band time = Maximum SDU * 8 / LINK_SPEED (sec).

If frame preemption is enabled and a gate operaton is SetAndHold, the guard band time in preemptable queues is automatically selected as the frame preemption minimum fragment size plus 64 bytes.

A queue is said to be preemptible, if frame preemption is enabled, and if this queue is not opened in a SetAndHold gate operation.

[Status]

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



TAS Status Parameters

Port	Oper Gate									Cycle Time			Time		Config Change		Tick Granularity	Config Pending	Gate Control List	
	Enabled	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Value	Unit	Extension, ns	Base	Current	Time	Error			Length	GCL
1	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	39	0	0	1	false	0	Status
2	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	39	0	0	1	false	0	Status
3	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	39	0	0	1	false	0	Status
4	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	39	0	0	1	false	0	Status
5	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	39	0	0	1	false	0	Status
6	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	39	0	0	1	false	0	Status
7	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	39	0	0	1	false	0	Status
8	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	39	0	0	1	false	0	Status
9	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	39	0	0	1	false	0	Status
10	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	39	0	0	1	false	0	Status
11	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	39	0	0	1	false	0	Status
12	✕	✓	✓	✓	✓	✓	✓	✓	✓	100	MilliSeconds	256	0	39	0	0	1	false	0	Status

TAS Status Parameters

Port

Port number of the switch.

Oper Gate Enabled

The Enabled parameter shows whether traffic scheduling is active (true) or inactive (false).

Oper Gate States

The current state of the gate associated with each queue for the Port.

Cycle Time Value

The operational value of the gating cycle for the Port. The Cycle Time variable is a rational number of seconds, defined by value and a unit.

Cycle Time Unit

The operational Cycle Time unit. May be milliseconds, microseconds or nanoseconds.

Cycle Time Extension

An integer number of nanoseconds, defining the maximum amount of time by which the gating cycle for the Port is permitted to be extended when a new cycle configuration is installed.

Base Time

The operational value of base time, expressed as an IEEE 1588 precision time protocol (PTP) timescale.

Current Time

The current time, in PTP time, as maintained by the local system. The value is a representation of a PTP time value, consisting of a 48-bit integer number of seconds and a 32-bit integer number of nanoseconds. Only the seconds are displayed.

Config Change Time

The PTP time at which the next config change is scheduled to occur. The value is a representation of a PTP time value, consisting of a 48-bit integer number of seconds and a 32-bit integer number of nanoseconds.

Config Change Error

A counter of the number of times that a re-configuration of the traffic schedule has been requested with the old schedule still running and the requested base time was in the past.

Tick Granularity

The granularity of the cycle time clock, represented as an unsigned number of tenths of nanoseconds.

Config Pending

The value of the ConfigPending state machine variable. The value is TRUE if a configuration change is in progress but has not yet completed.

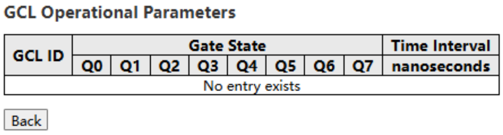
Gate Control List Length

The operational value of the gate control list length parameter for the Port. The integer value indicates the number of entries (TLVs) in the operational gate control list.

GCL

A link to the GCL parameter status.

Click on Status, the page will display as follows. This page allows the user to inspect the current TAS configurations.



GCL Operational Parameters

GCL ID	Gate State								Time Interval
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	nanoseconds
No entry exists									

GCL ID

Index of Gate control list.

Gate State

The Gate State shows for each queue whether it is open or closed in the given time interval.

Time Interval

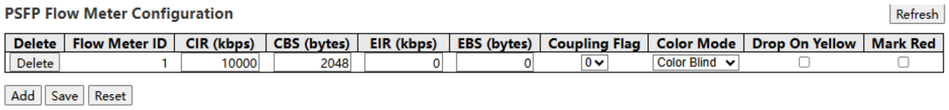
Time Interval is specified in number of nanoseconds.

2.6.6. PSFP

Flow Meter

[Time > TSN > PSFP >Flow Meter]

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



PSFP Flow Meter Configuration

Delete	Flow Meter ID	CIR (kbps)	CBS (bytes)	EIR (kbps)	EBS (bytes)	Coupling Flag	Color Mode	Drop On Yellow	Mark Red
Delete	1	10000	2048	0	0	0	Color Blind	□	□

PSFP Flow Meter Configuration

Delete

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

Flow Meter ID

The Flow Meter Instance parameter is an index into the Flow Meter Table.

CIR

The Flow Meter CIR parameter contains an integer value that represents the CIR value for the flow meter, in bit/s.This rate refers to the payload rate of the data frame.

CBS

The Flow Meter CBS parameter contains an integer value that represents the CBS value for the flow meter, in octets.

EIR

Configure excess information rate in kbps.This rate refers to the payload rate of the data frame.

EBS

Configure flow meter excess burst size in bytes.

Coupling Flag

Configure coupling flag to be enabled or disable.

Color Mode

Configure color mode enabled or disable.

Drop On Yellow

Set PSFP flow meter Drop on Yellow.

Mark Red

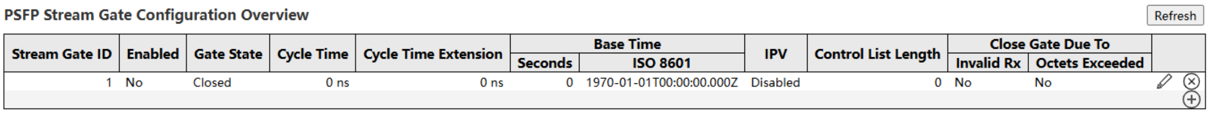
The Flow Meter Mark All Frames Red parameter contains a Boolean value that indicates whether, if the Mark All Frames Red function is enabled, all frames are to be discarded (TRUE) or not (FALSE).

Stream Gate

[Time > TSN > PSFP >Stream Gate]

[Configuration]

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



PSFP Stream Gate Configuration Overview

Stream Gate ID	Enabled	Gate State	Cycle Time	Cycle Time Extension	Base Time		IPV	Control List Length	Close Gate Due To		
					Seconds	ISO 8601			Invalid Rx	Octets Exceeded	
1	No	Closed	0 ns	0 ns	0	1970-01-01T00:00:00.000Z	Disabled	0	No	No	

PSFP Stream Gate Configuration Overview

Stream Gate ID

The Stream Gate Instance parameter is an index into the Stream Gate Table.

Enabled

The Gate Enabled parameter determines whether the stream gate is active (true) or inactive (false).

Gate States

The administrative value of the Gate States parameter for the stream gate. The open value indicates that the gate is open, the closed value indicates that the gate is closed.

Cycle Time

The administrative value of the cycle time for the gate. The time may be specified in either milli seconds, micro seconds or nano seconds as defined by the field Cycle Time unit.

Cycle Time extension

The administrative value of the Cycle Time Extension parameter for the gate. The value is an unsigned integer number of nanoseconds.

Base Time Seconds

The administrative value of the Base Time parameter for the gate. The value is a representation of a PTP time value, consisting of decimal number of seconds since epoch. The time can be given with a resolution of nine decimals.

Base Time ISO 8601

The administrative value of the Base Time parameter for the gate. The "Seconds"; value indicates the time in seconds and sub seconds since epoch where the configuration is configured to change - if the Config Change flag has been issued. The "ISO 8601"; value represents the same, but is displayed as a string formatted according to ISO 8601.

IPV

The administrative value of the IPV parameter represents the IPV value of the switch.

Control List Length

Number of entries in the Access Control List (ACL).

Close Gate Due To Invalid Rx

If checked, the stream gate gets permanently closed if receiving a frame during a closed gate state.

Close Gate Due To Octets Exceeded

If checked, the stream gate gets permanently closed if receiving a frame that exceeds the configured Octet Max.

Configuration Buttons

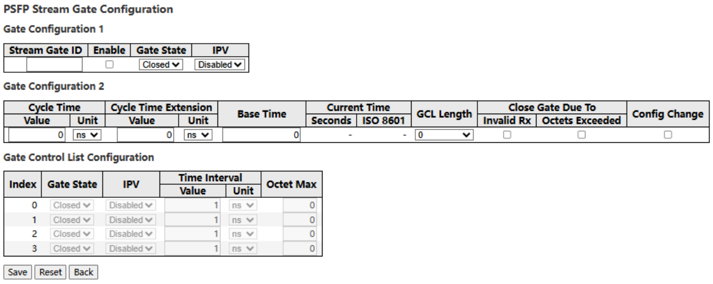
You can modify each Stream in the table using the following buttons:

✎: Edits the Stream Gate row.

⊗: Deletes the Stream Gate.

⊕: Adds new Stream Gate.

Click on ⊕ add Stream configuration.



PSFP Stream Gate Configuration

Gate Configuration 1

Stream Gate ID	Enable	Gate State	IPV
	□	Closed	Disabled

Gate Configuration 2

Cycle Time		Cycle Time Extension		Base Time	Current Time		GCL Length	Close Gate Due To		Config Change
Value	Unit	Value	Unit		Seconds	ISO 8601		Invalid Rx	Octets Exceeded	
0	ns	0	ns	0	-	-	0	□	□	□

Gate Control List Configuration

Index	Gate State	IPV	Time Interval		Octet Max
			Value	Unit	
0	Closed	Disabled	1	ns	0
1	Closed	Disabled	1	ns	0
2	Closed	Disabled	1	ns	0
3	Closed	Disabled	1	ns	0

GCL Configuration 1

Stream Gate ID

The Stream Gate Instance parameter is an index into the Stream Gate Table.

Enable

The Gate Enabled parameter determines whether the stream gate is active (true) or inactive (false).

Gate State

The administrative value of the Gate States parameter for the stream gate. The open value indicates that the gate is open, the closed value indicates that the gate is closed.

IPV

The administrative value of the IPV parameter represents the IPV value of the switch.

GCL Configuration 2

Cycle Time value

The administrative value of the cycle time represents the cycle time of the switch.

Cycle Time Unit

The time unit can be specified in milliseconds (ms), microseconds (µs), or nanoseconds (ns).

Cycle Time Extension value

The administrative value of the cycle time extension parameter represents the cycle time extension value of the switch.

Cycle Time Extension Unit

The time unit can be specified in milliseconds (ms), microseconds (µs), or nanoseconds (ns).

Base Time

The administrative value of the reference time parameter represents the reference time of the switch. This value is a representation of a PTP time value, expressed as decimal seconds since the epoch. The time can be specified with a precision of nine decimal places.

Cuttent Time Seconds

The administrative value of the Base Time parameter for the gate. The value is a representation of a PTP time value, consisting of decimal number of seconds since epoch. The time can be given with a resolution of nine decimals.

Cuttent Time ISO8601

The administrative value of the Base Time parameter for the gate. The "Seconds"; value indicates the time in seconds and sub seconds since epoch where the configuration is configured to change - if the Config Change flag has been issued. The "ISO 8601"; value represents the same, but is displayed as a string formatted according to ISO 8601.

GCL Length

The operational value of the gate control list length parameter for the Port. The integer value indicates the number of entries (TLVs) in the operational gate control list.

Close Gate Due To Invalid RX

If checked, the stream gate gets permanently closed if receiving a frame during a closed gate state.

Close Gate Due To Octets Exceeded

If checked, the stream gate gets permanently closed if receiving a frame that exceeds the configured Octet Max.

Config Change

The Configuration Change parameter signals the start of a configuration change. After a successfull configuration change, the configured Admin values will become the Oper values, which are displayed in the Time > TSN > PSFP > Stream Gate web page.

If the value of parameter Base Time is in the future, the configuration change will be executed at Base Time.

If Base Time is in the past, the configuration change will be executed as soon as possible. In practice it will be within approx 2 seconds, at a time which is an integral number of Cycle Time ahead of the configured value of Base Time. This way, the synchronisation between schedules in elements across a sceduled network can be maintained.

Gate Control List Configuration

Index

Serial Number of Gate List Configuration.

Gate State

The administrative value of the Gate States parameter for the stream gate. The open value indicates that the gate is open, the closed value indicates that the gate is closed.

IPV

The administrative value of the IPV parameter represents the IPV value of the switch.

Time Interval Value

The number of configurable entries corresponds to the GCL length value. Up to 4 entries can be configured, and the sum of time intervals across all entries must be less than or equal to the cycle time value.

Time Interval Unit

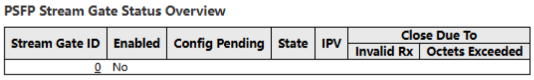
Time interval units: available options are milliseconds (ms), microseconds (us), or nanoseconds (ns).

Octet Max

Maximum configurable 8-byte value.

[Status]

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



PSFP Stream Gate Status Overview

Stream Gate ID	Enabled	Config Pending	State	IPV	Close Due To	
					Invalid Rx	Octets Exceeded
0	No					

PSFP Stream Gate Status Overview

Stream Gate ID

The Stream Gate Instance parameter is an index into the Stream Gate Table.

Enabled

The Gate Enabled parameter determines whether the stream gate is active (true) or inactive (false).

Config Pending

The value of the Configuration Pending state machine variable. If a configuration change is ongoing but not yet completed, this value is TRUE.

State

The operational value of the gating state parameter for flow gating. An open value indicates the gate is open, and a closed value indicates the gate is closed.

IPV

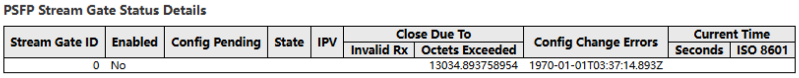
The administrative value of the IPV parameter represents the IPV value of the switch.

Close Due To Invalid RX

If checked, the stream gate gets permanently closed if receiving a frame during a closed gate state.

Close Gate Due To Octets Exceeded

If checked, the stream gate gets permanently closed if receiving a frame that exceeds the configured Octet Max.



PSFP Stream Gate Status Details

Stream Gate ID	Enabled	Config Pending	State	IPV	Close Due To		Config Change Errors	Current Time	
					Invalid Rx	Octets Exceeded		Seconds	ISO 8601
0	No					13034.893758954	1970-01-01T03:37:14.893Z		

PSFP Stream Gate Status Details

Config Change Errors

A counter of the number of times that a re-configuration of the traffic schedule has been requested with the old schedule still running and the requested base time was in the past.

Cuttent Time Seconds

The administrative value of the Base Time parameter for the gate. The value is a representation of a PTP time value, consisting of decimal number of seconds since epoch. The time can be given with a resolution of nine decimals.

Cuttent Time ISO8601

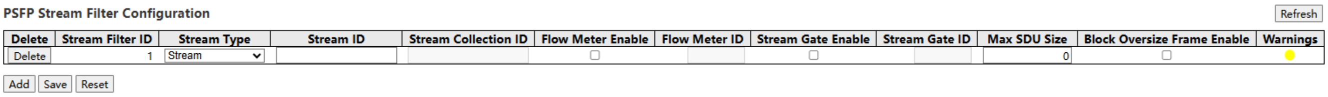
The administrative value of the Base Time parameter for the gate. The "Seconds"; value indicates the time in seconds and sub seconds since epoch where the configuration is configured to change - if the Config Change flag has been issued. The "ISO 8601"; value represents the same, but is displayed as a string formatted according to ISO 8601.

Stream Filter

[Time > TSN > PSFP >Stream Filter]

[Configuration]

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



PSFP Stream Filter Configuration

Delete	Stream Filter ID	Stream Type	Stream ID	Stream Collection ID	Flow Meter Enable	Flow Meter ID	Stream Gate Enable	Stream Gate ID	Max SDU Size	Block Oversize Frame Enable	Warnings
Delete	1	Stream			□		□		0	□	●

PSFP Stream Filter Configuration

Delete

Click to delete the stream filter instance. It will be deleted right away without any request for confirmation. If the stream filter was added with a click on the Add button, it is simply removed again.

Stream FilterI ID

An ID uniquely identifying the stream filter. Valid values are in the range 0 to ?. This can only be changed if adding a new stream filter.

Stream Type

PSFP allows for two different methods for specifying streams that should map to this PSFP stream filter instance.

The first, "Stream", allows for setting one particular stream ID. The second, "Stream Collection", allows for specifying an ID of a stream collection. A stream collection compiles multiple streams into one single.

The two methods are mutually exclusive.

Stream ID

Specify the ID of the stream that should map to this PSFP stream filter. This field is only available if "Stream Type" is set to "Stream ID".

Stream Collection ID

Specify the ID of a stream collection that should map to this PSFP stream filter. This field is only available if "Stream Type" is set to "Stream Collection".

Flow Meter Enable

Check this to enable setting a Flow Meter ID that this stream filter will use.

Flow Meter ID

The ID of the Flow Meter that this stream filter will use. This field is only available if "Flow meter Enable" is checked.

Stream Gate Enable

Check this to enable setting a Stream Gate ID that this stream filter will use.

Stream Gate ID

The ID of the Stream Gate that this stream filter will use. This field is only available if "Stream Gate Enable" is checked.

Max SDU Size

The maximum allowed frame size for the filter. Any frame exceeding this value will be discarded. A value of 0 disables this feature.

Block Oversize Frame Enable

Whenever a frame gets discarded because its SDU size is greater than the configured Maximum SDU Size, this one control what shapp happen with subsequenct frames that go through the stream filter.

If checked, subsequent frames will also be discarded whether they are larger or smaller than the configured Maximum SDU Size. Otherwise they will remain being subject to only the Maximum SDU Size check - if enabled.

An administrative action is required to reset the discarting. Use the PSFP Stream Filter Status page to perform this action.

Warnings

Configuration of a stream filter may result in configurational warnings. For instance, if a stream filter is neither assigned to a Flow Meter nor a Stream Gate, it is not of any use, and a warning will appear. any use, and a warning will appear.

A color indicates the warning state as follows:

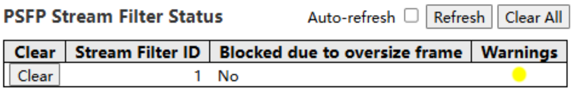
●: The stream filter is not yet created.

🟢: The stream filter has no configurational warnings.

🟡: The stream filter has at least one configurational warning.

[Status]

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



PSFP Stream Filter Status

Clear	Stream Filter ID	Blocked due to oversize frame	Warnings
Clear	1	No	🟡

PSFP Stream Filter Status

Clear

This box is used to mark an entry for clearance in next Clear operation.

Stream Filter ID

The id of the stream filter instance.

Blocked due to oversize frame

True if the filter has been blocked due to an oversize frame, otherwise false.

Warnings

Configuration of a stream filter may result in configurational warnings. For instance, if a stream filter is neither assigned to a Flow Meter nor a Stream Gate, it is not of any use, and a warning will appear. any use, and a warning will appear.

A color indicates the warning state as follows:

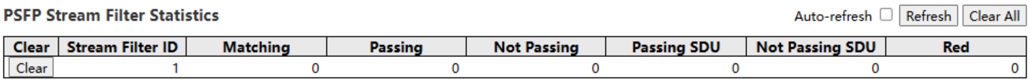
●: The stream filter is not yet created.

🟢: The stream filter has no configurational warnings.

🟡: The stream filter has at least one configurational warning.

[Statistics]

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



PSFP Stream Filter Statistics

Auto-refresh □ Refresh Clear All

Clear	Stream Filter ID	Matching	Passing	Not Passing	Passing SDU	Not Passing SDU	Red
Clear	1	0	0	0	0	0	0

PSFP Stream Filter Statistics

Clear

This box is used to mark an entry for clearance in next Clear operation.

Stream Filter ID

The Max Stream Filter Instances parameter defines the maximum number of stream filter instances that are supported by this Bridge component.

Matching

The Matching Frames Count counter counts received frames that match this stream filter.

Passing

The Passing Frames Count counter counts received frames that pass the gate associated with this stream filter.

Not Passing

The Not Passing Frames Count counter counts received frames that do not pass the gate associated with this stream filter.

Passing SDU

The Passing SDU Count counter counts received frames that pass the SDU size filter specification associated with this stream filter.

Not Passing SDU

The Not Passing SDU Count counter counts received frames that do not pass the SDU size filter specification associated with this stream filter.

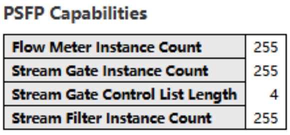
Red

The RED Frames Count counter counts received random early detection (Red) frames associated with this stream filter.

PSFP Capabilities

[Time > TSN > PSFP > PSFP Capabilities]

This page allows the user to inspect the current PSFP configurations.



PSFP Capabilities

Flow Meter Instance Count	255
Stream Gate Instance Count	255
Stream Gate Control List Length	4
Stream Filter Instance Count	255

PSFP Capabilities

Flow Meter Instances Count

The Max Flow Meter Instances parameter defines the maximum number of flow meter instances that are supported by this Bridge component.

Stream Gate Instances Count

The Max Stream Gate Instances parameter defines the maximum number of stream gate instances that are supported by this Bridge component.

Stream Gate Control List Length

The Supported List Max parameter defines the The maximum value supported by this Bridge component of the Admin Control List Length and Oper Control List Length parameters.

Stream Filter Instances Count

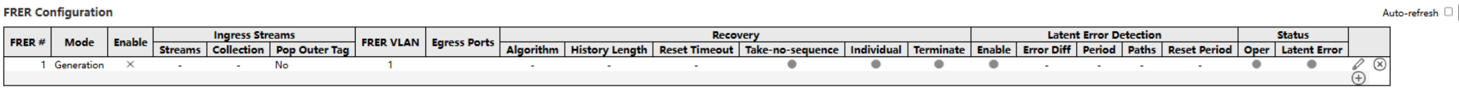
The Max Stream Filter Instances parameter defines the maximum number of stream filter instances that are supported by this Bridge component.

2.6.7. FRER

[Time > TSN > FRER]

[Configuration]

This page allows the user to inspect the current FRER configurations.



FRER Configuration

Auto-refresh □

FRER #	Mode	Enable	Ingress Streams			FRER VLAN	Egress Ports	Recovery						Latent Error Detection					Status		
			Streams	Collection	Pop Outer Tag			Algorithm	History Length	Reset Timeout	Take-no-sequence	Individual	Terminate	Enable	Error Diff	Period	Paths	Reset Period	Oper	Latent Error	
1	Generation	×	-	-	No	1		-	-	-	●	●	●	●	-	-	-	-	●	●	✎ ⊗
																					⊕

This page allows users to check the current FRER configurations and may also modify them.

FRER Configuration

FRER#

Identifier for FRER instances.

Mode

Mode of operation. Generation or Recovery.

Enable

FRER instance enabled or disabled.

✓: Enabled.

×: Disabled.

Ingress Streams Streams

List of ingress stream Ids.

Ingress Streams Collection

Indicates the ID of a stream collection, or a dash if not configured or individual ingress streams are used instead.

Ingress Streams Pop Outer Tag

Only used in generation mode and shows a dash in recovery mode. When "Yes", a possible outer VLAN tag in the ingressing frames gets popped before egressing with an R-tag. When "No", a possible outer VLAN tag in the ingressing frames is preserved beneath the R-tag on egress.

FRER VLAN

The VLAN ID that ingress flows get classified to.

Egress Ports

The port numbers that this FRER instance will hit.

Recovery Algorithm

The algorithm used by Recovery function. Vector or match.

Recovery History Length

history length of vector algorithm.

Recovery Reset Timeout

Reset timeout of Recovery function.

Recovery Take-no-sequence

If true, accept all frames whether they are R-tagged or not.

Recovery Individual

Use individual recovery.

Recovery Terminate

Strip R-Tag from a frame before presenting it on egress. Strip R-Tag from a frame before presenting it on egress.

Latent Error Detection Enable

Enable/disable Latent error detection.

Latent Error Detection Error Diff

Latent error detection error difference.

Latent Error Detection Period

Latent error detection period.

Latent Error Detection Paths

Latent error detection paths.

Latent Error Detection Reset Period

Latent error detection reset period.

Status Oper

The operational state of FRER instance.

🟢: Active.

🔴: Disabled or Internal error.

Status Latent Error

🟢: No errors.

🔴: There are latent errors.

Configuration Buttons

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

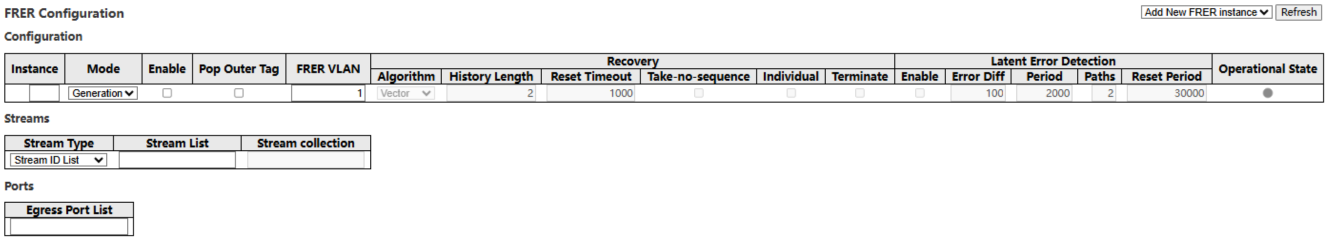
✎: Edits the FRER instance.

⊗: Deletes the FRER instance.

⊕: Adds new FRER instance.

Click on ⊕ as shown in the following figure :

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



FRER Configuration

Configuration

Instance	Mode	Enable	Pop Outer Tag	FRER VLAN	Recovery						Latent Error Detection					Operational State
					Algorithm	History Length	Reset Timeout	Take-no-sequence	Individual	Terminate	Enable	Error Diff	Period	Paths	Reset Period	
	Generation	□	□	1	Vector	2	1000	□	□	□	□	100	2000	2	30000	●

Streams

Stream Type	Stream List	Stream collection
Stream ID List		

Ports

Egress Port List

Configuration

Instance

Identifier for FRER instances.

Mode

Decides if this FRER instance shall run in Generation or Recovery mode. Default is Generation.

Enable

Enable or disable a FRER instance.

Pop Outer Tag

Set to expand the outer container tabs; check and save to complete the configuration.

FRER VLAN

Select the VLAN ID that ingress flows get classified to.

Recovery Algorithm

IEEE 802.1CB-2017 requires implementations to provide two different recovery function algorithms, match and vector.

Match is the simplest algorithm: It basically says: Discard all packets with a sequence number equal to the last sequence number seen. Accept all others. The algorithm also comes with a reset timer that - when it expires - causes the algorithm to accept any sequence number - even the same as the previous. The reset timer is restarted every time a packet is accepted. The match algorithm counts the number of times the reset timer has expired and the number of passed, discarded, and out-of-order packets. Out-of-order happens when the sequence number of a given packet is not one higher than the previous (and the timer has not expired).

Vector is somewhat more complicated. When a packet with a given sequence number arrives, it must be within the previous accepted packets sequence number +/- a configurable history length, or it will be discarded. If the packet is already seen (within the history length window), it is also discarded. Also this algorithm comes with a reset timer that - when it expires - causes the algorithm to accept any sequence number next time a packet arrives. The reset timer is restarted every time a packet is accepted.

The vector algorithm counts the number of times the reset timer has expired and the number of passed, discarded, out-of-order, and so-called rogue packets. Out-of-order happens when the sequence number of a given packet is "older" than a previous packets (taking wrap-around into account), and the packet has not been accepted before. Out-of-order packets are accepted. Rogue packets are packets with a sequence number beyond the history length window. Rogue packets are also counted as discarded. Furthermore, the vector algorithm counts lost packets, that is, the number of unreceived sequence numbers when the history window moves.

Both algorithms also counts the number of packets arriving without an R-tag. This is done with the tagless counter. By default, such packets will be discarded. A per-FRER instance parameter recovery take-no-sequence, however, allows such frames to pass through. Notice: The 802.1CB standard utilizes the frerSeqRcvyTakeNoSequence only in the vector algorithm, but the switches that the present guide is meant for also utilizes it in the match algorithm. Notice: This feature should only be used on terminating switches, because such tagless packets will be R-tagged (with sequence number 0) on their way out on non-terminating switches.

The selected algorithm on a given FRER instance will be used in both compound and individual recovery functions.

Default is the vector algorithm.

Recovery History Length

Configure the recvery functions history length. Valid range is 2-32 and default is 2.

Recovery Reset Timeout

Configure recovery function's reset timeout in milliseconds. Valid range is 1-4095 and default is 1000.

Recovery Take-no-sequence

Select this option to accept all frames whether they are R-tagged or not.

Recovery Individual

Individual recovery means that a member stream undergoes recovery before it reaches the compound recovery function. The compound recovery function sits on each and every egress port in the FRER instance. The one and only thing that individual recovery can do that compound recovery can not is to filter out member streams that keep presenting the same R-tag sequence number because of a defect transmitter. It goes like this:

Suppose the transmitter of member stream 1 is working perfectly. It will send out frames with an increasing sequence number and wrap back to 0 after 65535 frames. Suppose the transmitter of member stream 2 is sending out the same frame with the same sequence number, X, over and over again. If we only had a compound recovery function, that function would at times be presented with frames with sequence number X from stream 1 and sequence number X from stream 2, and the first of these two frames would be sent to the egress port.

So - depending on timing - sometimes the frame with sequence number X would come from stream 1 and sometimes it would come from the erroneous stream 2. The effect of enabling individual recovery is to have the individual recovery function for stream 2 filter out all identically numbered frames before they are presented to the compound recovery function. This is a very unlikely situation, and most network administrators will not need individual recovery.

Moreover, individual recovery is very expensive in terms of hardware resources: Every ingress stream needs an individual recovery function per egress port. So if a FRER instance defines 8 ingress streams and 8 egress ports, the switch needs 64 individual recovery instances - just for this one FRER instance.

Recovery Terminate

Select this option to strip an R-Tag from a frame before presenting it on egress.

Latent Error Detection

The purpose of latent error detection is to raise a flag if the number of discarded packets is "relatively few" compared to the number of passed packets. The algorithm relies on four user inputs: Period, Reset period, Paths, Error difference.

The reset function algorithm is as follows: Every Reset period milliseconds, read number of passed and discarded packet counters, and set a per-FRER instance variable, CurDiff, as follows:
CurDiff = passed_packets * (paths - 1) - discarded_packets;
The test function algorithm is as follows: Every timeout milliseconds, read the discarded and passed packet counters, and perform the following:
diff = Abs(CurDiff - (passed_packets * (paths - 1) - discarded_packets));
if (diff > difference) { raise_flag() }.

Basically, it says: If you expect N member streams to ingress this FRER instance, N-1 of these member streams are expected to be discarded, and only one is expected to pass. To allow for some slack due to random packet losses and the fact that counters are not neccessarily read simultaneously, set the difference to account for that. The reset function makes sure that CurDiff is updated to avoid that occassional packet losses do not accumulate forever.

Latent Error Detection Enable

Enable/disable Latent error detection.

Latent Error Detection Error Diff

The number of packets "allowed" to be in difference without raising the flag.

Valid range is 0-10000000 and default is 100.

Latent Error Detection Period

The number of milliseconds between invoking the test function.

Valid range is 1000-86400000 and default is 2000.

Latent Error Detection Paths

The number of member streams expected to ingress this FRER instance.

Valid range is 2-8 and default is 2.

Latent Error Detection Reset Period

The number of milliseconds between invoking the reset function.

Valid range is 1000-86400000 and default is 30000.

Operational State

The operational state of FRER instance.

🟢: Active.

🔴: Disabled or Internal error.

Streams

Stream Type

Select the matching type for this flow.

Flow ID List: When selecting this option, values can be assigned to flow IDs in the subsequent flow list configuration area.

Flow Group: When selecting this option, values can be defined for flow groups in the subsequent flow list configuration area.

Stream List

Configure Stream ID values.

Stream collection

Configure Stream Set values.

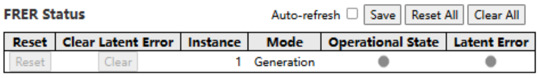
Ports

Egress port list

Specify the egress ports that this FRER instance will hit. There is a maximum of 8 egress ports per FRER instance.

[Status]

This page allows the user to inspect the current FRER status, and possible reset/clear them as well.



FRER Status

Auto-refresh □ Save Reset All Clear All

Reset	Clear Latent Error	Instance	Mode	Operational State	Latent Error
Reset	Clear	1	Generation	●	●

FRER Status

Reset

Click to perform function reset.

If this FRER instance is in generation mode, this is used to reset the sequence number of the sequence generator.

If this FRER instance is in recovery mode, this is used to reset the recovery function. It resets both possible individual recovery functions and the compound recovery functions.

Clear Latent Error

Click to clear a Sticky latent error.

Instance

The id of the FRER instance.

Mode

Decides if this FRER instance shall run in Generation or Recovery mode. Default is Generation.

Operational State

The operational state of FRER instance.

🟢: Active.

🔴: Disabled or Internal error.

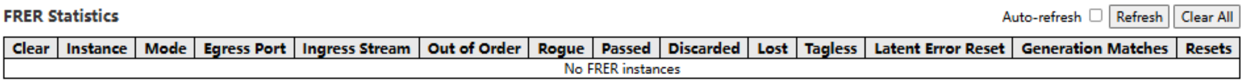
Latent Error

🟢: No errors.

🔴: There are latent errors.

[Statistics]

This page allows the user to inspect the current FRER statistics counters, and possibly clear them as well.



FRER Statistics

Auto-refresh □ Refresh Clear All

Clear	Instance	Mode	Egress Port	Ingress Stream	Out of Order	Rogue	Passed	Discarded	Lost	Tagless	Latent Error Reset	Generation Matches	Resets
No FRER instances													

FRER Statistics

Clear

This box is used to mark an entry for clearance in next Clear operation.

Instance

The FRER instance id.

Mode

Mode of operation. Generation or Recovery.

Egress Port

List of egress port numbers.

Ingress Stream

List of Ingress stream Ids.

Out of Order

IEEE 802.1CB-2017: frerCpsSeqRcvyOutOfOrderPackets.

Rogue

IEEE 802.1CB-2017: frerCpsSeqRcvyRoguePackets.

Passed

IEEE 802.1CB-2017: frerCpsSeqRcvyPassedPackets.

Discarded

IEEE 802.1CB-2017: frerCpsSeqRcvyDiscardedPackets.

Lost

IEEE 802.1CB-2017: frerCpsSeqRcvyLostPackets.

Tagless

IEEE 802.1CB-2017: frerCpsSeqRcvyTaglessPackets.

Latent Error Reset

IEEE 802.1CB-2017: frerCpsSeqRcvyLatentErrorResets.

Generation Matches

Number of matches on ingress stream. Only valid in Generation mode.

Reset

IEEE 802.1CB-2017: frerCpsSeqRcvyResets.

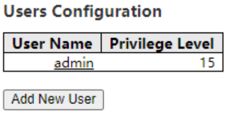
3. Device Security

The menu contains the following dialogs:
Users
Password Policy
Auth Method
Management Access
RMON

3.1. Users

[Device Security > Users]

This page provides an overview of the current users. Currently the only way to login as another user on the web server is to logout and reenter the username and password.



Users Configuration

User Name	Privilege Level
admin	15

Users Configuration

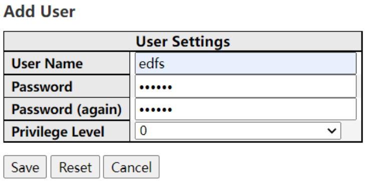
User Name

The name identifying the user. This is also a link to Add/Edit User.

Privilege Level

The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be the same or greater than the group privilege level to have 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.

Click on "Add New User" on this page to Add a User. Open the configuration page, as shown in the following figure:



Add User

User Settings	
User Name	edfs
Password	••••••
Password (again)	••••••
Privilege Level	0

Add User

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

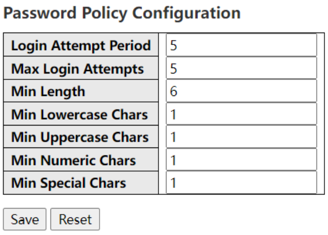
The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be the same or greater than the group privilege level to have 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.) needs 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.

Note : If 'Password' for creating the 'User Name' is empty. After logging out of the system, logging in with the new 'User Name' and password 'admin' will force a pop-up window to modify the 'User Name' password. Then, log into the system with the new "username" and modified "password".

3.2. Password Policy

[Device Security > Password Policy]

On this page, you can configure password policy related configurations. When applying for a new user or modifying the password of an existing user, the operator checks the password according to the set password policy after entering the password.



Password Policy Configuration

Login Attempt Period	5
Max Login Attempts	5
Min Length	6
Min Lowercase Chars	1
Min Uppercase Chars	1
Min Numeric Chars	1
Min Special Chars	1

Password Policy Configuration

Login Attempt Period

Limit the number of login attempts per IP or user within a specified time period. Set the lockout duration for the IP or username, with a value ranging from 0 to 60. Setting it to 0 disables this feature.

Max Login Attempts

Limit the number of login attempts per user within a certain amount of time. The value ranges from 0-5 and is set to 0 to disable the setting.

Min Length

Configure the minimum password length for the password policy; The default value is 6. The value ranges from 1-31.

Min Lowercase Chars

Configure the minimum number of lowercase letters in the password policy; The default value is 1. The value ranges from 0-7.

Min Uppercase Chars

Configure the minimum number of uppercase letters in passwords in the password policy; The default value is 1. The value ranges from 0-7.

Min Numeric Chars

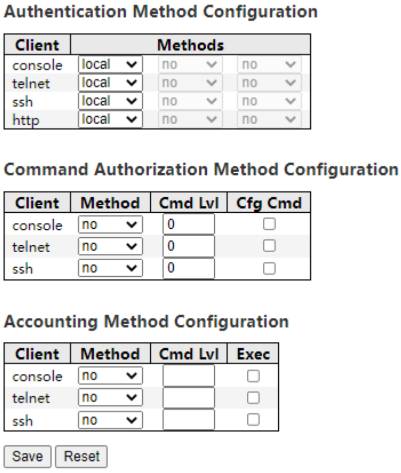
Configure the minimum number of numbers that passwords should contain in the password policy; The default value is 1. The value ranges from 0-7.

Min Special Chars

Configure the minimum number of special characters that passwords should contain in the password policy; The default value is 1. The value ranges from 0-7.

3.3. Auth Method

[Device Security > Auth Method]



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		□

Authentication Method Configuration

On this page, you can configure authentication method related configurations. The authentication section allows you to configure how a user is authenticated when he or she logs into the switch via one of the management client interfaces.

Client

The management client for which the configuration below applies.

Methods

Method can be set to one of the following values:

- no: Authentication is disabled and login is not possible.
- local: Use the local user database on the switch for authentication.
- radius: Use remote RADIUS server(s) for authentication.
- tacacs: Use remote TACACS+ server(s) for authentication.

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

Command Authorization Method Configuration

On this page, you can configure command authorization method related configurations. The command authorization section allows you to limit the CLI commands available to a user.

Client

The management client for which the configuration below applies.

Method

Method can be set to one of the following values:

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

Cmd Lvl

Authorize all commands with a privilege level higher than or equal to this level.

Valid values are in the range 0 to 15.

Cfg Cmd

Also authorize configuration commands.

Accounting Method Configuration

On this page, you can configure accounting method related configurations. The accounting section allows you to configure command and exec (login) accounting.

Client

The management client for which the configuration below applies.

Method

Method can be set to one of the following values:

- no: Accounting is disabled.
- tacacs: Use remote TACACS+ server(s) for accounting.

Cmd Lvl

Enable accounting of all commands with a privilege level higher than or equal to this level.

Valid values are in the range 0 to 15. Leave the field empty to disable command accounting.

Exec

Enable exec (login) accounting.

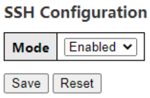
3.4. Management Access

3.4.1. Server

[Device Security > Management Access > Server]

[SSH]

On this page, you can configure SSH related configurations.



SSH Configuration

Mode: Enabled

SSH Configuration

Mode

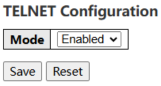
Indicates the SSH mode operation. Possible modes are:

Enabled: Enable SSH mode operation.

Disabled: Disable SSH mode operation.

[TELNET]

On this page, you can configure telnet related configurations.



TELNET Configuration

Mode: Enabled

TELNET Configuration

Mode

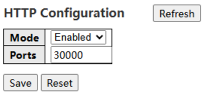
Indicates the telnet mode operation. Possible modes are:

Enabled: Enable telnet mode operation.

Disabled: Disable telnet mode operation.

[HTTP]

On this page, you can configure the HTTP settings and maintain the current ports on the switch.



HTTP Configuration

Mode	Enabled
Ports	30000

HTTP Configuration

Mode

Indicate the HTTP mode operation. Possible modes are:

Enabled: Enable HTTP mode operation.

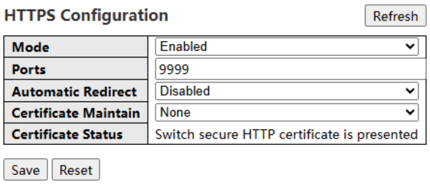
Disabled: Disable HTTP mode operation.

Ports

HTTP Port Configuration. Default port number range: 80 or 1024-65535.

[HTTPS]

On this page, you can configure the HTTPS settings and maintain the current Certificate on the switch.



HTTPS Configuration

Mode	Enabled
Ports	9999
Automatic Redirect	Disabled
Certificate Maintain	None
Certificate Status	Switch secure HTTP certificate is presented

HTTPS Configuration

Mode

Indicate the HTTPS mode operation. Possible modes are:

Enabled: Enable HTTPS mode operation.

Disabled: Disable HTTPS mode operation.

Ports

HTTPS Port Configuration. Default port number range: 443 or 1024-65535.

Automatic Redirect

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

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

Possible modes are:

Enabled: Enable HTTPS redirect mode operation.

Disabled: Disable HTTPS redirect mode operation.

Certificate Maintain

The operation of certificate maintenance.

Possible operations are:

None: No operation.

Delete: Delete the current certificate.

Upload: Upload a certificate PEM file. Possible methods are: **Web Browser** or **URL**.

Generate: Generate a new self-signed RSA certificate.

Certificate Pass Phrase

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

Certificate Upload

Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem
Notice that the RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g. Chrome v39.
Possible methods are:

Web Browser: Upload a certificate via Web browser.

URL: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is <protocol> : // [<username> [: <password>] @] <host> [: <port>] [/ <path>] / <file_name>.

For example:

tftp://10.10.10.10/new_image_path/new_image.dat,

http://username:password@10.10.10.10:80/new_image_path/new_image.dat.

A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score(_). The maximum length is 63 and hyphen must not be the 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:

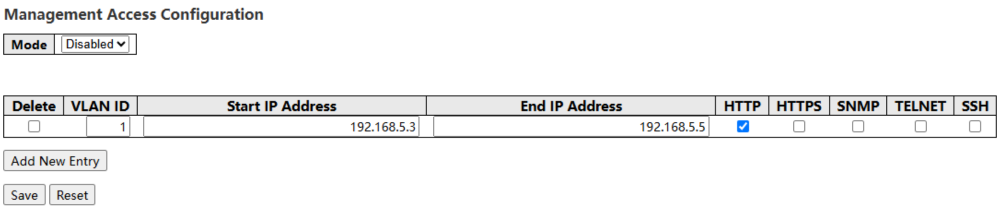
Switch secure HTTP certificate is presented.

Switch secure HTTP certificate is not presented.

Switch secure HTTP certificate is generating ...

[Configuration]

On this page, you can configure access management related configurations. Click on "Add New Entry" on this page to add a new access management entry. The maximum number of entries is 16. If the application's type match any one of the access management entries, it will allow access to the switch.



Management Access Configuration

Mode	Disabled

Delete	VLAN ID	Start IP Address	End IP Address	HTTP	HTTPS	SNMP	TELNET	SSH
☐	1	192.168.5.3	192.168.5.5	☑	☐	☐	☐	☐

Management Access Configuration

Mode

Indicates the access management mode operation. Possible modes are:

Enabled: Enable access management mode operation.

Disabled: Disable access management mode operation.

Delete

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

VLAN ID

Indicates the VLAN ID for the access management entry.

Start IP address

Indicates the start IP unicast address for the access management entry.

End IP address

Indicates the end IP unicast address for the access management entry.

HTTP

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

HTTPS

Indicates that the host can access the switch from 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

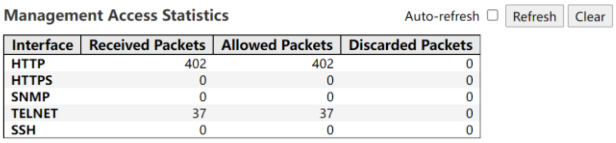
Indicates that the host can access the switch from TELNET interface if the host IP address matches the IP address range provided in the entry.

SSH

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

[Statistics]

This page provides statistics for access management.



Management Access Statistics

Auto-refresh □ Refresh Clear

Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	402	402	0
HTTPS	0	0	0
SNMP	0	0	0
TELNET	37	37	0
SSH	0	0	0

Management Access Statistics

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

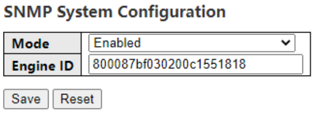
Number of discarded packets from the interface when access management mode is enabled.

3.4.2. SNMP

System

[Device Security > Management Access > SNMP > System]

On this page, you can configure the SNMP feature.



SNMP System Configuration

Mode	Enabled
Engine ID	800087bf030200c1551818

SNMP System Configuration

Mode

Indicates the SNMP mode operation. Possible modes are:

Enabled: Enable SNMP mode operation.

Disabled: Disable SNMP mode operation.

Engine ID

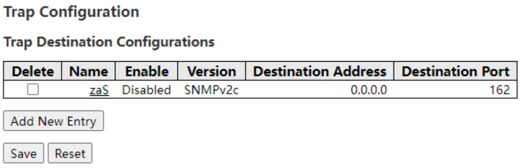
Indicates the SNMPv3 engine ID. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Only users on this Engine ID can access the device (local users), so changing the Engine ID will revoke access for all current local users.

Trap

[Device Security > Management Access > SNMP > Trap]

[Destinations]

On this page, you can configure the trap destinations.



Trap Configuration

Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port
□	zaS	Disabled	SNMPv2c	0.0.0.0	162

Trap Destination Configurations

Delete

The selected entry will be deleted upon the next save.

Name

Indicates the trap Configuration's name.

Enable

Indicates the trap destination mode operation. Possible modes are:

Enabled: Enable SNMP trap mode operation.

Disabled: Disable SNMP trap mode operation.

Version

Indicates the SNMP trap supported version. Possible versions are:

SNMPv1: Set SNMP trap supported version 1.

SNMPv2c: Set SNMP trap supported version 2c.

SNMPv3: Set SNMP trap supported version 3.

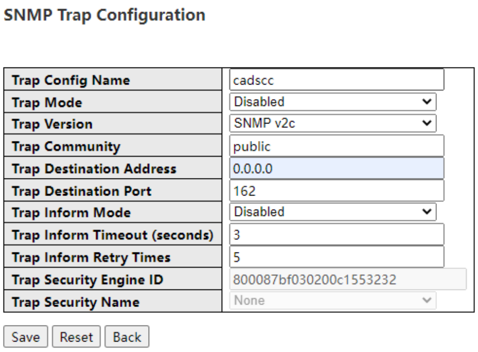
Destination Address

Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w'). And it also allow a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash. Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Destination port

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

Click to add a new entry.



SNMP Trap Configuration

Trap Config Name	cadscc
Trap Mode	Disabled
Trap Version	SNMP v2c
Trap Community	public
Trap Destination Address	0.0.0.0
Trap Destination Port	162
Trap Inform Mode	Disabled
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Security Engine ID	800087bf030200c1553232
Trap Security Name	None

Trap Inform Mode

Enable Tarp notification mode.

Trap Inform Timeout (seconds)

Trap notification timeout (seconds).

Trap Inform Retry Times

Trap notification retry count.

Trap Security Engine ID

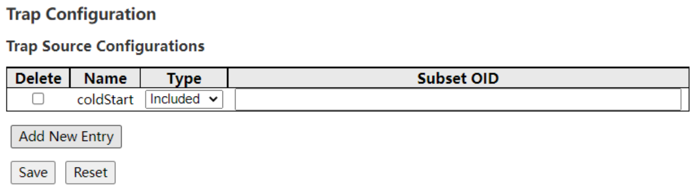
Trap security engine ID.

Trap Security Name

Trap Security Name.

[Sources]

On this page, you can configure the trap source.



Trap Configuration

Trap Source Configurations

Delete	Name	Type	Subset OID
□	coldStart	Included	

Trap Source Configurations

Delete

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

Name

Indicates the name for the entry.

1、coldStart

2、warmStart

3、linkUp

4、linkDown

5、authenticationFailure

6、entConfigChange

7、newRoot

8、topologyChange

9、LldpRemTablesChange

10、risingAlarm

11、fallingAlarm

12、alarmTrapStatus

13、frerTrap

14、ipTrapGlobalsMain

15、ipTrapInterfacesLink

16、portTrapInterfacePortMonitor

17、psecTrapGlobalMain

18、psecTrapInterfaces

19、selftestActionTrap

20、trackTrapStatusChange

21、vrrpTrapAuthFailure

22、VrrpTrapNewMaster

Type

The filter type for the entry. Possible types are:

included: An optional flag to indicate a trap is sent for the given trap source is matched.

excluded: An optional flag to indicate a trap is not sent for the given trap source is matched.

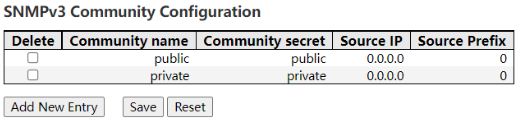
Subset OID

The subset OID for the entry. The value should depend on the what kind of trap name. For example, the ifIdex is the subset OID of linkUp and linkDown. A valid subset OID is one or more digital number(0-4294967295) or asterisk(*) which are separated by dots(.). The first character must not begin withasterisk(*) and the maximum of OID count must not exceed 128.

Communities

[Device Security > Management Access > SNMP > Communities]

On this page, you can configure the SNMPv3 community table.



SNMPv3 Community Configuration

Delete	Community name	Community secret	Source IP	Source Prefix
□	public	public	0.0.0.0	0
□	private	private	0.0.0.0	0

SNMPv3 Community Configuration

Delete

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

Community Name

Indicates the security name to map the community to the SNMP Groups configuration. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Community Secret

Indicates the community secret (access string) to permit access using SNMPv1 and SNMPv2c to the SNMP agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

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 prefix.

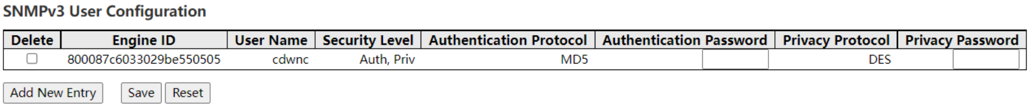
Source Prefix

Indicates the SNMP access source address prefix.

Users

[Device Security > Management Access > SNMP > Users]

On this page, you can configure the SNMPv3 user table.



SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
□	800087c6033029be550505	cdwnc	Auth, Priv	MD5		DES	

SNMPv3 User Configuration

Delete

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

Engine ID

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

User Name

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

Security Level

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

NoAuth, **NoPriv**: No authentication and no privacy.

Auth, **NoPriv**: Authentication and no privacy.

Auth, **Priv**: Authentication and privacy.

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

Authentication Protocol

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

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 it must first be ensured 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:

DES: An optional flag to indicate that this user uses DES authentication protocol.

AES: When available, an optional flag to indicate that this user uses AES authentication protocol.

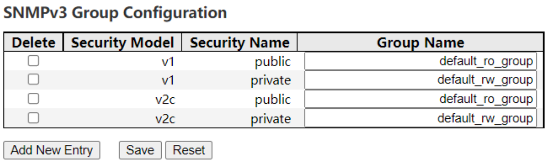
Privacy Password

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.

Groups

[Device Security > Management Access > SNMP > Groups]

On this page, you can configure the SNMPv3 group table.



SNMPv3 Group Configuration

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

SNMPv3 Group Configuration

Delete

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

Security Model

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

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: SNMPv3, 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.

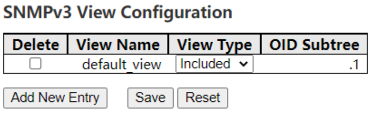
Group Name

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.

Views

[Device Security > Management Access > SNMP > Views]

On this page, you can configure the SNMPv3 view table.



SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
□	default_view	Included	.1

SNMPv3 View Configuration

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:

included: An optional flag to indicate that this view subtree should be included.

excluded: An optional flag to indicate that this view subtree should be excluded.

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

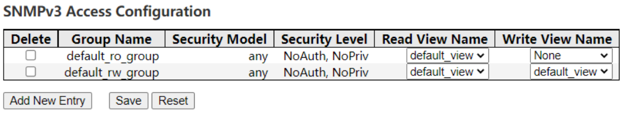
OID Subtree

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

Access

[Device Security > Management Access > SNMP > Access]

On this page, you can configure the SNMPv3 access table.



SNMPv3 Access Configuration

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

SNMPv3 Access Configuration

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 Model

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

any: Any security model accepted(v1 | v2c | usm).

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: SNMPv3, 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 privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

Read View Name

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

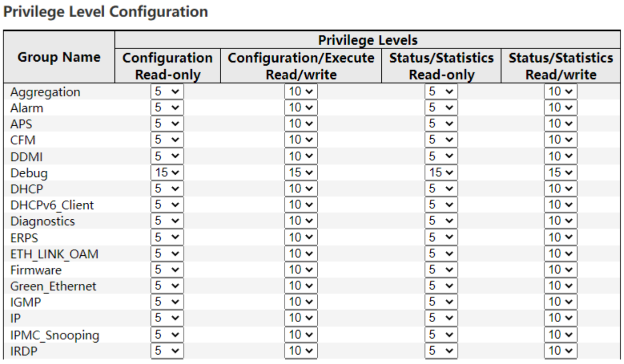
Write View Name

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

3.4.3. Privilege Levels

[Device Security > Management Access > Privilege Levels]

On this page, you can configure privilege levels related configurations.



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
Alarm	5	10	5	10
APS	5	10	5	10
CFM	5	10	5	10
DDMI	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
ERPS	5	10	5	10
ETH_LINK_OAM	5	10	5	10
Firmware	5	10	5	10
Green_Ethernet	5	10	5	10
IGMP	5	10	5	10
IP	5	10	5	10
IPMC_Snooping	5	10	5	10
IRDP	5	10	5	10

Privilege Levels Configuration

Group Name

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

System: Contact, Name, Location, Timezone, Daylight Saving Time, Log.

Security: Authentication, System Access Management (access), Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard, Users, Privilege Levels.

IP: Everything except 'ping'.

Ports: Everything except 'VeriPHY'.

Diagnostics: 'ping' and 'VeriPHY'.

Basic Setting: System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load.

Privilege Levels

The Privilege Levels can be configured between 0 to 15 (where 0 is lowest level and 15 is highest 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 (e.g. for clearing of statistics). User Privilege should be same or greater than the authorization Privilege level to have the access to that group.

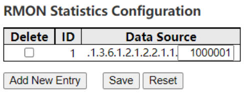
3.5. RMON

3.5.1. Statistics

[Device Security > RMON > Statistics]

[Configuration]

On this page, you can configure RMON statistics related configurations. Click on "Add New Entry" on this page to add a new RMON statistics entry. The entry index key is **ID**.



RMON Statistics Configuration

Delete	ID	Data Source
□	1	.1.3.6.1.2.1.2.2.1.1. 1000001

RMON Statistics Configuration

Delete

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

ID

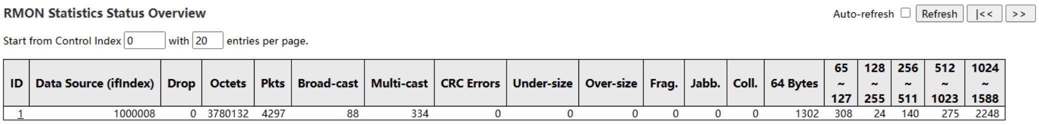
Indicates the index of the entry. The range is from 1 to 65535.

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.

[Status]

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



RMON Statistics Status Overview

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.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
1	1000008	0	3780132	4297	88	334	0	0	0	0	0	0	1302	308	24	140	275	2248

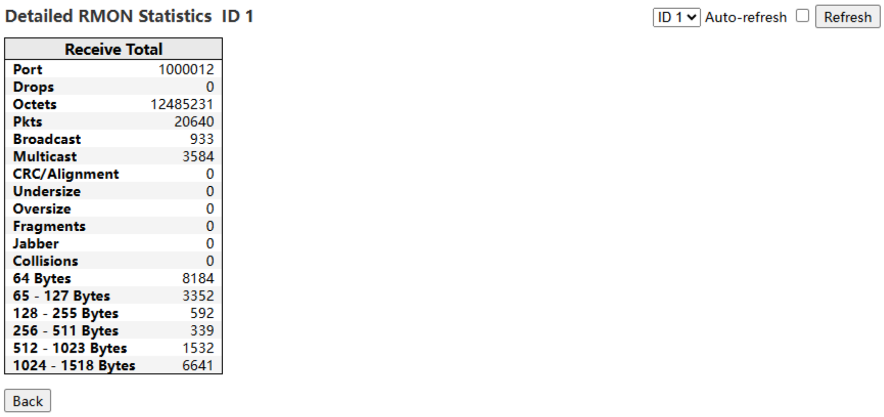
The "Start from Control Index" allows the user to select the starting point in the Statistics table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Statistics table match.

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.

RMON Statistics Status Overview

ID

Indicates the index of Statistics entry. Click the index to enter the corresponding Detailed RMON Statistics page.



Detailed RMON Statistics ID 1

ID 1 ▾ Auto-refresh □ Refresh

Receive Total	
Port	1000012
Drops	0
Octets	12485231
Pkts	20640
Broadcast	933
Multicast	3584
CRC/Alignment	0
Undersize	0
Oversize	0
Fragments	0
Jabber	0
Collisions	0
64 Bytes	8184
65 - 127 Bytes	3352
128 - 255 Bytes	592
256 - 511 Bytes	339
512 - 1023 Bytes	1532
1024 - 1518 Bytes	6641

Data Source(ifIndex)

The port ID which wants to be monitored.

Drop

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

Octets

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

Pkts

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

Broad-cast

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

Multi-cast

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

CRC Errors

The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Under-size

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

Over-size

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

Frag.

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

Jabb.

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

Coll.

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

64 Bytes

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

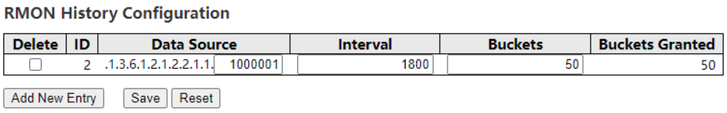
The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

3.5.2. History

[Device Security > RMON > History]

[Configuration]

On this page, you can configure RMON history related configurations. Click on "Add New Entry" on this page to add a new RMON history entry. The entry index key is **ID**.



RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
☐	2	.1.3.6.1.2.1.2.2.1.1. 1000001	1800	50	50

RMON History Configuration

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

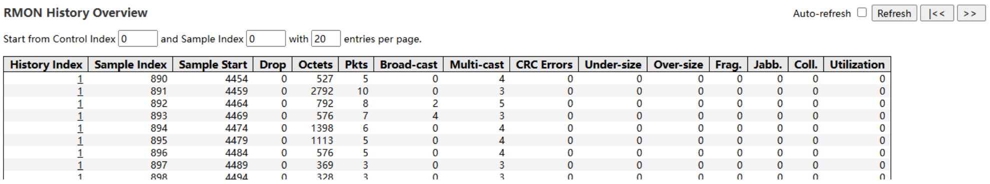
Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 50, default value is 50.

Buckets Granted

The number of data shall be saved in the RMON.

[Status]

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.



RMON History Overview

Auto-refresh □ Refresh |<< >>

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
1	890	4454	0	527	5	0	4	0	0	0	0	0	0	0
1	891	4459	0	2792	10	0	3	0	0	0	0	0	0	0
1	892	4464	0	792	8	2	5	0	0	0	0	0	0	0
1	893	4469	0	576	7	4	3	0	0	0	0	0	0	0
1	894	4474	0	1398	6	0	4	0	0	0	0	0	0	0
1	895	4479	0	1113	5	0	4	0	0	0	0	0	0	0
1	896	4484	0	576	5	0	4	0	0	0	0	0	0	0
1	897	4489	0	369	3	0	3	0	0	0	0	0	0	0
1	898	4494	0	328	3	0	3	0	0	0	0	0	0	0

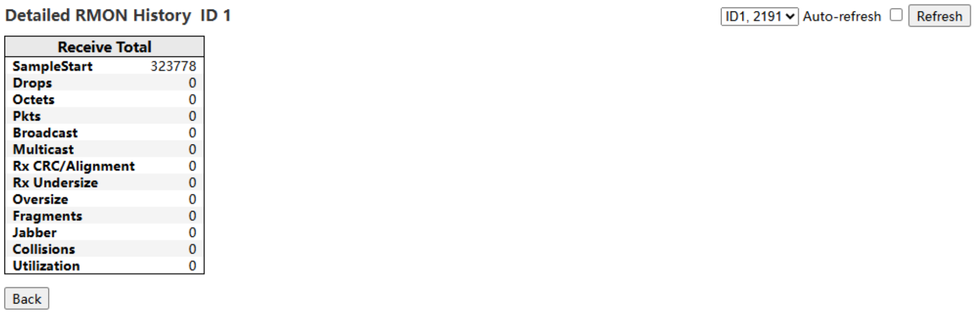
The "Start from History Index and Sample Index" allows the user to select the starting point in the History table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest History table match.

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 more entries" is shown in the displayed table. Use the **"|<<"** button to start over.

RMON History Overview

History Index

Indicates the index of History control entry. Click the index to enter the corresponding Detailed RMON History page.



Detailed RMON History ID 1

ID1, 2191 Auto-refresh □ Refresh

Receive Total	
SampleStart	323778
Drops	0
Octets	0
Pkts	0
Broadcast	0
Multicast	0
Rx CRC/Alignment	0
Rx Undersize	0
Oversize	0
Fragments	0
Jabber	0
Collisions	0
Utilization	0

Back

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.

Broad-cast

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

Multi-cast

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

CRC Errors

The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

Under-size

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

Over-size

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

Frag.

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

Jabb.

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

Coll.

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

Utilization

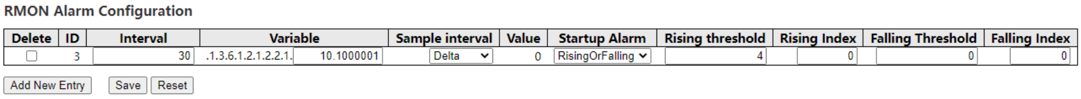
The best estimate of the mean physical layer network utilization on this interface during this sampling interval, typically displayed as a percentage.

3.5.3. Alarm

[Device Security > RMON > Alarm]

[Configuration]

On this page, you can configure RMON alarm related configurations. Click on "Add New Entry" on this page to add a new RMON alarm entry. The entry index key is **ID**.



RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample interval	Value	Startup Alarm	Rising threshold	Rising Index	Falling Threshold	Falling Index
□	3	30	.1.3.6.1.2.1.2.2.1. 10.1000001	Delta	0	RisingOrFalling	4	0	0	0

RMON Alarm Configuration

Delete

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

ID

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

Interval

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

Variable

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

InOctets（10）: The total number of octets received on the interface, including framing characters.

InUcastPkts（11）: The number of uni-cast packets delivered to a higher-layer protocol.

InNUcastPkts（12）: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.

InDiscards（13）: The number of inbound packets that are discarded even the packets are normal.

InErrors（14）: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

InUnknownProtos（15）: The number of the inbound packets that were discarded because of the unknown or un-support protocol.

OutOctets（16）: The number of octets transmitted out of the interface , including framing characters.

OutUcastPkts（17）: The number of uni-cast packets that request to transmit.

OutNUcastPkts（18）: The number of broad-cast and multi-cast packets that request to transmit.

OutDiscards（19）: The number of outbound packets that are discarded event the packets is normal.

OutErrors（20）: The number of outbound packets that could not be transmitted because of errors.

OutQLen（21）: The length of the output packet queue (in packets).

Sample Type

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

Absolute: Get the sample directly.

Delta: Calculate the difference between samples (default).

Value

The value of the statistic during the last sampling period.

Startup Alarm

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

Rising Trigger alarm when the first value is larger than the rising threshold.

Falling Trigger alarm when the first value is less than the falling threshold.

RisingOrFalling Trigger 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 (0-65535). If this value is zero, no associated event will be generated, as zero is not a valid event index.

Falling Threshold

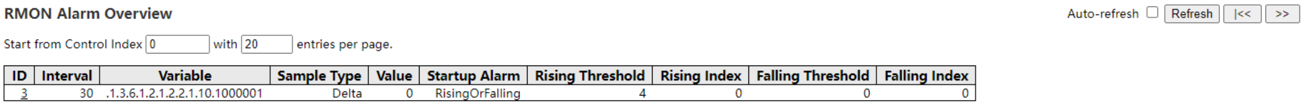
Falling threshold value (-2147483648-2147483647).

Falling Index

Falling event index (0-65535). If this value is zero, no associated event will be generated, as zero is not a valid event index.

[Status]

This page provides an overview of RMON Alarm 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.



RMON Alarm Overview

Auto-refresh □ Refresh |<< >>

Start from Control Index 0 with 20 entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
3	30	.1.3.6.1.2.1.2.2.1.10.1000001	Delta	0	RisingOrFalling	4	0	0	0

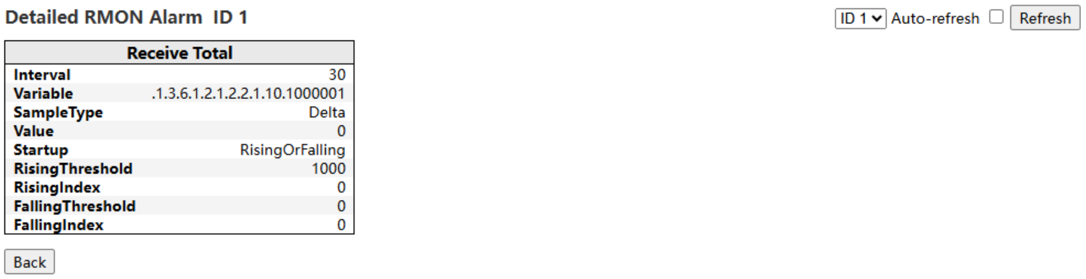
The "Start from Control Index" allows the user to select the starting point in the Alarm table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest Alarm table match.

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.

RMON Alarm Overview

ID

Indicates the index of Alarm control entry. Click the ID to enter the corresponding Detailed RMON Alarm page.



Detailed RMON Alarm ID 1

ID 1 Auto-refresh □ Refresh

Receive Total	
Interval	30
Variable	.1.3.6.1.2.1.2.2.1.10.1000001
SampleType	Delta
Value	0
Startup	RisingOrFalling
RisingThreshold	1000
RisingIndex	0
FallingThreshold	0
FallingIndex	0

Back

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

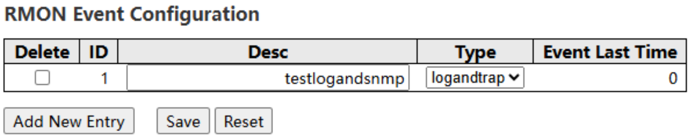
Falling event index.

3.5.4. Event

[Device Security > RMON > Event]

[Configuration]

On this page, you can configure RMON event related configurations. Click on "Add New Entry" on this page to add a new RMON event entry. The entry index key is **ID**.



RMON Event Configuration

Delete	ID	Desc	Type	Event Last Time
□	1	testlogandsnmp	logandtrap	0

RMON Event Configuration

Delete

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

ID

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

Desc

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

Type

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

none: No SNMP log is created, no SNMP trap is sent.

log: Create SNMP log entry when the event is triggered.

snmptrap: Send SNMP trap when the event is triggered.

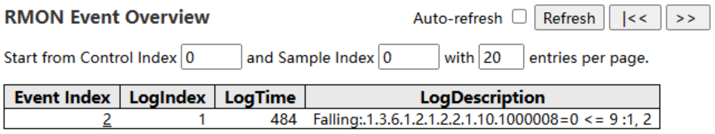
logandtrap: Create SNMP log entry and sent SNMP trap when the event is triggered.

Event Last Time

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

[Status]

This page provides an overview of RMON Event table 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.



RMON Event Overview

Start from Control Index 0 and Sample Index 0 with 20 entries per page.

Event Index	LogIndex	LogTime	LogDescription
2	1	484	Falling:.1.3.6.1.2.1.2.2.1.10.1000008=0 <= 9 :1, 2

The "Start from Event Index and Log Index" allows the user to select the 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.

RMON Event Overview

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.

4. Network Security

The menu contains the following dialogs:
Port Security
RADIUS
TACACS+
NAS
IP Source Guard
IPv6 Source Guard
ARP Inspection
ACL
Key-Chain

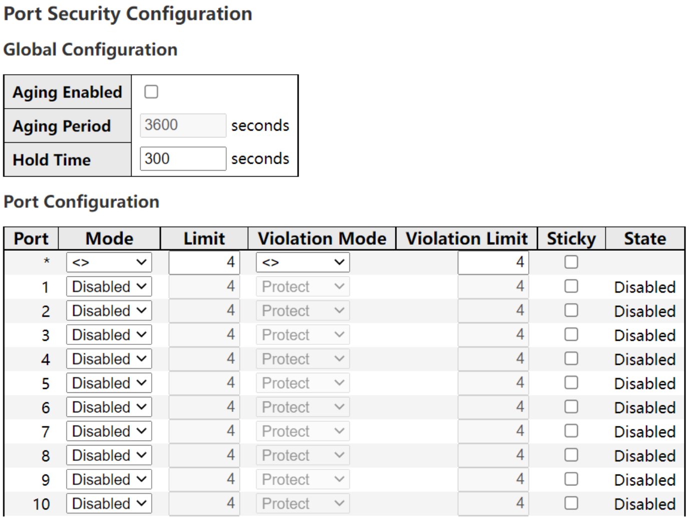
4.1. Port Security

4.1.1. Port

[Network Security > Port Security > Port]

[Configuration]

On this page, you can configure the Port Security global and per-port settings.



Port Security Configuration

Global Configuration

Aging Enabled	□
Aging Period	3600 seconds
Hold Time	300 seconds

Port Configuration

Port	Mode	Limit	Violation Mode	Violation Limit	Sticky	State
*	<>	4	<>	4	□	
1	Disabled	4	Protect	4	□	Disabled
2	Disabled	4	Protect	4	□	Disabled
3	Disabled	4	Protect	4	□	Disabled
4	Disabled	4	Protect	4	□	Disabled
5	Disabled	4	Protect	4	□	Disabled
6	Disabled	4	Protect	4	□	Disabled
7	Disabled	4	Protect	4	□	Disabled
8	Disabled	4	Protect	4	□	Disabled
9	Disabled	4	Protect	4	□	Disabled
10	Disabled	4	Protect	4	□	Disabled

Port Security allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Port Security 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 depending on violation mode. The violation mode can be one of the three different described below.

The Port Security configuration consists of two sections, a global and a per-port.

Global Configuration

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 functionality for securing MAC addresses, they may have other requirements to the aging period. The underlying functionality will use the shorter requested aging period of all modules that have aging enabled.

The Aging Period can be set to a number between 10 and 10000000 seconds with a default of 3600 seconds.

To understand why aging is needed, consider the following scenario: Suppose a terminal host is connected to a third-party switch or hub, which is then connected to a port on this switch where port security is enabled. If the limit is not exceeded, the terminal host will be allowed to forward traffic. Now, suppose the terminal host logs off or powers down. If not for aging, the terminal host would still occupy resources on this switch and be allowed to forward traffic. To address this situation, the aging feature is designed. When aging is enabled, a timer starts once the host's aging period ends.

Hold Time

The hold time - measured in seconds - is used to determine how long a MAC address is held in the MAC table if it has been found to violate the limit. Valid range is between 10 and 10000000 seconds with a default of 300 seconds.

The reason for holding a violating MAC address in the MAC table is primarily to ensure that the same MAC address doesn't give rise to continuous notifications (if notifications on violation count is enabled).

Port Configuration

Port

The port number to which the configuration below applies.

Mode

Controls whether Port Security is enabled on this port. Notice that other modules may still use the underlying port security features without enabling Port Security on a given port.

Limit

The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1023. Default is 4. If the limit is exceeded, an action is taken corresponding to the violation mode.

Violation Mode

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

Protect: Do not allow more than Limit MAC addresses on the port, but take no further action.

Restrict: If Limit is reached, subsequent MAC addresses on the port will be counted and marked as violating. Such MAC addresses are removed from the MAC table when the hold time expires. At most Violation Limit MAC addresses can be marked as violating at any given time.

Shutdown: If Limit is reached, one additional MAC address will cause the port to be shut down. This implies that all secured MAC addresses be removed from the port, and no new addresses be learned. There are three ways to re-open the port:

1) In the "Basic Settings→Port" page's "Ports Configured" column, Re-enable the port (select port → disable → auto).

2) Make a Port Security configuration change on the port.

3) Reboot the switch.

Violation Limit

The maximum number of MAC addresses that can be marked as violating on this port. This number cannot exceed 1023. Default is 4. It is only used when Violation Mode is **Restrict**.

Sticky

Enables Sticky learning of MAC addresses on this port. When the port is in Sticky mode, all MAC addresses that would otherwise have been learned as dynamic are learned as Sticky.
Sticky MAC addresses are part of the running-config and can therefore be saved to startup-config. Sticky MAC addresses survive link changes (in contrast to Dynamic, which will have to be learned again). They also survive reboots if running-config is saved to startup-config.

A port can be Sticky-enabled whether or not Port Security is enabled on that interface. In that way, it is possible to add Sticky MAC addresses management wise before enabling Port Security. To do that, use the "Networks Security→Port Security→MAC Addresses" page.

State

This column shows the current Port Security state of the port. The state takes one of four values:

Disabled: Port Security is disabled on the port.

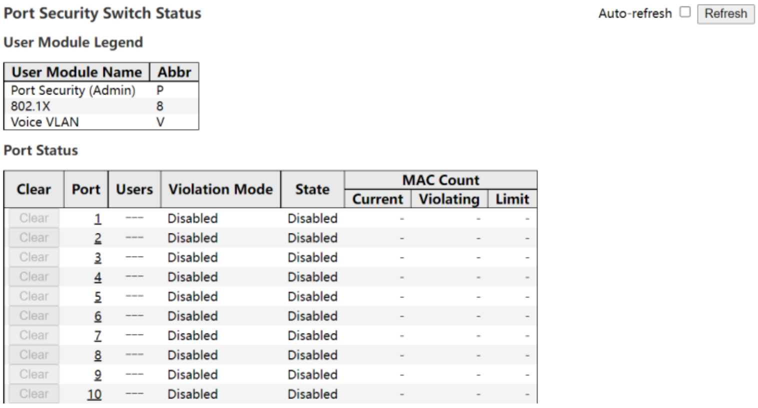
Ready: The limit is not yet reached. This can be shown for all violation modes.

Limit Reached: Indicates that the limit is reached on this port. This can be shown for all violation modes.

Shutdown: Indicates that the port is shut down by Port Security. This state can only be shown if violation mode is set to Shutdown.

[Status]

This page shows the Port Security status. Port Security may be configured both administratively and indirectly through other software modules - the so-called 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.



Port Security Switch Status

Auto-refresh □ Refresh

User Module Legend

User Module Name	Abbr
Port Security (Admin)	P
802.1X	8
Voice VLAN	V

Port Status

Clear	Port	Users	Violation Mode	State	MAC Count		
					Current	Violating	Limit
Clear	1	---	Disabled	Disabled	-	-	-
Clear	2	---	Disabled	Disabled	-	-	-
Clear	3	---	Disabled	Disabled	-	-	-
Clear	4	---	Disabled	Disabled	-	-	-
Clear	5	---	Disabled	Disabled	-	-	-
Clear	6	---	Disabled	Disabled	-	-	-
Clear	7	---	Disabled	Disabled	-	-	-
Clear	8	---	Disabled	Disabled	-	-	-
Clear	9	---	Disabled	Disabled	-	-	-
Clear	10	---	Disabled	Disabled	-	-	-

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

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:

Clear

Click to remove all dynamic MAC addresses on all VLANs on this port. The button is only clickable if number of secured MAC addresses is non-zero.

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.

Violation Mode

Shows the configured Violation Mode of the port. It can take one of four values:

Disabled: Port Security is not administratively enabled on this port.

Protect: Port Security is administratively enabled in Protect mode.

Restrict: Port Security is administratively enabled in Restrict mode.

Shutdown: Port Security is administratively enabled in Shutdown mode.

State

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

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

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

Limit Reached: The Port Security service is administratively enabled and the limit is reached.

Shut down: Indicates that the port is shut down by Port Security. This state can only be shown if violation mode is set to Shutdown.

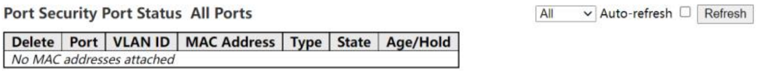
MAC Count (Current, Violating, Limit)

The three columns indicate the number of currently learned MAC addresses (forwarding as well as blocked), the number of violating MAC address (only counting in Restrict mode) 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 Port Security is not administratively enabled on the port, the Violating and Limit columns will show a dash (-).

Click on "Network Security" in the navigation bar > "Port Security" > "Port" > "Status", then click on the port number. The page displays as follows:

This page shows the MAC addresses secured by the Port Security module. Port Security may be configured both administratively and indirectly through other software modules - the so-called 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.



Port Security Port Status All Ports

Delete	Port	VLAN ID	MAC Address	Type	State	Age/Hold
No MAC addresses attached						

Notice that if you have added Static or Sticky MAC addresses, they will show up on this page only if Port Security is enabled on the interface to which they pertain.

Port Security Port Status All Ports

Delete

Click to remove this particular MAC addresses from MAC address table. The button is only clickable if the entry type is Dynamic. Use the "Network Security→Port Security→MAC Addresses" page to remove Static and Sticky entries.

Port

If all ports are shown (can be selected through the drop-down box on the top right), this one shows the port to which the MAC address is bound.

VLAN ID & MAC Address

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

Type

Indicates the type of entry. Takes one of three values:

Dynamic: The entry is learned through learn frames coming to the Port Security module while the port in question is not in Sticky mode.

Static: The entry is entered by the end-user through management. Entry is not subject to aging.

Sticky: When the port is in Sticky mode, all entries that would otherwise have been learned as dynamic are learned as Sticky.

Sticky entries are part of the running-config and can therefore be saved to startup-config. An important aspect of Sticky MAC addresses is that they survive link changes (in contrast to Dynamic, which will have to be learned again). They also survive reboots if running-config is saved to startup-config.

State

Indicates whether the corresponding MAC address is violating (administrative user has configured the interface in "Restrict" mode and the MAC address is blocked), blocked, or forwarding.

Age/Hold

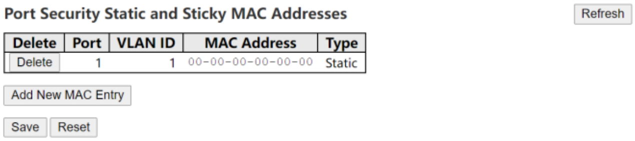
If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this 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 address table. Otherwise a new aging period will begin.

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

4.1.2. MAC Addresses

[Network Security > Port Security > MAC Addresses]

On this page, you can add and delete Static and Sticky MAC addresses managed by Port Security.



Port Security Static and Sticky MAC Addresses

Delete	Port	VLAN ID	MAC Address	Type
Delete	1	1	00-00-00-00-00-00	Static

Port Security Static and Sticky MAC Addresses

Port security defines three types of MAC addresses, of which Static and Sticky can be added and removed on this page:

- **Dynamic**: A MAC address learned through learn frames coming to the Port Security module while the interface in question is not in Sticky mode. Dynamic entries disappear if it ages out or if the interface link goes down.
- **Static**: A MAC address added by end-user through management. Static MAC addresses are not subject to aging and will be added to the MAC address table once Port Security gets enabled on the interface.

Static entries are part of the running-config and will survive interface link state changes and reboots if saved to startup-config. Static entries can be added to the running-config at any time whether or not Port Security is enabled.

- **Sticky**: When the interface is in Sticky mode, all entries that would otherwise have been learned as dynamic are learned as Sticky.

Like Static entries, Sticky entries are part of the running-config and will survive interface link state changes and reboots if saved to the startup-config.

When an interface is configured in sticky mode, administrators can add it to the running configuration at any time, regardless of whether port security is enabled on the interface. If the interface exits sticky mode, the sticky entries will also disappear.

Click on "Add New MAC Entry" on this page to add a new row to the table. This new row allows for adding a Static or Sticky MAC address to a particular interface. Once satisfied, click the Save-button to save the changes to running-config.

Notice that Sticky entries are normally added automatically through learning on the interface.

Delete

Press this button to remove the entry from the MAC address table (if present) and the running-config.

Notice that dynamic entries may be removed all-together on an interface through "Network Security→Port Security→Port" and one-by-one through "Status".

Port

The port number to which this MAC address is bound.

VLAN ID

The VLAN ID in question.

MAC Address

The MAC address in question.

Type

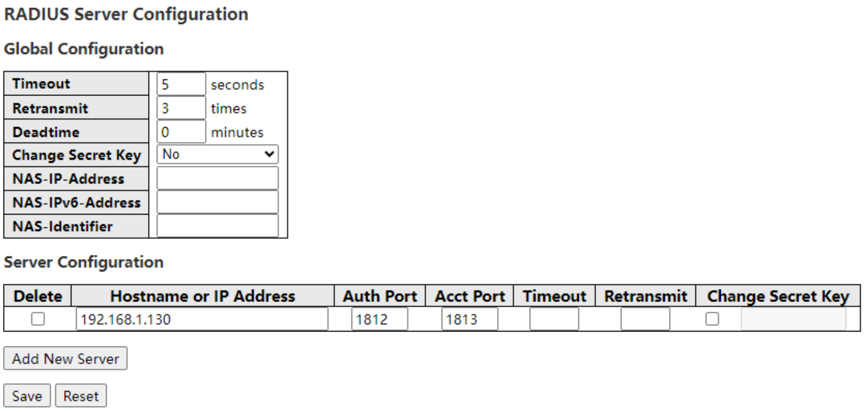
Indicates the type of entry and may be either Static or Sticky (see description above).

4.2. RADIUS

[Network Security > RADIUS]

[Configuration]

This page allows you to configure up to 5 RADIUS servers.



RADIUS Server Configuration

Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Change Secret Key	No	
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

Server Configuration

Delete	Hostname or IP Address	Auth Port	Acct Port	Timeout	Retransmit	Change Secret Key
☐	192.168.1.130	1812	1813			☐

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 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

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

Change Secret Key

Specify to change the secret key or not. When "Yes" is selected for the option, you can change the secret key - up to 63 characters long - shared between the RADIUS server and the switch.

NAS-IP-Address

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

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

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. Click on "Add New Server" on this page 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. The "Delete" button can be used to undo the addition of the new server.

Delete

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

Hostname

The IPv4/IPv6 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

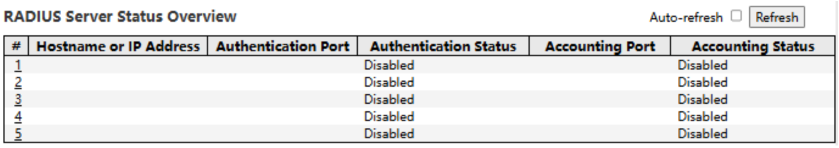
This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.

Change Secret Key

Specify to change the secret key or not. When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key.

[Status]

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



RADIUS Server Status Overview

#	Hostname or 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 Status Overview

#

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

Hostname or IP Address

The IP address of this server.

Authentication Port

UDP port number for authentication.

Authentication Status

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

Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Accounting Port

UDP port number for accounting.

Accounting Status

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

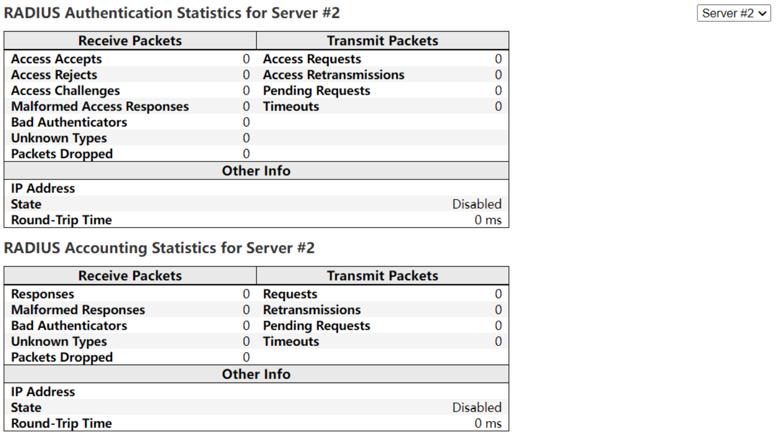
Disabled: The server is disabled.

Not Ready: The server is enabled, but IP communication is not yet up and running.

Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Click on # to jump to the hidden interface, This page provides detailed statistics for a particular RADIUS server.



RADIUS Authentication Statistics for Server #2

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		

Other Info	
IP Address	
State	Disabled
Round-Trip Time	0 ms

RADIUS Accounting Statistics for Server #2

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		

Other Info	
IP Address	
State	Disabled
Round-Trip Time	0 ms

RADIUS Authentication Statistics for Server #

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.

Receive Packets

RADIUS authentication server packet counter. There are seven receive counters.

Access Accepts: The number of RADIUS Access-Accept packets (valid or invalid) received from the server.

Access Rejects: The number of RADIUS Access-Reject packets (valid or invalid) received from the server.

Access Challenges: The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.

Malformed Access Responses: The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.

Bad Authenticators: The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.

Unknown Types: The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.

Packets Dropped: The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.

Transmit Packets

RADIUS authentication server packet counter. There are four transmit counters.

Access Requests: The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.

Access Retransmissions: The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.

Pending Requests: The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.

Timeouts: The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Other Info

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

IP Address: IP address and UDP port for the authentication server in question.

State: Shows the state of the server. It takes one of the following values:

- **Disabled**: The selected server is disabled.

- **Not Ready**: The server is enabled, but IP communication is not yet up and running.

- **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts.

- **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Round-Trip Time: The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

RADIUS Accounting Statistics for Server #

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.

Receive Packets

RADIUS accounting server packet counter. There are five receive counters.

Responses: The number of RADIUS packets (valid or invalid) received from the server.

Malformed Responses: The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.

Bad Authenticators: The number of RADIUS packets containing invalid authenticators received from the server.

Unknown Types: The number of RADIUS packets of unknown types that were received from the server on the accounting port.

Packets Dropped: The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.

Transmit Packets

RADIUS accounting server packet counter. There are four transmit counters.

Requests: The number of RADIUS packets sent to the server. This does not include retransmissions.

Retransmissions: The number of RADIUS packets retransmitted to the RADIUS accounting server.

Pending Requests: The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.

Timeouts: The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Other Info

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

IP Address: IP address and UDP port for the accounting server in question.

State: Shows the state of the server. It takes one of the following values:

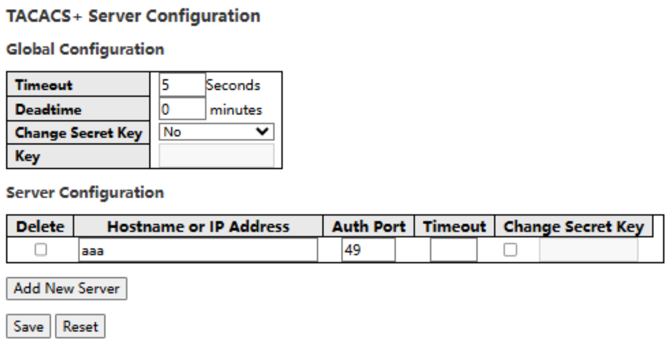
- **Disabled**: The selected server is disabled.
- **Not Ready**: The server is enabled, but IP communication is not yet up and running.
- **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.
- **Dead (X seconds left)**: Accounting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

Round-Trip Time: The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

4.3. TACACS+

[Network Security > TACACS+]

This page allows you to configure up to 5 TACACS+ servers.



TACACS+ Server Configuration

Global Configuration

Timeout	5 Seconds
Deadtime	0 minutes
Change Secret Key	No
Key	

Server Configuration

Delete	Hostname or IP Address	Auth Port	Timeout	Change Secret Key
□	aaa	49		□

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 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.

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

Change Secret Key

Specify to change the secret key or not. When "Yes" is selected for the option, you can change the secret key - up to 63 characters long - shared between the TACACS+ server and the switch.

Key

The aggregation key assigned to this port. Only ports sharing identical keys can join the same aggregation group.

Server Configuration

The table has one row for each TACACS+ server and a number of columns. Click on "Add New Server" on this page 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.

Delete

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

Hostname

The IPv4/IPv6 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.

Change Secret Key

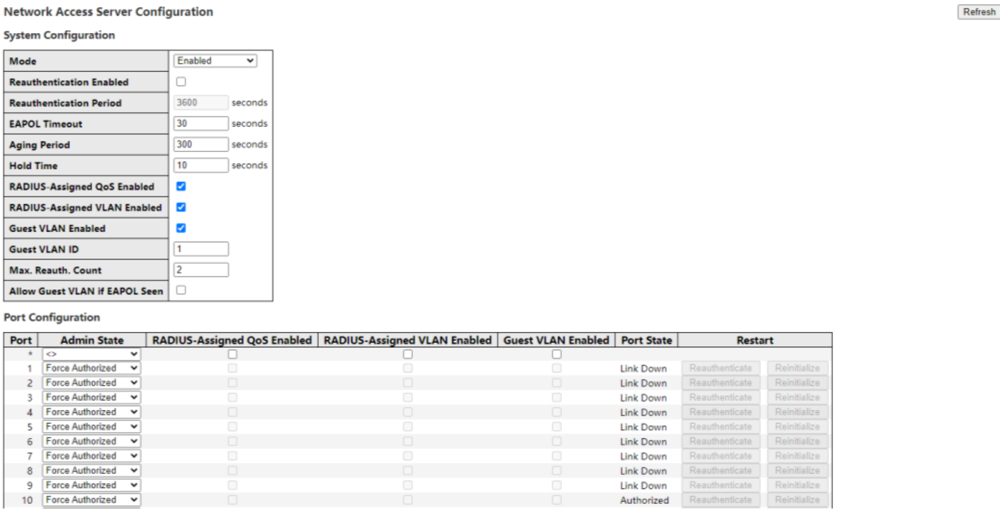
Specify to change the secret key or not. When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key.

4.4. NAS

[Network Security > NAS]

[Configuration]

On this page, you can configure the IEEE 802.1X and MAC-based authentication system and port settings.



Network Access Server Configuration

System Configuration

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

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<>	☐	☐	☐			
1	Force Authorized	☐	☐	☐	Link Down	Reauthenticate	Reinitialize
2	Force Authorized	☐	☐	☐	Link Down	Reauthenticate	Reinitialize
3	Force Authorized	☐	☐	☐	Link Down	Reauthenticate	Reinitialize
4	Force Authorized	☐	☐	☐	Link Down	Reauthenticate	Reinitialize
5	Force Authorized	☐	☐	☐	Link Down	Reauthenticate	Reinitialize
6	Force Authorized	☐	☐	☐	Link Down	Reauthenticate	Reinitialize
7	Force Authorized	☐	☐	☐	Link Down	Reauthenticate	Reinitialize
8	Force Authorized	☐	☐	☐	Link Down	Reauthenticate	Reinitialize
9	Force Authorized	☐	☐	☐	Link Down	Reauthenticate	Reinitialize
10	Force Authorized	☐	☐	☐	Authorized	Reauthenticate	Reinitialize

Network Access Server Configuration

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 "Network Security→RADIUS" 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 "Networks Security→RADIUS" 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

Port

The port number to 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.

Single 802.1X

In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach, use the Single 802.1X variant.

Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.

Multi 802.1X

Multi 802.1X is - like Single 802.1X - not an IEEE standard, but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.

In Multi 802.1X it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.
The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.

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.

RADIUS-Assigned QoS Enabled

When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).
This option is only available for single-client modes, i.e.

- Port-based 802.1X
- Single 802.1X

RADIUS attributes used in identifying a QoS Class:

The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet.

Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule:

- All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].

RADIUS-Assigned VLAN Enabled

When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID.

If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned).

This option is only available for single-client modes, i.e.

- Port-based 802.1X

- Single 802.1X

For trouble-shooting VLAN assignments, use the "Switching→VLAN→Status→Membership and Ports" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

RADIUS attributes used in identifying a VLAN ID:

RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used:

- The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet.

- The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag):

- Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6).

- Value of Tunnel-Type must be set to "VLAN" (ordinal 13).

- Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].

Guest VLAN Enabled

When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below.

This option is only available for EAPOL-based modes, i.e.

- Port-based 802.1X

- Single 802.1X

- Multi 802.1X

For trouble-shooting VLAN assignments, use the "Switching→VLAN→Status→Membership and Ports" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration.

Guest VLAN Operation:

When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout.

Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN.

While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.

Port State

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

Globally Disabled: NAS is globally disabled.

Link Down: NAS is globally enabled, but there is no link on the port.

Authorized: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.

Unauthorized: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.

X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.

Restart

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

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

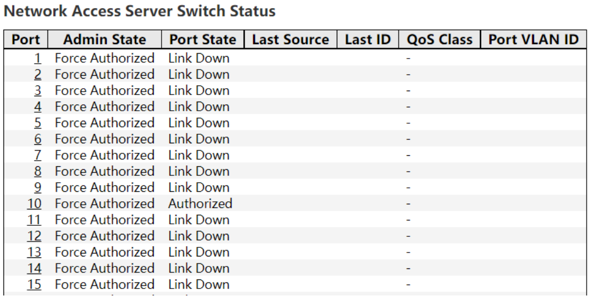
Reauthenticate: Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.

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

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

[Status]

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



Network Access Server Switch Status

Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Link Down			-	
2	Force Authorized	Link Down			-	
3	Force Authorized	Link Down			-	
4	Force Authorized	Link Down			-	
5	Force Authorized	Link Down			-	
6	Force Authorized	Link Down			-	
7	Force Authorized	Link Down			-	
8	Force Authorized	Link Down			-	
9	Force Authorized	Link Down			-	
10	Force Authorized	Authorized			-	
11	Force Authorized	Link Down			-	
12	Force Authorized	Link Down			-	
13	Force Authorized	Link Down			-	
14	Force Authorized	Link Down			-	
15	Force Authorized	Link Down			-	

Network Access Server Switch Status

Port

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

Admin State

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

Port State

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

Last Source

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

Last ID

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

QoS Class

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

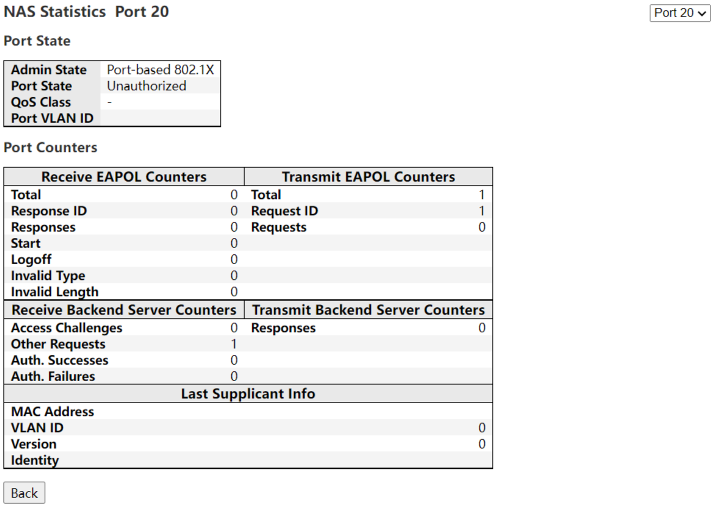
Port VLAN ID

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

If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID.

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Click on port as shown in the following figure. 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.



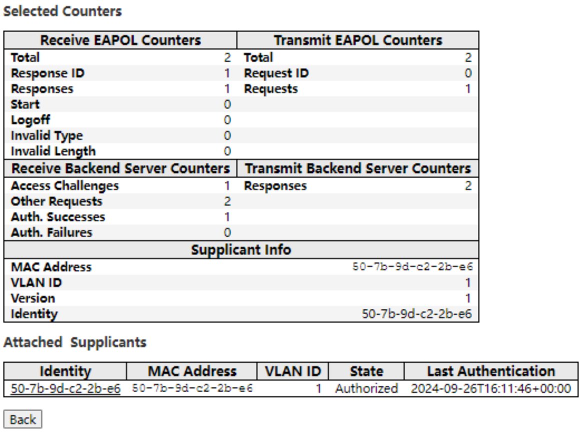
NAS Statistics Port 20

Port State

Admin State	Port-based 802.1X
Port State	Unauthorized
QoS Class	-
Port VLAN ID	

Port Counters

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	**Total**	1
Response ID	0	**Request ID**	1
Responses	0	**Requests**	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		
Receive Backend Server Counters		**Transmit Backend Server Counters**	
Access Challenges	0	**Responses**	0
Other Requests	1		
Auth. Successes	0		
Auth. Failures	0		
Last Supplicant Info			
MAC Address			
VLAN ID			0
Version			0
Identity			



Selected Counters

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	2	**Total**	2
Response ID	1	**Request ID**	0
Responses	1	**Requests**	1
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		
Receive Backend Server Counters		**Transmit Backend Server Counters**	
Access Challenges	1	**Responses**	2
Other Requests	2		
Auth. Successes	1		
Auth. Failures	0		
Supplicant Info			
MAC Address			50-7b-9d-c2-2b-e6
VLAN ID			1
Version			1
Identity			50-7b-9d-c2-2b-e6

Attached Supplicants

Identity	MAC Address	VLAN ID	State	Last Authentication
50-7b-9d-c2-2b-e6	50-7b-9d-c2-2b-e6	1	Authorized	2024-09-26T16:11:46+00:00

Use the port select box to select which port details to be displayed.

Port State

Admin State

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

Port State

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

QoS Class

The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.

Port VLAN ID

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

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

If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Port Counters

Receive EAPOL Counters

These supplicant frame counters are available for the following administrative states:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

EAPOL Counters Description:

Total: The number of valid EAPOL frames of any type that have been received by the switch.

Response ID: The number of valid EAPOL Response Identity frames that have been received by the switch.

Responses: The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.

Start: The number of EAPOL Start frames that have been received by the switch.

Logoff: The number of valid EAPOL Logoff frames that have been received by the switch.

Invalid Type: The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.

Invalid Length: The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.

Transmit EAPOL Counters

These supplicant frame counters are available for the following administrative states:

- Force Authorized
- Force Unauthorized
- Port-based 802.1X
- Single 802.1X
- Multi 802.1X

EAPOL Counters Description:

Total: The number of EAPOL frames of any type that have been transmitted by the switch.

Request ID: The number of EAPOL Request Identity frames that have been transmitted by the switch.

Requests: The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

Receive Backend Server Counters

These backend (RADIUS) frame counters are available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth.

Backend Server Counters Description:

Access Challenges:

802.1X-based:

Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch.

MAC-based:

Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).

Other Requests:

802.1X-based:

Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method.

MAC-based:

Not applicable.

Auth. Successes:

802.1X- and MAC-based:

Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.

Auth. Failures:

802.1X- and MAC-based:

Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.

Transmit Backend Server Counters

These supplicant frame counters are available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth

Backend Server Counters Description:

Responses: 802.1X-based:

Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted.

MAC-based:

Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

Last Supplicant/Client Info

Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:

- Port-based 802.1X
- Single 802.1X
- Multi 802.1X
- MAC-based Auth

Last Supplicant/Client Info Description:

MAC Address: The MAC address of the last supplicant/client.

VLAN ID: The VLAN ID on which the last frame from the last supplicant/client was received.

Version:

802.1X-based:

The protocol version number carried in the most recently received EAPOL frame.

MAC-based: Not applicable.

Identity:

802.1X-based:

The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame.

MAC-based: Not applicable.

Selected Counters

Selected Counters

The Selected Counters table is visible when the port is in one of the following administrative states:

- Multi 802.1X
- MAC-based Auth

The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.

Attached Supplicants/Clients

Identity

Shows the identity of the supplicant, as received in the Response Identity EAPOL frame.

Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached.

This column is not available for MAC-based Auth.

MAC Address

For Multi 802.1X, this column holds the MAC address of the attached supplicant.

For MAC-based Auth., this column holds the MAC address of the attached client.

Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.

VLAN ID

This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.

State

The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.

Last Authentication

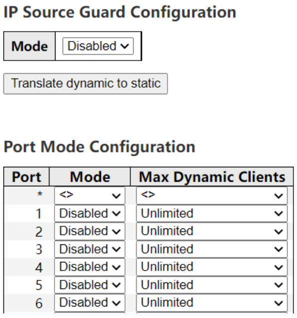
Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

4.5. IP Source Guard

4.5.1. Configuration

[Network Security > IP Source Guard > Configuration]

On this page, you can configure IP Source Guard related configuration. Click on "Translate dynamic to Static" on this page to translate all dynamic entries to Static entries.



IP Source Guard Configuration

Mode	Disabled

Translate dynamic to static

Port Mode Configuration

Port	Mode	Max Dynamic Clients
*	<>	<>
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited

IP Source Guard Configuration

Mode

Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

Port Mode Configuration

Mode

Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.

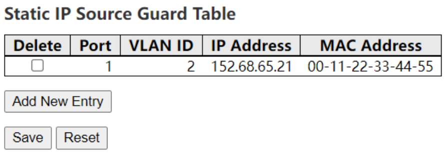
Max Dynamic Clients

Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in Static entries on the specific port.

4.5.2. Static Table

[Network Security > IP Source Guard > Static Table]

On this page, you can configure the Static IP Source Guard rules. The maximum number of rules is 112 on the switch. Click on "Add New Entry" on this page to add a new entry to the Static IP Source Guard table.



Static IP Source Guard Table

Delete	Port	VLAN ID	IP Address	MAC Address
□	1	2	152.68.65.21	00-11-22-33-44-55

Static IP Source Guard Table

Delete

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

Port

The logical port for the settings.

VLAN ID

The vlan id for the settings.

IP Address

Allowed Source IP address.

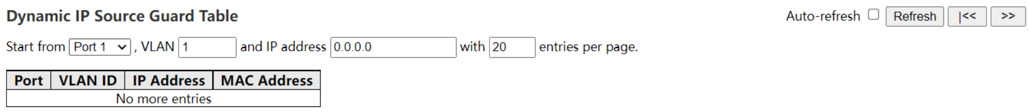
MAC address

Allowed Source MAC address.

4.5.3. Dynamic Table

[Network Security > IP Source Guard > Dynamic Table]

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.



Dynamic IP Source Guard Table

Auto-refresh □ Refresh |<< >>

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

Port	VLAN ID	IP Address	MAC Address
No more entries			

Navigating the IP Source Guard Table

Each page shows up to 99 entries from the Dynamic IP Source Guard 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 IP Source Guard Table.

The "Start from port address", "VLAN" and "IP address" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next Dynamic IP Source Guard 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.

Dynamic IP Source Guard Table

Port

Switch Port Number for which the entries are displayed.

VLAN ID

VLAN-ID in which the IP traffic is permitted.

IP Address

User IP address of the entry.

MAC Address

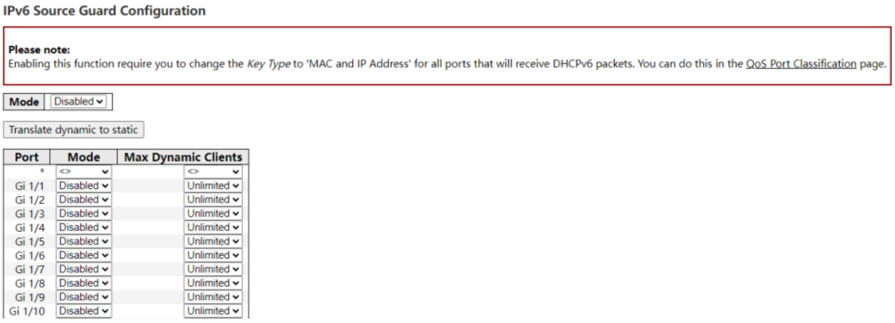
Source MAC address.

4.6. IPv6 Source Guard

4.6.1. Configuration

[Network Security > IPv6 Source Guard > Configuration]

On this page, you can configure IPv6 Source Guard related configuration. Click on "Translate dynamic to Static" on this page to translate all dynamic entries to Static entries."**Please note**" that this entry will only be displayed on certain devices. Refer to the specific device documentation for details.



IPv6 Source Guard Configuration

Please note:
Enabling this function require you to change the *Key Type* to 'MAC and IP Address' for all ports that will receive DHCPv6 packets. You can do this in the QoS Port Classification page.

Mode Disabled

Port	Mode	Max Dynamic Clients
*	<>	<>
Gi 1/1	Disabled	Unlimited
Gi 1/2	Disabled	Unlimited
Gi 1/3	Disabled	Unlimited
Gi 1/4	Disabled	Unlimited
Gi 1/5	Disabled	Unlimited
Gi 1/6	Disabled	Unlimited
Gi 1/7	Disabled	Unlimited
Gi 1/8	Disabled	Unlimited
Gi 1/9	Disabled	Unlimited
Gi 1/10	Disabled	Unlimited

IPv6 Source Guard Configuration

IPv6 Source Guard Mode

Enable or disable the IPv6 Source Guard globally.

Port Mode

The table shows all ports on the device. There IPv6 Source Guard can be enabled/disabled on individual ports. Only when both Global Mode and Port Mode on a given port are enabled, IPv6 Source Guard is enabled on this given port.

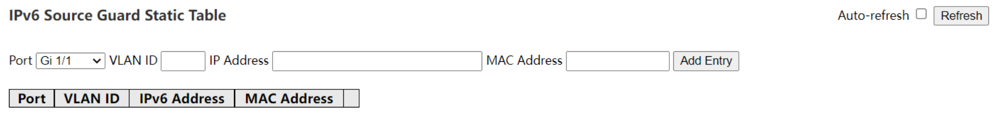
Max Dynamic Clients

Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, only IPv6 packets that are matched in Static entries on the specific port are forwarded.

4.6.2. Static Table

[Network Security > IPv6 Source Guard > Static Table]

On this page, you can configure the Static IPv6 Source Guard entries. The maximum number of entries is 112 on the switch. Click on "Add Entry" on this page to add a new entry to the Static IPv6 Source Guard table.



IPv6 Source Guard Static Table

Auto-refresh □ Refresh

Port Gi 1/1 VLAN ID IP Address MAC Address Add Entry

Port	VLAN ID	IPv6 Address	MAC Address	

Static IPv6 Source Guard Table

Port

The logical port the entry is bound to.

VLAN ID

The VLAN Id for the entry. If no VLAN Id is associated with the entry, this field shows 0.

IPv6 Address

Allowed Source IPv6 address.

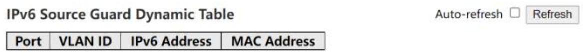
MAC address

Allowed Source MAC address.

4.6.3. Dynamic Table

[Network Security > IPv6 Source Guard > Dynamic Table]

Entries in the Dynamic IPv6 Source Guard Table are shown on this page.



IPv6 Source Guard Dynamic Table

Auto-refresh □ Refresh

Port	VLAN ID	IPv6 Address	MAC Address

Navigating the IPv6 Source Guard Table

All dynamic entries are shown in the table which can be scrolled up and down when the number of entries exeeds the space allotted for the table.

IPv6 Source Guard Dynamic Table

Port

Switch Port Number to which the entries are bound.

VLAN ID

VLAN-ID in which the IP traffic is permitted. If no VLAN-ID is associated with the entry, this field shows 0.

IPv6 Address

Source IPv6 address of the entry.

MAC Address

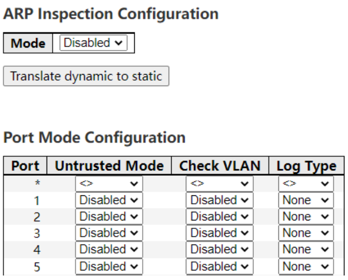
Source MAC address.

4.7. ARP Inspection

4.7.1. Port Configuration

[Network Security > ARP Inspection > Port Configuration]

On this page, you can configure ARP Inspection related configuration. Click on "Translate dynamic to Static" on this page to translate all dynamic entries to Static entries.



ARP Inspection Configuration

Mode	Disabled

Port Mode Configuration

Port	Untrusted Mode	Check VLAN	Log Type
*	<>	<>	<>
1	Disabled	Disabled	None
2	Disabled	Disabled	None
3	Disabled	Disabled	None
4	Disabled	Disabled	None
5	Disabled	Disabled	None

ARP Inspection Configuration

Mode

Enable the Global ARP Inspection or disable the Global ARP Inspection.

Port Mode Configuration

Untrusted Mode

Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:

Enabled: Enable ARP Inspection operation.

Disabled: Disable ARP Inspection operation.

Check VLAN

If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are:

Enabled: Enable check VLAN operation.

Disabled: Disable check VLAN operation.

Log Type

Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types are:

None: Log nothing.

Deny: Log denied entries.

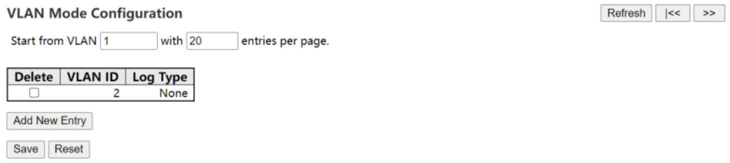
Permit: Log permitted entries.

ALL: Log all entries.

4.7.2. VLAN Configuration

[Network Security > ARP Inspection > VLAN Configuration]

On this page, you can configure ARP Inspection related configuration. Click on "Add New Entry" on this page to add a new VLAN to the ARP Inspection VLAN table.



VLAN Mode Configuration

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Log Type
□	2	None

VLAN Mode Configuration

Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next VLAN Table match. The **">>"** will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. Use the **"|<<"** button to start over.

VLAN Mode Configuration

VLAN ID

Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page.

Log Type

The log type also can be configured on per VLAN setting.

Possible types are:

None: Log nothing.

Deny: Log denied entries.

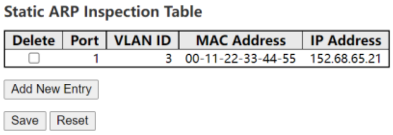
Permit: Log permitted entries.

ALL: Log all entries.

4.7.3. Static Table

[Network Security > ARP Inspection > Static Table]

On this page, you can configure the Static ARP Inspection rules. The maximum number of rules is 256 on the switch. Click on "Add New Entry" on this page to add a new entry to the Static ARP Inspection table.



Static ARP Inspection Table

Delete	Port	VLAN ID	MAC Address	IP Address
□	1	3	00-11-22-33-44-55	152.68.65.21

Static ARP Inspection Table

Delete

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

Port

The logical port for the settings.

VLAN ID

The VLAN ID for the settings.

MAC Address

Allowed Source MAC address in ARP request packets.

IP Address

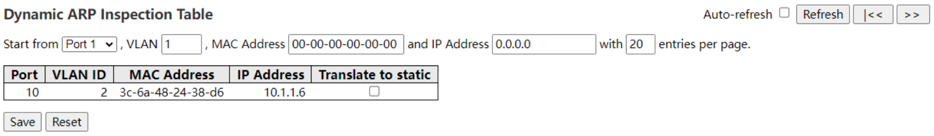
Allowed Source IP address in ARP request packets.

4.7.4. Dynamic Table

[Network Security > ARP Inspection > Dynamic Table]

[Configuration]

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learning from DHCP Snooping.



Dynamic ARP Inspection Table

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

Port	VLAN ID	MAC Address	IP Address	Translate to static
10	2	3c-6a-48-24-38-d6	10.1.1.6	□

Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection 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 ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next Dynamic ARP Inspection 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.

Dynamic ARP Inspection Table

Port

Switch Port Number for which the entries are displayed.

VLAN ID

VLAN-ID in which the ARP traffic is permitted.

MAC Address

User MAC address of the entry.

IP Address

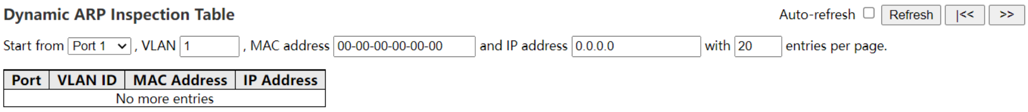
User IP address of the entry.

Translate to Static

Select the checkbox to translate the entry to Static entry.

[Status]

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learning from DHCP Snooping.



Dynamic ARP Inspection Table

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

Port	VLAN ID	MAC Address	IP Address
No more entries			

Navigating the ARP Inspection Table

Each page shows up to 99 entries from the Dynamic ARP Inspection 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 ARP Inspection Table.

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next Dynamic ARP Inspection 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.

Dynamic ARP Inspection Table

Port

Switch Port Number for which the entries are displayed.

VLAN ID

VLAN-ID in which the ARP traffic is permitted.

MAC Address

User MAC address of the entry.

IP Address

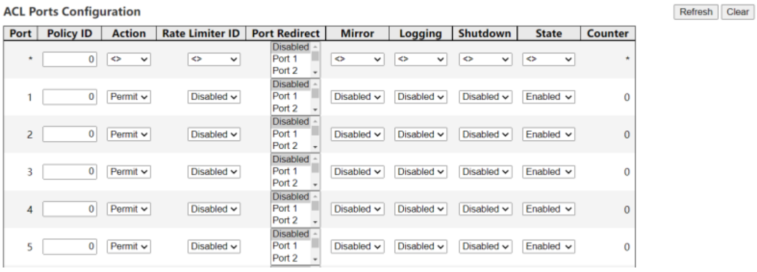
User IP address of the entry.

4.8. ACL

[Network Security > ACL]

[Ports]

On this page, you can configure the ACL parameters (ACE) of each switch port. These parameters will affect frames received on a port when the frame matches a specific ACE. Click on "Clear" on this page to clear the counters.



ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled Port 1 Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled Port 1 Port 2	Disabled	Disabled	Disabled	Enabled	0

ACL Ports Configuration

Port

The physical port for the settings contained in the same row.

Policy ID

Select the policy to be applied to this port. Allowed values range from 0 to 255, and the specific policy ID depends on the product form. 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".

Port Redirect

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

Mirror

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

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

Logging

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

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

Disabled: Frames received on the port are not logged.

The default value is "Disabled".

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

Shutdown

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

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

Disabled: Port shut down is disabled.

The default value is "Disabled".

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

State

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

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

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

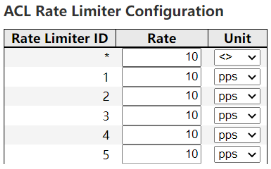
The default value is "Enabled".

Counter

Counts the number of frames that match this ACE.

[Rate Limiters]

On this page, you can configure the rate limiter for the ACL of the switch.



ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	10	<>
1	10	pps
2	10	pps
3	10	pps
4	10	pps
5	10	pps

ACL Rate Limiter Configuration

Rate Limiter ID

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

Rate

When the effective rate is measured in pps, set the rate to a multiple of 10 within the range of <0-5000000>. If the unit is kbps, set the rate to a multiple of 25 within the range of <0-10000000>.

Unit

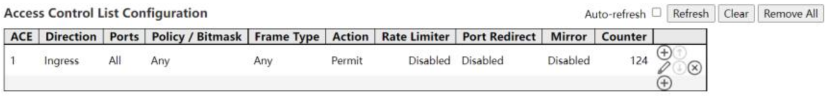
Specify the rate unit. The allowed values are:

pps: packets per second.

kbps: Kbits per second.

[Access Control List]

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 512 on each switch.



Access Control List Configuration

ACE	Direction	Ports	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter	
1	Ingress	All	Any	Any	Permit	Disabled	Disabled	Disabled	124	⊕ ⊗
										⊕

Access Control List Configuration

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.

On this page, click on "Clear" to clear the counters, click on "Remove All" to remove all ACEs.

ACE

Indicates the ACE ID.

Direction

The direction in the Access Control List (ACL) refers to the direction of traffic flow, indicating whether the rule is applied to the traffic entering or leaving the network interface.

Ingress: Applied to traffic entering the network interface.

Egress: Applied to traffic leaving the network interface.

Ports

Indicates the port of the ACE. Possible values are:

All: The ACE will match all port.

Port: The ACE will match a specific port.

Policy/Bitmask

Indicates the policy number and bitmask of the ACE.

Frame Type

Indicates the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

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

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

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

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

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

IPv4/Other: The ACE will match IPv4 frames except for IPv4-ICMP/UDP/TCP.

IPv6: The ACE will match all IPv6 standard frames.

IPv6 - NH:ICMP：The ACE will match IPv6 frames with ICMP protocol.

IPv6 - NH:UDP：The ACE will match IPv6 frames with UDP protocol.

IPv6 - NH:TCP：The ACE will match IPv6 frames with TCP protocol.

IPv6 - NH:Other：The ACE will match IPv6 frames except for IPv6 - NH:ICMP/UDP/TCP.

Action

Indicates the forwarding action of the ACE.

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

Deny: Frames matching the ACE are dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter

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

Port Redirect

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

Mirror

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

Enabled: Frames received on the port are mirrored.

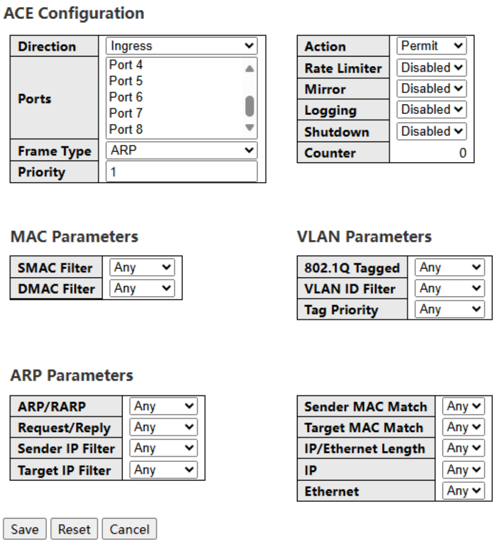
Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

Counter

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

Click on ⊕ and ✎ at the icons bar on this page to add/configure ACE. Open the configuration page, as shown in the following figure:



ACE Configuration

Direction	Ingress
Ports	Port 4 Port 5 Port 6 Port 7 Port 8
Frame Type	ARP
Priority	1

Action	Permit
Rate Limiter	Disabled
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

MAC Parameters

SMAC Filter	Any
DMAC Filter	Any

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

ARP Parameters

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

Sender MAC Match	Any
Target MAC Match	Any
IP/Ethernet Length	Any
IP	Any
Ethernet	Any

On this page, you can add/configures a ACE (Access Control Entry).

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

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

ACE Configuration

Direction

Select the direction for this ACE.

Ingress: Applied to traffic entering the network interface.

Egress: Applied to traffic leaving the network interface.

Ports

Select the port for which this ACE applies.

All: The ACE applies to all port.

Port n: The ACE applies to this port number, where n is the number of the switch port.

Policy Filter

Specify the policy number filter for this ACE.

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

Specific: If you want to filter a specific policy with this ACE, choose this value. Two field for entering an policy value and bitmask appears.

Policy Value

When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 255.

Policy Bitmask

When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0xff. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [policy_value & policy_bitmask]. For example, if the policy value is 3 and the policy bitmask is 0x10(bit 0 is "don't-care" bit), then policy 2 and 3 are applied to this rule.

Frame Type

Select the frame type for this ACE. These frame types are mutually exclusive.

Any: Any frame can match this ACE.

Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal) and the value should not be equal to 0x800(IPv4), 0x806(ARP) or 0x86DD(IPv6).

ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type.

IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type.

IPv6: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.

Priority

Higher-priority ACE will be matched first.'Priority ID' must be an integer value between 0 and 4294967295.

Action

ACE operation.

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

Deny: The frame that hits this ACE is dropped.

Filter: Frames matching the ACE are filtered.

Rate Limiter

Specify the rate limiter in number of base units. The allowed range is 1 to 16. **Disabled** indicates that the rate limiter operation is disabled.

Filter Port

Selectively filter single, multiple, or all ports by setting ACLs to monitor and audit traffic for specific ports.

Port Redirect

Frames that hit the ACE are redirected to the port number specified here. The rate limiter will affect these ports. The allowed range is the same as the switch port number range. **Disabled** indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted.

Mirror

Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port. The allowed values are:

Enabled: Frames received on the port are mirrored.

Disabled: Frames received on the port are not mirrored.

The default value is "Disabled".

Logging

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

Enabled: Frames matching the ACE are stored in the System Log.

Disabled: Frames matching the ACE are not logged.

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 the ACE. The allowed values are:

Enabled: If a frame matches the ACE, the ingress port will be disabled.

Disabled: Port shut down is disabled for the ACE.

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

Counter

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

MAC Parameters

SMAC Filter

(Only displayed when the frame type is Ethernet Type or ARP).
Specify the source MAC filter for this ACE.

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

Specific: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.

SMAC Value

When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.

DMAC Filter

Specify the destination MAC filter for this ACE.

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

MC: Frame must be multicast.

BC: Frame must be broadcast.

UC: Frame must be unicast.

Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.

DMAC Value

When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.

VLAN Parameters

802.1Q Tagged

Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are:

Any: Any value is allowed ("don't-care").

Enabled: Tagged frame only.

Disabled: Untagged frame only.

The default value is "Any".

VLAN ID Filter

Specify the VLAN ID filter for this ACE.

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

Specific: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.

VLAN ID

When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is 1 to 4095. A frame that hits this ACE matches this VLAN ID value.

Tag Priority

Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7 or range 0-1, 2-3, 4-5, 6-7, 0-3 and 4-7. The value Any means that no tag priority is specified (tag priority is "don't-care").

ARP Parameters

The ARP parameters can be configured when Frame Type "ARP" is selected.

ARP/RARP

Specify the available ARP/RARP opcode (OP) flag for this ACE.

Any: No ARP/RARP OP flag is specified (OP is "don't-care").

ARP: Frame must have ARP opcode set to ARP.

RARP: Frame must have RARP opcode set to RARP.

Other: Frame has unknown ARP/RARP Opcode flag.

Request/Reply

Specify the available Request/Reply opcode (OP) flag for this ACE.

Any: No Request/Reply OP flag is specified (OP is "don't-care").

Request: Frame must have ARP Request or RARP Request OP flag set.

Reply: Frame must have ARP Reply or RARP Reply OP flag.

Sender IP Filter

Specify the sender IP filter for this ACE.

Any: No sender IP filter is specified. (Sender IP filter is "don't-care").

Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears.

Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.

Sender IP Address

When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

Sender IP Mask

When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.

Target IP Filter

Specify the target IP filter for this specific ACE.

Any: No target IP filter is specified. (Target IP filter is "don't-care").

Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears.

Network: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.

Target IP Address

When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

Target IP Mask

When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.

Sender MAC Match

Specify whether frames can hit the action according to their sender hardware address field (SHA) settings.

0: ARP frames where SHA is not equal to the SMAC address.

1: ARP frames where SHA is equal to the SMAC address.

Any: Any value is allowed ("don't-care").

Target MAC Match

Specify whether frames can hit the action according to their target hardware address field (THA) settings.

0: RARP frames where THA is not equal to the target MAC address.

1: RARP frames where THA is equal to the target MAC address.

Any: Any value is allowed ("don't-care").

IP/Ethernet Length

Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings.

0: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04).

1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04).

Any: Any value is allowed ("don't-care").

IP

Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings.

0: ARP/RARP frames where the HRD is not equal to Ethernet (1).

1: ARP/RARP frames where the HRD is equal to Ethernet (1).

Any: Any value is allowed ("don't-care").

Ethernet

Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings.

0: ARP/RARP frames where the PRO is not equal to IP (0x800).

1: ARP/RARP frames where the PRO is equal to IP (0x800).

Any: Any value is allowed ("don't-care").

IP Parameters

The IPv4 parameters can be configured when Frame Type "IPv4" is selected.

IP Protocol Filter

Specify the IP protocol filter for this ACE.

Any: No IP protocol filter is specified ("don't-care").

Other: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears.

ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this documents.

UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this documents.

TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this documents.

IP Protocol Value

When the IP protocol value is set to "Other," a specific value can be entered. The allowed range is 0, 2-5, 7-16, 18-255. Frames that hit this ACE will match this IP protocol value.

IP TTL

Specify the Time-to-Live settings for this ACE.

zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.

non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry.

Any: Any value is allowed ("don't-care").

IP Fragment

Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.

No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry.

Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.

Any: Any value is allowed ("don't-care").

IP Option

Specify the options flag setting for this ACE.

No: IPv4 frames where the options flag is set must not be able to match this entry.

Yes: IPv4 frames where the options flag is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

SIP Filter

Specify the source IP filter for this ACE.

Any: No source IP filter is specified (Source IP filter is "don't-care").

Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.

Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.

SIP Address

When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

SIP Mask

When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.

DIP Filter

Specify the destination IP filter for this ACE.

Any: No destination IP filter is specified (Destination IP filter is "don't-care").

Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears.

Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.

DIP Address

When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.

DIP Mask

When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

IPv6 Parameters

The IPv6 parameters can be configured when Frame Type "IPv6" is selected.

Next Header Filter

Specify the IPv6 next header filter for this ACE.

Any: No IPv6 next header filter is specified ("don't-care").

Other: If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears.

ICMP: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this documents.

UDP: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this documents.

TCP: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this documents.

Next Header Value

When the IPv6 Next Header value is set to "Other," a specific value can be entered. The allowed range is 0-5, 7-16, 18-57, 59-255. Frames that hit this ACE will match this IPv6 protocol value.

SIP Filter

Specify the source IPv6 filter for this ACE.

Any: No source IPv6 filter is specified (Source IPv6 filter is "don't-care").

Specific: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.

SIP Address (32 bits)

When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address.

SIP BitMask (32 bits)

When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFE(bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.

Hop Limit

Specify the hop limit settings for this ACE.

zero: IPv6 frames with a hop limit field greater than zero must not be able to match this entry.

non-zero: IPv6 frames with a hop limit field greater than zero must be able to match this entry.

Any: Any value is allowed ("don't-care").

ICMP Parameters

ICMP Type Filter

Specify the ICMP filter for this ACE.

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

Specific: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.

ICMP Type Value

When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP value.

ICMP Code Filter

Specify the ICMP code filter for this ACE.

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

Specific: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.

ICMP Code Value

When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.

TCP/UDP Parameters

Source Port Filter

Specify the TCP/UDP source filter for this ACE.

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

Specific: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears.

Range: If you want to filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.

Source Port No.

When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP source value.

Source Port Range

When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535. The frames hitting this ACE match the range of TCP/UDP source ports.

Dest. Port Filter

Specify the TCP/UDP destination filter for this ACE.

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

Specific: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears.

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

Dest. Port No.

When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP/UDP destination value.

Dest. Port Range

When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535. The frames hitting this ACE match the range of TCP/UDP destination ports.

TCP FIN

Specify the TCP "No more data from sender" (FIN) value for this ACE.

0: TCP frames where the FIN field is set must not be able to match this entry.

1: TCP frames where the FIN field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP SYN

Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.

0: TCP frames where the SYN field is set must not be able to match this entry.

1: TCP frames where the SYN field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP RST

Specify the TCP "Reset the connection" (RST) value for this ACE.

0: TCP frames where the RST field is set must not be able to match this entry.

1: TCP frames where the RST field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP PSH

Specify the TCP "Push Function" (PSH) value for this ACE.

0: TCP frames where the PSH field is set must not be able to match this entry.

1: TCP frames where the PSH field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP ACK

Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.

0: TCP frames where the ACK field is set must not be able to match this entry.

1: TCP frames where the ACK field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

TCP URG

Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.

0: TCP frames where the URG field is set must not be able to match this entry.

1: TCP frames where the URG field is set must be able to match this entry.

Any: Any value is allowed ("don't-care").

Ethernet Type Parameters

The Ethernet Type parameters can be configured when Frame Type "Ethernet Type" is selected.

EtherType Filter

Specify the Ethernet type filter for this ACE.

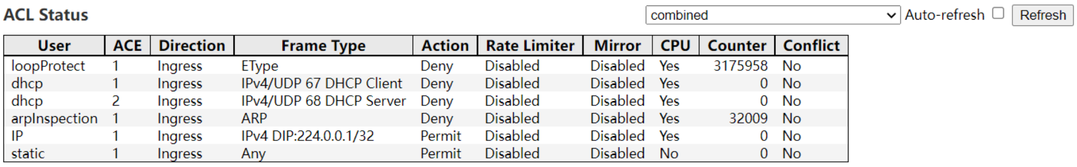
Any: No EtherType filter is specified (EtherType filter status is "don't-care").

Specific: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.

Ethernet Type Value

When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

[ACL Status]



ACL Status

User	ACE	Direction	Frame Type	Action	Rate Limiter	Mirror	CPU	Counter	Conflict
loopProtect	1	Ingress	EType	Deny	Disabled	Disabled	Yes	3175958	No
dhcp	1	Ingress	IPv4/UDP 67 DHCP Client	Deny	Disabled	Disabled	Yes	0	No
dhcp	2	Ingress	IPv4/UDP 68 DHCP Server	Deny	Disabled	Disabled	Yes	0	No
arpInspection	1	Ingress	ARP	Deny	Disabled	Disabled	Yes	32009	No
IP	1	Ingress	IPv4 DIP:224.0.0.1/32	Permit	Disabled	Disabled	Yes	0	No
static	1	Ingress	Any	Permit	Disabled	Disabled	No	0	No

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 512 on each switch.

Filter ACL settings under different protocols using the dropdown menu in the upper right corner.

1. combined
2. Static
3. ipSourceGuard
4. Ipv6SourceGuard
5. IP
6. Connectivity Fault Management
7. Automatic (Linear) Protection Switching
8. Ethernet Ring Protection Switching
9. Media Redundancy Protocol
10. arpInspection
11. upnp
12. ptp
13. dhcp
14. dhcp6Snooping
15. loopProtect
16. linkOAM
17. test
18. conflict

ACL Status

User

Indicates the ACL user.

ACE

Indicates the ACE ID on local switch.

Direction

Indicates the direction for this ACE.

Ingress: Applied to traffic entering the network interface.

Egress: Applied to traffic leaving the network interface.

Frame Type

Indicates the frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.

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

ARP: The ACE will match ARP/RARP frames.

IPv4: The ACE will match all IPv4 frames.

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

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

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

IPv4/Other: The ACE will match IPv4 frames except for IPv4-ICMP/UDP/TCP.

IPv6: The ACE will match all IPv6 standard frames.

IPv6 - NH:ICMP：The ACE will match IPv6 frames with ICMP protocol.

IPv6 - NH:UDP：The ACE will match IPv6 frames with UDP protocol.

IPv6 - NH:TCP：The ACE will match IPv6 frames with TCP protocol.

IPv6 - NH:Other：The ACE will match IPv6 frames except for IPv6 - NH:ICMP/UDP/TCP.

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.

Mirror

Show the mirroring operation of this port. Frames matching the ACE (Access Control Entry) will be mirrored to the target mirroring port, and rate limiting does not affect the frames on the mirroring port. "Enabled" indicates that frames received by this port will be mirrored, while "Disabled" indicates that frames received by this port will not be mirrored.

CPU

Forward packet that matched the specific ACE to CPU.

Counter

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

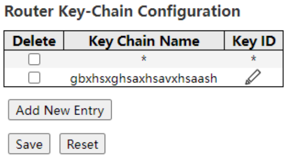
Conflict

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

4.9. Key-Chain

4.9.1. Configuration

[Network Security > Key-Chain > Configuration]



Router Key-Chain Configuration

Delete	Key Chain Name	Key ID
□	*	*
□	gbxhsxghsaxhsavxhsaash	✎

Router Key-Chain Configuration

Delete

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

Key Chain Name

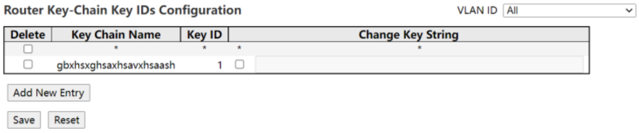
The key chain name.

Key ID

The key ID of key chain.

4.9.2. Key-Chain Key ID

[Network Security > Key-Chain > Key-Chain Key ID]



Router Key-Chain Key IDs Configuration

VLAN ID All

Delete	Key Chain Name	Key ID	Change Key String	
□	*	*	*	*
□	gbxhsxghsaxhsavxhsaash	1	□	

The dropdown menu in the upper right corner can display individual or all configured Key Chains.

Router Key-Chain Key IDs Configuration

Delete

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

Key Chain Name

The key chain name.

Key ID

The key ID of key chain.

Change Key String

Check the box on the page to change the key string.

5. Switching

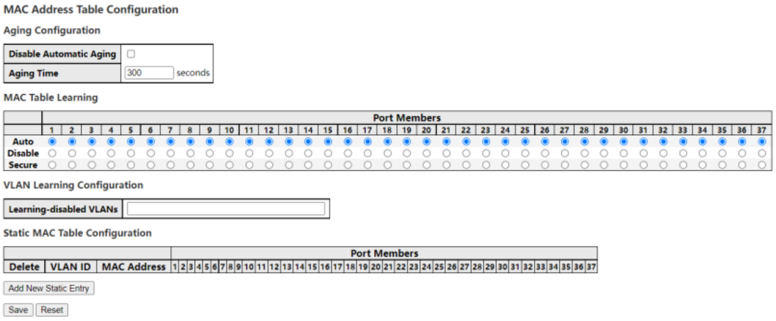
The menu contains the following dialogs:
MAC Table
Multiple Registration Protocol
GVRP
QoS
VLAN
MVR
L2-Multicast
L2-Redundancy

5.1. MAC Table

[Switching > MAC Table]

[Configuration]

Configure the MAC address table on this page. Set the aging configuration for MAC addresses, configure MAC table learning, VLAN learning, and the Static MAC table.



MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	□
Aging Time	300 seconds

MAC Table Learning

	Port Members																																				
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
Auto	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

VLAN Learning Configuration

Learning-disabled VLANs	

Static MAC Table Configuration

			Port Members																																			
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37

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.

VLAN Learning Configuration

Learning-disabled VLANs

This field shows the Learning-disabled VLANs. When a NEW MAC arrives into a learning-disabled VLAN, the MAC won't be learned. By default, the field is empty. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.

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.

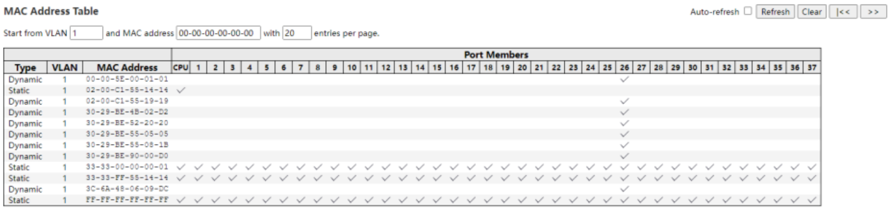
MAC Address

The MAC address of the entry.

Port Members

Check marks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

[Status]



MAC Address Table

Auto-refresh □

Start from VLAN 1 and MAC address 00-00-00-00-00-00 with 20 entries per page.

			Port Members																																					
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
Dynamic	1	00-00-5E-00-01-01																											✓											
Static	1	02-00-C1-55-14-14	✓																																					
Dynamic	1	02-00-C1-55-19-19																											✓											
Dynamic	1	30-29-BE-4B-02-D2																											✓											
Dynamic	1	30-29-BE-52-20-20																											✓											
Dynamic	1	30-29-BE-55-05-05																											✓											
Dynamic	1	30-29-BE-55-08-1B																											✓											
Dynamic	1	30-29-BE-90-00-D0																											✓											
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-55-14-14	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic	1	3C-6A-48-06-09-DC																											✓											
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

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.

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 Refresh 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 Address Table

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

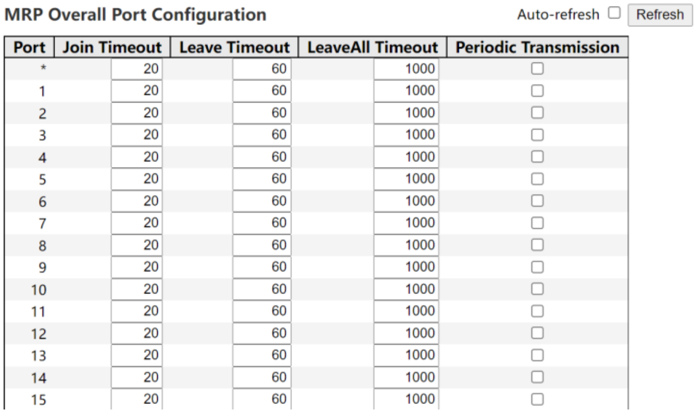
The ports that are members of the egress.

5.2. Multiple Registration Protocol

5.2.1. Ports

[Switching > Multiple Registration Protocol > Ports]

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



MRP Overall Port Configuration

Auto-refresh □ Refresh

Port	Join Timeout	Leave Timeout	LeaveAll Timeout	Periodic Transmission
*	20	60	1000	□
1	20	60	1000	□
2	20	60	1000	□
3	20	60	1000	□
4	20	60	1000	□
5	20	60	1000	□
6	20	60	1000	□
7	20	60	1000	□
8	20	60	1000	□
9	20	60	1000	□
10	20	60	1000	□
11	20	60	1000	□
12	20	60	1000	□
13	20	60	1000	□
14	20	60	1000	□
15	20	60	1000	□

MRP Overall Port Configuration

Port

The port number for which the following configuration applies.

Join Timeout

Controls the timeout of the Join Timer for all MRP Applications on this switch port. This value is restricted to 1-20 centiseconds.

Leave Timeout

Controls the timeout of the Leave Timer for all MRP Applications on this switch port. This value is restricted to 60-600 centiseconds.

LeaveAll Timeout

Controls the timeout of the LeaveAll Timer for all MRP Applications on this switch port. This value is restricted to 1000-5000 centiseconds.

Periodic Transmission

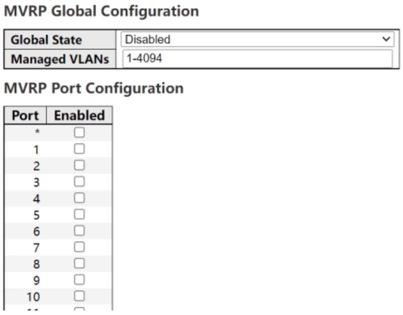
Enable or disable the PeriodicTransmission feature for all MRP Applications on this switch port.

5.2.2. MVRP

[Switching > Multiple Registration Protocol > MVRP]

[Configuration]

This page allows you to configure the MVRP global and per port settings altogether. The page is divided into a global section and a per-port configuration section.



MVRP Global Configuration

Global State	Disabled
Managed VLANs	1-4094

MVRP Port Configuration

Port	Enabled
*	□
1	□
2	□
3	□
4	□
5	□
6	□
7	□
8	□
9	□
10	□

MVRP Global Configuration

Global State

Enable or disable the MVRP protocol globally. This will enable or disable the protocol globally and at the same time on the switch ports that are MVRP enabled.

Managed VLANs

This field shows the managed VLANs, i.e. the VLANs that MVRP will operate upon. By default, only VLANs 1-4094 are managed, i.e. the entire range as defined in IEEE802.1Q-2014 for MVRP. However this range can be limited by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.

The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

MVRP Port Configuration

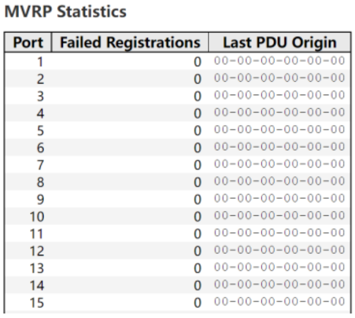
Port

The port number for which the following configuration applies.

Enabled

Enable or disable the MVRP protocol on this switch port. This will enable or disable the protocol on the switch port given that MVRP is also globally enabled.

[Status]



MVRP Statistics

Port	Failed Registrations	Last PDU Origin
1	0	00-00-00-00-00-00
2	0	00-00-00-00-00-00
3	0	00-00-00-00-00-00
4	0	00-00-00-00-00-00
5	0	00-00-00-00-00-00
6	0	00-00-00-00-00-00
7	0	00-00-00-00-00-00
8	0	00-00-00-00-00-00
9	0	00-00-00-00-00-00
10	0	00-00-00-00-00-00
11	0	00-00-00-00-00-00
12	0	00-00-00-00-00-00
13	0	00-00-00-00-00-00
14	0	00-00-00-00-00-00
15	0	00-00-00-00-00-00

MVRP Statistics

Port

The logical port for the statistic contained in the same row.

Failed Registration

The number of failed VLAN registrations on this switch port. Each port implementing the MVRP protocol maintains a count of the number of times it has received a VLAN registration request but has failed to register the VLAN due to lack of space in the Filtering Database.

Last PDU Origin

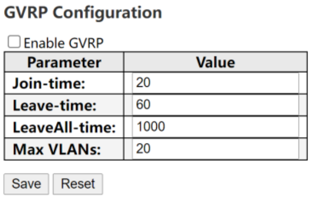
The MAC address of the most recent MVRP PDU received on this switch port. MAC is 00-00-00-00-00-00 if the protocol is not enabled on that switch port, or if the port has not received any MVRP PDUs yet.

5.3. GVRP

5.3.1. Global

[Switching > GVRP > Global]

This page allows you to configure the global GVRP configuration settings that are commonly applied to all GVRP enabled ports.



GVRP Configuration

□ Enable GVRP

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

GVRP Configuration

Enable GVRP globally

The GVRP feature is globally enabled by setting the check mark in the checkbox named Enable GVRP and pressing the Save button.

GVRP protocol timers

Join-time is a value in the range of 1-20cs, i.e. in units of one hundredth of a second. The default value is 20cs.

Leave-time is a value in the range of 60-600cs, i.e. in units of one hundredth of a second. The default is 60cs.

LeaveAll-time is a value in the range of 1000-5000cs, i.e. in units of one hundredth of a second. The default is 1000cs.

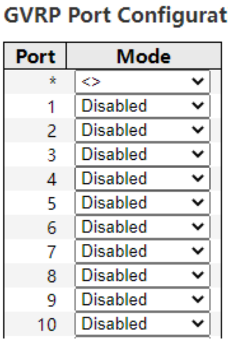
Max number of VLANs

When GVRP is enabled, a maximum number of VLANs supported by GVRP is specified. By default this number is 4094. This number can only be changed when GVRP is turned off.

5.3.2. Port

[Switching > GVRP > Port]

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



GVRP Port Configuration

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled

GVRP Port Configuration

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

Port

The logical port that is to be configured.

Mode

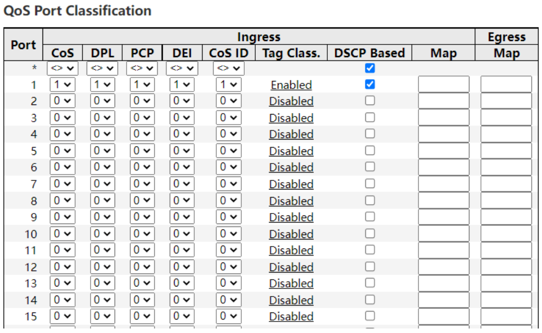
Mode can be either 'Disabled' or 'GVRP enabled'. These values turn the GVRP feature off or on respectively for the port in question.

5.4. QoS

5.4.1. Port Classification

[Switching > QoS > Port Classification]

This page allows you to configure the basic QoS Classification settings for all switch ports.



QoS Port Classification

Port	Ingress								Egress
	CoS	DPL	PCP	DEI	CoS ID	Tag Class.	DSCP Based	Map	Map
*	<>	<>	<>	<>	<>		☑		
1	1	1	1	1	1	Enabled	☑		
2	0	0	0	0	0	Disabled	□		
3	0	0	0	0	0	Disabled	□		
4	0	0	0	0	0	Disabled	□		
5	0	0	0	0	0	Disabled	□		
6	0	0	0	0	0	Disabled	□		
7	0	0	0	0	0	Disabled	□		
8	0	0	0	0	0	Disabled	□		
9	0	0	0	0	0	Disabled	□		
10	0	0	0	0	0	Disabled	□		
11	0	0	0	0	0	Disabled	□		
12	0	0	0	0	0	Disabled	□		
13	0	0	0	0	0	Disabled	□		
14	0	0	0	0	0	Disabled	□		
15	0	0	0	0	0	Disabled	□		

QoS Port Classification

Port

The port number for which the configuration below applies.

CoS

Controls the default CoS value.
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 DPL value.

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.

CoS ID

Controls the default CoS ID value.

Every incoming frame is classified to a CoS ID, which later can be used as basis for rewriting of different parts of the frame.

Tag Class.

Shows the classification mode for tagged frames on this port.

Disabled: Use default CoS and DPL for tagged frames.

Enabled: Use mapped versions of PCP and DEI for tagged frames.

Click on the mode in order to configure the mode and/or mapping.

Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.

DSCP Based

Click to Enable DSCP Based QoS Ingress Port Classification.

WRED Group

Controls the WRED group membership.

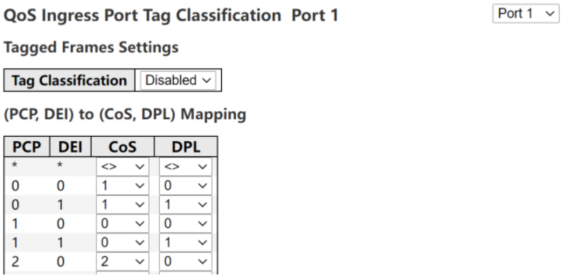
Ingress Map

Controls the Ingress Map selection through the Map ID. The Ingress Map ID ranges from 0 to 255. An empty field indicates no map selection.

Egress Map

Controls the Egress Map selection through the Map ID. The Egress Map ID ranges from 0 to 511. An empty field indicates no map selection.

Click on "Tag Class.", Open the hidden interface.



QoS Ingress Port Tag Classification Port 1

Tagged Frames Settings

Tag Classification	Disabled

(PCP, DEI) to (CoS, DPL) Mapping

PCP	DEI	CoS	DPL
*	*	<>	<>
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0

QoS Ingress Port Tag Classification Port

Tagged Frames Settings

The classification mode for tagged frames are configured on this page.

Tag Classification

Controls the classification mode for tagged frames on this port.

Disabled: Use default CoS and DPL for tagged frames.

Enabled: Use mapped versions of PCP and DEI for tagged frames.

(PCP, DEI) to (CoS, DPL) Mapping

Controls the mapping of the classified (PCP, DEI) to (CoS, DPL) values when Tag Classification is set to **Enabled**.

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.

CoS

Controls the default CoS value.
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 DPL value.

All frames are classified to a Drop Precedence Level.

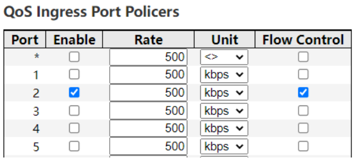
If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL.

The classified DPL can be overruled by a QCL entry.

5.4.2. Port Policing

[Switching > QoS > Port Policing]

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



QoS Ingress Port Policers

Port	Enable	Rate	Unit	Flow Control
*	□	500	<>	□
1	□	500	kbps	□
2	☑	500	kbps	☑
3	□	500	kbps	□
4	□	500	kbps	□
5	□	500	kbps	□

QoS Ingress Port Policers

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 10-13128147 when "Unit" is kbps or fps, and 1-13128 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.

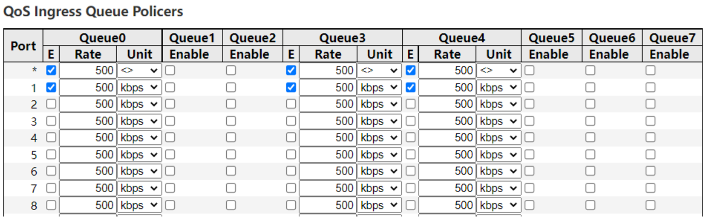
Flow Control

If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

5.4.3. Queue Policing

[Switching > QoS > Queue Policing]

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



QoS Ingress Queue Policers

Port	Queue0			Queue1	Queue2	Queue3			Queue4			Queue5	Queue6	Queue7
	E	Rate	Unit	Enable	Enable	E	Rate	Unit	E	Rate	Unit	Enable	Enable	Enable
*	☑	500	<>	☐	☐	☑	500	<>	☑	500	<>	☐	☐	☐
1	☑	500	kbps	☐	☐	☑	500	kbps	☑	500	kbps	☐	☐	☐
2	☐	500	kbps	☐	☐	☐	500	kbps	☐	500	kbps	☐	☐	☐
3	☐	500	kbps	☐	☐	☐	500	kbps	☐	500	kbps	☐	☐	☐
4	☐	500	kbps	☐	☐	☐	500	kbps	☐	500	kbps	☐	☐	☐
5	☐	500	kbps	☐	☐	☐	500	kbps	☐	500	kbps	☐	☐	☐
6	☐	500	kbps	☐	☐	☐	500	kbps	☐	500	kbps	☐	☐	☐
7	☐	500	kbps	☐	☐	☐	500	kbps	☐	500	kbps	☐	☐	☐
8	☐	500	kbps	☐	☐	☐	500	kbps	☐	500	kbps	☐	☐	☐

QoS Ingress Queue Policers

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 25-13128147 when "Unit" is kbps, and 1-13128 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

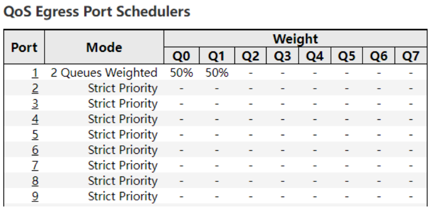
Controls the unit of measure for the queue policer rate as kbps or Mbps.

This field is only shown if at least one of the queue policers are enabled.

5.4.4. Port Scheduler

[Switching > QoS > Port Scheduler]

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



QoS Egress Port Schedulers

Port	Mode	Weight							
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7
1	2 Queues Weighted	50%	50%	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-	-	-

QoS Egress Port Schedulers

Port

The logical port for the settings contained in the same row.

Click on the port number in order to configure the schedulers.

Mode

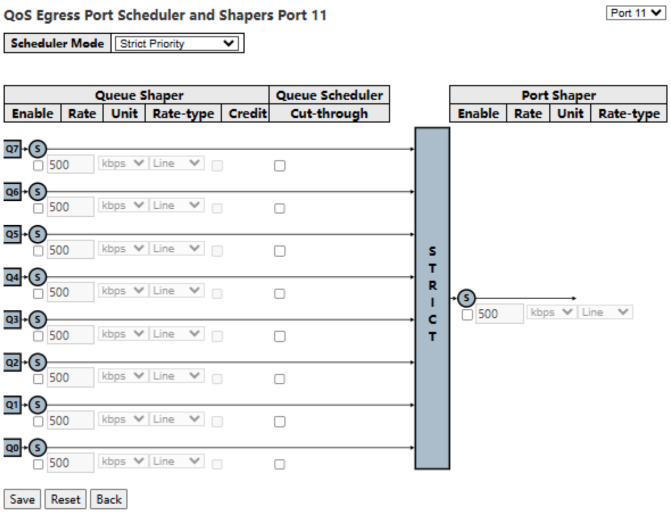
Shows the scheduling mode for this port.

Qn

Shows the weight for this queue and port.

Click on "Port", Open the hidden interface.

This page allows you to configure the Scheduler and Shapers for a specific port.



QoS Egress Port Scheduler and Shapers Port 11

Port 11

Scheduler Mode	Strict Priority

	Queue Shaper					Queue Scheduler
	Enable	Rate	Unit	Rate-type	Credit	Cut-through
Q7	□	500	kbps	Line	□	□
Q6	□	500	kbps	Line	□	□
Q5	□	500	kbps	Line	□	□
Q4	□	500	kbps	Line	□	□
Q3	□	500	kbps	Line	□	□
Q2	□	500	kbps	Line	□	□
Q1	□	500	kbps	Line	□	□
Q0	□	500	kbps	Line	□	□

Port Shaper			
Enable	Rate	Unit	Rate-type
□	500	kbps	Line

QoS Egress Port Scheduler and Shapers Port

Scheduler Mode

Controls how many of the queues are scheduled as strict and how many are scheduled as weighted on this switch port.

Queue Shaper Enable

Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate

Controls the rate for the queue shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper.

Queue Shaper Unit

Controls the unit of measure for the queue shaper rate as kbps or Mbps.

Queue Shaper Rate-type

The rate type of the queue shaper. The allowed values are:

Line: Specify that this shaper operates on line rate.

Data: Specify that this shaper operates on data rate.

Queue Shaper Excess

Control whether the queue is allowed to use excess bandwidth.

Queue Shaper Credit

Controls whether the queue has credit-based shaper enabled.

Queue Scheduler Cut-through

Control whether the queue switching function is enabled.

Queue Scheduler Weight

Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent

Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Cut-through

Controls whether the queue has cut-through enabled.

Port Shaper Enable

Controls whether the port shaper is enabled for this switch port.

Port Shaper Rate

Controls the rate for the port shaper. This value is restricted to 100-13107100 when "Unit" is kbps, and 1-13107 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the port shaper.

Port Shaper Unit

Controls the unit of measure for the port shaper rate as kbps or Mbps.

Port Shaper Rate-type

The rate type of the port shaper. The allowed values are:

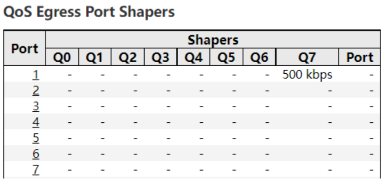
Line: Specify that this shaper operates on line rate.

Data: Specify that this shaper operates on data rate.

5.4.5. Port Shaping

[Switching > QoS > Port Shaping]

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



QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	-	-	-	-	-	-	-	500 kbps	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-

QoS Egress Port Shapers

Port

The logical port for the settings contained in the same row.

Click on the port number in order to configure the shapers.

Qn

Shows "-" for disabled or actual queue shaper rate - e.g. "800 Mbps".

Port

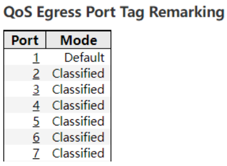
Shows "-" for disabled or actual port shaper rate - e.g. "800 Mbps".

Click on "Port", Opening the hidden interface is the same as in 5.4.4.

5.4.6. Port Tag Remarking

[Switching > QoS > Port Tag Remarking]

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



QoS Egress Port Tag Remarking

Port	Mode
1	Default
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified

QoS Egress Port Tag Remarking

Port

The logical port for the settings contained in the same row.

Click on the port number in order to configure tag remarking.

Mode

Shows the tag remarking mode for this port.

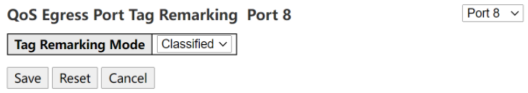
Classified: Use classified PCP/DEI values.

Default: Use default PCP/DEI values.

Mapped: Use mapped versions of CoS and DPL.

Click on "Port", Open the hidden interface.

The QoS Egress Port Tag Remarking for a specific port are configured on this page.



QoS Egress Port Tag Remarking Port 8

Port 8

Tag Remarking Mode	Classified

QoS Egress Port Tag Remarking Port #

Tag Remarking Mode

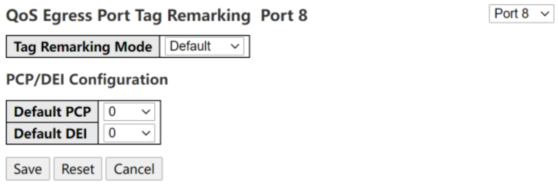
Controls the tag remarking mode for this port.

Classified: Use classified PCP/DEI values.

Default: Use default PCP/DEI values.

Mapped: Use mapped versions of CoS and DPL.

When the selection mode is set to default, the page displays as follows:



QoS Egress Port Tag Remarking Port 8

Port 8

Tag Remarking Mode	Default

PCP/DEI Configuration

Default PCP	0
Default DEI	0

PCP/DEI Configuration

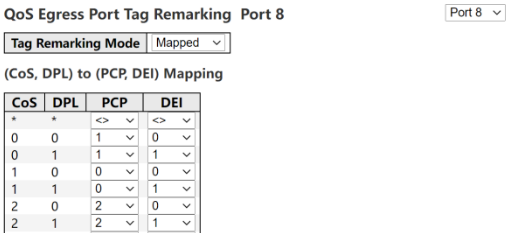
Default PCP

Control the default value of PCP, with a range from 0 to 7.

Default DEI

Control the default value of DEI, with a range from 0 to 1.

When the selection mode is set to mapping, the page displays as follows:



QoS Egress Port Tag Remarking Port 8

Port 8

Tag Remarking Mode	Mapped

(CoS, DPL) to (PCP, DEI) Mapping

CoS	DPL	PCP	DEI
*	*	<>	<>
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1

(CoS, DPL) to (PCP, DEI) Mapping

Controls the mapping of the classified (CoS, DPL) to (PCP, DEI) values when the mode is set to **Mapped**.

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.

CoS

Controls the default CoS value.
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 DPL value.

All frames are classified to a Drop Precedence Level.

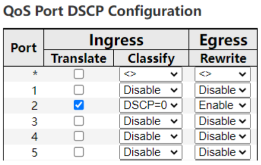
If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL.

The classified DPL can be overruled by a QCL entry.

5.4.7. Port DSCP

[Switching > QoS > Port DSCP]

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



QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	□	<>	<>
1	□	Disable	Disable
2	☑	DSCP=0	Enable
3	□	Disable	Disable
4	□	Disable	Disable
5	□	Disable	Disable

QoS Port DSCP Configuration

Port

The Port column shows the list of ports for which you can configure dscp ingress and egress settings.

Ingress

In Ingress settings you can change ingress translation and classification settings for individual ports.

There are two configuration parameters available in Ingress:

1. **Translate**

To Enable the Ingress Translation click the checkbox.

2. **Classify**

Classification for a port have 4 different values.

- **Disable**: No Ingress DSCP Classification.
- **DSCP=0**: Classify if incoming (or translated if enabled) DSCP is 0.
- **Selected**: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.
- **All**: Classify all DSCP.

Egress

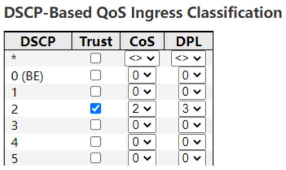
Port Egress Rewriting can be one of:

- **Disable**: No Egress rewrite.
- **Enable**: Rewrite enabled without remapping.
- **Remap**: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value.

5.4.8. DSCP-Based QoS

[Switching > QoS > DSCP-Based QoS]

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



DSCP-Based QoS Ingress Classification

DSCP	Trust	CoS	DPL
*	□	<>	<>
0 (BE)	□	0	0
1	□	0	0
2	☑	2	3
3	□	0	0
4	□	0	0
5	□	0	0

DSCP-Based QoS Ingress Classification

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 CoS and DPL. Frames with untrusted DSCP values are treated as a non-IP frame.

CoS

CoS value can be any of (0-7).

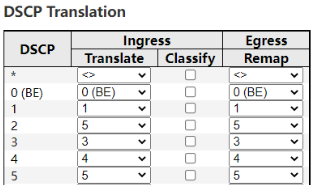
DPL

Drop Precedence Level (0-3).

5.4.9. DSCP Translation

[Switching > QoS > 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.



DSCP Translation

DSCP	Ingress		Egress
	Translate	Classify	Remap
*	<>	□	<>
0 (BE)	0 (BE)	□	0 (BE)
1	1	□	1
2	5	□	5
3	3	□	3
4	4	□	4
5	5	□	5

DSCP Translation

DSCP

Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

Ingress

Ingress side DSCP can be first translated to new DSCP before using the DSCP for CoS and DPL map.

There are two configuration parameters for DSCP Translation:

1. **Translate**

DSCP at Ingress side can be translated to any of (0-63) DSCP values.

2. **Classify**

Click to enable Classification at Ingress side.

Egress

There is the following configurable parameter for Egress side:

1. **Remap**

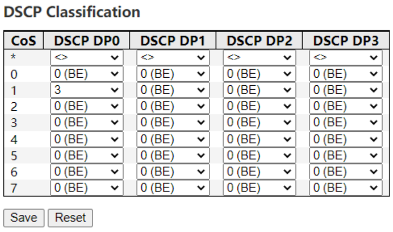
Remap

Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.

5.4.10. DSCP Classification

[Switching > QoS > DSCP Classification]

This page allows you to configure the mapping of CoS and DPL to DSCP value.



DSCP Classification

CoS	DSCP DP0	DSCP DP1	DSCP DP2	DSCP DP3
*	<>	<>	<>	<>
0	0 (BE)	0 (BE)	0 (BE)	0 (BE)
1	3	0 (BE)	0 (BE)	0 (BE)
2	0 (BE)	0 (BE)	0 (BE)	0 (BE)
3	0 (BE)	0 (BE)	0 (BE)	0 (BE)
4	0 (BE)	0 (BE)	0 (BE)	0 (BE)
5	0 (BE)	0 (BE)	0 (BE)	0 (BE)
6	0 (BE)	0 (BE)	0 (BE)	0 (BE)
7	0 (BE)	0 (BE)	0 (BE)	0 (BE)

DSCP Classification

CoS

Actual Class of Service.

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.

DSCP DP2

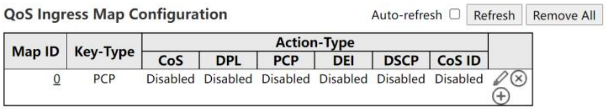
Select the classified DSCP value (0-63) for Drop Precedence Level 2.

DSCP DP3

Select the classified DSCP value (0-63) for Drop Precedence Level 3.

5.4.11. Ingress Map

[Switching > QoS > Ingress Map]



QoS Ingress Map Configuration

Map ID	Key-Type	Action-Type						
		CoS	DPL	PCP	DEI	DSCP	CoS ID	
0	PCP	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	

QoS Ingress Map Configuration

This page shows a table of QoS Ingress Maps which is made up of individual map entries. Each entry has a key and an action. The key indicates which fields of the frame will be mapped to the fields specified by and according to the action. Each Map can hold a number of map rules, or mappings between possible keys and actions. Which of those rules will be applied depends on the selection of (Key-Type, Action-Type). Each row describes a user-defined map. The maximum number of Ingress Maps is 256. Each Ingress Map uses a number of key-entries in a internal key mapping table which have 1004 key-entries available for configuration. The consumption of key-entries by Key Type are listed as table width in the Key-Type table below. A new Ingress Map can only be defined when there are sufficient free key-entries.

Note: This is just an overview of the configured maps. The user can add new ones or edit existing maps using the Add/Edit buttons. Click on the lowest plus sign (empty map entry) to add a new Ingress Map to the table.

Map ID

Indicates the Map (unique) ID. Range is **0** to **255**.

Key-Type

Indicates the Key Type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various keys and this is to make a select set of them. Possible Key types are:

PCP: Use PCP as key for tagged frames and none for the rest. Table width: **1**

PCP - DEI:Use PCP/DEI as key for tagged frames and none for the rest. Table width: **2**

DSCP: Use DSCP as key for IP frames and none for the rest. Table width: **8**

DSCP - PCP - DEI: Use DSCP as key for IP frames, PCP/DEI for tagged frames and none for the rest. Table width: **10**

Action-Type

Indicates the Action Type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various actions available and this is to make a select set of them. Possible Action types are:

CoS: Class of Service.

DPL: Drop Precedence Level.

PCP: Priority Code Point.

DEI: Drop Eligible Indicator.

DSCP: Differentiated Services Code Point.

CoS ID: CoS ID.

QoS Ingress Map Modification Buttons

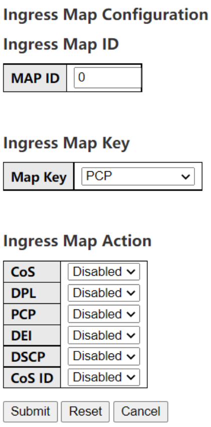
It is possible to modify each map (or add new maps) in the table using the following buttons:

✎: Edits the map.

⊗: Deletes the map.

⊕: Adds a new map in the table. (can also be used to overwrite an existing map, so care on the map id).

Click on "⊕", Open the hidden interface.



Ingress Map Configuration

Ingress Map ID

MAP ID	0

Ingress Map Key

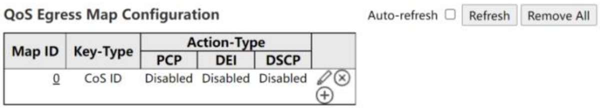
Map Key	PCP

Ingress Map Action

CoS	Disabled
DPL	Disabled
PCP	Disabled
DEI	Disabled
DSCP	Disabled
CoS ID	Disabled

5.4.12. Egress Map

[Switching > QoS > Egress Map]



QoS Egress Map Configuration

Map ID	Key-Type	Action-Type			
		PCP	DEI	DSCP	
0	CoS ID	Disabled	Disabled	Disabled	

QoS Egress Map Configuration

This page shows a table of QoS Egress Maps which is made up of individual map entries. Each entry has a key and an action. The key indicates which fields of the frame will be mapped to the fields specified by and according to the action. Each Map can hold a number of map rules, or mappings between possible keys and actions. Which of those rules will be applied depends on the selection of (Key-Type, Action-Type). Each row describes a user-defined map. The maximum number of Egress Maps is 512. Each Egress Map uses a number of key-entries in a internal key mapping table which have 960 key-entries available. The consumption of key-entries by Key Type are listed as table width in the Key-Type table below. A new Egress Map can only be defined when there are sufficient free key-entries.

Note: This is just an overview of the configured maps. The user can add new ones or edit existing maps using the Add/Edit buttons. Click on the lowest plus sign (empty map entry) to add a new Egress Map to the table.

Map ID

Indicates the Map (unique) ID. Range is **0** to **511**.

Key-Type

Indicates the Key Type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various keys and this is to make a select set of them. Possible Key types are:

CoS ID: Use classified COS ID as key. Table width: **1**

CoS ID - DPL:Use classified COS ID and DPL as key. Table width: **4**

DSCP: Use classified DSCP as key. Table width: **8**

DSCP - DPL: Use classified DSCP and DPL as key. Table width: **32**

Action-Type

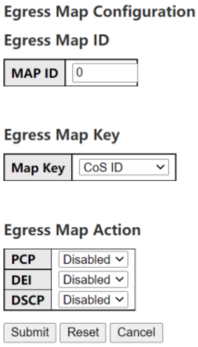
Indicates the Action Type that will be used to filter the map rules when applying the map. As mentioned above, map rules can have various actions available and this is to make a select set of them. Possible Action types are:

PCP: Priority Code Point.

DEI: Drop Eligible Indicator.

DSCP: Differentiated Services Code Point.

Click "⊕" to open the hidden interface as shown in the figure below:



Egress Map Configuration

Egress Map ID

MAP ID	0

Egress Map Key

Map Key	CoS ID

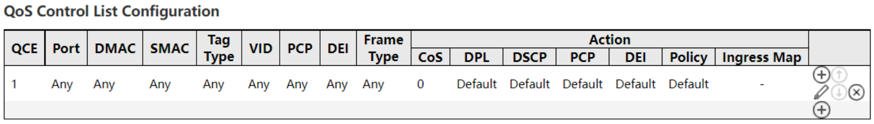
Egress Map Action

PCP	Disabled
DEI	Disabled
DSCP	Disabled

5.4.13. QoS Control List

[Switching > QoS > QoS Control List]

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.



QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action							
									CoS	DPL	DSCP	PCP	DEI	Policy	Ingress Map	
1	Any	Any	Any	Any	Any	Any	Any	Any	0	Default	Default	Default	Default	Default	-	⊕ ✎ ⊗
																⊕

QoS Control List Configuration

Click on the lowest plus sign to add a new QCE to the list.

QCE

Indicates the Map (unique) ID. Range is **0** to **256**.

Port

Physical ports of the corresponding device.

DMAC

Match a specific destination MAC address or 'any'.

SMAC

Match specific source MAC address or 'Any'.

Tag Type

Indicates tag type. Possible values are:

Any: Match tagged and untagged frames.

Untagged: Match untagged frames.

Tagged: Match tagged frames.

C-Tagged: Match C-tagged frames.

S-Tagged: Match S-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.

Ingress Map: Classify Ingress Map ID.

Modification Buttons

You can modify each QCE (QoS Control Entry) in the table using the following buttons:

⊕: Inserts a new QCE before the current row.

✎: Edits the QCE.

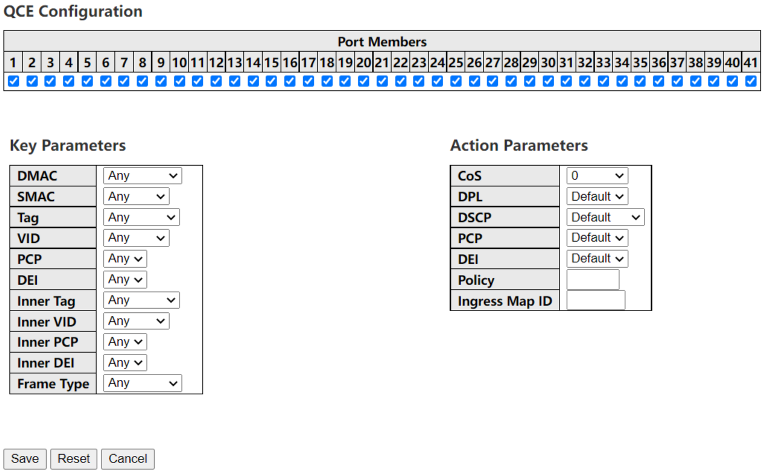
↑: Moves the QCE up the list.

↓: Moves the QCE down the list.

⊗: Deletes the QCE.

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

Click on "⊕", Open the hidden interface.



QCE Configuration

Port Members																																								
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Key Parameters

DMAC	Any
SMAC	Any
Tag	Any
VID	Any
PCP	Any
DEI	Any
Inner Tag	Any
Inner VID	Any
Inner PCP	Any
Inner DEI	Any
Frame Type	Any

Action Parameters

CoS	0
DPL	Default
DSCP	Default
PCP	Default
DEI	Default
Policy	
Ingress Map ID	

QCE Configuration

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

Note: All frame types are explained below.

Port Members

Check the checkbox button to include the port in the QCL entry. By default all ports are included.

Key Parameters

DMAC

Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast', 'Specific' (xx-xx-xx-xx-xx-xx) or 'Any'.

SMAC

Source MAC address: xx-xx-xx-xx-xx-xx or 'Any'.

Tag

Value of Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.

VID

Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.

PCP

Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI

Valid value of DEI can be '0', '1' or 'Any'.

Inner Tag

Value of Inner Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.

Inner VID

Valid value of Inner VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.

Inner PCP

Valid value of Inner 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'.

Inner DEI

Valid value of Inner DEI can be '0', '1' or 'Any'.

Frame Type

Frame Type can have any of the following values:

1. **Any:**

   Allow all types of frames.
2. **EtherType:**

   Ether Type Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.
3. **LLC:**

   DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'.

   SSAP Address Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.

   Control Valid Control field can vary from 0x00 to 0xFF or 'Any'.
4. **SNAP:**

   PID Valid PID(a.k.a Ether Type) can be 0x0000-0xFFFF or 'Any'.

5. **IPv4:**

    Protocol: IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.

    Source IP: Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero.

    Destination IP: Specific Destination IP address in value/mask format or 'Any'.

    IP Fragment: IPv4 frame fragmented option: 'Yes', 'No' or 'Any'.

    DSCP: Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

    Sport: Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

    Dport: Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

    Note: It is not recommended to configure the protocol value for IPv4 or IPv6 as 0 in QCE.

6. **IPv6:**

    Protocol: IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.

    Source IP: 32 LS bits of IPv6 source address in value/mask format or 'Any'.

    Destination IP: Specific Destination IP address in value/mask format or 'Any'.

    DSCP: Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.

    Sport: Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

    Dport: Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

    Note: It is not recommended to configure the protocol value for IPv4 or IPv6 as 0 in QCE.

Action Parameters

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

CoS

Class of Service: (0-7) or 'Default'.

DPL

Drop Precedence Level: (0-3) or 'Default'.

DSCP

DSCP: (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.

PCP

PCP: (0-7) or 'Default'. Note: PCP and DEI cannot be set individually.

DEI

DEI: (0-1) or 'Default'.

Policy

ACL: Policy number: (0-127) or 'Default' (empty field).

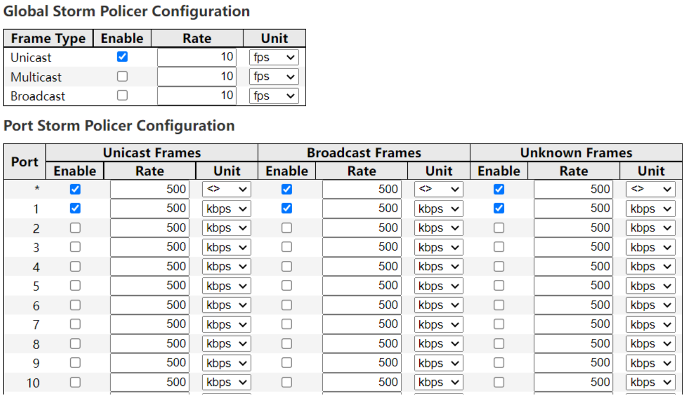
Ingress Map ID

Ingress Map ID: (0-255) or no Ingress Map (empty field).

5.4.14. Storm Policing

[Switching > QoS > Storm Policing]

Global and port storm policers for the switch are configured on this page.



Global Storm Policer Configuration

Frame Type	Enable	Rate	Unit
Unicast	☑	10	fps
Multicast	□	10	fps
Broadcast	□	10	fps

Port Storm Policer Configuration

Port	Unicast Frames			Broadcast Frames			Unknown Frames		
	Enable	Rate	Unit	Enable	Rate	Unit	Enable	Rate	Unit
*	☑	500	<>	☑	500	<>	☑	500	<>
1	☑	500	kbps	☑	500	kbps	☑	500	kbps
2	□	500	kbps	□	500	kbps	□	500	kbps
3	□	500	kbps	□	500	kbps	□	500	kbps
4	□	500	kbps	□	500	kbps	□	500	kbps
5	□	500	kbps	□	500	kbps	□	500	kbps
6	□	500	kbps	□	500	kbps	□	500	kbps
7	□	500	kbps	□	500	kbps	□	500	kbps
8	□	500	kbps	□	500	kbps	□	500	kbps
9	□	500	kbps	□	500	kbps	□	500	kbps
10	□	500	kbps	□	500	kbps	□	500	kbps

Global Storm Policer Configuration

There is a unicast storm policer, multicast storm policer, and a broadcast storm policer.

These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

The multicast rate limiting differs among different product models. Some models limit traffic where the 40th bit of the MAC address is 1, while other models exclude IPv4 multicast traffic with MAC addresses starting with 0x01005E and IPv6 multicast traffic with MAC addresses starting with 0x3333.

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 10-13128147 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the global storm policer. Supported rates are divisible by 10 fps or 25 kbps.

Unit

Controls the unit of measure for the global storm policer rate as fps, kfps, kbps or Mbps.

Port Storm Policer Configuration

Port storm policers for all switch ports are configured on this page.

There is a storm policer for unicast frames, broadcast frames, unknown (flooded) frames, unknown (flooded) unicast frames, unknown (flooded) multicast frames.

The displayed settings are:

Port

The port number for which the configuration below applies.

Enable

Enable or disable the storm policer for this switch port.

Rate

Controls the rate for the port storm policer. This value is restricted to 10-13128147 when "Unit" is fps or kbps, and 1-13128 when "Unit" is kfps or Mbps. The rate is internally rounded up to the nearest value supported by the port storm policer. Supported rates are divisible by 10 fps or 25 kbps.

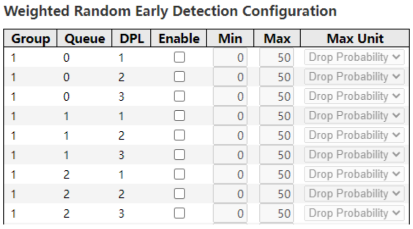
Unit

Controls the unit of measure for the port storm policer rate as fps, kfps, kbps or Mbps.

5.4.15. WRED

[Switching > QoS > WRED]

This page allows you to configure the Random Early Detection (RED) settings.



Weighted Random Early Detection Configuration

Group	Queue	DPL	Enable	Min	Max	Max Unit
1	0	1	☐	0	50	Drop Probability
1	0	2	☐	0	50	Drop Probability
1	0	3	☐	0	50	Drop Probability
1	1	1	☐	0	50	Drop Probability
1	1	2	☐	0	50	Drop Probability
1	1	3	☐	0	50	Drop Probability
1	2	1	☐	0	50	Drop Probability
1	2	2	☐	0	50	Drop Probability
1	2	3	☐	0	50	Drop Probability

Weighted Random Early Detection Configuration

Through different RED configuration for the queues it is possible to obtain Weighted Random Early Detection (WRED) operation between queues.

The settings are global for all ports in the switch.

Group

The WRED group number for which the configuration below applies.

Queue

The queue number (CoS) for which the configuration below applies.

DPL

The Drop Precedence Level for which the configuration below applies.

Enable

Controls whether RED is enabled for this entry.

Min

Controls the lower RED fill level threshold. If the queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100%.

Max

Controls the upper RED drop probability or fill level threshold for frames marked with Drop Precedence Level > 0 (yellow frames). This value is restricted to 1-100%.

Max Unit

Selects the unit for Max. Possible values are:

Drop Probability: Max controls the drop probability just below 100% fill level.

Fill Level: Max controls the fill level where drop probability reaches 100%.

5.5. VLAN

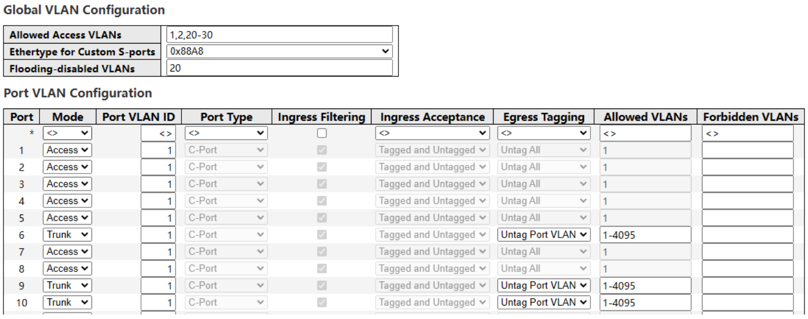
5.5.1. Configuration

[Switching > VLAN > Configuration]

[Global and Port VLAN]

This page allows for controlling VLAN configuration on the switch.

The page is divided into a global section and a per-port configuration section.



Global VLAN Configuration

Allowed Access VLANs	1,2,20-30
Ethertype for Custom S-ports	0x88A8
Flooding-disabled VLANs	20

Port VLAN Configuration

Port	Mode	Port VLAN ID	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	<>	<>	□	<>	<>	<>	<>
1	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
2	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
6	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
9	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
10	Trunk	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	

Global VLAN Configuration

Allowed Access VLANs

This field shows the allowed Access VLANs, i.e. it only affects ports configured as Access ports. Ports in other modes are members of the VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.

The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

Ethertype for Custom S-ports

This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

Flooding-disabled VLANs

This field displays VLANs where Layer 2 flooding is disabled. Layer 2 flooding includes broadcasting, multicasting, and unknown unicasting. By default, this field is empty, indicating that Layer 2 flooding is enabled for all VLANs. If the input box appears greyed out, it indicates that the current device does not support this feature.

Additional VLANs can be specified using list syntax, with each element separated by commas. Use hyphens to specify a range of VLANs. For example, to create VLANs 1, 10, 11, 12, 13, 200, and 300, use the following format: 1,10-13,200,300. Spaces are allowed between delimiters.

Port VLAN Configuration

Port

The line shows the physical port number.

Mode

The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below.
Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question.

Grayed out fields show the value that the port will get when the mode is applied.

Access:

Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:

- Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1.
- Accepts untagged and C-tagged frames.
- Discards all frames not classified to the Access VLAN.
- On egress all frames are transmitted untagged.

Trunk:

Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:

- By default, a trunk port is member of all VLANs (1-4095).
- The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs.
- Frames classified to a VLAN that the port is not a member of are discarded.
- By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress.
- Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress.

Hybrid:

Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:

- Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware.
- Ingress filtering can be controlled.
- Ingress acceptance of frames and configuration of egress tagging can be configured independently.

Port VLAN ID

Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1.

On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).

On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN.

The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

Port Type

Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.

Unaware:

On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.

C-Port:

On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag.

If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN.

If frames must be tagged on egress, they will be tagged with a C-tag.

S-Port:

On egress, if frames must be tagged, they will be tagged with an S-tag.

On ingress, frames with a VLAN tag with TPID = 0x88A8 get classified to the VLAN ID embedded in the tag.

Priority-tagged frames are classified to the Port VLAN.

If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped.

S-Custom-Port:

On egress, if frames must be tagged, they will be tagged with the custom S-tag.

On ingress, frames with a VLAN tag with a TPID equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag.

Priority-tagged frames are classified to the Port VLAN.

If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped.

Ingress Filtering

Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.

If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.

If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

Ingress Acceptance

Hybrid ports allow for changing the type of frames that are accepted on ingress.

Tagged and Untagged

Both tagged and untagged frames are accepted. See Port Type for a description of when a frame is considered tagged.

Tagged Only

Only frames tagged with the corresponding Port Type tag are accepted on ingress.

Untagged Only

Only untagged frames are accepted on ingress. See Port Type for a description of when a frame is considered untagged.

Egress Tagging

Ports in Trunk and Hybrid mode may control the tagging of frames on egress.

Untag Port VLAN

Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.

Tag All

All frames, whether classified to the Port VLAN or not, are transmitted with a tag.

Untag All

All frames, whether classified to the Port VLAN or not, are transmitted without a tag.

This option is only available for ports in Hybrid mode.

Allowed VLANs

Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN.

The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to 1-4095.

The field may be left empty, which means that the port will not become member of any VLANs.

Forbidden VLANs

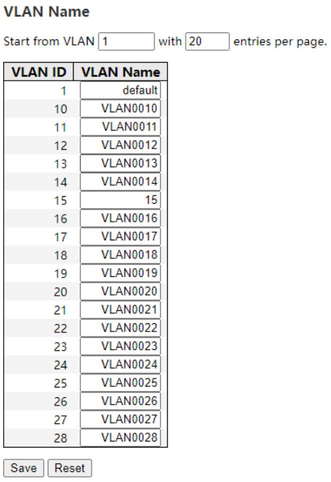
A port may be configured to never become member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs.

The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field.

By default, the field is left blank, which means that the port may become a member of all possible VLANs.

[VLAN Name]

This page allows you to query and modify the names of Static VLANs.



VLAN Name

Start from VLAN 1 with 20 entries per page.

VLAN ID	VLAN Name
1	default
10	VLAN0010
11	VLAN0011
12	VLAN0012
13	VLAN0013
14	VLAN0014
15	15
16	VLAN0016
17	VLAN0017
18	VLAN0018
19	VLAN0019
20	VLAN0020
21	VLAN0021
22	VLAN0022
23	VLAN0023
24	VLAN0024
25	VLAN0025
26	VLAN0026
27	VLAN0027
28	VLAN0028

VLAN ID

VLAN ID of the entry.

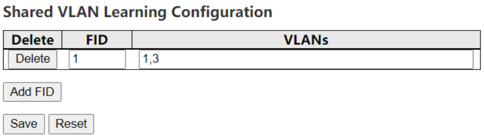
VLAN Name

Name of the VLAN. The names of VLANs, except for VLAN 1, can be modified.

5.5.2. SVL

[Switching > VLAN > SVL]

This page allows for controlling SVL configuration on the switch.



Shared VLAN Learning Configuration

Delete	FID	VLANs
Delete	1	1,3

Shared VLAN Learning Configuration

In SVL, one or more VLANs map to a Filter ID (FID). By default, there is a one-to-one mapping from VLAN to FID, in which case the switch acts as an IVL bridge, but with SVL multiple VLANs may share the same MAC address table entries.

Delete

A previously allocated FID can be deleted by the use of this button.

FID

The Filter ID (FID) is the ID that VLANs get learned on in the MAC table when SVL is in effect.

No two rows in the table can have the same FID and the FID must be a number between 1 and 4095.

VLANs

List of VLANs mapped into FID.

The syntax is as follows: Individual VLANs are separated by commas. Ranges are specified with a dash separating the lower and upper bound.

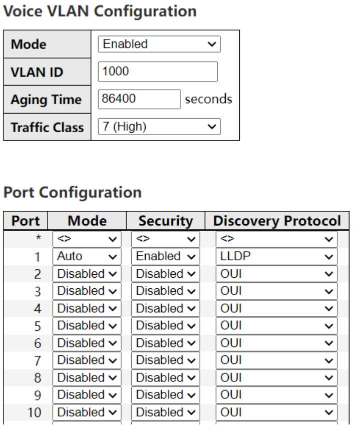
The following example will map VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters. The range of valid VLANs is 1 to 4095.
The same VLAN can only be a member of one FID. A message will be displayed if one VLAN is grouped into two or more FIDs.

All VLANs must map to a particular FID, and by default VLAN x maps to FID x. This implies that if FID x is defined, then VLAN x is implicitly a member of FID x unless it is specified for another FID. If FID x doesn't exist, a confirmation message will be displayed, asking whether to continue adding VLAN x implicitly to FID x.

5.5.3. Voice VLAN

Configuration

[Switching > VLAN > Voice VLAN > Configuration]



Voice VLAN Configuration

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

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<>	<>	<>
1	Auto	Enabled	LLDP
2	Disabled	Disabled	OUI
3	Disabled	Disabled	OUI
4	Disabled	Disabled	OUI
5	Disabled	Disabled	OUI
6	Disabled	Disabled	OUI
7	Disabled	Disabled	OUI
8	Disabled	Disabled	OUI
9	Disabled	Disabled	OUI
10	Disabled	Disabled	OUI

Voice VLAN Configuration

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

Mode

Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering. Possible modes are:

Enabled: Enable Voice VLAN mode operation.

Disabled: Disable Voice VLAN mode operation.

VLAN ID

Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.

Aging Time

Indicates the Voice VLAN secure learning aging time. The allowed range is 10 to 10000000 seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.

Traffic Class

Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.

Port Configuration

Mode

Indicates the Voice VLAN port mode. Possible port modes are:

Disabled: Disjoin from Voice VLAN.

Auto: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically.

Forced: Force join to Voice VLAN.

Security

Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are:

Enabled: Enable Voice VLAN security mode operation.

Disabled: Disable Voice VLAN security mode operation.

Discovery Protocol

Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are:

OUI: Detect telephony device by OUI address.

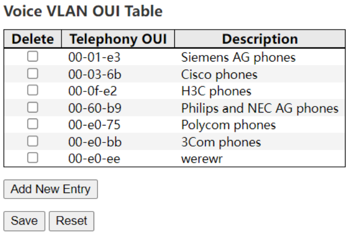
LLDP: Detect telephony device by LLDP.

Both: Both OUI and LLDP.

OUI

[Switching > VLAN > Voice VLAN > OUI]

Configure VOICE VLAN OUI table on this page. The maximum number of entries is 16. Modifying the OUI table will restart auto detection of OUI process.



Voice VLAN OUI Table

Delete	Telephony OUI	Description
□	00-01-e3	Siemens AG phones
□	00-03-6b	Cisco phones
□	00-0f-e2	H3C phones
□	00-60-b9	Philips and NEC AG phones
□	00-e0-75	Polycom phones
□	00-e0-bb	3Com phones
□	00-e0-ee	werewr

Voice VLAN OUI Table

Delete

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

Telephony OUI

A telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be 6 characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).

Description

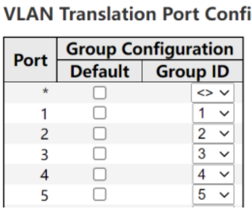
The description of OUI address. Normally, it describes which vendor telephony device it belongs to. The allowed string length is 0 to 32.

5.5.4. VLAN Translation

Port to Group Configuration

[Switching > VLAN > VLAN Translation > Port to Group Configuration]

This page allows you to configure switch Ports to use a given VLAN Translation Mapping Group. This will enable all VLAN Translation mappings of that group (if any) on the selected switch port.



VLAN Translation Port Configuration

Port	Group Configuration	
	Default	Group ID
*	□	<>
1	□	1
2	□	2
3	□	3
4	□	4
5	□	5

VLAN Translation Port Configuration

Port

The Port column shows the list of ports for which you can configure the VLAN Translation Mapping Group.

Default

To set the switch port to use the default VLAN Translation Group. Click the checkbox and press Save.

Group ID

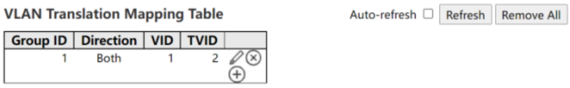
The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group.

Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.

VLAN Translation Mappings

[Switching > VLAN > VLAN Translation > VLAN Translation Mappings]

This page allows you to create mappings of VLANs -> Translated VLANs and organize these mappings into global Groups.



VLAN Translation Mapping Table

Group ID	Direction	VID	TVID	
1	Both	1	2	✎ ⊗
				⊕

VLAN Translation Mapping Table

Group ID

The VLAN Translation mappings are organized into Groups, identified by the Group ID. This way a port is configured to use a number of VLAN Translation mappings easily by simply configuring it to use a given group. Then number of possible groups in a switch is equal to the number of ports present in this switch. A port can be configured to use any of the groups, but only one at any given time. Multiple ports can be configured to use the same group.

Note: By default, each port is set to use the group with Group ID equal to the port number. For example, port #1 is by default set to use group with GID = 1.

Direction

Indicates the direction of the VLAN Translation and it refers to the switch. The direction can be 'Ingress', where the translation takes place on the VLAN ID of frames entering the switch port, 'Egress', where the translation takes place on the VLAN ID of frames exiting the switch port, or 'Both', where the translation takes place on both of the above directions.

VID

Indicates the VLAN ID of the mapping (i.e. 'source' VLAN). A valid VLAN ID ranges from 1 to 4095.

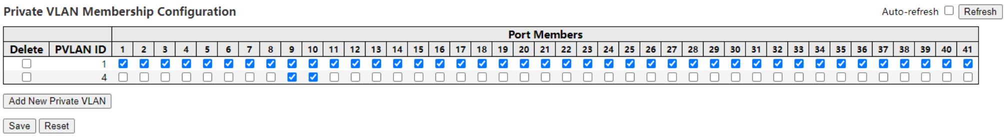
TVID

Indicates the translated VLAN ID to which a VLAN ID of a frame will be translated to. A valid translated VLAN ID ranges from 1 to 4095.

5.5.5. Private VLANs

Membership

[Switching > VLAN > Private VLANs > Membership]



Private VLAN Membership Configuration

Auto-refresh ☐ Refresh

		Port Members																																								
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
☐	1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
☐	4	☐	☐	☐	☐	☐	☐	☐	☐	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here.

Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.

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

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

Private VLAN Membership Configuration

Delete

To delete a private VLAN entry, check this box. The entry will be deleted during the next save.

Private VLAN ID

Indicates the ID of this particular private VLAN.

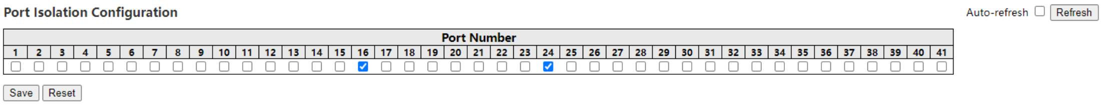
Port Members

A row of check boxes for each port is displayed for each private VLAN ID. To include a port in a Private VLAN, check the box. To remove or exclude the port from the Private VLAN, make sure the box is unchecked. By default, all ports are members, and all boxes are selected.

Port Isolation

[Switching > VLAN > Private VLANs > Port Isolation]

This page is used for enabling or disabling port isolation on ports in a Private VLAN.



Port Isolation Configuration

Auto-refresh ☐ Refresh

Port Number																																								
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Port Isolation Configuration

Port Members

A check box is provided for each port of a private VLAN.

When checked, port isolation is enabled on that port.

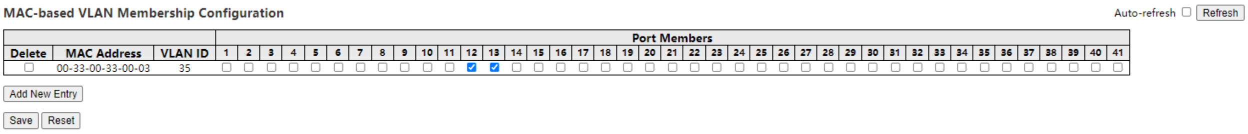
When unchecked, port isolation is disabled on that port.

By default, port isolation is disabled on all ports.

5.5.6. MAC-based VLAN

[Switching > VLAN > MAC-based VLAN]

Page Example 1:



MAC-based VLAN Membership Configuration

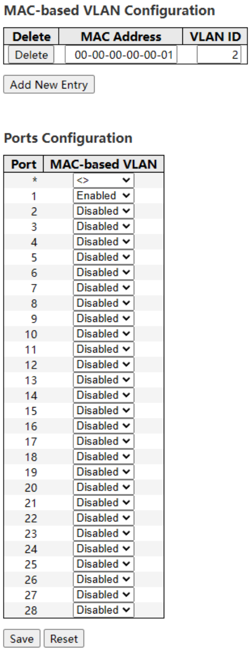
Auto-refresh □ Refresh

			Port Members																																							
Delete	MAC Address	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
□	00-33-00-33-00-03	35	□	□	□	□	□	□	□	□	□	□	□	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Add New Entry

Save Reset

Page Example 2:



MAC-based VLAN Configuration

Delete	MAC Address	VLAN ID
Delete	00-00-00-00-00-01	2

Add New Entry

Ports Configuration

Port	MAC-based VLAN
*	<>
1	Enabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled
25	Disabled
26	Disabled
27	Disabled
28	Disabled

Save Reset

The MAC address to VLAN ID mappings can be configured here. This page allows adding and deleting MAC-based VLAN Classification List entries and assigning the entries to different ports.

MAC-Based VLAN Membership Configuration

Delete

To delete a MAC to VLAN ID mapping entry, check this box and press save. The entry will be deleted in the stack.

MAC Address

Indicates the MAC address of the mapping.

VLAN ID

Indicates the VLAN ID the above MAC will be mapped to.

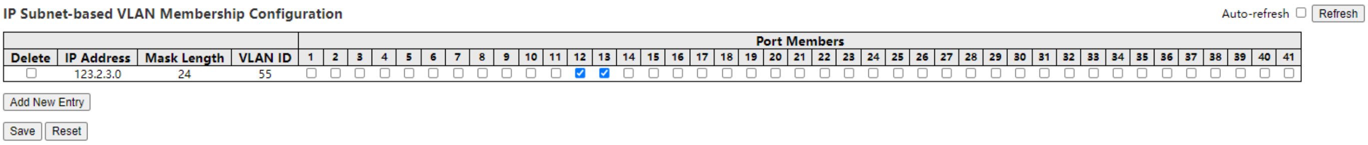
Port Members

Configure the port's enable or disable status for each MAC to VLAN ID mapping entry.

5.5.7. IP Subnet-based VLAN

[Switching > VLAN > IP Subnet-based VLAN]

Page Example 1:

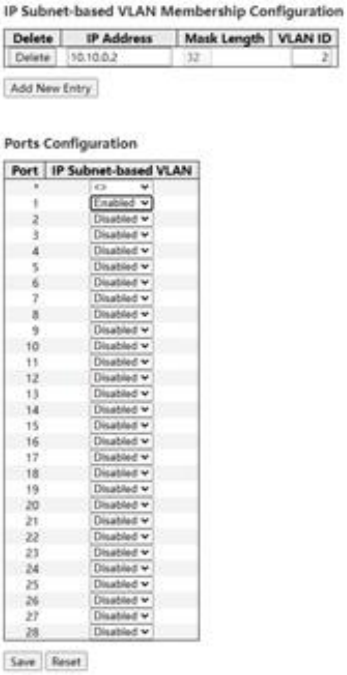


IP Subnet-based VLAN Membership Configuration

Auto-refresh □ Refresh

				Port Members																																								
Delete	IP Address	Mask Length	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
□	123.2.3.0	24	55	□	□	□	□	□	□	□	□	□	□	□	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Page Example 2:



IP Subnet-based VLAN Membership Configuration

Delete	IP Address	Mask Length	VLAN ID
Delete	10.10.0.2	32	2

Ports Configuration

Port	IP Subnet-based VLAN
*	<>
1	Enabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled
25	Disabled
26	Disabled
27	Disabled
28	Disabled

The IP subnet to VLAN ID mappings can be configured here. This page allows adding, updating and deleting IP subnet to VLAN ID mapping entries and assigning them to different ports.

IP Subnet-based VLAN Membership Configuration

Delete

To delete a mapping, check this box and press save. The entry will be deleted in the stack.

IP Address

Indicates the subnet's IP address (Any of the subnet's host addresses can be also provided here, the application will convert it automatically).

Mask Length

Indicates the subnet's mask length.

VLAN ID

Indicates the VLAN ID the subnet will be mapped to. IP Subnet to VLAN ID is a unique matching.

Port Members

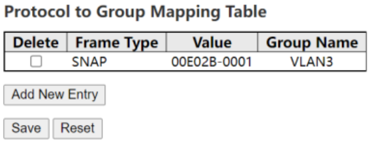
Configure the port's enable or disable status for each IP Subnet to VLAN ID mapping entry.

5.5.8. Protocol-based VLAN

Protocol to Group

[Switching > VLAN > Protocol-based VLAN > Protocol to Group]

This page allows you to add new Protocol to Group Name (each protocol can be part of only one Group) mapping entries as well as allow you to see and delete already mapped entries for the switch.



Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
□	SNAP	00E02B-0001	VLAN3

Protocol to Group Mapping Table

Delete

To delete a Protocol to Group Name map entry, check this box. The entry will be deleted from the switch during the next Save.

Frame Type

Frame Type can have one of the following values:

1. **Ethernet**

2. **LLC**

3. **SNAP**

Note: When changing the Frame type field, the valid value of the following text field will vary depending on the new frame type you selected.

Value

Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu.

Below are the criteria for the three different Frame Types:

1. **Ethernet**: Value in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype range between 0x0600 and 0xffff.

2. **LLC**: Valid value in this case is comprised of two different sub-values.

   a. **DSAP**: 1-byte long string (0x00-0xff).

   b. **SSAP**: 1-byte long string (0x00-0xff).

3. **SNAP**: Valid value in this case is also comprised of two different sub-values.

   a. **OUI**: OUI (Organizationally Unique Identifier) is a parameter in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value ranging between 0x00 and 0xff.

   b. **PID**: PID (Protocol ID). If OUI is hexadecimal 000000, then the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.

In other words, if the value of OUI field is 00-00-00 then the value of PID will be etype (0x0600-0xffff) and if the value of OUI is other than 00-00-00 then valid values of PID will be any value between 0x0000 and 0xffff.

Group Name

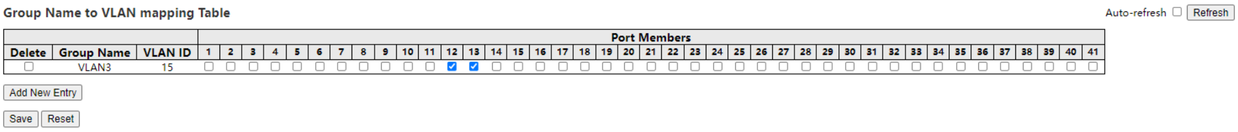
A valid Group Name is a 16-character long string, unique for every entry, which consists of a combination of alphabets (a-z or A-Z) and integers(0-9).

Note: Special characters and underscores (_) are not allowed.

Group to VLAN

[Switching > VLAN > Protocol-based VLAN > Group to VLAN]

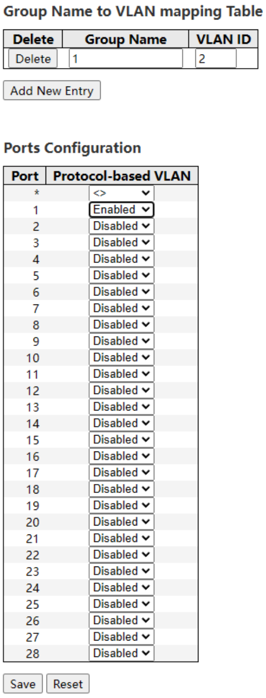
Page Example 1:



Group Name to VLAN mapping Table

			Port Members																																							
Delete	**Group Name**	**VLAN ID**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**
□	VLAN3	15	□	□	□	□	□	□	□	□	□	□	□	☑	☑	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Page Example 2:



Group Name to VLAN mapping Table

Delete	Group Name	VLAN ID
Delete	1	2

Ports Configuration

Port	Protocol-based VLAN
*	<>
1	Enabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled
25	Disabled
26	Disabled
27	Disabled
28	Disabled

This page allows you to map a Group Name (already configured or to be configured in the future) to a VLAN for the switch.

Group Name to VLAN mapping Table

Delete

To delete a Protocol to Group Name map entry, check this box. The entry will be deleted from the switch during the next Save.

Group Name

A valid Group Name is a string, at the most 16 characters long, which consists of a combination of alphabets (a-z or A-Z) and integers(0-9) with no special characters allowed. You may either use a Group that already includes one or more protocols (see Protocol to Group mappings), or create a Group to VLAN ID mapping that will become active the moment you add one or more protocols inside that Group. Furthermore, the Group to VLAN ID mapping is not unique, as long as the port lists of these mappings are mutually exclusive (e.g. Group1 can be mapped to VID 1 on port#1 and to VID 2 on port#2).

VLAN ID

Indicates the VLAN ID to which the Group Name will be mapped. A valid VLAN ID ranges from 1 to 4095.

Port Members

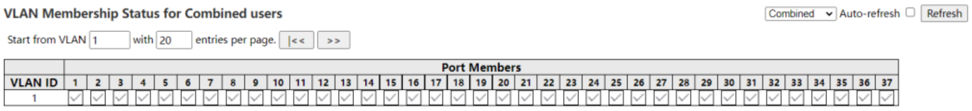
Configure the port's enable or disable status for each Protocol Group Name to VLAN ID mapping entry.

5.5.9. Status

[Switching > VLAN > status]

[Membership]

This page provides an overview of membership status of VLAN users.



VLAN Membership Status for Combined users

Start from VLAN 1 with 20 entries per page.

	Port Members																																			
VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

VLAN Membership Status

VLAN User

Various internal software modules may use VLAN services to configure VLAN memberships on the fly.

The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Static) or as configured by one of these internal software modules.

The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

VLAN ID

VLAN ID for which the Port members are displayed.

Port Members

A row of check boxes for each port is displayed for each VLAN ID.

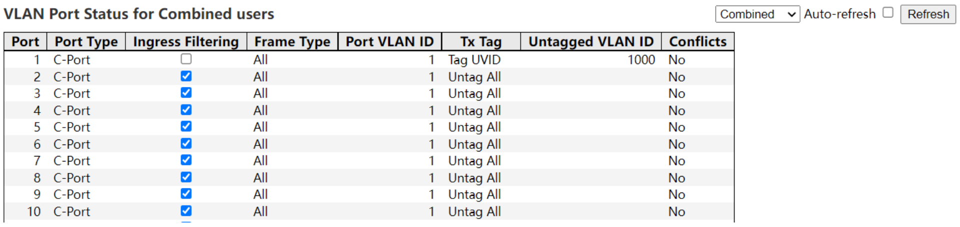
If a port is included in a VLAN, the following image will be displayed: ✓.

If a port is in the forbidden port list, the following image will be displayed: ✕.

If a port is in the forbidden port list and at the same time attempted included in the VLAN, the following image will be displayed: ⓘ. The port will not be a member of the VLAN in this case.

[Ports]

This page provides VLAN Port Status.



VLAN Port Status for Combined users

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	□	All	1	Tag UVID	1000	No
2	C-Port	☑	All	1	Untag All		No
3	C-Port	☑	All	1	Untag All		No
4	C-Port	☑	All	1	Untag All		No
5	C-Port	☑	All	1	Untag All		No
6	C-Port	☑	All	1	Untag All		No
7	C-Port	☑	All	1	Untag All		No
8	C-Port	☑	All	1	Untag All		No
9	C-Port	☑	All	1	Untag All		No
10	C-Port	☑	All	1	Untag All		No

VLAN Port Status

VLAN User

Various internal software modules may use VLAN services to configure VLAN port configuration on the fly.

The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Static) or as configured by one of these internal software modules.

The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

If a given software modules hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table.

Port

The physical port for the settings contained in the same row.

Port Type

Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the port.

The field is empty if not overridden by the selected user.

Ingress Filtering

Shows whether a given user wants ingress filtering enabled or not.

The field is empty if not overridden by the selected user.

Frame Type

Shows the acceptable frame types (All, Taged, Untagged) that a given user wants to configure on the port.

The field is empty if not overridden by the selected user.

Port VLAN ID

Shows the Port VLAN ID (PVID) that a given user wants the port to have.

The field is empty if not overridden by the selected user.

Tx Tag

Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port.

The field is empty if not overridden by the selected user.

Untagged VLAN ID

If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field will show the VLAN ID the user wants to tag or untag on egress.

The field is empty if not overridden by the selected user.

Conflicts

Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress.

Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority.

If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module.

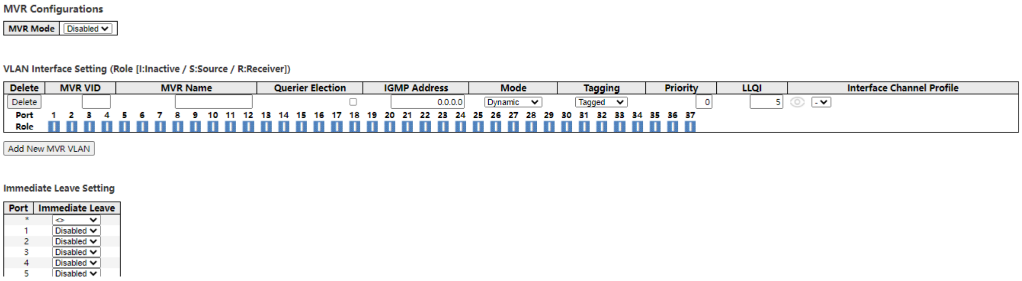
The "Combined" user reflects what is actually configured in hardware.

5.6. MVR

[Switching > MVR]

[Configuration]

This page provides MVR related configurations.



MVR Configurations

MVR Mode	Disabled

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

Delete	MVR VID	MVR Name	Querier Election	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile
Delete			□	0.0.0.0	Dynamic	Tagged	0	5	-

Port 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37
Role

Add New MVR VLAN

Immediate Leave Setting

Port	Immediate Leave
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled

The MVR feature enables multicast traffic forwarding on the Multicast VLANs.

In a multicast television application, a PC or a network television or a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

The Querier should to connect on the source port. By giving the Static membership of MVR VLAN, device only forwards the IGMP reports from downstream(receiver ports) to upstream(source ports) and the Query packet which comes from the downstream will be ignored silently.

After the MVR VLAN members are properly configured, it is required to associate an IPMC profile with the specific MVR VLAN to be the expected channel. The channel profile is defined by the IPMC Profile which provides the filtering conditions. Notice that the profile only work when the global profile mode is enabled. It is allowed to create at most 4 MVR VLANs with corresponding channel profile.

MVR Configurations

MVR Mode

Enable/Disable the Global MVR.

The Unregistered Flooding control depends on the current configuration in IGMP/MLD Snooping.

It is suggested to enable Unregistered Flooding control when the MVR group table is full.

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

Delete

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

MVR VID

Specify the Multicast VLAN ID.

Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

MVR Name

MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. Maximum length of the MVR VLAN Name string is 16. MVR VLAN Name can only contain alphabets or numbers. When the optional MVR VLAN name is given, it should contain at least one alphabet. MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.

Querier Election

Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

IGMP Address

The parameter is used when the device acts IGMP Querier. It defines the IPv4 address as source address used in IP header for IGMP control frames.

The default IGMP address is not set (0.0.0.0).

When the IGMP 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.

Mode

Specify the MVR mode of operation. In Dynamic mode, MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports. The default is Dynamic mode.

Tagging

Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged with MVR VID. The default is Tagged.

Priority

Specify how the traversed IGMP/MLD control frames will be sent in prioritized manner. The default Priority is 0.

LLQI

The parameter is used when the device act an Querier. It define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is 5 tenths or one-half second.

Interface Channel Profile

When the MVR VLAN is created, select the IPMC Profile as the channel filtering condition for the specific MVR VLAN. Summary about the Interface Channel Profiling (of the MVR VLAN) will be shown by clicking the view button. Profile selected for designated interface channel is not allowed to have overlapped permit group address.

Profile Management Button

You can inspect the rules of the designated profile by using the following button:

👁: List the rules associated with the designated profile.

Interface Channel Profile

Port

The logical port for the settings.

Port Role

Configure an MVR port of the designated MVR VLAN as one of the following roles.

Inactive: The designated port does not participate MVR operations.

Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports.

Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages.

Be Caution: MVR source ports are not recommended to be overlapped with management VLAN ports.

Select the port role by clicking the Role symbol to switch the setting.

I indicates Inactive; S indicates Source; R indicates Receiver.

The default Role is Inactive.

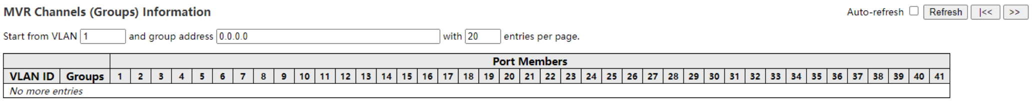
Immediate Leave

Enable the fast leave on the port.

System will remove group record and stop forwarding data upon receiving the IGMPv2/MLDv1 leave message without sending last member query messages.

It is recommended to enable this feature only when a single IGMPv2/MLDv1 host is connected to the specific port.

[MVR Channel Groups]



MVR Channels (Groups) Information

Start from VLAN 1 and group address 0.0.0.0 with 20 entries per page.

		Port Members																																								
VLAN ID	**Groups**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**
No more entries																																										

Entries in the MVR Channels (Groups) Information Table are shown on this page. The MVR Channels (Groups) Information Table is sorted first by VLAN ID, and then by group.

Each page shows up to 99 entries from the MVR 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 MVR Channels (Groups) Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR Channels (Groups) Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MVR Channels (Groups) 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 "**|<<**" button to start over.

VLAN ID

VLAN ID of the group.

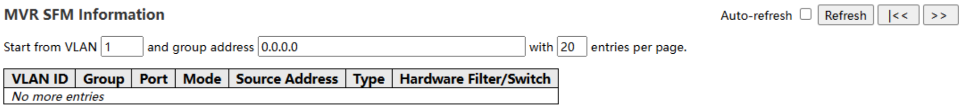
Groups

Group ID of the group displayed.

Port Members

Ports under this group.

[MVR SFM Information]



MVR SFM Information

Auto-refresh □

Start from VLAN 1 and group address 0.0.0.0 with 20 entries per page.

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

Entries in the MVR SFM Information Table are shown on this page. The MVR 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.

Each page shows up to 99 entries from the MVR 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 MVR SFM Information Table.

The "Start from VLAN", and "Group Address" input fields allow the user to select the starting point in the MVR SFM Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MVR 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 "**|<<**" button to start over.

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port

Switch port number.

Mode

Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.

Source Address

IP Address of the source.

Currently, the maximum number of IP 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

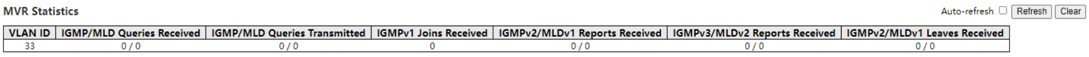
Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch

Indicates whether data plane destined to the specific group address from the source IPv4/IPv6 address could be handled by chip or not.

[Statistics]

This page provides MVR Statistics information.



MVR Statistics

VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
33	0 / 0	0 / 0	0	0 / 0	0 / 0	0 / 0

MVR Statistics Table

VLAN ID

VLAN ID of the group.

IGMP/MLD Queries Received

The number of Received Queries for IGMP and MLD, respectively.

IGMP/MLD Queries Transmitted

The number of Transmitted Queries for IGMP and MLD, respectively.

IGMPv1 Joins Received

The number of Received IGMPv1 Join's.

IGMPv2/MLDv1 Report's Received

The number of Received IGMPv2 Join's and MLDv1 Report's, respectively.

IGMPv3/MLDv2 Report's Received

The number of Received IGMPv3 Join's and MLDv2 Report's, respectively.

IGMPv2/MLDv1 Leave's Received

The number of Received IGMPv2 Leave's and MLDv1 Done's, respectively.

5.7. L2-Multicast

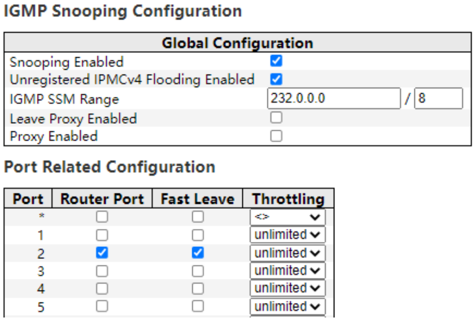
5.7.1. IGMP Snooping

Configuration

[Switching > L2-Multicast > IGMP Snooping > Configuration]

[Basic Configuration]

This page provides IGMP Snooping related configuration.



IGMP Snooping Configuration

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

Port Related Configuration

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

Global 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.

Requests made by IGMPv1 and IGMPv2 hosts in this range are ignored.

Assign a 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.

Port Related Configuration

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.

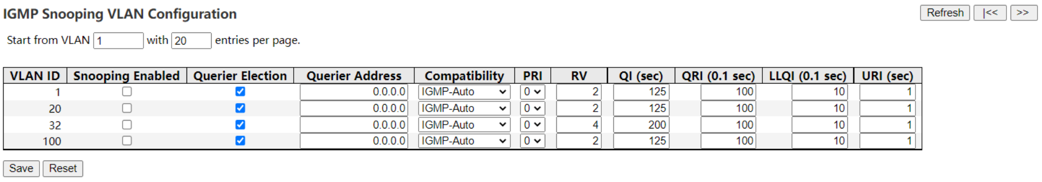
System will remove group record and stop forwarding data upon receiving the IGMPv2 leave message without sending last member query messages.

It is recommended to enable this feature only when a single IGMPv2 host is connected to the specific port.

Throttling

Enable to limit the number of multicast groups to which a switch port can belong.

[VLAN Configuration]



IGMP Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	□	☑	0.0.0.0	IGMP-Auto	0	2	125	100	10	1
20	□	☑	0.0.0.0	IGMP-Auto	0	2	125	100	10	1
32	□	☑	0.0.0.0	IGMP-Auto	0	4	200	100	10	1
100	□	☑	0.0.0.0	IGMP-Auto	0	2	125	100	10	1

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

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the next closest VLAN Table match.

The "**>>**" 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.

IGMP Snooping VLAN Configuration

When creating an IGMP VLAN interface, you need to first go to Routing > IP > IP Configuration page to add the interface. Then, go to Switch > Layer 2 Multicast > IGMP Snooping > Configure > VLAN Configuration to view the configuration results.

VLAN ID

The VLAN ID of the entry.

Snooping Enabled

Enable the per-VLAN IGMP Snooping. Up to 128 VLANs can be selected for IGMP Snooping.

Querier Election

Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Querier Address

Define the IPv4 address as source address used in IP header for IGMP Querier election.

When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN.

When the IPv4 management address is not set, system uses the first available IPv4 management address.

Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

Compatibility

Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network.

The allowed selection is Auto, IGMPv1, IGMPv2, IGMPv3, default compatibility value is Auto.

PRI

Priority of Interface.

It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.

The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.

RV

Robustness Variable.

The Robustness Variable allows tuning for the expected packet loss on a network.

The allowed range is 2 to 255, default robustness variable value is 2.

QI

Query Interval.

The Query Interval is the interval between General Queries sent by the Querier.

The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.

QRI

Query Response Interval.

The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.

The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP)

Last Member Query Interval.

The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count.

The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).

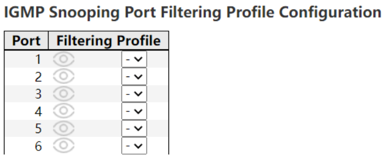
URI

Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group.

The allowed range is 1 to 31744 seconds, default unsolicited report interval is 1 second.

[Port Filtering Profile]

This page provides Port Filtering Profile related configuration.



IGMP Snooping Port Filtering Profile Configuration

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

Port Filtering Profile

Port

The physical port for the settings.

Filtering Profile

Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

Profile Management Button

You can inspect the rules of the designated profile by using the following button:

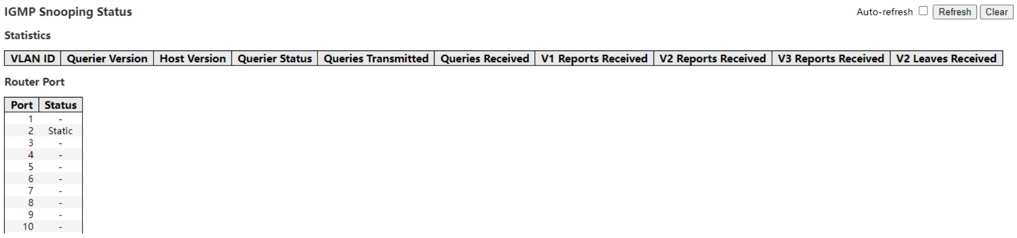
👁: List the rules associated with the designated profile.

Status

[Switching > L2-Multicast > IGMP Snooping > Status]

[Status]

This page provides IGMP Snooping status.



IGMP Snooping Status

Auto-refresh ☐ Refresh Clear

Statistics

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

Router Port

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

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 Reports.

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 and learnt to be a router port.

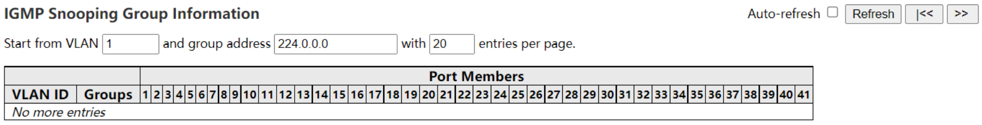
Port

Switch port number.

Status

Indicate whether specific port is a router port or not.

[Groups Information]



IGMP Snooping Group Information

Start from VLAN 1 and group address 224.0.0.0 with 20 entries per page.

		Port Members																																								
VLAN ID	**Groups**	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
No more entries																																										

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.

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

VLAN ID

VLAN ID of the group.

Groups

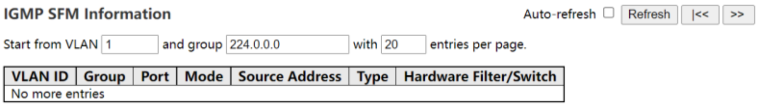
Group address of the group displayed.

Port Members

Ports under this group.

[IPv4 SFM Information]

This page shows the IGMP registered multicast entries sorted by VLAN ID, group address, port number and source address.



IGMP SFM Information

Auto-refresh □ Refresh |<< >>

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/Switch
No more entries						

Each page shows up to 99 entries 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 "**|<<**" button to start over.

IGMP SFM Information Table

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port

Switch port number.

Mode

Each <VLAN ID, Group, Port> has a filter mode of either Include or Exclude, described further in section 6.2.1 of RFC3376.

Source Address

IP Address of the source.

If there are no specific source addresses the text is "< Any>". This may happen if a host on the port is in IGMPv1 or IGMPv2 mode or simply hasn't specified particular sources in the IGMPv3 reports.

On the contrary, if there indeed are sources in the IGMPv3 reports, there is also a "Catch-remaining" entry, which matches on source addresses not already specified above its line. This is marked with " <Other>".

Currently, the maximum number of IPv4 source address per VLAN ID per group is 8.

Type

This field indicates whether the entry is forwarding (Allow) or blocking (Deny).

Hardware Filter/Switch

Shows whether blocking/forwarding of this entry is handled by hardware or not.

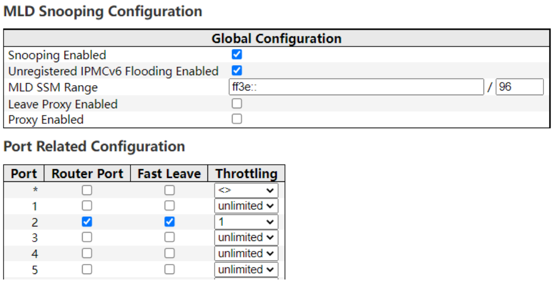
5.7.2. MLD Snooping

Configuration

[Switching > L2-Multicast > MLD Snooping > Configuration]

[Basic Configuration]

This page provides MLD Snooping related configuration.



MLD Snooping Configuration

Global Configuration	
Snooping Enabled	☑
Unregistered IPMCv6 Flooding Enabled	☑
MLD SSM Range	ff3e:: / 96
Leave Proxy Enabled	□
Proxy Enabled	□

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	□	□	<>
1	□	□	unlimited
2	☑	☑	1
3	□	□	unlimited
4	□	□	unlimited
5	□	□	unlimited

MLD Snooping Configuration

Snooping Enabled

Enable the Global MLD Snooping.

Unregistered IPMCv6 Flooding Enabled

Enable unregistered IPMCv6 traffic flooding.

The flooding control takes effect only when MLD Snooping is enabled.

When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

MLD 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.

Requests made by MLDv1 hosts in this range are ignored.

Assign a valid IPv6 multicast address as prefix with a prefix length (from 8 to 128) for the range.

Leave Proxy Enabled

Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled

Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Port Related Configuration

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 MLD 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.

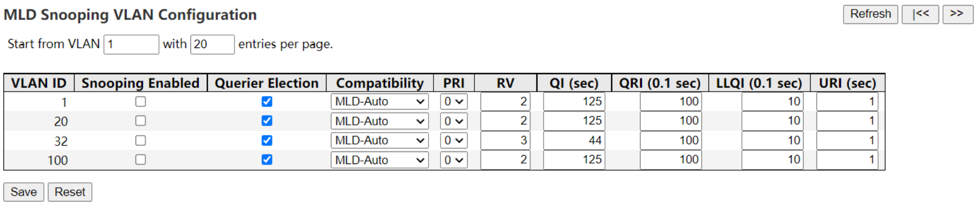
System will remove group record and stop forwarding data upon receiving the MLDv1 leave message without sending last member query messages.

It is recommended to enable this feature only when a single MLDv1 host is connected to the specific port.

Throttling

Enable to limit the number of multicast groups to which a switch port can belong.

[VLAN Configuration]



MLD Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

VLAN ID	Snooping Enabled	Querier Election	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	□	☑	MLD-Auto	0	2	125	100	10	1
20	□	☑	MLD-Auto	0	2	125	100	10	1
32	□	☑	MLD-Auto	0	3	44	100	10	1
100	□	☑	MLD-Auto	0	2	125	100	10	1

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

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the button will update the displayed table starting from that or the next closest VLAN Table match.

The "**>>**" 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.

MLD Snooping VLAN Configuration

For MLD VLAN interface creation, you need to first go to Routing > IP > IP Configuration page to add the interface. Then, go to Switch > Layer 2 Multicast > MLD Snooping > Configure > VLAN Configuration to view the configuration results.

VLAN ID

The VLAN ID of the entry.

MLD Snooping Enabled

Enable the per-VLAN MLD Snooping. Up to 128 VLANs can be selected for MLD Snooping.

Querier Election

Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.

Compatibility

Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network.

The allowed selection is Auto, MLDv1, MLDv2, default compatibility value is Auto.

PRI

Priority of Interface.

It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic.

The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.

RV

Robustness Variable.

The Robustness Variable allows tuning for the expected packet loss on a link.

The allowed range is 2 to 255, default robustness variable value is 2.

QI (sec)

Query Interval.

The Query Interval is the interval between General Queries sent by the Querier.

The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.

QRI (0.1 sec)

Query Response Interval.

The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries.

The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (0.1 sec)

Last member query time.

The "Last Member Query Time" is the time value obtained by multiplying the "Last Member Query Interval" by the "Last Member Query Count." The allowed range is 0 to 31744 (in tenths of a second). The default "Last Member Query Interval" is 10 (which is 1 second).

URI (sec)

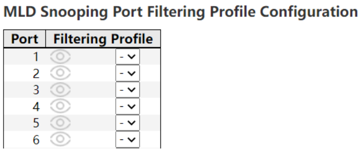
Unsolicited Report Interval.

The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address.

The allowed range is 1 to 31744 seconds, default unsolicited report interval is 1 second.

[Port Filtering Profile]

This page provides Port Filtering Profile related configuration.



MLD Snooping Port Filtering Profile Configuration

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

MLD Snooping Port Filtering Profile Configuration

Port

The logical port for the settings.

Filtering Profile

Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

Profile Management Button

You can inspect the rules of the designated profile by using the following button:

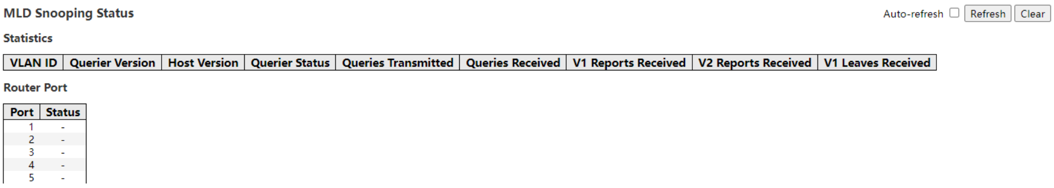
👁: List the rules associated with the designated profile.

Status

[Switching > L2-Multicast > MLD Snooping > Status]

[Status]

This page provides MLD Snooping status.



MLD Snooping Status

Auto-refresh □ Refresh Clear

Statistics

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

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-

MLD 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.

V1 Leaves Received

The number of Received V1 Leaves Reports.

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 MLD querier.

Static denotes the specific port is configured to be a router port.

Dynamic denotes the specific port is learnt to be a router port.

Both denote the specific port is configured or learnt to be a router port.

Port

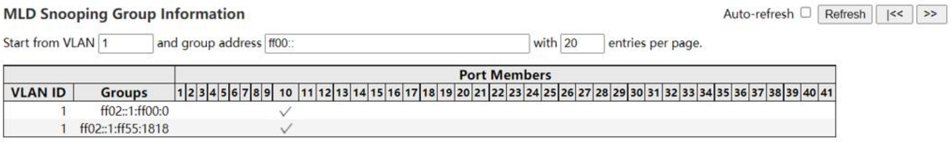
Switch port number.

Status

Indicate whether specific port is a router port or not.

[Groups Information]

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



MLD Snooping Group Information

Start from VLAN 1 and group address ff00:: with 20 entries per page.

		Port Members																																								
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
1	ff02::1:ff00:0										✓																															
1	ff02::1:ff55:1818										✓																															

Each page shows up to 99 entries from the MLD 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 MLD Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD Group Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MLD 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.

MLD Snooping Group Information

VLAN ID

VLAN ID of the group.

Groups

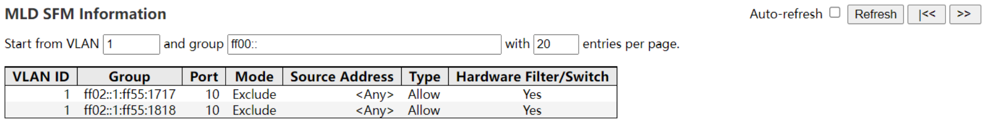
Group address of the group displayed.

Port Members

Ports under this group.

[IPv6 SFM Information]

This page shows the MLD registered multicast entries sorted by VLAN ID, group address, port number and source address.



MLD SFM Information

Start from VLAN 1 and group ff00:: with 20 entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
1	ff02::1:ff55:1717	10	Exclude	<Any>	Allow	Yes
1	ff02::1:ff55:1818	10	Exclude	<Any>	Allow	Yes

Each page shows up to 99 entries from the MLD 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 MLD SFM Information Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the MLD SFM Information Table. Clicking the Refresh button will update the displayed table starting from that or the closest next MLD 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 "**|<<**" button to start over.

MLD SFM Information Table

VLAN ID

VLAN ID of the group.

Group

Group address of the group displayed.

Port

Switch port number.

Mode

Each <VLAN ID, Group, Port> has a filter mode of either Include or Exclude, described further in section 7.2.1 of RFC3810.

Source Address

which matches on source addresses not already specified above its line. This is marked with " <Other>".

Currently, the maximum number of IPv6 source address per VLAN ID per group is 8.

Type

This field indicates whether the entry is forwarding (Allow) or blocking (Deny).

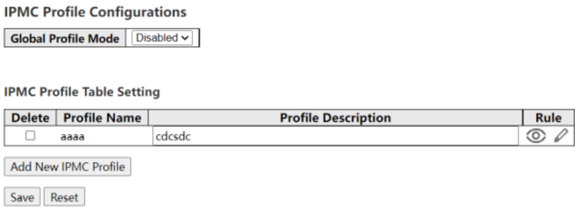
Hardware Filter/Switch

Shows whether blocking/forwarding of this entry is handled by hardware or not.

5.7.3. IPMC Profile

Profile Table

[Switching > L2-Multicast > IPMC Profile > Profile Table]



IPMC Profile Configurations

Global Profile Mode	Disabled

IPMC Profile Table Setting

Delete	Profile Name	Profile Description	Rule
□	aaaa	cdcsdc	

This page provides IPMC Profile related configurations.

The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each.

IPMC Profile Configurations

Global Profile Mode

Enable/Disable the Global IPMC Profile.

System starts to do filtering based on profile settings only when the global profile mode is enabled.

IPMC Profile Table Setting

Delete

Check to delete the entry.

The designated entry will be deleted during the next save.

Profile Name

The name used for indexing the profile table.

Each entry has a unique name.

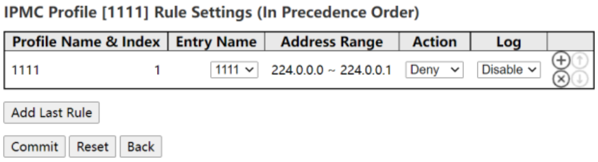
Profile Description

Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile.Rule.

When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons:

👁: List the rules associated with the designated profile.

✎: Adjust the rules associated with the designated profile.


IPMC Profile [1111] Rule Settings (In Precedence Order)

Profile Name & Index		Entry Name	Address Range	Action	Log
1111	1	1111	224.0.0.0 ~ 224.0.0.1	Deny	Disable

IPMC Profile [name] Rule Settings (In Precedence Order)

Profile Name & Index

The name used for indexing the profile table. Each entry has a unique name.

Entry Name

The name used for indexing the profile table.

Address Range

Multicast address range configured in the address entry.

Action

Can it be operated.

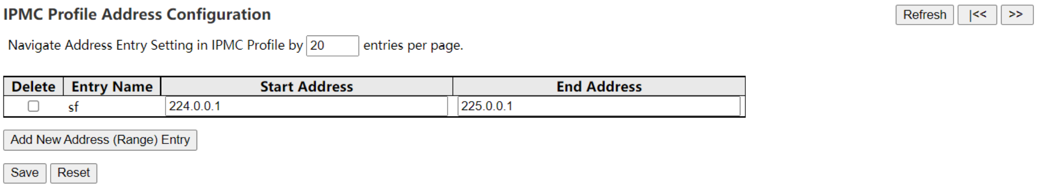
Log

Is logging turned on.

Address Entry

[Switching > L2-Multicast > IPMC Profile > Address Entry]

This page provides IPMC Profile related configurations.


IPMC Profile Address Configuration

Navigate Address Entry Setting in IPMC Profile by 20 entries per page.

Delete	Entry Name	Start Address	End Address
□	sf	224.0.0.1	225.0.0.1

The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with at maximum 128 corresponding rules for each.

IPMC Profile Address Configuration

Delete

Check to delete the entry.

The designated entry will be deleted during the next save.

Entry Name

The name used for indexing the address entry table.

Start Address

The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.

End Address

The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

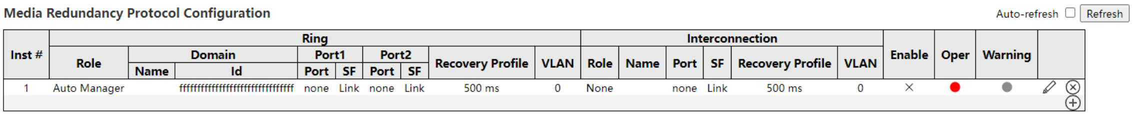
5.8. L2-Redundancy

5.8.1. MRP

[Switching > L2-Redundancy > MRP]

[Configuration]

The MRP instances are configured here.



Media Redundancy Protocol Configuration

Auto-refresh □ Refresh

Inst #	Ring									Interconnection						Enable	Oper	Warning	
	Role	Domain		Port1		Port2		Recovery Profile	VLAN	Role	Name	Port	SF	Recovery Profile	VLAN				
		Name	Id	Port	SF	Port	SF												
1	Auto Manager		ffffffffffffffffffffffffffffffff	none	Link	none	Link	500 ms	0	None		none	Link	500 ms	0	×	●	●	✎ ⊗ ⊕

Media Redundancy Protocol Configuration

Inst #

The MRP instance ID. Valid range 1 - 2.

Ring Role

Set the role of this node for this ring instance. Possible operations are:

•**mra**: Set this node to be a Media Redundancy Auto Manager (MRA) for this ring. Eventually it will become an MRM or MRC.

•**mrc**: Set this node to be a Media Redundancy Client (MRC) for this ring.

•**mrm**: Set this node to be the Media Redundancy Manager (MRM) for this ring.

Priority

Select the MRM/MRA priority. If role is 'mrm', valid values are 0x0000, 0x1000-0x7000, 0x8000. If role is 'mra', valid values are 0x9000-0xF000, 0xFFFF. Smaller values give higher priority.

Manager react on link change

Indicates whether the MRM reacts on MRP_LinkDown PDUs. Corresponds to the standard's MRP_REACT_ON_LINK_CHANGE.

Ring Domain Name

Set a domain name for this media-redundancy instance for easy identification.

Ring Domain Id

Set a UUID for this media-redundancy instance. Also used in PDUs.

OUI Type

Set the OUI used in MRP_Option TLVs. Possible operations are:

- **custom**: Use the following OUI in MRP_Option TLVs.
- **default**: Use the switch's own OUI in MRP_option TLVs.
- **siemens**: Use Siemens OUI (08-00-06) to get Wireshark to dissect MRP PDUs with MRP_option TLVs correctly.

OUI value

OUI to use in MRP_Option TLVs.

Ring Port 1

Assign an interface to ring port1.

Ring Port 2

Assign an interface to ring port2.

Ring Recovery Profile

Select a recovery profile, adhering to the timing parameters of Table 59 and 60 of IEC 62439-2:2016.

Ring VLAN

Set the media-redundancy instance's VLAN used in MRP PDUs transmitted on both ring ports. Use no-form to force untagged.

Enable

Enable or disable this media-redundancy instance.

Port1 SF Type

Choose whether port1's interface link state or a MEP installed on port1's interface is used as signal-fail trigger. Possible operations are:

- **link**: Port1's interface link state is used as signal-fail trigger.
- **mep**: A MEP installed on port1 is used as signal-fail trigger.

Port1 SF Domain

The MEP's domain.

Port1 SF Service

The MEP's service within the domain.

Port1 SF MEPID

The MEP's MEP-ID.

Interconnection Role

Set the interconnection role of this node for this ring instance.

Interconnection Mode

Set the interconnection mode of this node for this ring instance.

Interconnection Name

Set a domain name for this media-redundancy interconnection instance for easy identification.

Interconnection ID

Set an ID for this interconnection domain.

Interconnection Port

Assign an interface to the interconnection port.

Interconnection Recovery Profile

Select an interconnection recovery profile, adhering to the timing parameters of Table 61 and 62 of IEC 62439-2:2016.

Interconnection VLAN

Set the media-redundancy instance's VLAN used in MRP PDUs transmitted on the interconnection port. Use no-form to force untagged.

Interconnection SF Type

Choose whether the interconnection port's link state or a MEP installed on the interconnection port is used as signal-fail trigger. Possible operations are:

- **link**: Interconnection interface link state is used as signal-fail trigger.
- **mep**: A MEP installed on the interconnection port is used as signal-fail trigger.

Interconnection SF Domain

The MEP's domain.

Interconnection SF Service

The MEP's service within the domain.

Interconnection SF MEPID

The MEP's MEP-ID.

Modification icons

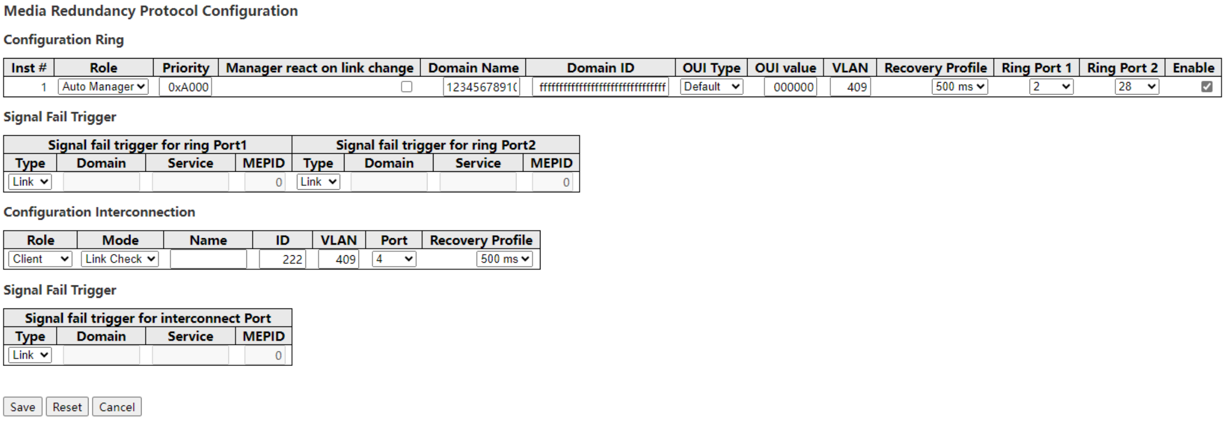
You can modify MRP in the table by using the following icons:

✎: Edits the MRP row.

⊗: Deletes the MRP.

⊕: Inserts a new MRP instance.

Click 🖉 and ⊕ at the icons bar to enter the following page:



Media Redundancy Protocol Configuration

Configuration Ring

Inst #	Role	Priority	Manager react on link change	Domain Name	Domain ID	OUI Type	OUI value	VLAN	Recovery Profile	Ring Port 1	Ring Port 2	Enable
1	Auto Manager	0xA000	□	1234567891(	ffffffffffffffffffffffffffffffff	Default	000000	409	500 ms	2	28	☑

Signal Fail Trigger

Signal fail trigger for ring Port1				Signal fail trigger for ring Port2			
Type	Domain	Service	MEPID	Type	Domain	Service	MEPID
Link			0	Link			0

Configuration Interconnection

Role	Mode	Name	ID	VLAN	Port	Recovery Profile
Client	Link Check		222	409	4	500 ms

Signal Fail Trigger

Signal fail trigger for interconnect Port			
Type	Domain	Service	MEPID
Link			0

Fill in configuration at every configuration and click Save at the bottom bar to save. Click Reset to revert to previously saved values. And click Cancel to go back to previous level page.

Media Redundancy Protocol Configuration

Configuration Ring

Inst #

The ID of the MRP instance. Click on link to get to detailed MRP instance page, where you can reset counters and issue commands.

Role

Set the role of this node for this ring instance. Possible operations are:

•**mra**: Set this node to be a Media Redundancy Auto Manager (MRA) for this ring. Eventually it will become an MRM or MRC.

•**mrc**: Set this node to be a Media Redundancy Client (MRC) for this ring.

•**mrm**: Set this node to be the Media Redundancy Manager (MRM) for this ring.

Priority

Select the MRM/MRA priority. If role is 'mrm', valid values are 0x0000, 0x1000-0x7000, 0x8000. If role is 'mra', valid values are 0x9000-0xF000, 0xFFFF. Smaller values give higher priority.

Manager react on link change

Indicates whether the MRM reacts on MRP_LinkDown PDUs. Corresponds to the standard's MRP_REACT_ON_LINK_CHANGE.

Domain Name

Set a domain name for this media-redundancy instance for easy identification.

Domain Id

Set a UUID for this media-redundancy instance. Also used in PDUs.

OUI Type

Set the OUI used in MRP_Option TLVs. Possible operations are:

•**custom**: Use the following OUI in MRP_Option TLVs.

•**default**: Use the switch's own OUI in MRP_option TLVs.

•**siemens**: Use Siemens OUI (08-00-06) to get Wireshark to dissect MRP PDUs with MRP_option TLVs correctly.

OUI value

Set the OUI used in MRP_Option TLVs. Possible operations are:

•**custom**: Use the following OUI in MRP_Option TLVs.

•**default**: Use the switch's own OUI in MRP_option TLVs.

•**siemens**: Use Siemens OUI (08-00-06) to get Wireshark to dissect MRP PDUs with MRP_option TLVs correctly.

VLAN

Set the media-redundancy instance's VLAN used in MRP PDUs transmitted on both ring ports. Use no-form to force untagged.

Recovery Profile

Select an interconnection recovery profile, adhering to the timing parameters of Table 61 and 62 of IEC 62439-2:2016.

Ring Port 1

Assign an interface to ring port1.

Ring Port 2

Assign an interface to ring port2.

Enable

Enable or disable this media-redundancy instance.

Signal Fail Trigger

Type

Choose whether port1's or port 2's interface link state or a MEP installed on port1's interface is used as signal-fail trigger. Possible operations are:

•**link**: Port1's interface link state is used as signal-fail trigger.

•**mep**: A MEP installed on port1 is used as signal-fail trigger.

Domain

The MEP's domain.

Service

The MEP's service within the domain.

MEPID

The MEP's MEP-ID.

Configuration Interconnection

Role

Set the interconnection role of this node for this ring instance.

Mode

Set the interconnection mode of this node for this ring instance.

Name

Set a domain name for this media-redundancy interconnection instance for easy identification.

ID

Set an ID for this interconnection domain.

VLAN

Set the media-redundancy instance's VLAN used in MRP PDUs transmitted on the interconnection port. Use no-form to force untagged.

Port

Assign an interface to the interconnection port.

Recovery Profile

Select an interconnection recovery profile, adhering to the timing parameters of Table 61 and 62 of IEC 62439-2:2016.

Signal Fail Trigger

Type

Choose whether the interconnection port's link state or a MEP installed on the interconnection port is used as signal-fail trigger. Possible operations are:

- **link**: Interconnection interface link state is used as signal-fail trigger.
- **mep**: A MEP installed on the interconnection port is used as signal-fail trigger.

Domain

The MEP's domain.

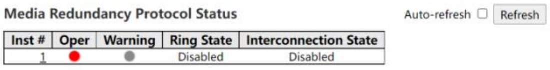
Service

The MEP's service within the domain.

MEPID

The MEP's MEP-ID.

[Status]



Media Redundancy Protocol Status

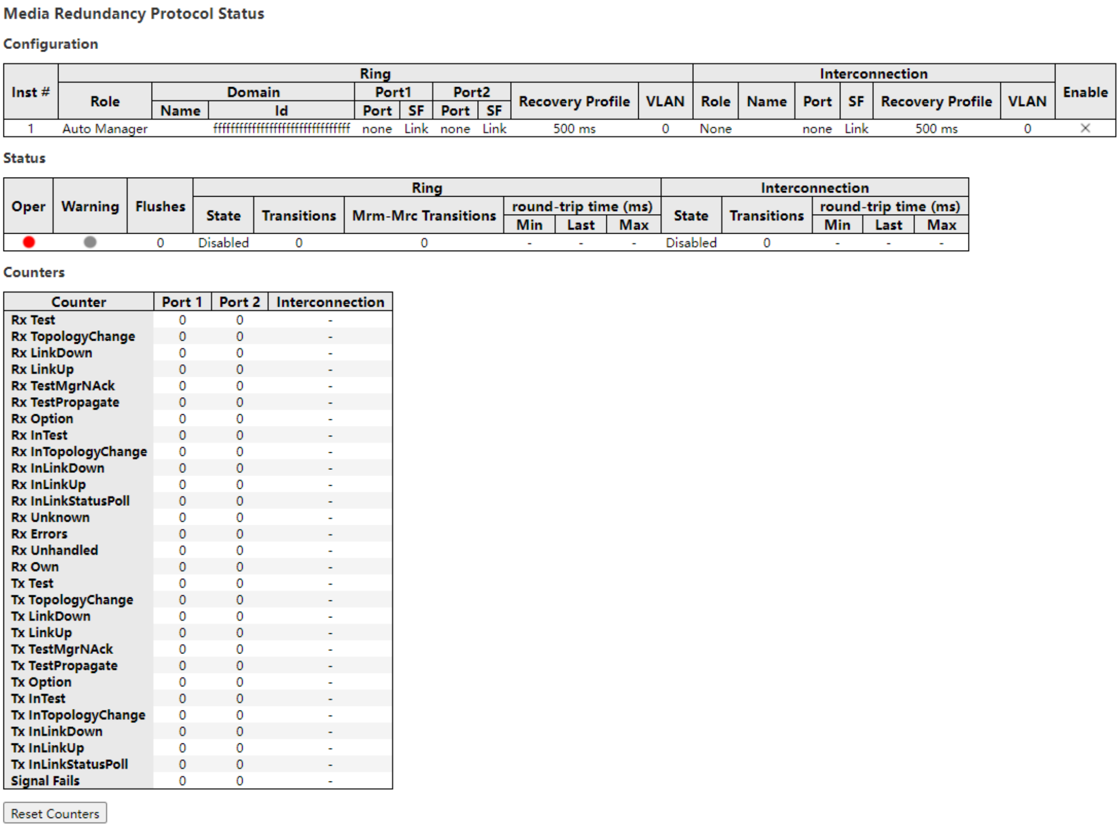
Inst #	Oper	Warning	Ring State	Interconnection State
1	🔴	●	Disabled	Disabled

Media Redundancy Protocol Status

Inst #

The ID of the MRP instance. Click on link to get to detailed MRP instance page, where you can reset counters and issue commands.

Click link at the Inst # to enter the following page to displaying MRP detailed status:



Media Redundancy Protocol Status

Configuration

Inst #	Ring									Interconnection						Enable
	Role	Domain		Port1		Port2		Recovery Profile	VLAN	Role	Name	Port	SF	Recovery Profile	VLAN	
		Name	Id	Port	SF	Port	SF									
1	Auto Manager		ffffffffffffffffffffffffffffffff	none	Link	none	Link	500 ms	0	None		none	Link	500 ms	0	×

Status

Oper	Warning	Flushes	Ring						Interconnection				
			State	Transitions	Mrm-Mrc Transitions	round-trip time (ms)			State	Transitions	round-trip time (ms)		
						Min	Last	Max			Min	Last	Max
🔴	●	0	Disabled	0	0	-	-	-	Disabled	0	-	-	-

Counters

Counter	Port 1	Port 2	Interconnection
Rx Test	0	0	-
Rx TopologyChange	0	0	-
Rx LinkDown	0	0	-
Rx LinkUp	0	0	-
Rx TestMgrNAck	0	0	-
Rx TestPropagate	0	0	-
Rx Option	0	0	-
Rx InTest	0	0	-
Rx InTopologyChange	0	0	-
Rx InLinkDown	0	0	-
Rx InLinkUp	0	0	-
Rx InLinkStatusPoll	0	0	-
Rx Unknown	0	0	-
Rx Errors	0	0	-
Rx Unhandled	0	0	-
Rx Own	0	0	-
Tx Test	0	0	-
Tx TopologyChange	0	0	-
Tx LinkDown	0	0	-
Tx LinkUp	0	0	-
Tx TestMgrNAck	0	0	-
Tx TestPropagate	0	0	-
Tx Option	0	0	-
Tx InTest	0	0	-
Tx InTopologyChange	0	0	-
Tx InLinkDown	0	0	-
Tx InLinkUp	0	0	-
Tx InLinkStatusPoll	0	0	-
Signal Fails	0	0	-

Media Redundancy Protocol Status

Configuration

Inst #

The ID of the MRP instance. Click on link to get to detailed MRP instance page, where you can reset counters and issue commands.

Role

Show the role of this node for this ring instance.

Domain Name

Show domain name for this media-redundancy instance for easy identification.

Domain Id

Show UUID for this media-redundancy instance. Also used in PDUs.

Port

Show Assign an interface to ring port1 or port 2.

SF

Show whether port1's or port2's interface link state or a MEP installed on port1's or port2's interface is used as signal-fail trigger.

Recovery Profile

Show a recovery profile.

VLAN

Show the media-redundancy instance's VLAN used in MRP PDUs transmitted on both ring ports. Use no-form to force untagged.

Role

Show the interconnection role of this node for this ring instance.

Name

Show domain name for this media-redundancy interconnection instance for easy identification.

Port

Show the interconnection port.

SF

Show whether the interconnection port's link state or a MEP installed on the interconnection port is used as signal-fail trigger.

Recovery Profile

Show an interconnection recovery profile.

VLAN

Show the media-redundancy instance's VLAN used in MRP PDUs transmitted on the interconnection port. Use no-form to force untagged.

Enable

Enable or disable this media-redundancy instance.

Status

Oper

The operational state of MRP instance.

🟢: Active.

🔴: Disabled or Internal error.

Warning

Operational warnings of MRP instance.

●: No warnings.

🟡: There are warnings.

Flushes

Displaying the status of clearing old and invalid MAC address table entries.

State

The status of this media-redundancy instance.

Ring Transitions

Displaying loop state transition: MRP adjusts its protocol operation state based on changes in network topology and link status to ensure that loops do not form.

Ring Mrm-Mrc Transitions

Displaying loop MRM-MRC transition: When the network structure or link status changes, devices may switch roles between MRM and MRC.

Ring round-trip time (ms) Min / Last / Max

Round-trip time represents the time required for a data packet to travel from the source node to the destination node and back to the source node. It includes the display of the maximum, minimum, and last round-trip times.

Interconnection State

The status of this interconnection instance.

Interconnection Transitions

Displaying the protocol transition achieved through interconnection between different network devices during the operation of the MRP protocol.

Interconnection round-trip time (ms) Min / Last / Max

Round-trip time represents the time required for a data packet to travel from the source node to the destination node and back to the source node. It includes the display of the maximum, minimum, and last round-trip times.

Counters

Rx / Tx Test

Count of received or sent Test messages.

Rx / Tx TopologyChange

Count of received or sent TopologyChange messages.

Rx / Tx LinkDown

Count of received or sent LinkDown messages.

Rx / Tx LinkUp

Count of received or sent LinkUp messages.

Rx / Tx TestMgrNAck

Count of received or sent TestMgrNAck messages.

Rx / Tx TestPropagate

Count of received or sent TestMgrNAck messages.

Rx / Tx Option

Count of received or sent Option messages.

Rx / Tx InTest

Count of received or sent InTest messages.

Rx / Tx InTopologyChange

Count of received or sent InTest messages.

Rx / Tx InLinkDown

Count of received or sent InLinkDown messages.

Rx / Tx InLinkUp

Count of received or sent InLinkUp messages.

Rx InLinkStatusPoll

Count of received InLinkStatusPoll messages.

Rx Unknown

Count of received Unknown messages.

Rx Errors

Count of received Errors messages.

Rx Unhandled

Count of received Unhandled messages.

Rx Own

Count of received Own messages.

Signal Fails

Number of local signal fails.

Oper

The operational state of MRP instance.

🟢: Active.

🔴: Disabled or Internal error.

Warning

Operational warnings of MRP instance.

●: No warnings.

🟡: There are warnings.

Ring State

Displays the loop detection enabled status.

Interconnection State

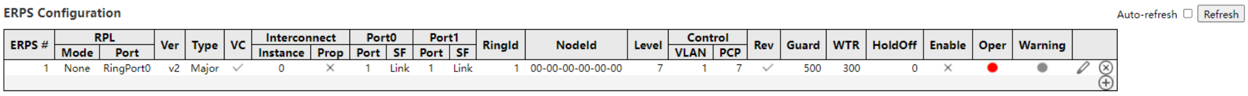
Displays the status of interconnected ports.

5.8.2. ERPS

[Switching > L2-Redundancy > ERPS]

[Configuration]

The ERPS instances are configured here.



ERPS Configuration

Auto-refresh ☐ Refresh

ERPS #	RPL		Ver	Type	VC	Interconnect		Port0		Port1		RingId	NodeId	Level	Control		Rev	Guard	WTR	HoldOff	Enable	Oper	Warning	
	Mode	Port				Instance	Prop	Port	SF	Port	SF				VLAN	PCP								
1	None	RingPort0	v2	Major	✓	0	×	1	Link	1	Link	1	00-00-00-00-00-00	7	1	7	✓	500	300	0	×	🔴	●	✎ ⊗
																								⊕

ERPS Configuration

ERPS #

The ID of ERPS. Valid range 1 - 64.

RPL Mode

Ring Protection Link mode. Possible values:

None: No protection ring mode.

Owner: Owner protection ring mode.

Neighbor: Neighbor protection ring mode.

RPL Port

Indicates whether it is port0 or port1 that is the Ring Protection Link. Not used if RPL Mode is none.

Ver

ERPS protocol version. v1 and v2 are supported.

Type

Type of ring. Possible values:

Major: ERPS major ring (G.8001-2016, clause 3.2.39).

Sub: ERPS sub-ring (G.8001-2016, clause 3.2.66).

InterSub: ERPS sub-ring on an interconnection node (G.8001-2016, clause 3.2.66).

VC

Controls whether to use a Virtual Channel with a sub-ring.

Interconnect Instance

For a sub-ring on an interconnection node, this must reference the instance ID of the ring to which this sub-ring is connected.

Interconnect Prop

Controls whether the ring referenced by Interconnect Instance shall propagate R-APS flush PDUs whenever this sub-ring's topology changes.

Port0/Port1 Interface

Interface index of ring protection Port0/Port1.

Port0/Port1 SF

Selects whether Signal Fail (SF) comes from the link state of a given interface, or from a Down-MEP. Possible values:

MEP: Down-MEP.

Link: Link.

Ring Id

The Ring ID is used - along with the control VLAN - to identify R-APS PDUs as belonging to a particular ring.

Node Id

The Node ID is used inside the R-APS specific PDU to uniquely identify this node (switch) on the ring.

Level

MD/MEG Level of R-APS PDUs we transmit.

Control VLAN

The VLAN on which R-APS PDUs are transmitted and received on the ring ports.

Control PCP

The PCP value used in the VLAN tag of the R-APS PDUs.

Rev

Revertive (true) or Non-revertive (false) mode.

Guard

Guard time in ms. Valid range is 10 - 2000 ms.

WTR

"Wait-to-Restore time in seconds. Valid range 1 - 720 sec.

Hold Off

Hold off time in ms. Value is rounded down to 100ms precision. Valid range is 0 - 10000 ms.

Enable

The administrative state of this APS ERPS. Check to make it function normally and uncheck to make it cease functioning.

Oper

The operational state of ERPS instance.

🟢: Active.

🔴: Disabled or Internal error.

Warning

Operational warnings of ERPS instance.

●: No warnings.

🟡: There are warnings.

Configuration Buttons

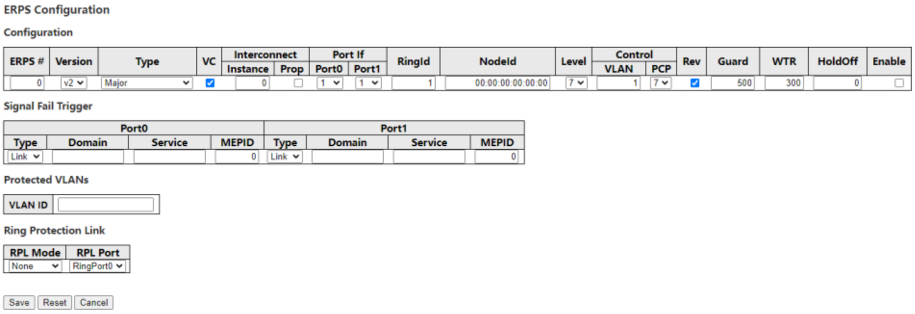
You can modify each ERPS in the table using the following buttons:

✎: Edits the ERPS row.

⊗: Deletes the ERPS.

⊕: Adds new ERPS.

Click ✎ and ⊕ at the configuration bar to enter the following page:



ERPS Configuration

Configuration

ERPS #	Version	Type	VC	Interconnect		Port If		RingId	NodeId	Level	Control		Rev	Guard	WTR	HoldOff	Enable
				Instance	Prop	Port0	Port1				VLAN	PCP					
0	v2	Major	☑	0	□	1	1	1	00:00:00:00:00:00	7	1	7	☑	500	300	0	□

Signal Fail Trigger

Port0				Port1			
Type	Domain	Service	MEPID	Type	Domain	Service	MEPID
Link			0	Link			0

Protected VLANs

VLAN ID	

Ring Protection Link

RPL Mode	RPL Port
None	RingPort0

ERPS Configuration

Configuration

ERPS #

The ID of ERPS. Valid range 1 - 64.

Version

ERPS protocol version. v1 and v2 are supported.

Type

Type of ring. Possible values:

Major: ERPS major ring (G.8001-2016, clause 3.2.39).

Sub: ERPS sub-ring (G.8001-2016, clause 3.2.66).

InterSub: ERPS sub-ring on an interconnection node (G.8001-2016, clause 3.2.66).

VC

Controls whether to use a Virtual Channel with a sub-ring.

Instance

For a sub-ring on an interconnection node, this must reference the instance ID of the ring to which this sub-ring is connected.

Prop

Controls whether the ring referenced by Interconnect Instance shall propagate R-APS flush PDUs whenever this sub-ring's topology changes.

Port#

Interface index of ring protection Port0/Port1.

RingId

The Ring ID is used - along with the control VLAN - to identify R-APS PDUs as belonging to a particular ring.

NodeId

The Node ID is used inside the R-APS specific PDU to uniquely identify this node (switch) on the ring.

Level

MD/MEG Level of R-APS PDUs we transmit.

VLAN

The VLAN on which R-APS PDUs are transmitted and received on the ring ports.

PCP

The PCP value used in the VLAN tag of the R-APS PDUs.

Rev

Revertive (true) or Non-revertive (false) mode.

Guard

Guard time in ms. Valid range is 10 - 2000 ms.

WTR

"Wait-to-Restore time in seconds. Valid range 1 - 720 sec.

HoldOff

Hold off time in ms. Value is rounded down to 100ms precision. Valid range is 0 - 10000 ms.

Enable

The administrative state of this APS ERPS. Check to make it function normally and uncheck to make it cease functioning.

Signal Fail Trigger

Type

Choose whether the interconnection port's link state or a MEP installed on the interconnection port is used as signal-fail trigger. Possible operations are:

- **link**: Interconnection interface link state is used as signal-fail trigger.
- **mep**: A MEP installed on the interconnection port is used as signal-fail trigger.

Domain

The MEP's domain.

Service

The MEP's service within the domain.

MEPID

The MEP's MEP-ID.

Protected VLANs

VLAN ID

VLAN ID.

Ring Protection Link

RPL Mode

Ring Protection Link mode. Possible values:

None: No protection ring mode.

Owner: Owner protection ring mode.

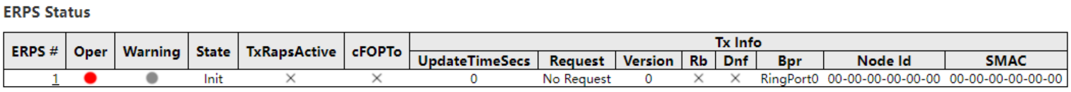
Neighbor: Neighbor protection ring mode.

RPL Port

Indicates whether it is port0 or port1 that is the Ring Protection Link. Not used if RPL Mode is None.

[Status]

This shows the current status of the ERPS instances.



ERPS Status

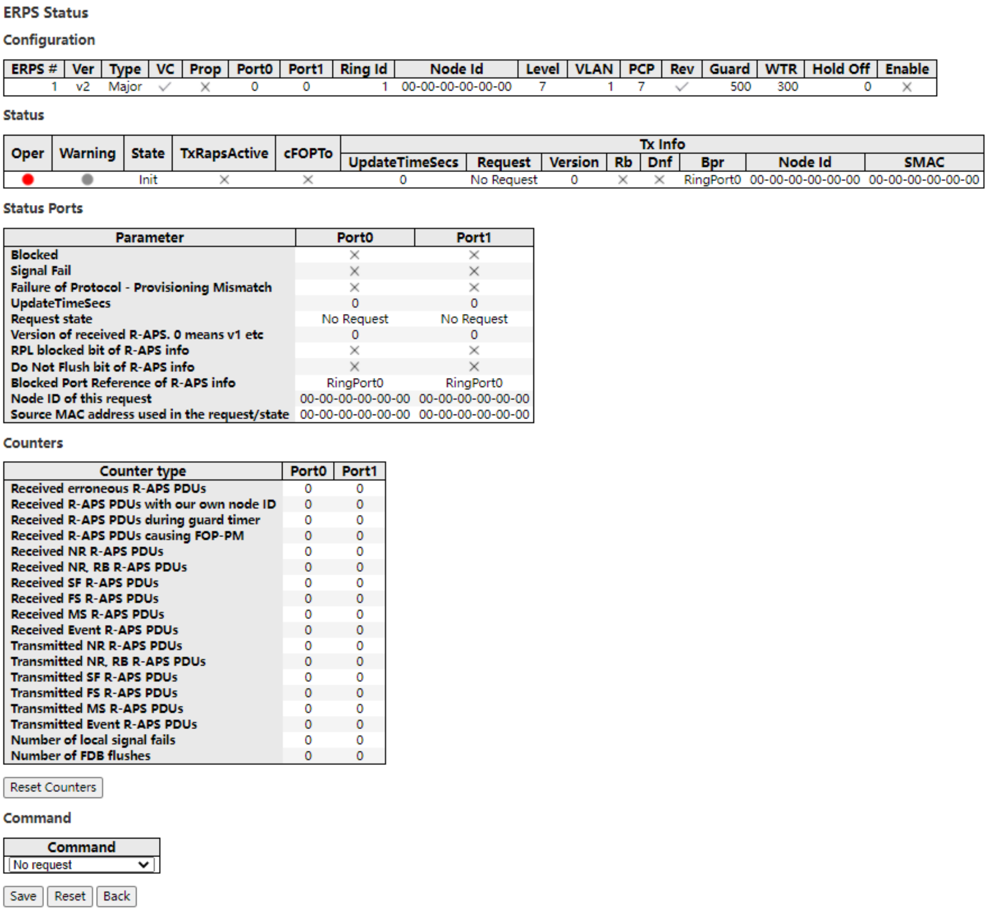
ERPS #	Oper	Warning	State	TxRapsActive	cFOPTo	Tx Info							
						UpdateTimeSecs	Request	Version	Rb	Dnf	Bpr	Node Id	SMAC
1	●	●	Init	×	×	0	No Request	0	×	×	RingPort0	00-00-00-00-00-00	00-00-00-00-00-00

ERPS Status

ERPS #

The ID of the ERPS. Click on link to get to ERPS detailed instance page, you can reset counters and issue commands.

Click on ERPS # can see the page as flows:



ERPS Status

Configuration

ERPS #	Ver	Type	VC	Prop	Port0	Port1	Ring Id	Node Id	Level	VLAN	PCP	Rev	Guard	WTR	Hold Off	Enable
1	v2	Major	✓	×	0	0	1	00-00-00-00-00-00	7	1	7	✓	500	300	0	×

Status

Oper	Warning	State	TxRapsActive	cFOPTo	Tx Info							
					UpdateTimeSecs	Request	Version	Rb	Dnf	Bpr	Node Id	SMAC
●	●	Init	×	×	0	No Request	0	×	×	RingPort0	00-00-00-00-00-00	00-00-00-00-00-00

Status Ports

Parameter	Port0	Port1
Blocked	×	×
Signal Fail	×	×
Failure of Protocol - Provisioning Mismatch	×	×
UpdateTimeSecs	0	0
Request state	No Request	No Request
Version of received R-APS. 0 means v1 etc	0	0
RPL blocked bit of R-APS info	×	×
Do Not Flush bit of R-APS info	×	×
Blocked Port Reference of R-APS info	RingPort0	RingPort0
Node ID of this request	00-00-00-00-00-00	00-00-00-00-00-00
Source MAC address used in the request/state	00-00-00-00-00-00	00-00-00-00-00-00

Counters

Counter type	Port0	Port1
Received erroneous R-APS PDUs	0	0
Received R-APS PDUs with our own node ID	0	0
Received R-APS PDUs during guard timer	0	0
Received R-APS PDUs causing FOP-PM	0	0
Received NR R-APS PDUs	0	0
Received NR, RB R-APS PDUs	0	0
Received SF R-APS PDUs	0	0
Received FS R-APS PDUs	0	0
Received MS R-APS PDUs	0	0
Received Event R-APS PDUs	0	0
Transmitted NR R-APS PDUs	0	0
Transmitted NR, RB R-APS PDUs	0	0
Transmitted SF R-APS PDUs	0	0
Transmitted FS R-APS PDUs	0	0
Transmitted MS R-APS PDUs	0	0
Transmitted Event R-APS PDUs	0	0
Number of local signal fails	0	0
Number of FDB flushes	0	0

Command

Command
No request

ERPS Status

Configuration

ERPS #

The ID of the ERPS.

Ver

ERPS protocol version. v1 and v2 are supported.

Type

Show the type of ring.

VC

Show whether to use a Virtual Channel with a sub-ring.

Prop

Show whether the ring referenced by Interconnect Instance shall propagate R-APS flush PDUs whenever this sub-ring's topology changes.

Port#

Interface index of ring protection Port0/Port1.

Ring Id

The Ring ID is used - along with the control VLAN - to identify R-APS PDUs as belonging to a particular ring.

Node Id

The Node ID is used inside the R-APS specific PDU to uniquely identify this node (switch) on the ring.

Level

MD/MEG Level of R-APS PDUs we transmit.

VLAN

The VLAN on which R-APS PDUs are transmitted and received on the ring ports.

PCP

The PCP value used in the VLAN tag of the R-APS PDUs.

Rev

Show Revertive (true) or Non-revertive (false) mode.

Guard

Guard time in ms. Valid range is 10 - 2000 ms.

WTR

"Wait-to-Restore time in seconds. Valid range 1 - 720 sec.

Hold Off

Hold off time in ms. Value is rounded down to 100ms precision. Valid range is 0 - 10000 ms.

Enable

The administrative state of this APS ERPS. Check to make it function normally and uncheck to make it cease functioning.

Status

Oper

The operational state of ERPS instance.

🟢: Active.

🔴: Disabled or Internal error.

Warning

Operational warnings of ERPS instance.

●: No warnings.

🟡: There are warnings.

State

Specifies protection/node state of ERPS.

TxRapsActive

Specifies whether we are currently supposed to be transmitting R-APS PDUs on our ring ports.

cFOPTo

Failure of Protocol - R-APS Rx Time Out.

UpdateTimeSecs

Time in seconds since boot that this structure was last updated.

Request

Request/state according to G.8032, table 10-3.

Version

Version of received/used R-APS Protocol. 0 means v1, 1 means v2, etc.

Rb

RB (RPL blocked) bit of R-APS info. See Figure 10-3 of G.8032.

Dnf

DNF (Do Not Flush) bit of R-APS info. See Figure 10-3 of G.8032.

Bpr

BPR (Blocked Port Reference) of R-APS info. See Figure 10-3 of G.8032.

Node Id

Node ID of this request.

SMAC

The Source MAC address used in the request/state.

Status Ports

Parameter

Include Blocked, Signal Fail Failure of Protocol - Provisioning Mismatch, UpdateTimeSecs, Request state, Version of received R-APS. 0 means v1 etc, RPL blocked bit of R-APS info, Do Not Flush bit of R-APS info, Blocked Port Reference of R-APS info, Node ID of this request, Source MAC address used in the request/state.

Port #

The status or count of the parameters corresponding to port 1 and port 0.

Counters

Counter type

Include Received erroneous R-APS PDUs, Received R-APS PDUs with our own node ID, Received R-APS PDUs during guard timer, Received R-APS PDUs causing FOP-PM, Received NR R-APS PDUs, Received NR, RB R-APS PDUs, Received SF R-APS PDUs, Received FS R-APS PDUs, Received MS R-APS PDUs, Received Event R-APS PDUs, Transmitted NR R-APS PDUs, Transmitted NR, RB R-APS PDUs, Transmitted SF R-APS PDUs, Transmitted FS R-APS PDUs, Transmitted MS R-APS PDUs, Transmitted Event R-APS PDUs, Number of local signal fails, Number of FDB flushes.

Port #

The count of the parameters corresponding to port 1 and port 0.

Command

Command

The selectable parameters are: No request, Force switch Port0, Force switch Port1, Manual switch to Port0, Manual switch to Port1, Clear.

Oper

The operational state of ERPS instance.

🟢: Active.

🔴: Disabled or Internal error.

Warning

Operational warnings of ERPS instance.

●: No warnings.

🟡: There are warnings, use tooltip to see.

State

Specifies protection/node state of ERPS.

TxRapsActive

Specifies whether we are currently supposed to be transmitting R-APS PDUs on our ring ports.

cFOPTo

Failure of Protocol - R-APS Rx Time Out.

UpdateTimeSecs

Time in seconds since boot that this structure was last updated.

Request

Request/state according to G.8032, table 10-3.

Version

Version of received/used R-APS Protocol. 0 means v1, 1 means v2, etc.

Rb

RB (RPL blocked) bit of R-APS info. See Figure 10-3 of G.8032.

Dnf

DNF (Do Not Flush) bit of R-APS info. See Figure 10-3 of G.8032.

Bpr

BPR (Blocked Port Reference) of R-APS info. See Figure 10-3 of G.8032.

Node Id

Node ID of this request.

SMAC

The Source MAC address used in the request/state.

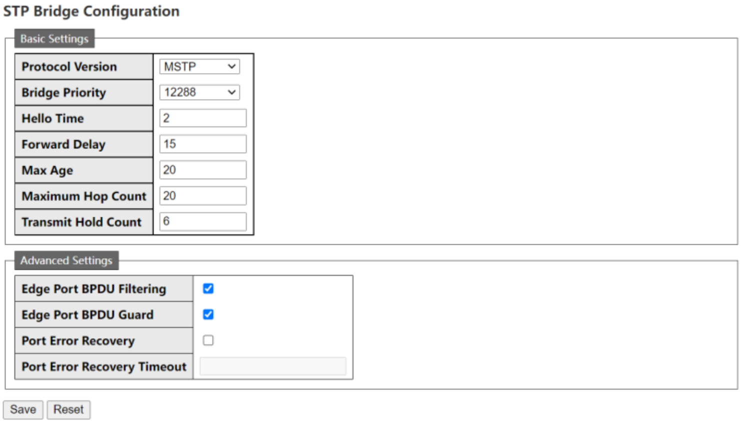
5.8.3. Spanning Tree

Global

[Switching > L2-Redundancy > Spanning Tree > Global]

[Bridge Settings]

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



STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Bridge Priority	12288
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

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

Basic Settings

Protocol Version

The MSTP/RSTP/STP protocol version setting. Valid values are MSTP, RSTP and STP.

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.

Advanced Settings

Edge Port BPDU Filtering

Control whether a port explicitly configured as Edge will transmit and receive BPDUs.

Edge Port BPDU Guard

Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state, and will be removed from the active topology.

Port Error Recovery

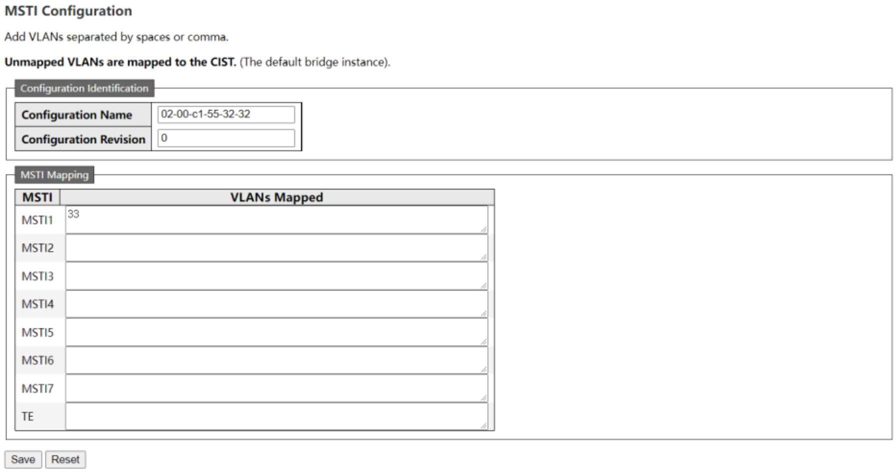
Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

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 (24hours).

[MSTI Mapping]

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



MSTI Configuration

Add VLANs separated by spaces or comma.

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

Configuration Identification

Configuration Name	02-00-c1-55-32-32
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	33
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	
TE	

Configuration Identification

Configuration Name

The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

Configuration Revision

The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI Mapping

MSTI

The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

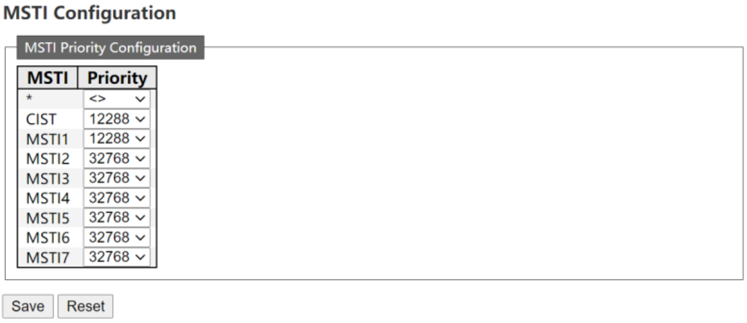
Note: The TE (Traffic Engineering) instance is special, as it will not be controlled by MSTP itself. The TE instance will always be forwarding for all ports. The TE-MSTID is defined by IEEE 802.1Q-2018.

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.

[MSTI Priorities]

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



MSTI Configuration

MSTI Priority Configuration

MSTI	Priority
*	<>
CIST	12288
MSTI1	12288
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

MSTI Priority Configuration

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.

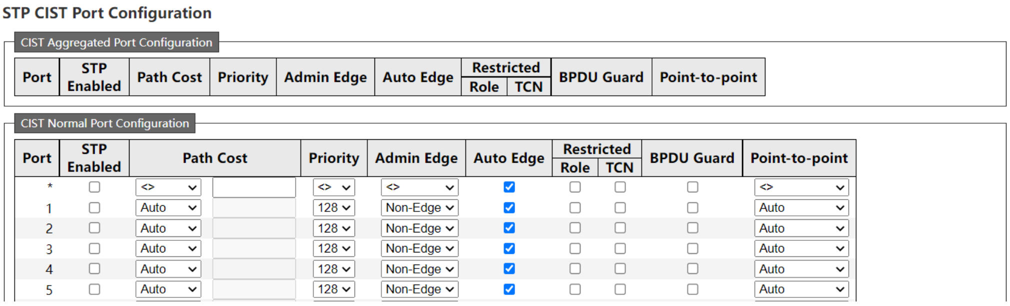
Ports

[Switching > L2-Redundancy > Spanning Tree > Ports]

[CIST Ports]

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

This page contains settings for physical and aggregated ports.



STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
						Role	TCN		

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
							Role	TCN		
*	□	<>		<>	<>	☑	□	□	□	<>
1	□	Auto		128	Non-Edge	☑	□	□	□	Auto
2	□	Auto		128	Non-Edge	☑	□	□	□	Auto
3	□	Auto		128	Non-Edge	☑	□	□	□	Auto
4	□	Auto		128	Non-Edge	☑	□	□	□	Auto
5	□	Auto		128	Non-Edge	☑	□	□	□	Auto

STP CIST Port Configuration

Port

The switch port number of the logical STP port.

STP Enabled

Controls whether STP is enabled on this switch port.

Path Cost

Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in 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).

Lower priority is better.

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 Switching > L2 Redundancy > Spanning Tree >Status > 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.

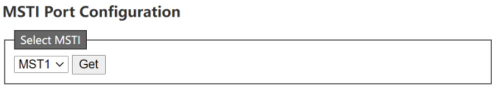
A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

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.

[MSTI Ports]

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

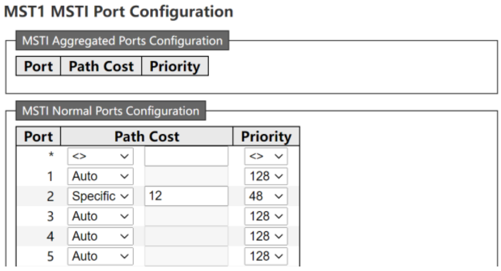


MSTI Port Configuration

Select MSTI

MST1 Get

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



MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost	Priority

MSTI Normal Ports Configuration

Port	Path Cost		Priority
*	<>		<>
1	Auto		128
2	Specific	12	48
3	Auto		128
4	Auto		128
5	Auto		128

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.

MSTI Port Configuration

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

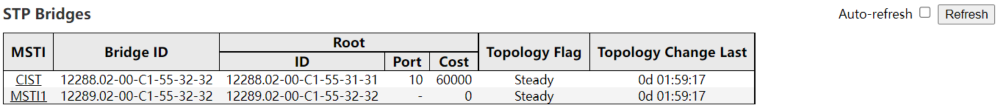
Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). Lower priority is better.

Status

[Switching > L2-Redundancy > Spanning Tree > Status]

[Bridge Status]

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



STP Bridges

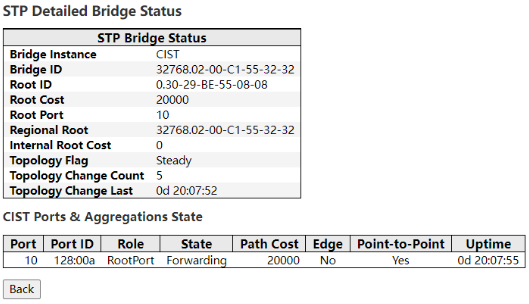
MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	12288.02-00-C1-55-32-32	12288.02-00-C1-55-31-31	10	60000	Steady	0d 01:59:17
MSTI1	12289.02-00-C1-55-32-32	12289.02-00-C1-55-32-32	-	0	Steady	0d 01:59:17

STP Bridge Status

MSTI

The Bridge Instance. This is also a link to the STP Detailed Bridge Status.

Click on Multiple Instance Generation Tree Protocol, and the following page appears.



STP Detailed Bridge Status

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.02-00-C1-55-32-32
Root ID	0.30-29-BE-55-08-08
Root Cost	20000
Root Port	10
Regional Root	32768.02-00-C1-55-32-32
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	5
Topology Change Last	0d 20:07:52

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
10	128:00a	RootPort	Forwarding	20000	No	Yes	0d 20:07:55

STP Detailed Bridge Status

Bridge Instance

The Bridge Instance.

Bridge ID

The Bridge ID of this Bridge instance.

Root ID

The Bridge ID of the currently elected root bridge.

Root Cost

Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Root Port

The switch port currently assigned the root port role.

Regional Root

Keep the value consistent with the Bridge ID.

Internal Root Cost

Root Path Cost. For the Root Bridge it 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 Count

The number of topology changes of this bridge instance.

Topology Change Last

The time since last Topology Change occurred.

CIST Ports & Aggregations State

Port

The port number of the switch where the physical STP port is located.

Port ID

CIST Port ID.

Role

When the limit role is enabled, the port is displayed as a Root Port or a Backup Port.

State

The port status has the following states: Forwarding, Discarding, and Learning.

Path Cost

Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Edge

The bridge edge detection result is displayed. The operEdge status is shown based on whether BPDU is received on the port.

Point-to-Point

Whether the port is connected to a point-to-point LAN rather than a shared medium. This can be automatically determined or forced to true or false.

Uptime

The time since the last initialization of the self-bridging port.

Bridge ID

The Bridge ID of this Bridge instance.

Root ID

The Bridge ID of the currently elected root bridge.

Root Port

The switch port currently assigned the root port role.

Root Cost

Root Path Cost. For the Root Bridge it 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

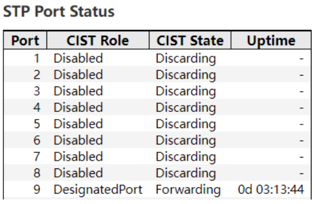
The current state of the Topology Change Flag of this Bridge instance.

Topology Change Last

The time since last Topology Change occurred.

[Port Status]

This page displays the STP CIST port status for physical ports of the switch.



STP Port Status

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	DesignatedPort	Forwarding	0d 03:13:44

STP Port Status

Port

The switch port number of the logical STP port.

CIST Role

The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort, BackupPort, RootPort, DesignatedPort, Disabled.

CIST State

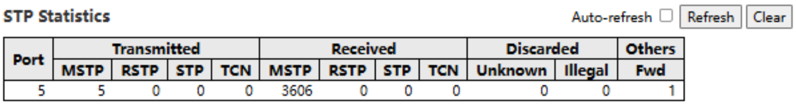
The current STP port state of the CIST port. The port state can be one of the following values: Discarding Learning Forwarding.

Uptime

The time since the bridge port was last initialized.

[Port Statistics]

This page displays the STP port statistics counters of bridge ports in the switch.



STP Statistics

Port	Transmitted				Received				Discarded		Others
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal	Fwd
5	5	0	0	0	3606	0	0	0	0	0	1

STP Port Statistics

Port

The switch port number of the logical STP port.

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.

Others Fwd

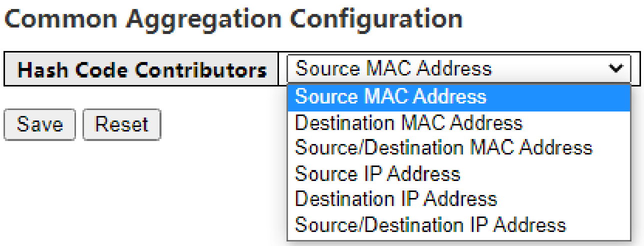
Number of forwarding packets.

5.8.4. Aggregation

Common

[Switching > L2-Redundancy > Aggregation > Common]

This page is used to configure the Aggregation hash mode. This mode applies to the whole network element.



Common Aggregation Configuration

Hash Code Contributors: Source MAC Address

Common Aggregation Configuration

Hash Code Contributors

Source MAC Address：The Source MAC address can be used to calculate the destination port for the frame.

Destination MAC Address：The Destination MAC address can be used to calculate the destination port for the frame.

Source/Destination MAC Address：The Source and Destination MAC addresses can be used to calculate the destination port for the frame. This is the default option.

Source IP Address：The Source IP address can be used to calculate the destination port for the frame.

Destination IP Address：The Destination IP address can be used to calculate the destination port for the frame.

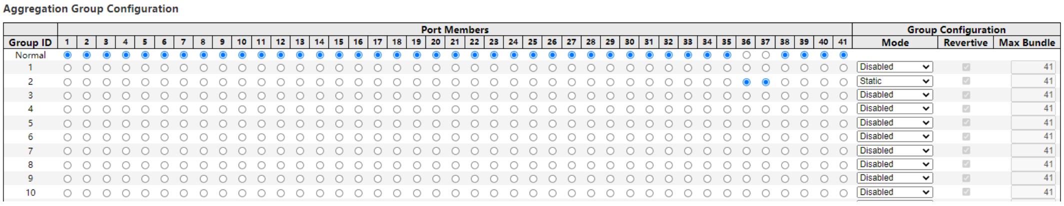
Source/Destination IP Address：The Source and Destination IP addresses can be used to calculate the destination port for the frame.

Groups

[Switching > L2-Redundancy > Aggregation > Groups]

[Configuration]

This page is used to configure the aggregation groups.



Aggregation Group Configuration

	Port Members																																								Group Configuration		
Group ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	Mode	Revertive	Max Bundle
Normal	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	○	○	●	●	●	●			
1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	Disabled	☑	41
2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●	○	○	○	○	Static	☑	41
3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	Disabled	☑	41
4	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	Disabled	☑	41
5	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	Disabled	☑	41
6	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	Disabled	☑	41
7	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	Disabled	☑	41
8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	Disabled	☑	41
9	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	Disabled	☑	41
10	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	Disabled	☑	41

Aggregation Group Configuration

Group ID

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

Port Members

Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

Mode

This parameter determines the mode for the aggregation group.

Disabled: The group is disabled.

Static: The group operates in Static aggregation mode.

LACP (Active): The group operates in LACP active aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details.

LACP (Passive): The group operates in LACP passive aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for details.

Revertive

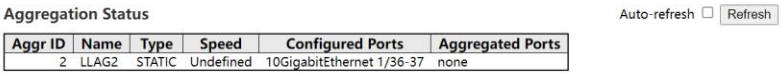
This parameter only applies to LACP-enabled groups. It determines if the group will perform automatic link (re-)calculation when links with higher priority becomes available.

Max Bundle

This parameter only applies to LACP-enabled groups. It determines the maximum number of active bundled LACP ports allowed in an aggregation.

[Status]

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



Aggregation Status

Aggr ID	Name	Type	Speed	Configured Ports	Aggregated Ports
2	LLAG2	STATIC	Undefined	10GigabitEthernet 1/36-37	none

Aggregation 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

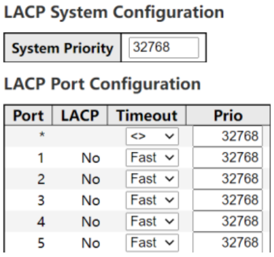
Aggregated member ports of the Aggregation group.

LACP

[Switching > L2-Redundancy > Aggregation > LACP]

[Configuration]

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



LACP System Configuration

System Priority	32768

LACP Port Configuration

Port	LACP	Timeout	Prio
*		<>	32768
1	No	Fast	32768
2	No	Fast	32768
3	No	Fast	32768
4	No	Fast	32768
5	No	Fast	32768

LACP System Configuration

System Priority

The Prio controls the priority of the system, range 1-65535.

LACP Port Configuration

Port

The switch port number.

LACP

Show whether LACP is currently enabled on this switch port.

Timeout

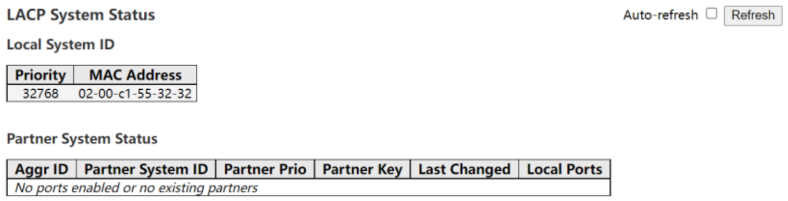
The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.

Prio

The Prio controls the priority of the 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.

[System Status]

This page provides a status overview for the system-level LACP information.



LACP System Status

Local System ID

Priority	MAC Address
32768	02-00-c1-55-32-32

Partner System Status

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

Local System ID

Priority

The local system priority which forms the local LACP System ID.

MAC Address

The local system MAC address which forms the local LACP System ID.

Partner System Status

This table display the partner system information for each LACP aggregation group.

Aggr ID

The Aggregation ID associated with this aggregation instance.

Partner System ID

The system ID (MAC address) of the aggregation partner.

Partner Prio

The priority that the partner has assigned to this aggregation ID.

Partner Key

The Key that the partner has assigned to this aggregation ID.

Last Changed

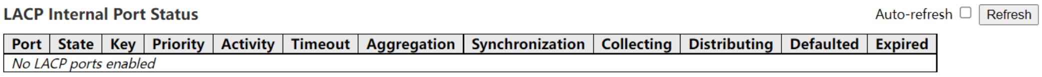
The time since this aggregation changed.

Local Ports

Shows which ports are a part of this aggregation for this switch.

[Internal Status]

This page provides a status overview for the LACP internal (i.e. local system) status for all ports.



LACP Internal Port Status

Port	State	Key	Priority	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
No LACP ports enabled											

Only ports that are part of an LACP group are shown.

For details on the shown parameters please refer to IEEE 801.AX-2014.

LACP Internal Port Status

Port

The switch port number.

State

The current port state:

Down: The port is not active.

Active: The port is in active state.

Standby: The port is in standby state.

Key

The key assigned to this port. Only ports with the same key can aggregate together.

Priority

The priority assigned to this aggregation group.

Activity

The LACP mode of the group (Active or Passive).

Timeout

The timeout mode configured for the port (Fast or Slow).

Aggregation

Show whether the system considers this link to be "aggregateable"; i.e., a potential candidate for aggregation.

Synchronization

Show whether the system considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.

Collecting

Show if collection of incoming frames on this link is enabled.

Distributing

Show if distribution of outgoing frames on this link is enabled.

Defaulted

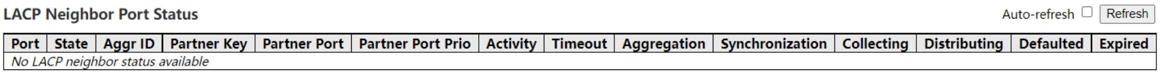
Show if the Actor's Receive machine is using Defaulted operational Partner information.

Expired

Show if that the Actor's Receive machine is in the EXPIRED state.

[Neighbor Status]

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



LACP Neighbor Port Status

Auto-refresh □ Refresh

Port	State	Aggr ID	Partner Key	Partner Port	Partner Port Prio	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
No LACP neighbor status available													

Only ports that are part of an LACP group are shown.

For details on the shown parameters please refer to IEEE 801.AX-2014.

LACP Neighbor Port Status

Port

The switch port number.

State

The current port state:

Down: The port is not active.

Active: The port is in active state.

Standby: The port is in standby state.

Aggr ID

The aggregation group ID which the port is assigned to.

Partner Key

The key assigned to this port by the partner.

Partner Port

The partner port number associated with this link.

Partner Port Priority

The priority assigned to this partner port.

Activity

The LACP mode of the group (Active or Passive).

Timeout

The timeout mode configured for the partner port (Fast or Slow).

Aggregation

Show whether the partner considers this link to be "aggregateable"; i.e., a potential candidate for aggregation.

Synchronization

Show whether the partner considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.

Collecting

Show if collection of incoming frames on this link is enabled.

Distributing

Show if distribution of outgoing frames on this link is enabled.

Defaulted

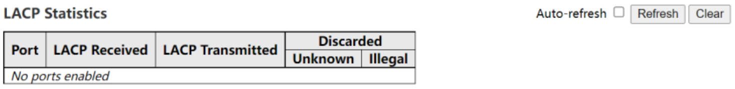
Show if the partners Receive machine is using Defaulted operational Partner information.

Expired

Show if that the partners Receive machine is in the EXPIRED state.

[Port Statistics]

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



LACP Statistics

Auto-refresh □ Refresh Clear

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
No ports enabled				

LACP Statistics

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

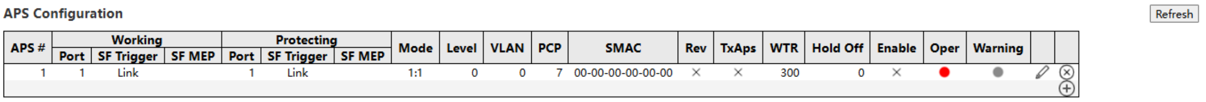
Shows how many unknown or illegal LACP frames have been discarded at each port.

5.8.5. APS

[Switching > L2-Redundancy > APS]

[Configuration]

This page allows the user to create and configure an APS Instance.



APS Configuration

Refresh

APS #	Working			Protecting			Mode	Level	VLAN	PCP	SMAC	Rev	TxAps	WTR	Hold Off	Enable	Oper	Warning		
	Port	SF Trigger	SF MEP	Port	SF Trigger	SF MEP														
1	1	Link		1	Link		1:1	0	0	7	00-00-00-00-00-00	×	×	300	0	×	●	●	✎	⊗
																				⊕

APS Configuration

The APS module implements the protocol and linear protection switching mechanisms for point-to-point VLAN-based ETH SNC in Ethernet transport networks. Automatic Protection Switching is defined by the ITU G.8031 standard.

APS #

The ID of the APS. Maximum number of creatable APS instances is 26 . Click on link to get to APS instance page, you can reset counters and issue commands.

Port

The Port this flow is attached to.

SF Trigger

Selects whether Signal Fail (SF) comes from the link state of a given Port, or from a Down-MEP.

SF MEP

The Domain::Service::MEPID refers to a MEP instance which shall represent the Working flow. Only used when SF Trigger is MEP. The selected MEP instance does not need to exist when this APS is configured.

Mode

1:1 This will create a 1:1 APS.

In the linear 1:1 protection switching architecture, the protection transport entity is dedicated to the working transport entity. However, the normal traffic is transported either on the working transport entity or on the protection transport entity using a selector bridge at the source of the protected domain. The selector at the sink of the protected domain selects the entity which carries the normal traffic.

1+1 Uni This will create a 1+1 Unidirectional APS.

1+1 Bi This will create a 1+1 Bidirectional APS.

In the linear 1+1 protection switching architecture, a protection transport entity is dedicated to each working transport entity. The normal traffic is copied and fed to both working and protection transport entities with a permanent bridge at the source of the protected domain. The traffic on working and protection transport entities is transmitted simultaneously to the sink of the protected domain, where a selection between the working and protection transport entities is made based on some predetermined criteria, such as server defect indication.

Level

MD/MEG Level (0-7).

VLAN

The VLAN ID used in the L-APS PDUs. 0 means untagged.

PCP

PCP (priority) (default 7). The PCP value used in the VLAN tag unless the L-APS PDU is untagged. Must be a value in range 0 - 7.

SMAC

Source MAC address used in L-APS PDUs. Must be a unicast address. If all-zeros, the switch port's MAC address will be used.

Rev

When checked, the port recovery mode is revertive, that is, traffic switches back to the working port after the condition(s) causing a switch has cleared. In the case of clearing a command (e.g. forced switch), this happens immediately. In the case of clearing of a defect, this generally happens after the expiry of the WTR (Wait-To-Restore) timer.

When unchecked, the port recovery mode is non-revertive and traffic is allowed to remain on the protect port after a switch reason has cleared.

TxAps

Choose whether this end transmits APS PDUs. Only used for 1+1, unidirectional.

WTR

When Rev is checked, WTR (Wait-To-Restore) tells how many seconds to wait before restoring to the working port after a fault condition has cleared. Valid range 1 - 720.

Hold Off

When a new (or more severe) defect occurs, the hold-off timer will be started and the event will be reported after the timer expires. HoldOff time is measured in milliseconds, and valid values are in the range 0 - 10000. Default is 0, which means immediate reporting of the defect.

Enable

The administrative state of this APS instance. Check to make it function normally and uncheck to make it cease functioning.

Oper

This field can not be configured, but shows the operational state. You can click on the link in the APS # field to get more details on the status.

🟢: APS instance is functional.

🔴: APS instance is not functional.

Warning

If the operational state is Active, the APS instance is indeed active, but it may be that it doesn't run as the administrator thinks, because of configuration errors, which are reflected in the warnings below.

The Warning information is indicated by

●: no warning.

🟡: warning.

Use the tooltip to get the detailed warning information.

Configuration Buttons

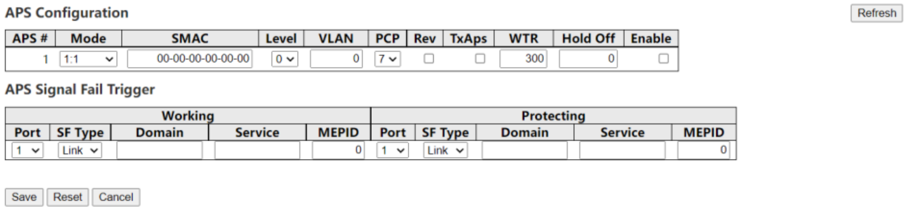
You can modify each APS in the table using the following buttons:

✎: Edits the APS row.

⊗: Deletes the APS.

⊕: Adds new APS.

Click ✎ and ⊕ at the configuration bar to enter the following page:



APS Configuration

APS #	Mode	SMAC	Level	VLAN	PCP	Rev	TxAps	WTR	Hold Off	Enable
1	1:1	00-00-00-00-00-00	0	0	7	□	□	300	0	□

APS Signal Fail Trigger

Working					Protecting				
Port	SF Type	Domain	Service	MEPID	Port	SF Type	Domain	Service	MEPID
1	Link			0	1	Link			0

APS Configuration

APS #

The ID of the APS. Maximum number of creatable APS instances is 26 . Click on link to get to APS instance page, you can reset counters and issue commands.

Mode

1:1 This will create a 1:1 APS.

In the linear 1:1 protection switching architecture, the protection transport entity is dedicated to the working transport entity. However, the normal traffic is transported either on the working transport entity or on the protection transport entity using a selector bridge at the source of the protected domain. The selector at the sink of the protected domain selects the entity which carries the normal traffic.

1+1 Uni This will create a 1+1 Unidirectional APS.

1+1 Bi This will create a 1+1 Bidirectional APS.

In the linear 1+1 protection switching architecture, a protection transport entity is dedicated to each working transport entity. The normal traffic is copied and fed to both working and protection transport entities with a permanent bridge at the source of the protected domain. The traffic on working and protection transport entities is transmitted simultaneously to the sink of the protected domain, where a selection between the working and protection transport entities is made based on some predetermined criteria, such as server defect indication.

SMAC

Source MAC address used in L-APS PDUs. Must be a unicast address. If all-zeros, the switch port's MAC address will be used.

Level

MD/MEG Level (0-7).

VLAN

The VLAN ID used in the L-APS PDUs. 0 means untagged.

PCP

PCP (priority) (default 7). The PCP value used in the VLAN tag unless the L-APS PDU is untagged. Must be a value in range 0 - 7.

Rev

When checked, the port recovery mode is revertive, that is, traffic switches back to the working port after the condition(s) causing a switch has cleared. In the case of clearing a command (e.g. forced switch), this happens immediately. In the case of clearing of a defect, this generally happens after the expiry of the WTR (Wait-To-Restore) timer.

When unchecked, the port recovery mode is non-revertive and traffic is allowed to remain on the protect port after a switch reason has cleared.

TxAps

Choose whether this end transmits APS PDUs. Only used for 1+1, unidirectional.

WTR

When Rev is checked, WTR (Wait-To-Restore) tells how many seconds to wait before restoring to the working port after a fault condition has cleared. Valid range 1 - 720.

HoldOff

When a new (or more severe) defect occurs, the hold-off timer will be started and the event will be reported after the timer expires. HoldOff time is measured in milliseconds, and valid values are in the range 0 - 10000. Default is 0, which means immediate reporting of the defect.

Enable

The administrative state of this APS instance. Check to make it function normally and uncheck to make it cease functioning.

APS Signal Fail Trigger

Port

The Port this flow is attached to.

SF Type

Selects whether Signal Fail (SF) comes from the link state of a given Port, or from a Down-MEP.

Domain

The name of the domain where this service is located.

Service

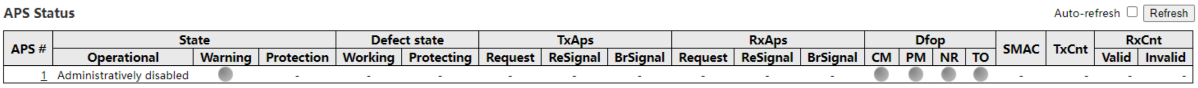
The value is a single word that starts with a letter (A-Z or a-z) and has a length of 1 to 15 characters.

MEPID

The Domain::Service::MEPID refers to a MEP instance which shall represent the Working flow. Only used when SF Trigger is MEP. The selected MEP instance does not need to exist when this APS is configured.

[Status]

This shows the current status of the APS instances.



APS Status

Auto-refresh □ Refresh

APS #	State			Defect state		TxAps			RxAps			Dfop				SMAC	TxCnt	RxCnt	
	Operational	Warning	Protection	Working	Protecting	Request	ReSignal	BrSignal	Request	ReSignal	BrSignal	CM	PM	NR	TO			Valid	Invalid
1	Administratively disabled	●	-	-	-	-	-	-	-	-	-	●	●	●	●	-	-	-	-

APS Status

APS #

The ID of the APS. Click on link to get to APS instance page, you can reset counters and issue commands.

State, Operational

The operational state of the APS instance. There are many ways to not have the instance active. Each of them has its own value. Only when the state is Active, will the APS instance be active and up and running. If the Operational state is not "Active", the remaining fields are invalid. The possible values of this field are shown below:

Administratively disabled: Instance is inactive, because it is administratively disabled.

Active: The instance is active and up and running.

Internal Error: Instance is inactive, because an internal error has occurred.

Working MEP not Found: Instance is inactive, because the Working MEP is not found.

Protecting MEP not Found: Instance is inactive, because the Protecting MEP is not found.

Working MEP is not administrative active: Instance is inactive, because the Working MEP is not admin enabled.

Protecting MEP is not administrative active: Instance is inactive, because the Protecting MEP is not admin enabled.

Working MEP is not a Down MEP: Instance is inactive, because the Working MEP is not a Down-MEP.

Protecting MEP is not a Down MEP: Instance is inactive, because the Protecting MEP is not a Down-MEP.

Working and Protecting MEP use the same interface: Instance is inactive, because both Working and Protecting MEPs use the same I/F.

Another instance use the same Working port: Instance is inactive, because another instance uses the same Working port.

State, Warning

If the operational state is Active, the APS instance is indeed active, but it may be that it doesn't run as the administrator thinks, because of configuration errors, which are reflected in the warnings below.

The Warning information is indicated by

●: no warning.

🟡: warning.

Use the tooltip to get the detailed warning information.

State, Protection

The possible protection group states. The letters refers to the state as described in G.8031 Annex.

No request Working: A

No request Protecting: B

Lockout: C

Forced Switch: D

Signal fail Working: E

Signal fail Protecting: F

Manual switch to Protecting: G

Manual switch to Working: H

Wait to restore: I

Do not revert: J

Exercise Working: K

Exercise Protecting: L

Reverse request Working: M

Reverse request Protecting: N

Signal degrade Working: P

Signal degrade Protecting: Q

Defect state, Working, Protection

The possible values of this field are shown below:

ok: The port defect state is OK.

sd: The port defect state is Signal Degrade.

sf: The port defect state is Signal Fail.

TxAps, RxAps - Request

The possible transmitted or received APS request according to G.8031, Table 11-1.

nr: No Request.

dnr: Do Not Revert.

rr: Reverse Request.

exer: Exercise.

wtr: Wait-To-Restore.

ms: Manual Switch.

sd: Signal Degrade.

sfW: Signal Fail for Working.

fs: Forced Switch.

sfP: Signal Fail for Protect.

lo: Lockout.

TxAps, ReSignal

Transmitted requested signal according to G.8031 figure 11-2.

TxAps, BrSignal

Transmitted bridged signal according to G.8031 figure 11-2.

RxAps, ReSignal

Received requested signal according to G.8031 figure 11-2.

RxAps, BrSignal

Received bridged signal according to G.8031 figure 11-2.

Dfop

Dfop is "Failure of Protocol defect" and the presence of a defect is indicated by up: no defect, down: defect.

CM: Configuration Mismatch (received APS PDU on working interface within last 17.5 seconds).

PM: Provisioning Mismatch (far and near ends are not using the same mode; bidir only).

NR: No Response (far end hasn't agreed on 'Requested Signal' within 50 ms; bidir only).

TO: Time Out (near end hasn't received a valid APS PDU within last 17.5 seconds; bidir only).

SMAC

Source MAC address of last received APS PDU or all-zeros if no PDU has been received.

TxCnt

Number of APS PDU frames transmitted.

RxCnt, Valid

Number of valid APS PDU frames received on the protect port.

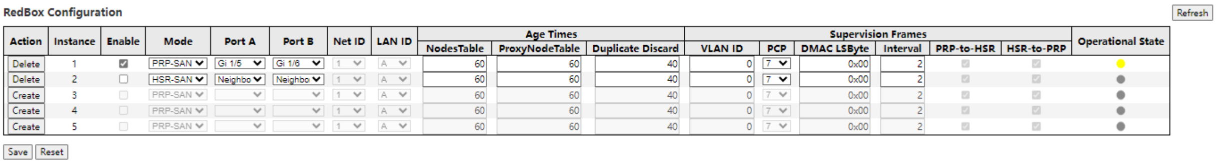
RxCnt, Invalid

Number of invalid APS PDU frames received on the protect port.

5.8.6. RedBox

RedBox

[Switching > L2-Redundancy > RedBox > RedBox]



RedBox Configuration

Action	Instance	Enable	Mode	Port A	Port B	Net ID	LAN ID	Age Times			Supervision Frames						Operational State
								NodesTable	ProxyNodeTable	Duplicate Discard	VLAN ID	PCP	DMAC LSByte	Interval	PRP-to-HSR	HSR-to-PRP	
Delete	1	☑	PRP-SAN	Gi 1/5	Gi 1/6	1	A	60	60	40	0	7	0x00	2	☑	☑	●
Delete	2	□	HSR-SAN	Neighbo	Neighbo	1	A	60	60	40	0	7	0x00	2	☑	☑	●
Create	3	□	PRP-SAN			1	A	60	60	40	0	7	0x00	2	☑	☑	●
Create	4	□	PRP-SAN			1	A	60	60	40	0	7	0x00	2	☑	☑	●
Create	5	□	PRP-SAN			1	A	60	60	40	0	7	0x00	2	☑	☑	●

RedBox Configuration

Action

Control whether the instance is created or deleted.

Instance

RedBox instance number.

Enable

Enable RedBox instance.

Mode

There are four modes: PRP-SAN, HSR-SAN, HSR-PRP, and HSR-HSR.

Port #

Interface index of port A or B.

Net ID

NetId used to filter frames in HSR-PRP and HSR-HSR modes.

LAN ID

LanId used to filter frames in HSR-PRP mode.

Age Times NodesTable

Number of seconds without activity before a remote node is removed from the NodesTable.

Age Times ProxyNodeTable

Number of seconds without activity before a proxy node is removed from the ProxyNodeTable.

Age Times Duplicate Discard

Number of milliseconds that an entry is considered a duplicate.

Supervision Frames VLAN ID

VLAN ID on which supervision PDUs are transmitted on port A and port B. Use 0 to indicate the interlink port's native VLAN (Port VLAN ID).

Supervision Frames PCP

PCP value used in the VLAN tag of supervision PDUs transmitted on port A and port B.

Supervision Frames DMAC LSByte

Least significant byte of destination MAC address used in supervision frames transmitted on port A and port B.

Supervision Frames Interval

Number of seconds between transmission of supervision frames.

Supervision Frames PRP-to-HSR

Enable proxy-translation of supervision frames from HSR ring to PRP network (HSR-PRP mode only).

Supervision Frames HSR-to-PRP

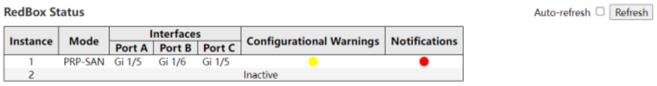
Enable proxy-translation of supervision frames from PRP network to HSR ring (HSR-PRP mode only).

Operational State

Operational state of this RedBox instance.

Status

[Switching > L2-Redundancy > RedBox > Status]



RedBox Status

Instance	Mode	Interfaces			Configurational Warnings	Notifications
		Port A	Port B	Port C		
1	PRP-SAN	Gi 1/5	Gi 1/6	Gi 1/5	●	●
2	Inactive					

RedBox Status

Instance

RedBox instance number.

Mode

There are four modes: PRP-SAN, HSR-SAN, HSR-PRP, and HSR-HSR.

Interfaces Port #

Interface index of port A or B.

Configurational Warnings

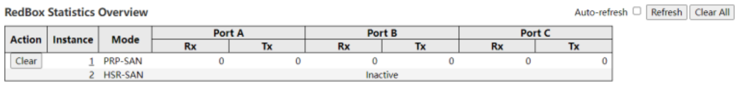
Display whether there is a configuration warning.

Notifications

Display whether there are notifications, such as warnings, etc.

Statistics

[Switching > L2-Redundancy > RedBox > Statistics]



RedBox Statistics Overview

Action	Instance	Mode	Port A		Port B		Port C	
			Rx	Tx	Rx	Tx	Rx	Tx
Clear	1	PRP-SAN	0	0	0	0	0	0
	2	HSR-SAN	Inactive					

RedBox Statistics Overview

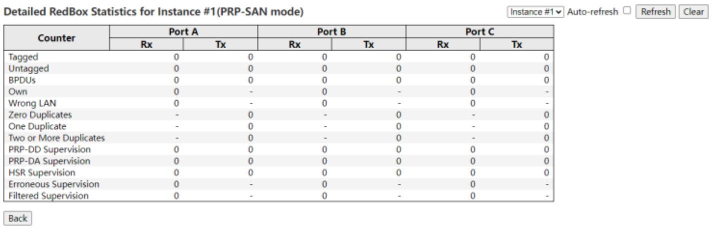
Action

Clear statistics.

Instance

RedBox instance number.

Click the instance number to display the following page:



Detailed RedBox Statistics for Instance #1(PRP-SAN mode)

Counter	Port A		Port B		Port C	
	Rx	Tx	Rx	Tx	Rx	Tx
Tagged	0	0	0	0	0	0
Untagged	0	0	0	0	0	0
BPDUs	0	0	0	0	0	0
Own	0	-	0	-	0	-
Wrong LAN	0	-	0	-	0	-
Zero Duplicates	-	0	-	0	-	0
One Duplicate	-	0	-	0	-	0
Two or More Duplicates	-	0	-	0	-	0
PRP-DD Supervision	0	0	0	0	0	0
PRP-DA Supervision	0	0	0	0	0	0
HSR Supervision	0	0	0	0	0	0
Erroneous Supervision	0	-	0	-	0	-
Filtered Supervision	0	-	0	-	0	-

Counter

Tagged : Number of HSR- and/or PRP-tagged frames received or transmitted on port.

Untagged : Number of frames received or transmitted on port that are neither HSR- nor PRP-tagged.

BPDUs : Number of link-local (BPDUs) received or transmitted on port.

Own : Number of HSR-tagged frames received on port whose SMAC appears in the ProxyNodeTable).

Wrong LAN : Number of frames received on port with wrong LanId.

Zero Duplicates : Number of frames transmitted on port without any duplicates seen.

One Duplicate : Number of frames transmitted on port with one duplicate discarded.

Two or More Duplicates : Number of frames transmitted on port with two or more duplicates discarded.

PRP-DD Supervision : Number of PRP-DD supervision frames transmitted on port.

PRP-DA Supervision : Number of PRP-DA supervision frames transmitted on port.

HSR Supervision : Number of HSR supervision frames transmitted on port.

Erroneous Supervision : Number of Erroneous supervision frames transmitted on port.

Filtered Supervision : Number of Filtered supervision frames transmitted on port.

Mode

There are four modes: PRP-SAN, HSR-SAN, HSR-PRP, and HSR-HSR.

Port # Rx

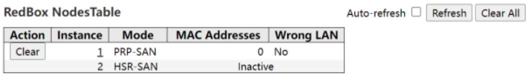
Receive count of ports A, B, and C.

Port # Tx

Transmit count of ports A, B, and C.

NodesTable

[Switching > L2-Redundancy > RedBox > NodesTable]



RedBox NodesTable

Auto-refresh □ Refresh Clear All

Action	Instance	Mode	MAC Addresses	Wrong LAN
Clear	1	PRP-SAN	0	No
	2	HSR-SAN	Inactive	

RedBox NodesTable

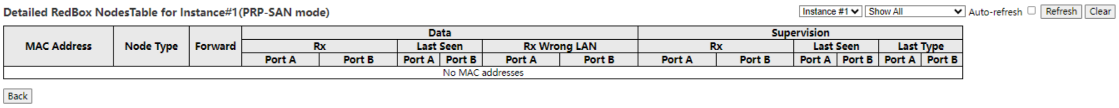
Action

Clear statistics.

Instance

RedBox instance number.

Click the instance number to display the following page:



Detailed RedBox NodesTable for Instance#1(PRP-SAN mode)

Instance #1 Show All Auto-refresh □ Refresh Clear

MAC Address	Node Type	Forward	Data						Supervision					
			Rx		Last Seen		Rx Wrong LAN		Rx		Last Seen		Last Type	
			Port A	Port B	Port A	Port B	Port A	Port B	Port A	Port B	Port A	Port B	Port A	Port B
No MAC addresses														

Back

Node Type

Node type.

Forwarded

Indicates whether the a frame from switch core will be forwarded on %s (PRP-SAN mode only).

Data (Rx)

Number of frames received on port.

Data (Last Seen)

Number of seconds since this MAC address was last seen on port.

Data (Rx Wrong LAN)

True if at least one MAC address in the NodesTable has a non-zero Rx Wrong LAN count (PRP-SAN mode only).

Supervision (Rx)

Number of valid supervision frames received on port.

Supervision (Last Seen)

Number of seconds since a supervision frame was last seen on port.

Supervision (Last Type)

The supervision frame type last received on port.

Mode

There are four modes: PRP-SAN, HSR-SAN, HSR-PRP, and HSR-HSR.

MAC Addresses

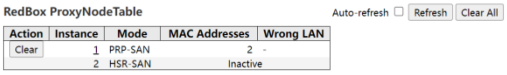
MAC address in NodesTable.

Wrong LAN

Number of frames received on port A or port B with wrong LanId.

ProxyNodeTable

[Switching > L2-Redundancy > RedBox > ProxyNodeTable]



RedBox ProxyNodeTable

Auto-refresh □ Refresh Clear All

Action	Instance	Mode	MAC Addresses	Wrong LAN
Clear	1	PRP-SAN	2	-
	2	HSR-SAN	Inactive	

RedBox ProxyNodeTable

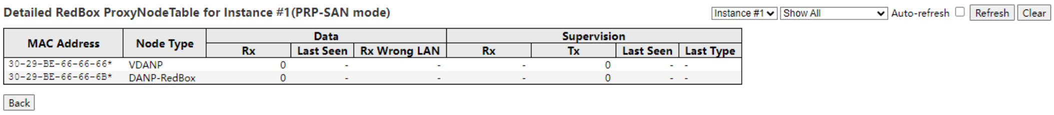
Action

Clear statistics.

Instance

RedBox instance number.

Click the instance number to display the following page:



Detailed RedBox ProxyNodeTable for Instance #1(PRP-SAN mode)

Instance #1 Show All Auto-refresh □ Refresh Clear

MAC Address	Node Type	Data			Supervision			
		Rx	Last Seen	Rx Wrong LAN	Rx	Tx	Last Seen	Last Type
30-29-BE-66-66-66*	VDANP	0	-	-	-	0	-	-
30-29-BE-66-66-6B*	DANP-RedBox	0	-	-	-	0	-	-

Back

Node Type

Node type.

Data (Rx)

Number of frames received on port.

Data (Last Seen)

Number of seconds since this MAC address was last seen on port.

Data (Rx Wrong LAN)

True if at least one MAC address in the ProxyNodeTable has a non-zero Rx Wrong LAN count (PRP-SAN mode only).

Supervision (Rx)

Number of valid supervision frames received on port.

Supervision (Tx)

Number of valid supervision frames transmitted on port.

Supervision (Last Seen)

Number of seconds since a supervision frame was last seen on port.

Supervision (Last Type)

The supervision frame type last received on port.

Mode

There are four modes: PRP-SAN, HSR-SAN, HSR-PRP, and HSR-HSR.

MAC Addresses

MAC address in ProxyNodeTable.

Wrong LAN

Number of frames received on port A or port B with wrong LanId.

6. Routing

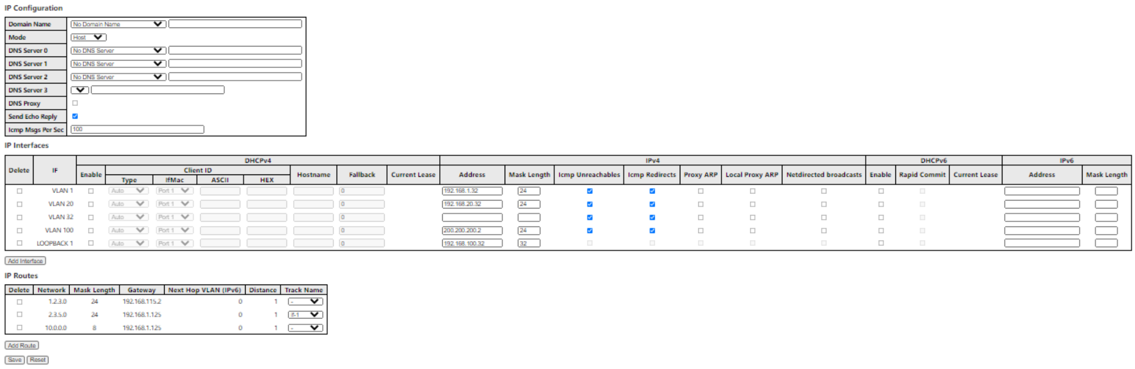
The menu contains the following dialogs:

IP
IRDP
RIP
OSPF
OSPFv3
Tracking
Multicast Routing
L3-Redundancy
Access-list
Prefix-list

6.1. IP

[Routing > IP]

[IP configuration]



IP Configuration

Domain Name	No Domain Name
Mode	Host
DNS Server 0	No DNS Server
DNS Server 1	No DNS Server
DNS Server 2	No DNS Server
DNS Server 3	
DNS Proxy	☐
Send Echo Reply	☑
Icmp Msgs Per Sec	100

IP Interfaces

Delete	IF	DHCPv4								IPv4							DHCPv6			IPv6	
		Enable	Client ID				Hostname	Fallback	Current Lease	Address	Mask Length	Icmp Unreachables	Icmp Redirects	Proxy ARP	Local Proxy ARP	Netdirected broadcasts	Enable	Rapid Commit	Current Lease	Address	Mask Length
			Type	IfMac	ASCII	HEX															
☐	VLAN 1	☐	Auto	Port 1				0		192.168.1.32	24	☑	☑	☐	☐	☐	☐	☐			
☐	VLAN 20	☐	Auto	Port 1				0		192.168.20.32	24	☑	☑	☐	☐	☐	☐	☐			
☐	VLAN 32	☐	Auto	Port 1				0				☑	☑	☐	☐	☐	☐	☐			
☐	VLAN 100	☐	Auto	Port 1				0		200.200.200.2	24	☑	☑	☐	☐	☐	☐	☐			
☐	LOOPBACK 1	☐	Auto	Port 1				0		192.168.100.32	32	☐	☐	☐	☐	☐	☐	☐			

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN (IPv6)	Distance	Track Name
☐	1.2.3.0	24	192.168.115.2	0	1	-
☐	2.3.5.0	24	192.168.1.125	0	1	tt-1
☐	10.0.0.0	8	192.168.1.125	0	1	-

IP Configuration

Domain Name

The name string of local domain where the device belongs.

Most queries for names within this domain can use short names relative to the local domain. The system then appends the domain name as a suffix to unqualified names.

For example, if domain name is set as 'example.com' and you specify the PING destination by the unqualified name as 'test', then the system will qualify the name to be 'test.example.com'. The following modes are supported:

No Domain Name: No domain name will be used.

Configured Domain Name: Explicitly specify the name of local domain. Make sure the configured domain name meets your organization's given domain.

From any DHCPv4 interfaces: The first domain name offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.

From this DHCPv4 interface: Specify from which DHCPv4-enabled interface a provided Domain Name should be preferred.

From any DHCPv6 interfaces: The first domain name offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used.

From this DHCPv6 interface: Specify from which DHCPv6-enabled interface a provided Domain Name should be preferred.

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.

DNS Server

This setting controls the DNS name resolution done by the switch. There are three servers available for configuration, and the index of the server presents the preference (less index has higher priority) in doing DNS name resolution. The following modes are supported:

No DNS server: No DNS server will be used.

Configured IPv4 or IPv6: Explicitly provide the valid IPv4 or IPv6 unicast address of the DNS Server in dotted decimal notation. Make sure the configured DNS server could be reachable (e.g. via PING or PING6) for activating DNS service.

From any DHCPv4 interface: The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.

From this DHCPv4 interface: Specify from which DHCPv4-enabled interface a provided DNS server should be preferred.

From any DHCPv6 interface: The first DNS server offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used.

From this DHCPv6 interface: Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.

DNS Proxy

When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network. Only IPv4 DNS proxy is now supported.

Send Echo Reply

Send icmp reply packet.

Icmp Msgs Per Sec

Send icmp packet rate.The default icmp send packet rate is 100pps.

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 Enable

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.

IPv4 DHCP Client Identifier Type

This specified which of the three type below, i.e. IfMac, ASCII or HEX, shall be used for the Client Identifier. See RFC-2132 section 9.14.

IPv4 DHCP Client Identifier IfMac

The interface name of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ifmac', the configured interface's hardware MAC address will be used in the DHCP option 61 field.

IPv4 DHCP Client Identifier ASCII

The ASCII string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ascii', the ASCII string will be used in the DHCP option 61 field.

IPv4 DHCP Client Identifier HEX

The hexadecimal string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type 'hex', the hexadecimal value will be used in the DHCP option 61 field.

IPv4 DHCP Hostname

The hostname of DHCP client. If DHCPv4 client is enabled, the configured hostname will be used in the DHCP option 12 field. When this value is empty string, the field use the configured system name plus the latest three bytes of system MAC addresses as the hostname.

IPv4 DHCP Fallback Timeout:

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

IPv4 DHCP Current Lease

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

IPv4 Address

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 an 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.

Icmp Unreachables

Send icmp unreachables packet. The default icmp unreachables send packet rate is 100pps.

Icmp Redirects

Enable the icmp redirects by checking this box. If this option is enabled, the device sends icmp redirects packet. The default is enabled.

Proxy ARP

Enable the Proxy ARP by checking this box. If this option is enabled, The communication between different vlans is enabled. The default is disabled.

Local Proxy ARP

Enable the Local Proxy ARP by checking this box. If this option is enabled, The communication between different ports under the same vlan is enabled.The default is disabled.

Netdirected broadcasts

Enable the netdirected broadcasts by checking this box. If this option is enabled, the device sends to the network broadcast address of a network to contact every receiver of the network. The default is disabled.

IPv6 DHCP Enable

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

IPv6 DHCP Rapid Commit

Accelerate the speed at which clients obtain network configuration. This is achieved by reducing the number of exchanges required between the client and the DHCP server, resulting in faster address allocation and configuration.

IPv6 DHCP Current Lease

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

IPv6 Address

The IPv6 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 IPv6 operation on the interface is not desired - or no DHCP fallback address is desired.

IPv6 Mask Length

The IPv6 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for an IPv6 address. If DHCP is enabled, this field configures the fallback address network mask. The field may be left blank if IPv6 operation on the interface is not desired - or no DHCP fallback address is desired.

IP Routes

Delete

Select this option to delete an existing IP route.

Network

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 0.0.0.0 or 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

Distance

The distance value of the route entry is used to provide the priority information of the routing protocols to routers. When two or more different routing protocols are involved and have the same destination, the distance value can be used to select the best path.

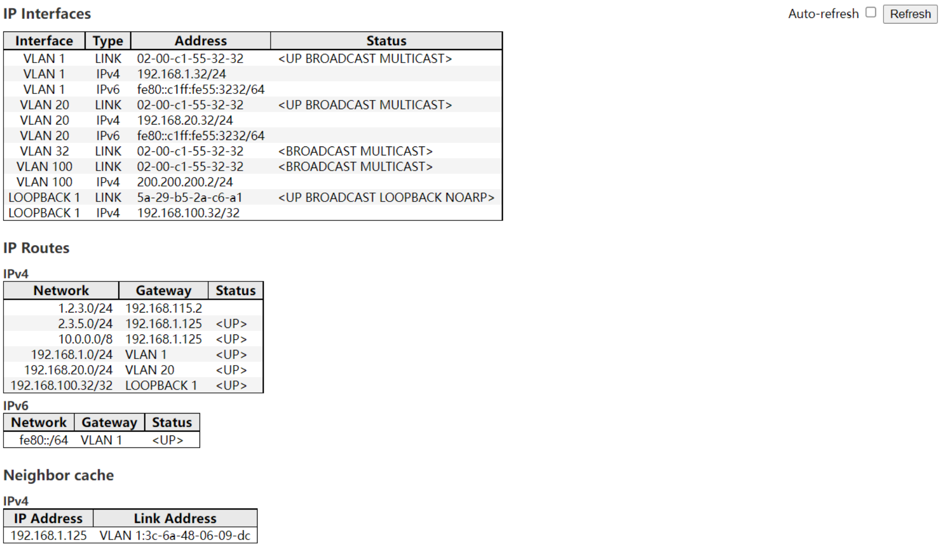
Track Name

Configure the Static route tracking.

Note: Currently, only one LOOPBACK port is supported for configuration, so only input 1 is currently supported after LOOPBACK. Configure Address and Mask Length under IPV4; The other columns' LOOPBACK do not currently support configuration.

[IP Status]

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IPv6 routes and the neighbour cache (ARP cache) status.



IP Interfaces

Interface	Type	Address	Status
VLAN 1	LINK	02-00-c1-55-32-32	<UP BROADCAST MULTICAST>
VLAN 1	IPv4	192.168.1.32/24	
VLAN 1	IPv6	fe80::c1ff:fe55:3232/64	
VLAN 20	LINK	02-00-c1-55-32-32	<UP BROADCAST MULTICAST>
VLAN 20	IPv4	192.168.20.32/24	
VLAN 20	IPv6	fe80::c1ff:fe55:3232/64	
VLAN 32	LINK	02-00-c1-55-32-32	<BROADCAST MULTICAST>
VLAN 100	LINK	02-00-c1-55-32-32	<BROADCAST MULTICAST>
VLAN 100	IPv4	200.200.200.2/24	
LOOPBACK 1	LINK	5a-29-b5-2a-c6-a1	<UP BROADCAST LOOPBACK NOARP>
LOOPBACK 1	IPv4	192.168.100.32/32	

IP Routes

IPv4

Network	Gateway	Status
1.2.3.0/24	192.168.115.2	
2.3.5.0/24	192.168.1.125	<UP>
10.0.0.0/8	192.168.1.125	<UP>
192.168.1.0/24	VLAN 1	<UP>
192.168.20.0/24	VLAN 20	<UP>
192.168.100.32/32	LOOPBACK 1	<UP>

IPv6

Network	Gateway	Status
fe80::/64	VLAN 1	<UP>

Neighbor cache

IPv4

IP Address	Link Address
192.168.1.125	VLAN 1:3c-6a-48-06-09-dc

IP Interfaces

Interface

The name of the interface.

Type

The address type of the entry. This may be LINK, IPv4 or IPv6.

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 IPv4/IPv6 network or host address of this route.

Gateway

The gateway address of this route.

Status

The status flags of the route.

Neighbor cache

IP Address

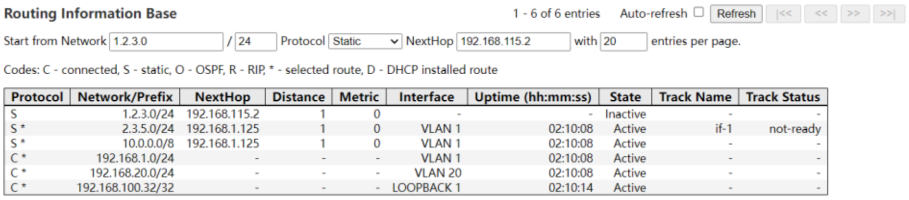
The IP address of the entry.

Link Address

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

[IPv4 Routing information]

This is IPv4 route entry table. It is used to provide the route entries status information.



Routing Information Base

1 - 6 of 6 entries Auto-refresh □

Start from Network 1.2.3.0 / 24 Protocol Static NextHop 192.168.115.2 with 20 entries per page.

Codes: C - connected, S - static, O - OSPF, R - RIP, * - selected route, D - DHCP installed route

Protocol	Network/Prefix	NextHop	Distance	Metric	Interface	Uptime (hh:mm:ss)	State	Track Name	Track Status
S	1.2.3.0/24	192.168.115.2	1	0	-	-	Inactive	-	-
S *	2.3.5.0/24	192.168.1.125	1	0	VLAN 1	02:10:08	Active	if-1	not-ready
S *	10.0.0.0/8	192.168.1.125	1	0	VLAN 1	02:10:08	Active	-	-
C *	192.168.1.0/24	-	-	-	VLAN 1	02:10:08	Active	-	-
C *	192.168.20.0/24	-	-	-	VLAN 20	02:10:08	Active	-	-
C *	192.168.100.32/32	-	-	-	LOOPBACK 1	02:10:14	Active	-	-

Routing Information Base

Protocol

The protocol of the route.

DHCP: The route is created by DHCP.

Connected: The destination network is connected directly.

Static: The route is created by user.

OSPF: The route is created by OSPF.

RIP: The route is created by RIP.

Network/Prefix

Network and prefix (example 10.0.0.0/16) of the given route entry.

NextHop

The IP address of nexthop. Value '0.0.0.0' indicates the link is directly connected.

Distance

The distance of the route.

Metric

The metric of the route.

Interface

The interface where the ip packet is outgoing.

Uptime (hh:ss:mm)

The time till the route is created. The unit is second.

State

Indicate if the destination network is reachable or not.

Track Name

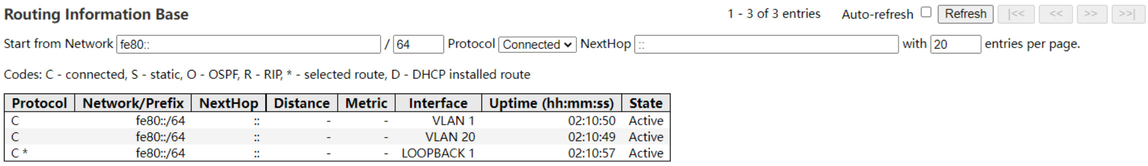
Name of the subscribed track instance.

Track Status

Status of the subscribed track instance.

[IPv6 Routing Information]

This table provides IPv6 routing status.



Routing Information Base

Start from Network fe80:: / 64 Protocol Connected NextHop :: with 20 entries per page.

Codes: C - connected, S - static, O - OSPF, R - RIP, * - selected route, D - DHCP installed route

Protocol	Network/Prefix	NextHop	Distance	Metric	Interface	Uptime (hh:mm:ss)	State
C	fe80::/64	::	-	-	VLAN 1	02:10:50	Active
C	fe80::/64	::	-	-	VLAN 20	02:10:49	Active
C *	fe80::/64	::	-	-	LOOPBACK 1	02:10:57	Active

Routing Information Base

Protocol

The protocol that installed this route.

DHCP: The route is created by DHCP.

Connected: The destination network is connected directly.

Static: The route is created by user.

OSPF: The route is created by OSPF.

RIP: The route is created by RIP.

Network/Prefix

Network and prefix (example 10.0.0.0/16) of the given route entry.

NextHop

Next-hop address. All-zeroes indicates the link is directly connected.

Interface

If the next-hop address is a link-local address, then this is the VLAN interface of the link-local address. Otherwise this value is not used.

Distance

Distance of the route.

Metric

Metric of the route.

Uptime (hh:ss:mm)

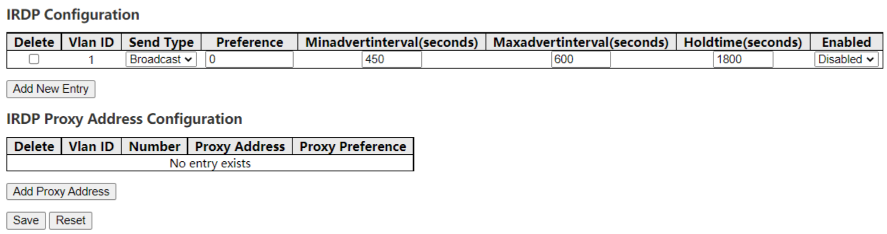
Time (in seconds) since this route was created.

State

Destination is active.

6.2. IRDP

[Routing > IRDP]



IRDP Configuration

Delete	Vlan ID	Send Type	Preference	Minadvertinterval(seconds)	Maxadvertinterval(seconds)	Holdtime(seconds)	Enabled
□	1	Broadcast	0	450	600	1800	Disabled

IRDP Proxy Address Configuration

Delete	Vlan ID	Number	Proxy Address	Proxy Preference
No entry exists				

You can configure IRDP settings.Click on "Add New Entry" on this page to add IRDP information. Click on "Add Proxy Address" on this page to add IRDP Proxy Address information.Then click the "Save" button to save the configuration. After checking, click "Delete" on the left side of the configuration display area to delete the corresponding IRDP configuration.

IRDP Configuration

Delete

Select this option to delete an existing IRDP.

Vlan ID

Specifies the VLAN-based router interface.

Send Type

Specifies advertisements are sent with multicast or broadcast.

Preference

Specifies preference level for this interface.

Minadvertinterval(seconds)

Specifies the mintime between sending router advertisement.

Maxadvertinterval(seconds)

Specifies the maxtime between sending router advertisement.

Holdtime(seconds)

Specifies the value of holdtime of the router advertisement.

Enable

Enables Router Discovery on the interface.

IRDP Proxy Address Configuration

Delete

Select this option to delete an existing IRDP.

Vlan ID

Specifies the VLAN-based router interface.

Number

Displays the proxy address of the current vlan.

Proxy Address

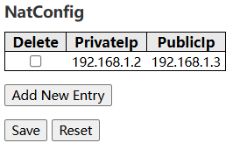
Specifies the address to be used to advertise the router.

Proxy Preference

Specifies the preferability of proxy address.

6.3. Nat

[Routing > Nat]



NatConfig

Delete	PrivateIp	PublicIp
□	192.168.1.2	192.168.1.3

NatConfig

This page allows configuration of NAT settings. Click 'Add New Entry' to create a new NAT entry. Then click 'Save' to store the configuration. To delete NAT configurations, select the corresponding checkbox and click 'Delete' in the left configuration panel.

Delete

Selecting this option will delete existing NAT-related configuration information.

PrivateIp

Private IP addresses are used within internal networks, defined by the IANA, to identify devices in local area networks (LANs) or other private network environments.

PublicIp

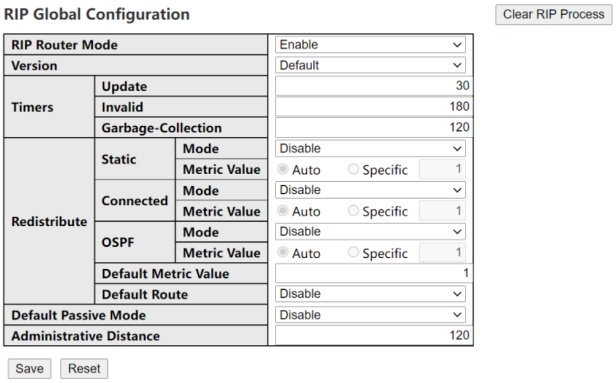
Public IP addresses are globally unique identifiers used to recognize devices on the Internet. Assigned by the IANA to Internet Service Providers (ISP), these addresses are then allocated to end users, enterprises, or organizations. They enable direct communication with other devices across the Internet.

6.4. RIP

6.4.1. Global

[Routing > RIP > Global]

[Configuration]



RIP Global Configuration

RIP Router Mode			Enable
Version			Default
Timers	Update		30
	Invalid		180
	Garbage-Collection		120
Redistribute	Static	Mode	Disable
		Metric Value	● Auto ○ Specific 1
	Connected	Mode	Disable
		Metric Value	● Auto ○ Specific 1
	OSPF	Mode	Disable
		Metric Value	● Auto ○ Specific 1
	Default Metric Value		1
	Default Route		Disable
Default Passive Mode			Disable
Administrative Distance			120

RIP Global Configuration

This is RIP router configuration table. It is a general group to configure the RIP common router parameters.

RIP Router Mode

Enable/Disable the RIP router mode.

Enable: Enable the the RIP router mode.

Disable: Disable the the RIP router mode.

Version

RIP version support.

Default: Base on the default version process.The router sends RIPv2 and accepts both RIPv1 and RIPv2. When the router receives either version of REQUESTS or triggered updates packets, it replies with the appropriate version.

Version 1: Receive/Send RIPv1 only.

Version 2: Receive/Send RIPv2 only.

Update Timer

The timer interval (in seconds) between the router sends the complete routing table to all neighboring RIP routers.The allowed range is 5 to 2147483.

Invalid Timer

The invalid timer is the number of seconds after which a route will be marked invalid.The allowed range is 5 to 2147483.

Garbage Collection Timer

The garbage collection timer is the number of seconds after which a route will be deleted.The allowed range is 5 to 2147483.

Static Redistribute Mode

Indicate if the router redistribute the Static routes in to the RIP domain or not.

Enable: Enable Static routes redistribution.

Disable: Disable Static routes redistribution.

Static Redistribute Metric Value

User specified metric value for the Static routes. The field is significant only when the argument 'StaticRedistIsSpecificMetric' is TRUE. If the specific metric setting is removed while the Static redistributed mode is enabled, the router will updates the original Static redistributed routes with metric value 16 before updates to the new metric value. The allowed range is 1 to 16.

Auto: The redistributed metric value is refer to redistributed default metric value.

Specific: User specified metric for the Static routes.

Connected Redistribute Mode

Indicate if the router redistribute the directly connected routes with RIP not enabled into the RIP domain or not.

Enable: Enable connected routes redistribution.

Disable: Disable connected routes redistribution.

Connected Redistribute Metric Value

User specified metric value for the connected interfaces. The field is significant only when the argument 'ConnectedRedistIsSpecificMetric' is TRUE. If the specific metric setting is removed while the connected redistributed mode is enabled, the router will updates the original connected redistributed routes with metric value 16 before updates to the new metric value. The allowed range is 1 to 16.

Auto: The redistributed metric value is refer to redistributed default metric value.

Specific: User specified metric for the connected routes.

OSPF Redistribute Mode

Indicate if the router redistribute the OSPF routes into the RIP domain or not. The field is significant only when the OSPF protocol is supported on the device.

Enable: Enable OSPF routes redistribution.

Disable: Enable OSPF routes redistribution.

OSPF Redistribute Metric Value

User specified metric value for the RIP routes. The field is significant only when the OSPF protocol is supported on the device and argument 'OspfRedistIsSpecificMetric' is TRUE. If the specific metric setting is removed while the OSPF redistributed mode is enabled, the router will updates the original OSPF redistributed routes with metric value 16 before updates to the new metric value. The allowed range is 1 to 16.

Auto: The redistributed metric value is refer to redistributed default metric value.

Specific: User specified metric for the OSPF routes.

Redistribute Default Metric Value

The RIP default redistributed metric.It is used when the metric value isn't specificed for the redistributed protocol type.The allowed range is 1 to 16.

Redistribute Default Route

The RIP default route redistribution.

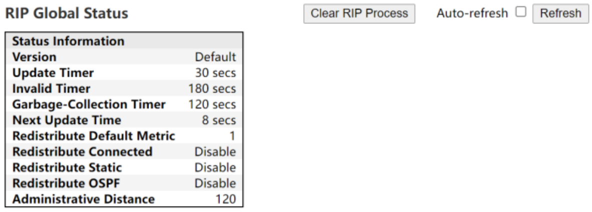
Default Passive Mode

Configure all interfaces as passive-interface by default.

Administrative Distance

The RIP administrative distance.The allowed range is 1 to 255.

[Status]



RIP Global Status

Status Information	
Version	Default
Update Timer	30 secs
Invalid Timer	180 secs
Garbage-Collection Timer	120 secs
Next Update Time	8 secs
Redistribute Default Metric	1
Redistribute Connected	Disable
Redistribute Static	Disable
Redistribute OSPF	Disable
Administrative Distance	120

RIP Global Status

The RIP general status information table.

Version

This indicates the global rip version. By default, the router sends RIPv2 and accepts both RIPv1 and RIPv2. When the router receive either version of REQUESTS or triggered updates packets, it replies with the appropriate version. Be aware that the RIP network class configuration when RIPv1 is involved in the topology. RIPv1 uses classful routing, the subnet information is not included in the routing updates. The limitation makes it impossible to have different-sized subnets inside of the same network class. In other words, all subnets in a network class must have the same size.

Update Timer

The timer interval (in seconds) between the router sends the complete routing table to all neighboring RIP routers.

Invalid Timer

The invalid timer is the number of seconds after which a route will be marked invalid.

Garbage-Collection Timer

The garbage collection timer is the number of seconds after which a route will be deleted.

Next Update Time

Specifies when the next round of updates will be sent out from this router in seconds.

Redistribute Default Metric

This indicates the default cost value for reallocating routes.

Redistribute Connected

This indicates the connected route is redistributed or not.

Redistribute Static

This indicates the Static route is redistributed or not.

Redistribute OSPF

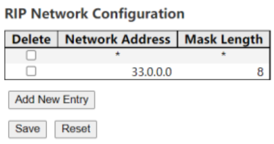
This indicates the OSPF route is redistributed or not.

Administrative Distance

This indicates administrative distance value.

6.4.2. Network

[Routing > RIP > Network]



RIP Network Configuration

Delete	Network Address	Mask Length
□	*	*
□	33.0.0.0	8

RIP Network Configuration

Delete

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

Network Address

IPv4 network address.

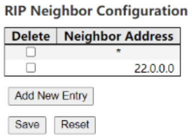
Mask Length

IPv4 network mask length.

6.4.3. Neighbors

[Routing > RIP > Neighbors]

[Configuration]



RIP Neighbor Configuration

Delete	Neighbor Address
□	*
□	22.0.0.0

RIP Neighbors Configuration

This is RIP neighbor connection table. It is used to configure the RIP router to send RIP updates to specific neighbors using the unicast, broadcast, or network IP address after update timer expiration. The maximum number of the RIP neighbor entries is 128.

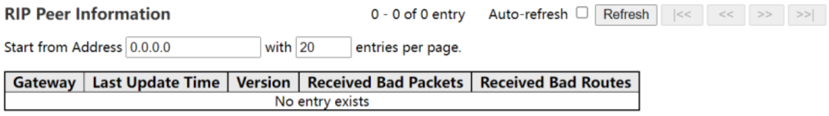
Delete

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

Neighbor Address

Ipv4 address encoded as "a.b.c.d", where a-d is a base-10 human readable integer in the range [0-255]The neighbor address can be an unicast(excluding loopback), broadcast, or network IP address.

[Status]



RIP Peer Information

0 - 0 of 0 entry

Auto-refresh □

Start from Address 0.0.0.0 with 20 entries per page.

Gateway	Last Update Time	Version	Received Bad Packets	Received Bad Routes
No entry exists				

RIP Peer Information

This is RIP peer table. It is used to provide the RIP peer information.

Navigating RIP Peer 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 "Start from Address" input field allows the user to change the starting point in this table. Clicking the 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.

Gateway

Peer IPv4 address.

Last Update Time

The time duration in seconds from the time the last RIP packet received from the neighbor to now.

Version

The RIP version number in the header of the last RIP packet received from the neighbor.

Received Bad Packets

The number of RIP response packets from the neighbor discarded as invalid.

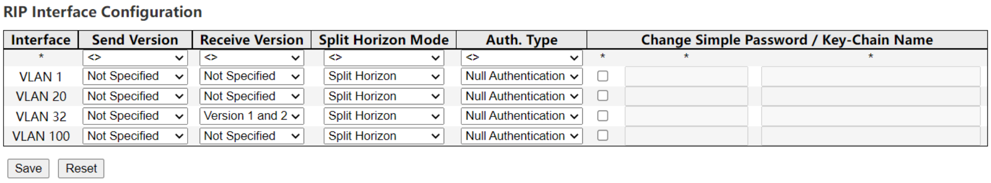
Received Bad Routes

The number of routes from the neighbor that were ignored because they were invalid.

6.4.4. Interfaces

[Routing > RIP > Interfaces]

[Interfaces]



RIP Interface Configuration

Interface	Send Version	Receive Version	Split Horizon Mode	Auth. Type	Change Simple Password / Key-Chain Name		
*	<>	<>	<>	<>	*	*	*
VLAN 1	Not Specified	Not Specified	Split Horizon	Null Authentication	□		
VLAN 20	Not Specified	Not Specified	Split Horizon	Null Authentication	□		
VLAN 32	Not Specified	Version 1 and 2	Split Horizon	Null Authentication	□		
VLAN 100	Not Specified	Not Specified	Split Horizon	Null Authentication	□		

RIP Interface Configuration

This is RIP interface configuration table.

Interface

Interface identification.

Send Version

The RIP version for the advertisement transmission on the interface.

Receive Version

The RIP version for the advertisement reception on the interface.

Split Horizon Mode

The split horizon mode.

Split Horizon: To omit routes learned from one neighbor in updates sent to that neighbor.

Poisoned Reverse: The neighbor learned routes are included in updates sent to the neighbors but their metrics are set to infinity.

Disabled: Split horizon is disabled.

Auth. Type

The authentication type.

Simple Password: It's using a plain text authentication. A password must be configured, but the password can be read by sniffer the packets.

Message Digest: It's message-digest algorithm 5 (MD5) authentication. Keying material must also be configured. This is the most secure method.

Null Authentication: No authentication.

Change Simple Password

It is used to change the simple password (fill with plain text). The allowed input length is from 1 to 15 printable characters excluding space character. The null string identifies none simple password is set on the interface.

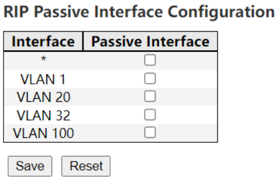
Notice that can not set key chain and simple password at the same time.

Change Key-Chain Name

It is used to change the key chain name used by MD5 authentication. The allowed input length is from 1 to 31 printable characters excluding space character. The null string identifies none key-chain name is set on the interface.

Notice that can not set key chain and simple password at the same time.

[Passive Interface]



RIP Passive Interface Configuration

Interface	Passive Interface
*	□
VLAN 1	□
VLAN 20	□
VLAN 32	□
VLAN 100	□

RIP Passive Interface Configuration

This is RIP router interface configuration table.

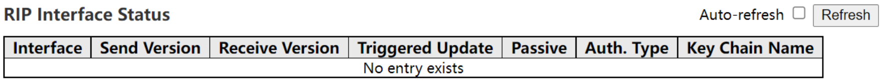
Interface

Interface identification.

Passive Interface

Enable the interface as RIP passive-interface.

[Status]



RIP Interface Status

Interface	Send Version	Receive Version	Triggered Update	Passive	Auth. Type	Key Chain Name
No entry exists						

RIP Interface Status

The RIP interface status information table.

Interface

Interface identification.

Send Version

The RIP version for the advertisement transmission on the interface.

Receive Version

The RIP version for the advertisement reception on the interface.

Triggered Update

This indicates the interface enable triggered update or not.

Passive

This indicates if the passive-interface is active on the interface or not.

Auth. Type

The authentication type.

Simple Password: It's using a plain text authentication. A password must be configured, but the password can be read by sniffer the packets.

Message Digest: It's message-digest algorithm 5 (MD5) authentication. Keying material must also be configured. This is the most secure method.

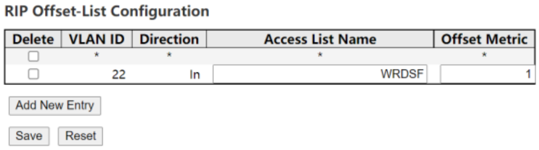
Null Authentication: No authentication.

Key-Chain Name

This indicates the interface is associate with a specific key-chain name.

6.4.5. Offset-List

[Routing > RIP > Offset-List]



RIP Offset-List Configuration

Delete	VLAN ID	Direction	Access List Name	Offset Metric
□	*	*	*	*
□	22	In	WRDSF	1

RIP Offset- Link Configuration

This is RIP offset-list configuration table. The maximum number of the RIP offset-list entries is 130.

Delete

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

VLAN ID

The VLAN interface which the offset list applies to. The range of VLAN ID is from 0 to 4095. 0 means that the offset list applies to all interfaces.

Direction

The direction to add the offset to routing metric update.

In: Apply to the inbound direction.

Out: Apply to the outbound direction.

Access List Name

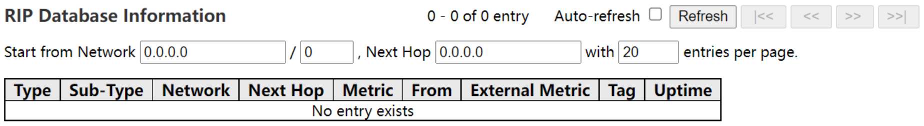
Access-list name. The valid name string length is from 1 to 31 and allows all printable characters excluding space character.

Offset Metric

The offset to incoming or outgoing routing metric.The allowed range is 0 to 16.

6.4.6. Database

[Routing > RIP > Database]



RIP Database Information   0 - 0 of 0 entry   Auto-refresh □

Start from Network 0.0.0.0 / 0 , Next Hop 0.0.0.0 with 20 entries per page.

Type	Sub-Type	Network	Next Hop	Metric	From	External Metric	Tag	Uptime
No entry exists								

RIP Database Information

The RIP database information table.

Navigating RIP Database 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 "Start from entry keys" input field allows the user to change the starting point in this table. Clicking the 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.

Type

The protocol type of the route.

Sub-Type

The protocol sub-type of the route.

Network

The destination IP address and mask of the route.

Next Hop

The first gateway along the route to the destination.

Metric

The metric of the route.

From

This indicates the route is learned an IP address or generated from one of the local interfaces.

External Metric

The field is significant only when the route is redistributed from other protocol type, for example, OSPF. This indicates the metric value from the original redistributed source.

Tag

The tag of the route. It is used to provide a method of separating 'internal' RIP routes, which may have been imported from an EGP (Exterior gateway protocol) or another IGP (Interior gateway protocol). For example, routes imported from OSPF can have a route tag value which the other routing protocols can use to prevent advertising the same route back to the original protocol routing domain.

Uptime

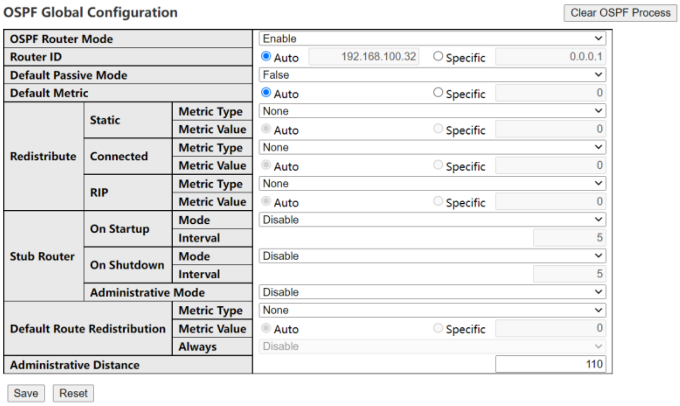
The time field is significant only when the route is learned from the neighbors. When the route destination is reachable (its metric value less than 16), the time field means the invalid time of the route. When the route destination is unreachable (its metric value greater than 16), the time field means the garbage-collection time of the route.

6.5. OSPF

6.5.1. Global

[Routing > OSPF > Global]

[Configuration]



OSPF Global Configuration

Clear OSPF Process

OSPF Router Mode			Enable
Router ID			● Auto 192.168.100.32 ○ Specific 0.0.0.1
Default Passive Mode			False
Default Metric			● Auto ○ Specific 0
Redistribute	Static	Metric Type	None
		Metric Value	○ Auto ○ Specific 0
	Connected	Metric Type	None
		Metric Value	○ Auto ○ Specific 0
	RIP	Metric Type	None
		Metric Value	○ Auto ○ Specific 0
Stub Router	On Startup	Mode	Disable
		Interval	5
	On Shutdown	Mode	Disable
		Interval	5
	Administrative Mode		Disable
Default Route Redistribution		Metric Type	None
		Metric Value	○ Auto ○ Specific 0
		Always	Disable
Administrative Distance			110

OSPF Global Configuration

This is OSPF router configuration table. It is a general group to configure the OSPF common router parameters.

OSPF Router Mode

Enable/Disable the OSPF router mode.

Router ID

The OSPF Router ID in IPv4 address format(A.B.C.D).The allowed range is from 0.0.0.1 to 255.255.255.254.

When the router's OSPF Router ID is changed, if there is one or more fully adjacent neighbors in current OSPF area, the new router ID will take effect after restarting OSPF process. Notice that the router ID should be unique in the Autonomous System and value '0.0.0.0' is invalid since it is reserved for the default algorithm.

Auto: The default algorithm will choose the largest IP address assigned to the router.

Specific: User specified router ID.

Default Passive Mode

Configure all interfaces as passive-interface by default.When an interface is configured as a passive-interface, the OSPF routing updates sending is suppressed, therefore the interface does not establish adjacencies (No OSPF Hellos). The subnet of all interfaces (both passive and active) is advertised by the OSPF router.

Default Metric

User specified default metric value for the OSPF routing protocol. The field is significant only when the arugment 'IsSpecificDefMetric' is TRUE.

Auto: The default metric is calculated automatically based on the routing protocols.

Specific: User specified default metric. The allowed range is 0 to 16777214.

Static Redistribute Metric Type

The OSPF redistributed metric type for the Static routes.

None: The Static routes are not redistributed.

External Type 1: External Type 1 of the Static routes.

External Type 2: External Type 2 of the Static routes.

Static Redistribute Metric Value

User specified metric value for the Static routes. The field is significant only when the argument 'StaticRedistIsSpecificMetric' is TRUE. The allowed range is 0 to 16777214.

Auto: The redistributed metric is the same as the original metric value.

Specific: User specified metric for the Static routes.

Connected Redistribute Metric Type

The OSPF redistributed metric type for the connected interfaces.

None: The connected interfaces are not redistributed.

External Type 1: External Type 1 of the connected interfaces routes.

External Type 2: External Type 2 of the connected interfaces routes.

Connected Redistribute Metric Value

User specified metric value for the connected interfaces. The field is significant only when the argument 'ConnectedRedistIsSpecificMetric' is TRUE. The allowed range is 0 to 16777214.

Auto: The redistributed metric is the same as the original metric value.

Specific: User specified metric for the connected routes.

RIP Redistribute Metric Type

The OSPF redistributed metric type for the RIP routes. The field is significant only when the RIP protocol is supported on the device.

None: The RIP routes are not redistributed.

External Type 1: External Type 1 of the RIP routes.

External Type 2: External Type 2 of the RIP routes.

RIP Redistribute Metric Value

User specified metric value for the RIP routes. The field is significant only when the RIP protocol is supported on the device and argument 'RipRedistIsSpecificMetric' is TRUE. The allowed range is 0 to 16777214.

Auto: The redistributed metric is the same as the original metric value.

Specific: User specified metric for the RIP routes.

Stub router during startup period

Configures OSPF to advertise a maximum metric during startup for a configured period of time.

Stub router on startup interval time

User specified time interval (seconds) to advertise itself as stub area. The field is significant only when the on-startup mode is enabled. The allowed range is 5 to 86400 seconds.

Stub router during shutdown period

Configures OSPF to advertise a maximum metric during shutdown for a configured period of time. The device advertises a maximum metric when the OSPF router mode is disabled and notice that the mechanism also works when the device reboots but not for the 'reload default' case.

Stub router on shutdown interval time

User specified time interval (seconds) to wait till shutdown completed. The field is significant only when the on-shutdown mode is enabled. The allowed range is 5 to 100 seconds.

Stub router administrative mode

Configures OSPF stub router mode administratively applied, for an indefinite period.

Default Route Redistribution Metric Type

The OSPF redistributed metric type for a default route.

None: The default route are not redistributed.

External Type 1: External Type 1 of the default route.

External Type 2: External Type 2 of the default route.

Default Route Redistribution Metric value

User specified metric value for a default route. The field is significant only when the argument 'DefaultRouteRedistIsSpecificMetric' is TRUE. The allowed range is 0 to 16777214.

Auto: The redistributed metric is the same as the original metric value.

Specific: User specified metric for the default route.

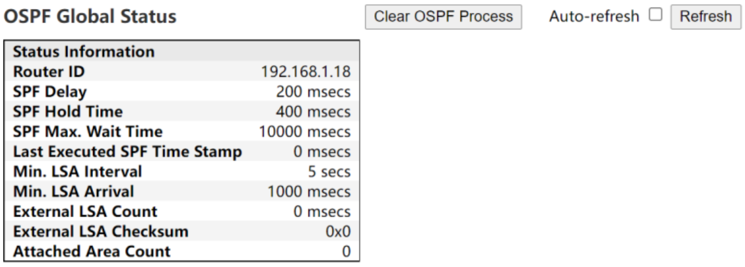
Default Route Redistribution Always

Specifies to always advertise a default route into all external-routing capable areas. Otherwise, the router only to advertise the default route when the advertising router already has a default route.

Administrative Distance

The OSPF administrative distance.The allowed range is 1 to 255.

[Status]



OSPF Global Status

Status Information	
Router ID	192.168.1.18
SPF Delay	200 msecs
SPF Hold Time	400 msecs
SPF Max. Wait Time	10000 msecs
Last Executed SPF Time Stamp	0 msecs
Min. LSA Interval	5 secs
Min. LSA Arrival	1000 msecs
External LSA Count	0 msecs
External LSA Checksum	0x0
Attached Area Count	0

OSPF Global Status

This is OSPF router status table. It is used to provide the OSPF router status information.

Router ID

OSPF router ID.

SPF Delay

Delay time (in milliseconds) of SPF calculations.

SPF Hold Time

Minimum hold time (in milliseconds) between consecutive SPF calculations.

SPF Max. Wait Time

Maximum wait time (in milliseconds) between consecutive SPF calculations.

Last Executed SPF Time Stamp

Time (in milliseconds) that has passed between the start of the SPF algorithm execution and the current time.

Min. LSA Interval

Minimum interval (in seconds) between link-state advertisements.

Min. LSA Arrival

Minimum arrival time (in milliseconds) of link-state advertisements.

External LSA Count

Number of external link-state advertisements.

External LSA Checksum

Number of external link-state checksum.

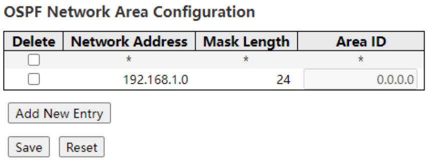
Attached Area Count

Number of areas attached for the router.

6.5.2. Area

[Routing > OSPF > Area]

[Network Area]



OSPF Network Area Configuration

Delete	Network Address	Mask Length	Area ID
□	*	*	*
□	192.168.1.0	24	0.0.0.0

OSPF Network Area Configuration

This is OSPF area configuration table. It is used to specify the OSPF enabled interface(s). When OSPF is enabled on the specific interface(s), the router can provide the network information to the other OSPF routers via those interfaces.

Delete

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

Network Address

IPv4 network address.

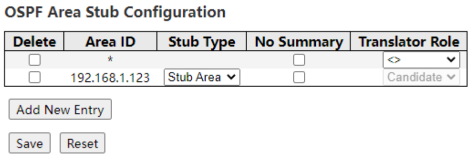
Mask Length

IPv4 network mask length.

Area ID

The OSPF area ID.

[Stub Area]



OSPF Area Stub Configuration

Delete	Area ID	Stub Type	No Summary	Translator Role
□	*		□	<>
□	192.168.1.123	Stub Area	□	Candidate

OSPF Area Stub Configuration

This is OSPF stub area configuration table. The configuration is used to reduce the link-state database size and therefore the memory and CPU requirement by forbidding some LSAs.

Delete

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

Area ID

The OSPF area ID.

Stub Type

The OSPF stub configured type.

Stub Area: Configure the area as stub area.

NSSA: Configure the area as not-so-stubby area (NSSA).

No Summary

The value is true to configure the inter-area routes do not inject into this stub area.

Translator Role

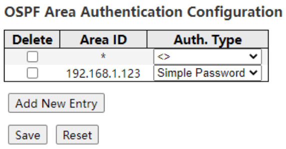
The OSPF NSSA translator role.

Candidate: this NSSA-ABR router will participate in the translator election.

Never: this NSSA-ABR router never translates.

Always: this NSSA-ABR router always translates.

[Area Authentication]



OSPF Area Authentication Configuration

Delete	Area ID	Auth. Type
□	*	<>
□	192.168.1.123	Simple Password

OSPF Area Authentication Configuration

This is OSPF area authentication configuration table. It is used to apply the authentication to all the interfaces belong to the area.

Delete

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

Area ID

The OSPF area ID.

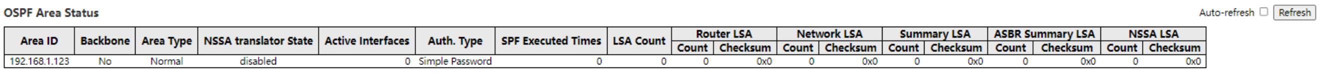
Auth. Type

The authentication type on an area is applied to all the interfaces belong to that area. The authentication type on an IP interface or a virtual link overrides the authentication type on an area and is useful if different interfaces in the same area use different authentication types.
Specify the authentication type.

Simple Password: Simple password authentication.

Message Digest: MD5 digest authentication.

[Status]



OSPF Area Status

Area ID	Backbone	Area Type	NSSA translator State	Active Interfaces	Auth. Type	SPF Executed Times	LSA Count	Router LSA		Network LSA		Summary LSA		ASBR Summary LSA		NSSA LSA	
								Count	Checksum	Count	Checksum	Count	Checksum	Count	Checksum	Count	Checksum
192.168.1.123	No	Normal	disabled	0	Simple Password	0	0	0	0x0	0	0x0	0	0x0	0	0x0	0	0x0

OSPF Area Status

Those are OSPF network area status parameters. It is used to provide the OSPF network area status information.

Area ID

The Area ID.

Backbone

Indicate if it's backbone area or not.

Area Type

The area type.

NSSA translator state

Indicate the current state of the NSSA-ABR translator which the router uses to translate Type-7 LSAs in the NSSA to Type-5 LSAs in backbone area.

Active Interfaces

Number of active interfaces attached in the area.

Auth. Type

The authentication type in the area.

SPF Executed Times

Number of times SPF algorithm has been executed for the particular area.

LSA Count

Number of the total LSAs for the particular area.

Router LSA Count

Number of the router-LSAs (Type-1) of a given type for the particular area.

Router LSA Checksum

The router-LSAs (Type-1) checksum.

Network LSA Count

Number of the network-LSAs (Type-2) of a given type for the particular area.

Network LSA Checksum

The network-LSAs (Type-2) checksum.

Summary LSA Count

Number of the summary-LSAs (Type-3) of a given type for the particular area.

Summary LSA Checksum

The summary-LSAs (Type-3) checksum.

ASBR Summary LSA Count

Number of the ASBR-summary-LSAs (Type-4) of a given type for the particular area.

ASBR Summary LSA Checksum

The ASBR-summary-LSAs (Type-4) checksum.

NSSA LSA Count

Number of the NSSA LSAs of a given type for the particular area.

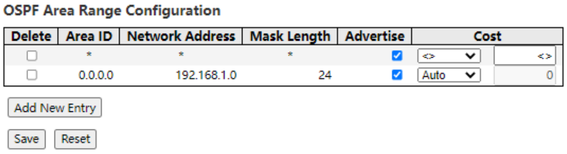
NSSA LSA Checksum

The NSSA LSAs checksum.

6.5.3. Routing

[Routing > OSPF > Routing]

[Configuration]



OSPF Area Range Configuration

Delete	Area ID	Network Address	Mask Length	Advertise	Cost	
□	*	*	*	☑	<>	<>
□	0.0.0.0	192.168.1.0	24	☑	Auto	0

Add New Entry

Save Reset

OSPF Area Range Configuration

This is OSPF area range configuration table. It is used to summarize the intra area paths from a specific address range in one summary-LSA (Type-3) and advertised to other areas or configure the address range status as 'DoNotAdvertise' which the summary-LSA (Type-3) is suppressed. The area range configuration is used for Area Border Routers (ABRs) and only router-LSAs (Type-1) and network-LSAs (Type-2) can be summarized. The AS-external-LSAs (Type-5) cannot be summarized because the scope is OSPF autonomous system (AS). The AS-external-LSAs (Type-7) cannot be summarized because the feature is not supported yet.

Delete

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

Area ID

The OSPF area ID.

Network Address

IPv4 network address.

Mask Length

IPv4 network mask length.

Advertised

When the value is true, it summarizes intra area paths from the address range in one summary-LSA (Type-3) and advertised to other areas. Otherwise, the intra area paths from the address range are not advertised to other areas.

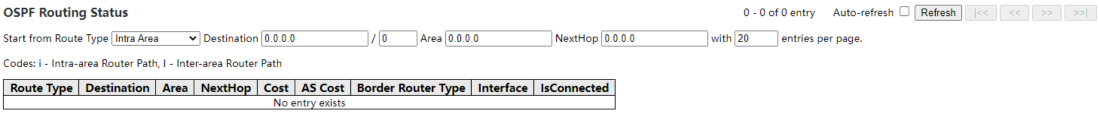
Auto/Specific

When 'Auto' is selected, the cost value is set to 0 automatically and isn't allowed to be configured.

Cost

User specified cost (or metric) for this summary route. It is allowed to be configured only when 'Specific' is selected. The allowed range is 0 to 16777215 and the default setting is 'auto cost' mode.

[Status]



OSPF Routing Status

0 - 0 of 0 entry Auto-refresh □

Start from Route Type Intra Area Destination 0.0.0.0 / 0 Area 0.0.0.0 NextHop 0.0.0.0 with 20 entries per page.

Codes: i - Intra-area Router Path, I - Inter-area Router Path

Route Type	Destination	Area	NextHop	Cost	AS Cost	Border Router Type	Interface	IsConnected
No entry exists								

OSPF Routing Status

This is OSPF routing status table. It is used to provide the OSPF routing status information.

Navigating the OSPF Routing Status 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 "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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Route Type

The OSPF route type.

Intra Area: The destination is an OSPF route which is located on intra-area.

Inter Area: The destination is an OSPF route which is located on inter-area.

Border Router: The destination is a border router.

External Type-1: The destination is an external Type-1 route.

External Type-2: The destination is an external Type-2 route.

Destination

Network and prefix (example 10.0.0.0/16) of the given route entry.

Area

It indicates which area the route or router can be reached via/to.

NextHop

Ipv4 address encoded as "a.b.c.d", where a-d is a base-10 human readable integer in the range [0-255].

Cost

The cost of the route.

AS Cost

The cost of the route within the OSPF network. It is valid for external Type-2 route and always '0' for other route type.

Border Router Type

The border router type of the OSPF route entry.

i-ABR: The border router is an ABR.

i-ASBR: The border router is an ASBR located on Intra-area.

I-ASBR: The border router is an ASBR located on Inter-area.

i-ABR/ASBR: The border router is an ASBR attached to at least 2 areas.

Interface

The interface where the ip packet is outgoing.

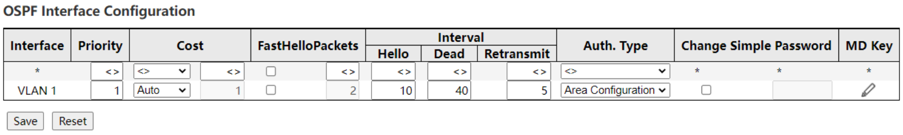
IsConnected

The destination is connected directly or not.

6.5.4. Interfaces

[Routing > OSPF > Interfaces]

[Configuration]



OSPF Interface Configuration

Interface	Priority	Cost		FastHelloPackets		Interval			Auth. Type	Change Simple Password		MD Key
						Hello	Dead	Retransmit				
*	<>	<>	<>	☐	<>	<>	<>	<>	<>	*	*	*
VLAN 1	1	Auto	1	☐	2	10	40	5	Area Configuration	☐		✎

OSPF Interface Configuration

This is interface configuration parameter table.

Interface

Interface identification.

Priority

User specified router priority for the interface. The allowed range is 0 to 255 and the default value is 1.

Cost

User specified cost for this interface. It's link state metric for the interface. The field is significant only when 'IsSpecificCost' is TRUE. The allowed range is 1 to 65535 and the default setting is 'auto cost' mode.

FastHelloPackets

How many Hello packets will be sent per second. The allowed range is 1 to 10 and the default setting is disabled.

Hello Interval

The time interval (in seconds) between hello packets. The allowed range is 1 to 65535 and the default value is 10 (seconds).

Dead Interval

The number of seconds to wait until the neighbor is declared to be dead. The allowed range is 1 to 65535 and the default value is 40 (seconds).

Retransmit Interval

The time interval (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies. The allowed range is 3 to 65535 and the default value is 5 (seconds).

Auth Type

The authentication type.

Simple Password: It's using a plain text authentication. A password must be configured, but the password can be read by sniffer the packets.

Message Digest: It's message-digest algorithm 5 (MD5) authentication. Keying material must also be configured. This is the most secure method.

Null Authentication: No authentication.

Area Configuration: Refer to OSPF -> Area -> Area authentication setting.

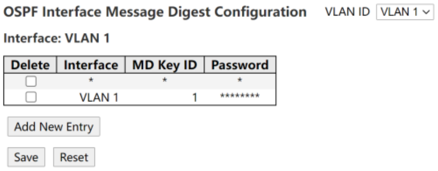
Change Simple Password

It is used to change the simple password (fill with plain text). The allowed input length is 1 to 8.

MD Key

Click edit icon to edit the message digest key for the entry.

Click MD Key to open the hidden interface, as shown below:



OSPF Interface Message Digest Configuration VLAN ID VLAN 1

Interface: VLAN 1

Delete	Interface	MD Key ID	Password
□	*	*	*
□	VLAN 1	1	********

Delete

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

Interface

Interface identification.

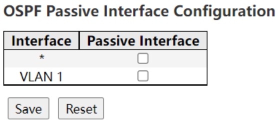
MD Key ID

The key ID for message digest authentication. The allowed range is 1 to 255.

Password

The message digest key. The allowed input length is 1 to 16.

[Passive Interface]



OSPF Passive Interface Configuration

Interface	Passive Interface
*	□
VLAN 1	□

OSPF Passive Interface Configuration

This is OSPF router interface configuration table.

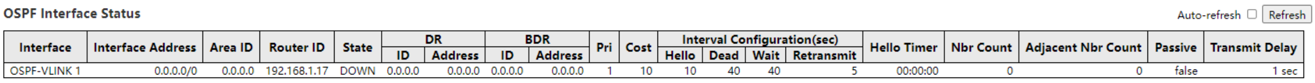
Interface

Interface identification.

Passive Interface

Enable the interface as OSPF passive-interface.

[Status]



OSPF Interface Status

Interface	Interface Address	Area ID	Router ID	State	DR		BDR		Pri	Cost	Interval Configuration(sec)				Hello Timer	Nbr Count	Adjacent Nbr Count	Passive	Transmit Delay
					ID	Address	ID	Address			Hello	Dead	Wait	Retransmit					
OSPF-VLINK 1	0.0.0.0/0	0.0.0.0	192.168.1.17	DOWN	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	1	10	10	40	40	5	00:00:00	0	0	false	1 sec

OSPF Interface Status

This is OSPF interface status table. It is used to provide the OSPF interface status information.

Interface

Interface identification.

Interface Address

IPv4 network address.

Area ID

The OSPF area ID.

Router ID

The OSPF router ID.

State

The state of the link.

DR ID

The router ID of DR.

DR Address

The IP address of DR.

BDR ID

The router ID of BDR.

BDR Address

The IP address of BDR.

Priority

The OSPF priority. It helps determine the DR and BDR on the network to which this interface is connected.

Cost

The cost of the interface.

Hello

Hello timer. A time interval that a router sends an OSPF hello packet.

Dead

Dead timer. Dead timer is a time interval to wait before declaring a neighbor dead. The unit of time is the second.

Wait

This interval is used in Wait Timer. Wait timer is a single shot timer that causes the interface to exit waiting and select a DR on the network. Wait Time interval is the same as Dead time interval.

Retransmit

Retransmit timer. A time interval to wait before retransmitting a database description packet when it has not been acknowledged.

Hello Timer

Hello due timer. An OSPF hello packet will be sent on this interface after this due time.

Nbr Count

Neighbor count. This is the number of OSPF neighbors discovered on this interface.

Adjacent Nbr Count

Adjacent neighbor count. This is the number of routers running OSPF that are fully adjacent with this router.

Passive

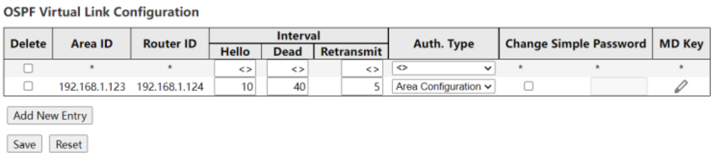
Indicate if the interface is passive interface.

Transmit Delay

The estimated time to transmit a link-state update packet on the interface.

6.5.5. Virtual Link

[Routing > OSPF > Virtual Link]



OSPF Virtual Link Configuration

Delete	Area ID	Router ID	Interval			Auth. Type	Change Simple Password	MD Key
			Hello	Dead	Retransmit			
☐	*	*	<>	<>	<>	<>	* *	*
☐	192.168.1.123	192.168.1.124	10	40	5	Area Configuration	☐	

OSPF Virtual Link Configuration

This is OSPF virtual link configuration table. The virtual link is established between 2 ABRs to overcome that all the areas have to be connected directly to the backbone area.

Delete

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

Area ID

OSPF Area ID.

Router ID

OSPF router ID.

Hello Interval

The time interval (in seconds) between hello packets. The allowed range is 1 to 65535 and the default value is 10 (seconds).

Dead Interval

the number of seconds to wait until the neighbor is declared to be dead. The allowed range is 1 to 65535 and the default value is 40 (seconds).

Retransmit Interval

The time interval (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies. The allowed range is 3 to 65535 and the default value is 5 (seconds).

Auth. Type

The authentication type on an area.

Simple Password: It's using a plain text authentication. A password must be configured, but the password can be read by sniffer the packets.

Message Digest: It's message-digest algorithm 5 (MD5) authentication. Keying material must also be configured. This is the most secure method.

Null Authentication: No authentication.

Area Configuration: Refer to OSPF -> Area -> Area authentication setting.

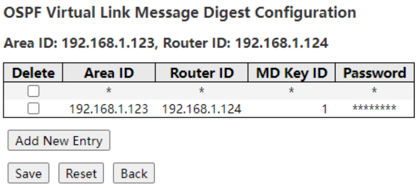
Change Simple Password

It is used to change the simple password (fill with plain text). The allowed input length is 1 to 8.

MD Key

Click the icon to edit the message digest key for the entry.

Click on the MD key, and the following page will appear:



OSPF Virtual Link Message Digest Configuration

Area ID: 192.168.1.123, Router ID: 192.168.1.124

Delete	Area ID	Router ID	MD Key ID	Password
□	*	*	*	*
□	192.168.1.123	192.168.1.124	1	********

OSPF Virtual Link Message Digest Configuration

Delete

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

Area ID

OSPF Area ID.

Router ID

OSPF router ID.

MD Key ID

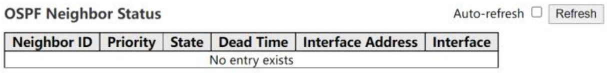
OSPF MD Key ID.

Password

simple password.

6.5.6. Neighbor

[Routing > OSPF > Neighbor]



OSPF Neighbor Status

Neighbor ID	Priority	State	Dead Time	Interface Address	Interface
No entry exists					

OSPF Neighbor Status

This is OSPF IPv4 neighbor status table. It is used to provide the OSPF neighbor status information.

Neighbor ID

The Neighbor ID.

Priority

The priority of OSPF neighbor. It indicates the priority of the neighbor router. This item is used when selecting the DR for the network. The router with the highest priority becomes the DR.

State

The state of OSPF neighbor. It indicates the functional state of the neighbor router.

Dead Time

Dead timer. It indicates the amount of time remaining that the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down.

Interface Address

The IP address.

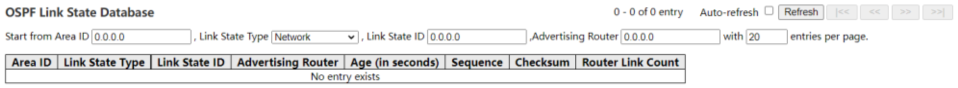
Interface

The network interface.

6.5.7. Database

General Database

[Routing > OSPF > Database > General Database]



OSPF Link State Database 0 - 0 of 0 entry Auto-refresh □ Refresh

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 ,Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Sequence	Checksum	Router Link Count
No entry exists							

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 "Start from entry keys" input field allows 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

OSPF Link State Database

Area ID

The OSPF area ID of the link state advertisement. It is not required for external LSA.

Link State Type

The type of the link state advertisement.

Link State ID

The OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router

The advertising router ID which originated the LSA.

Age

The time in seconds since the LSA was originated.

Sequence

The LS sequence number of the LSA.

Checksum

The checksum of the LSA contents.

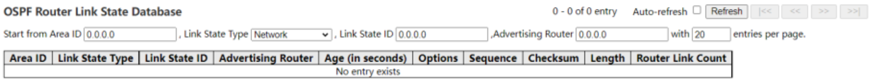
Router Link Count

The link count of the LSA. The field is significant only when the link state type is 'Router Link State' (Type 1).

Detail Database

[Routing > OSPF > Database > Detail Database]

[Router]



OSPF Router Link State Database

0 - 0 of 0 entry Auto-refresh □ Refresh |<< << >> >>|

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 ,Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Router Link Count
No entry exists									

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 "Start from entry keys" input field allows 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

OSPF Router Link State Database

Area ID

The OSPF area ID of the link state advertisement.

Link State Type

The type of the link state advertisement.

Link State ID

The OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router

The advertising router ID which originated the LSA.

Age (in seconds)

The time in seconds since the LSA was originated.

Options

The OSPF option field which is present in OSPF hello packets, which enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

Sequence

The LS sequence number of the LSA.

Checksum

The checksum of the LSA contents.

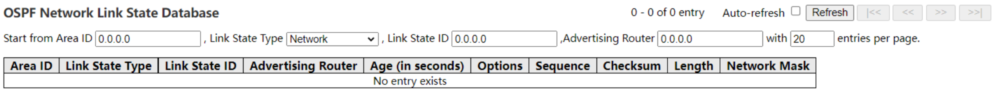
Length

The Length in bytes of the LSA.

Router Link Count

The link count of the LSA. The field is significant only when the link state type is 'Router Link State' (Type 1).

[Network]



OSPF Network Link State Database

0 - 0 of 0 entry Auto-refresh □ Refresh |<< << >> >>|

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 ,Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask
No entry exists									

OSPF Network Link State Database

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 "Start from entry keys" input field allows 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Area ID

The OSPF area ID of the link state advertisement.

Link State Type

The type of the link state advertisement.

Link State ID

The OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router

The advertising router ID which originated the LSA.

Age(in seconds)

The time in seconds since the LSA was originated.

Options

The OSPF option field which is present in OSPF hello packets, which enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

Sequence

The LS sequence number of the LSA.

Checksum

The checksum of the LSA contents.

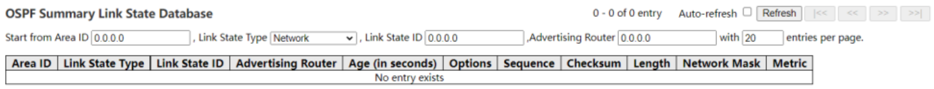
Length

The Length in bytes of the LSA.

Network Mask

Network mask length. The field is significant only when the link state type is 'Network Link State' (Type 2).

[Summary]



OSPF Summary Link State Database

0 - 0 of 0 entry Auto-refresh □ Refresh |<< << >> >>|

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 ,Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric
No entry exists										

OSPF Summary Link State Database

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 "Start from entry keys" input field allows 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Area ID

The OSPF area ID of the link state advertisement.

Link State Type

The type of the link state advertisement.

Link State ID

The OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router

The advertising router ID which originated the LSA.

Age

The time in seconds since the LSA was originated.

Options

The OSPF option field which is present in OSPF hello packets, which enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

Sequence

The LS sequence number of the LSA.

Checksum

The checksum of the LSA contents.

Length

The Length in bytes of the LSA.

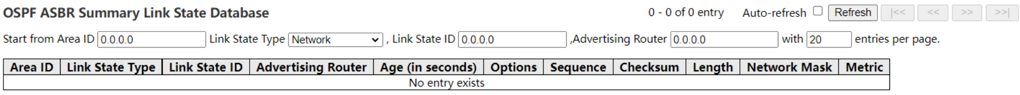
Network Mask

Network mask length. The field is significant only when the link state type is 'Summary/ASBR Summary Link State' (Type 3, 4).

Metric

User specified metric for this summary route. The field is significant only when the link state type is 'Summary/ASBR Summary Link State' (Type 3, 4).

[ASBR Summary]



OSPF ASBR Summary Link State Database

0 - 0 of 0 entry Auto-refresh ☐ Refresh |<< << >> >>|

Start from Area ID 0.0.0.0 Link State Type Network , Link State ID 0.0.0.0 ,Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric
No entry exists										

OSPF ASBR Summary Link State Database

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 "Start from entry keys" input field allows 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Area ID

The OSPF area ID of the link state advertisement.

Link State Type

The type of the link state advertisement.

Link State ID

The OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router

The advertising router ID which originated the LSA.

Age

The time in seconds since the LSA was originated.

Options

The OSPF option field which is present in OSPF hello packets, which enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

Sequence

The LS sequence number of the LSA.

Checksum

The checksum of the LSA contents.

Length

The Length in bytes of the LSA.

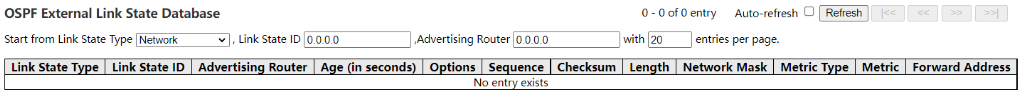
Network Mask

Network mask length. The field is significant only when the link state type is 'Summary/ASBR Summary Link State' (Type 3, 4).

Metric

User specified metric for this summary route. The field is significant only when the link state type is 'Summary/ASBR Summary Link State' (Type 3, 4).

[External]



OSPF External Link State Database

0 - 0 of 0 entry Auto-refresh □

Start from Link State Type Network , Link State ID 0.0.0.0 ,Advertising Router 0.0.0.0 with 20 entries per page.

Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric Type	Metric	Forward Address
No entry exists											

OSPF External Link State Database

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 "Start from entry keys" input field allows 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Link State Type

The type of the link state advertisement.

Link State ID

The OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router

The advertising router ID which originated the LSA.

Age

The time in seconds since the LSA was originated.

Options

The OSPF option field which is present in OSPF hello packets, which enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

Sequence

The LS sequence number of the LSA.

Checksum

The checksum of the LSA contents.

Length

The Length in bytes of the LSA.

Network Mask

Network mask length. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

Metric Type

The External type of the LSA. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

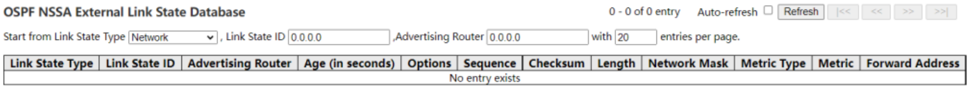
Metric

User specified metric for this summary route. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

Forward Address

The IP address of forward address. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

[NSSA External]



OSPF NSSA External Link State Database

0 - 0 of 0 entry Auto-refresh □ Refresh |<< << >> >>|

Start from Link State Type Network , Link State ID 0.0.0.0 ,Advertising Router 0.0.0.0 with 20 entries per page.

Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Network Mask	Metric Type	Metric	Forward Address
No entry exists											

OSPF NSSA External Link State Database

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 "Start from entry keys" input field allows 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Link State Type

The type of the link state advertisement.

Link State ID

The OSPF link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router

The advertising router ID which originated the LSA.

Age

The time in seconds since the LSA was originated.

Options

The OSPF option field which is present in OSPF hello packets, which enables OSPF routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF routers.

Sequence

The LS sequence number of the LSA.

Checksum

The checksum of the LSA contents.

Length

The Length in bytes of the LSA.

Network Mask

Network mask length. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

Metric Type

The External type of the LSA. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

Metric

User specified metric for this summary route. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

Forward Address

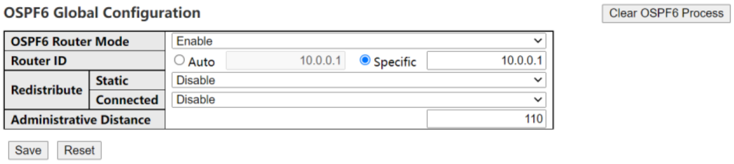
The IP address of forward address. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

6.6. OSPFv3

6.6.1. Global

[Routing > OSPFv3 > Global]

[Configuration]



OSPF6 Global Configuration

OSPF6 Router Mode		Enable
Router ID		○ Auto 10.0.0.1 ● Specific 10.0.0.1
Redistribute	Static	Disable
	Connected	Disable
Administrative Distance		110

OSPF6 Global Configuration

This is OSPF6 router configuration table. It is a general group to configure the OSPF6 common router parameters.

OSPF6 Router Mode

Enable/Disable the OSPF6 router mode.

Router ID

The OSPF6 Router ID in IPv4 address format(A.B.C.D).

When the router's OSPF6 Router ID is changed, if there is one or more fully adjacent neighbors in current OSPF6 area, the new router ID will take effect after restarting OSPF6 process. Notice that the router ID should be unique in the Autonomous System and value '0.0.0.0' is invalid since it is reserved for the default algorithm.

Auto: The default algorithm will choose the largest IP address assigned to the router.

Specific: User specified router ID.

The allowed range is from 0.0.0.1 to 255.255.255.254.

Static Redistribute

The OSPF redistribute enabled for the Static routes or not.

Enable: The Static routes are redistributed.

Disable: The Static routes are not redistributed.

Connected Redistribute

The OSPF redistribute enabled for connected route or not.

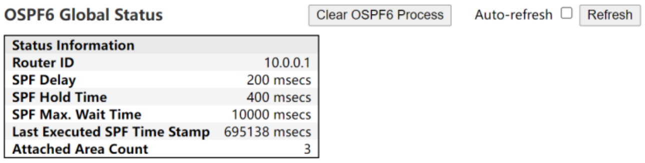
Enable: The connected interfaces are redistributed.

Disable: The connected interfaces are not redistributed.

Administrative Distance

The OSPF6 administrative distance.

[Status]



Status Information	
Router ID	10.0.0.1
SPF Delay	200 msecs
SPF Hold Time	400 msecs
SPF Max. Wait Time	10000 msecs
Last Executed SPF Time Stamp	695138 msecs
Attached Area Count	3

OSPF6 Global Status

This is OSPF6 router status table. It is used to provide the OSPF6 router status information.

Router ID

OSPF6 router ID.

SPF Delay

Delay time (in milliseconds) of SPF calculations.

SPF Hold Time

Minimum hold time (in milliseconds) between consecutive SPF calculations.

SPF Max. Wait Time

Maximum wait time (in milliseconds) between consecutive SPF calculations.

Last Executed SPF Time Stamp

Time (in milliseconds) that has passed between the start of the SPF algorithm execution and the current time.

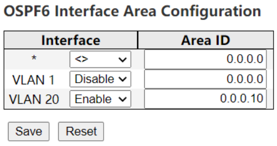
Attached Area Count

Number of areas attached for the router.

6.6.2. Area

[Routing > OSPFv3 > Area]

[Interface Area]



OSPF6 Interface Area Configuration

Interface		Area ID
*	<>	0.0.0.0
VLAN 1	Disable	0.0.0.0
VLAN 20	Enable	0.0.0.10

OSPF Interface Area Configuration

This is OSPF6 router interface configuration parameter.

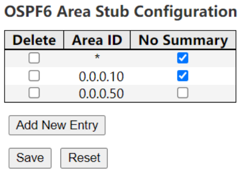
Interface

Interface identification.

Interface Area ID

The OSPF6 interface Area ID. Only valid if 'is_specific_id' is true.

[Stub Area]



OSPF6 Area Stub Configuration

Delete	Area ID	No Summary
☐	*	☑
☐	0.0.0.10	☑
☐	0.0.0.50	☐

OSPF Area Stub Configuration

This is OSPF6 stub area configuration table. The configuration is used to reduce the link-state database size and therefore the memory and CPU requirement by forbidding some LSAs.

Delete

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

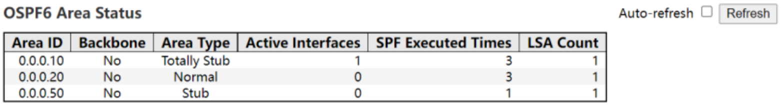
Area ID

The OSPF6 area ID.

No Summary

The value is true to configure the inter-area routes do not inject into this stub area.

[Status]



OSPF6 Area Status

Area ID	Backbone	Area Type	Active Interfaces	SPF Executed Times	LSA Count
0.0.0.10	No	Totally Stub	1	3	1
0.0.0.20	No	Normal	0	3	1
0.0.0.50	No	Stub	0	1	1

OSPF6 Area Status

This is OSPF6 network area status table. It is used to provide the OSPF6 network area status information.

Area ID

The Area ID.

Backbone

Indicate if it's backbone area or not.

Area Type

The area type.

Active Interfaces

Number of active interfaces attached in the area.

SPF Executed Times

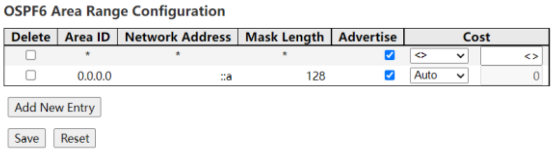
Number of times SPF algorithm has been executed for the particular area.

LSA Count

Number of the total LSAs for the particular area.

6.6.3. Routing

[Routing > OSPFv3 > Routing]



OSPF6 Area Range Configuration

Delete	Area ID	Network Address	Mask Length	Advertise	Cost	
□	*	*	*	☑	<>	<>
□	0.0.0.0	::a	128	☑	Auto	0

OSPF6 Area Range Configuration

This is OSPF6 area range configuration table. It is used to summarize the intra area paths from a specific address range in one summary-LSA (Type-0x2003) and advertised to other areas or configure the address range status as 'DoNotAdvertise' which the summary-LSA (Type-0x2003) is suppressed. The area range configuration is used for Area Border Routers (ABRs) and only router-LSAs (Type-0x2001) and network-LSAs (Type-0x2002) can be summarized. The AS-external-LSAs (Type-0x4005) cannot be summarized because the scope is OSPF6 autonomous system (AS). The AS-external-LSAs (Type-0x4007) cannot be summarized because the feature is not supported yet.

Delete

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

Area ID

The OSPF6 area ID.

Network Address

IPv6 network address.

Mask Length

IPv6 network mask length.

Advertised

When the value is true, it summarizes intra area paths from the address range in one Inter-Area Prefix LSA (Type-0x2003) and advertised to other areas. Otherwise, the intra area paths from the address range are not advertised to other areas.

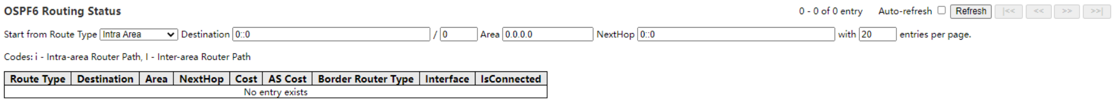
Auto/Specific

When 'Auto' is selected, the cost value is set to 0 automatically and isn't allowed to be configured.

Cost

User specified cost (or metric) for this summary route. It is allowed to be configured only when 'Specific' is selected. The allowed range is 0 to 16777215 and the default setting is 'auto cost' mode.

[Status]



OSPF6 Routing Status

0 - 0 of 0 entry Auto-refresh ☐

Start from Route Type Intra Area Destination 0::0 / 0 Area 0.0.0.0 NextHop 0::0 with 20 entries per page.

Codes: i - Intra-area Router Path, I - Inter-area Router Path

Route Type	Destination	Area	NextHop	Cost	AS Cost	Border Router Type	Interface	IsConnected
No entry exists								

OSPF6 Routing Status

This is OSPF6 routing status table. It is used to provide the OSPF6 routing status information.

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 "Start from Route Type" 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Route Type

The OSPF6 route type.

Intra Area: The destination is an OSPF6 route which is located on intra-area.

Inter Area: The destination is an OSPF6 route which is located on inter-area.

Border Router: The destination is a border router.

External Type-1: The destination is an external Type-1 route.

External Type-2: The destination is an external Type-2 route.

Destination

Network and prefix (example 10.0.0.0/16) of the given route entry.

Area

It indicates which area the route or router can be reached via/to.

NextHop

An Ipv6 address represented as human readable text as specified in RFC5952.

Cost

The cost of the route.

AS Cost

The cost of the route within the OSPF6 network. It is valid for external Type-2 route and always '0' for other route type.

Border Router Type

The border router type of the OSPF6 route entry.

i-ABR: The border router is an ABR.

i-ASBR: The border router is an ASBR located on Intra-area.

I-ASBR: The border router is an ASBR located on Inter-area.

i-ABR/ASBR: The border router is an ASBR attached to at least 2 areas.

Interface

The interface where the ip packet is outgoing.

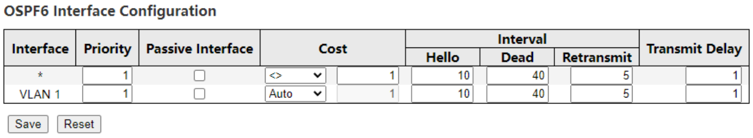
IsConnected

The destination is connected directly or not.

6.6.4. Interfaces

[Routing > OSPFv3 > Interfaces]

[Configuration]



OSPF6 Interface Configuration

Interface	Priority	Passive Interface	Cost		Interval			Transmit Delay
					Hello	Dead	Retransmit	
*	1	□	<>	1	10	40	5	1
VLAN 1	1	□	Auto	1	10	40	5	1

OSPF6 Interface Configuration

This is interface configuration parameters.

Interfaces

Interface identification.

Priority

User specified router priority for the interface. The allowed range is 0 to 255 and the default value is 1.

Passive Interface

Indicates whether the interface is passive or not.

Cost

User specified cost for this interface. It's link state metric for the interface. The field is significant only when 'IsSpecificCost' is TRUE. The allowed range is 1 to 65535 and the default setting is 'auto cost' mode.

Hello Interval

How many Hello packets will be sent per second. The allowed range is 1 to 65535 and the default value is 10 (seconds).

Dead Interval

The time interval (in seconds) between hello packets. The allowed range is 1 to 65535 and the default value is 40 (seconds).

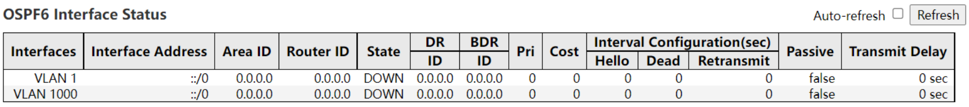
Retransmit Interval

The time interval (in seconds) between link-state advertisement(LSA) retransmissions for adjacencies. The allowed range is 3 to 65535 and the default value is 5 (seconds).

Transmit Delay

Set the transmit-delay value for the specified interface.

[Status]



OSPF6 Interface Status

Interfaces	Interface Address	Area ID	Router ID	State	DR	BDR	Pri	Cost	Interval Configuration(sec)			Passive	Transmit Delay
					ID	ID			Hello	Dead	Retransmit		
VLAN 1	::/0	0.0.0.0	0.0.0.0	DOWN	0.0.0.0	0.0.0.0	0	0	0	0	0	false	0 sec
VLAN 1000	::/0	0.0.0.0	0.0.0.0	DOWN	0.0.0.0	0.0.0.0	0	0	0	0	0	false	0 sec

OSPF6 Interface Status

This is OSPF6 interface status table. It is used to provide the OSPF6 interface status information.

Interface

Interface identification.

Interface Address

IPv6 network address.

Area ID

The OSPF6 area ID.

Router ID

The OSPF6 router ID.

State

The state of the link.

DR ID

The router ID of DR.

BDR ID

The router ID of BDR.

Priority

The OSPF6 priority. It helps determine the DR and BDR on the network to which this interface is connected.

Cost

The cost of the interface.

Hello

Hello timer. A time interval that a router sends an OSPF6 hello packet.

Dead

Dead timer. Dead timer is a time interval to wait before declaring a neighbor dead. The unit of time is the second.

Retransmit

Retransmit timer. A time interval to wait before retransmitting a database description packet when it has not been acknowledged.

Passive

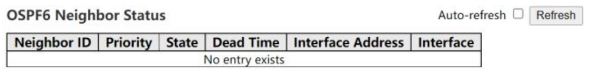
Indicate if the interface is passive interface.

Transmit Delay

The estimated time to transmit a link-state update packet on the interface.

6.6.5. Neighbor

[Routing > OSPFv3 > Neighbor]



OSPF6 Neighbor Status

Neighbor ID	Priority	State	Dead Time	Interface Address	Interface
No entry exists					

OSPF6 Neighbor Status

This is OSPF6 IPv6 neighbor status parameters. It is used to provide the OSPF6 neighbor status information.

Neighbor ID

The Neighbor ID.

Priority

The priority of OSPF6 neighbor. It indicates the priority of the neighbor router. This item is used when selecting the DR for the network. The router with the highest priority becomes the DR.

State

The state of OSPF6 neighbor. It indicates the functional state of the neighbor router.

Dead Time

Dead timer. It indicates the amount of time remaining that the router waits to receive an OSPF6 hello packet from the neighbor before declaring the neighbor down.

Interface Address

The IP address.

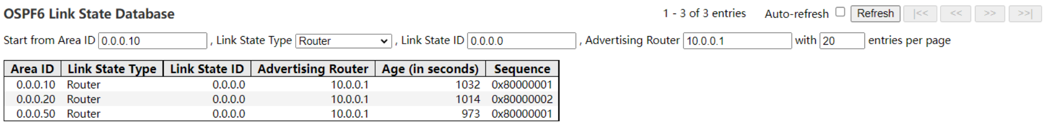
Interface

The network interface.

6.6.6. Database

General Database

[Routing > OSPFv3 > Database > General Database]



OSPF6 Link State Database

1 - 3 of 3 entries Auto-refresh ☐

Start from Area ID 0.0.0.10 , Link State Type Router , Link State ID 0.0.0.0 , Advertising Router 10.0.0.1 with 20 entries per page

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Sequence
0.0.0.10	Router	0.0.0.0	10.0.0.1	1032	0x80000001
0.0.0.20	Router	0.0.0.0	10.0.0.1	1014	0x80000002
0.0.0.50	Router	0.0.0.0	10.0.0.1	973	0x80000001

OSPF6 Link State Database

The OSPF6 LSA link state database 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 "Start from Area ID" input field allows 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Area ID

The OSPF6 area ID of the link state advertisement. It is not required for external LSA.

Link State Type

The type of the link state advertisement.

Link State ID

The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router

The advertising router ID which originated the LSA.

Age

The time in seconds since the LSA was originated.

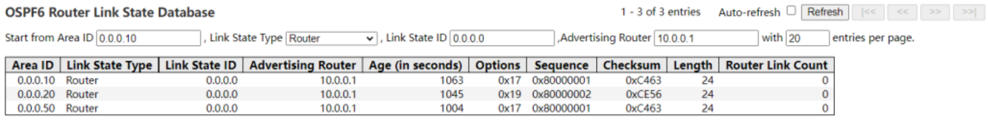
Sequence

The LS sequence number of the LSA.

Detail Database

[Routing > OSPFv3 > Database > Detail Database]

[Router]



OSPF6 Router Link State Database

1 - 3 of 3 entries Auto-refresh □ Refresh |<< << >> >>|

Start from Area ID 0.0.0.10 , Link State Type Router , Link State ID 0.0.0.0 ,Advertising Router 10.0.0.1 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Router Link Count
0.0.0.10	Router	0.0.0.0	10.0.0.1	1063	0x17	0x80000001	0xC463	24	0
0.0.0.20	Router	0.0.0.0	10.0.0.1	1045	0x19	0x80000002	0xCE56	24	0
0.0.0.50	Router	0.0.0.0	10.0.0.1	1004	0x17	0x80000001	0xC463	24	0

OSPF6 Router Link State Database

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 "Start from Area ID" input field allows 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Area ID

The OSPF6 area ID of the link state advertisement.

Link State Type

The type of the link state advertisement.

Link State ID

The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router

The advertising router ID which originated the LSA.

Age

The time in seconds since the LSA was originated.

Options

The OSPF6 option field which is present in OSPF6 hello packets, which enables OSPF6 routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF6 routers.

Sequence

The LS sequence number of the LSA.

Checksum

The checksum of the LSA contents.

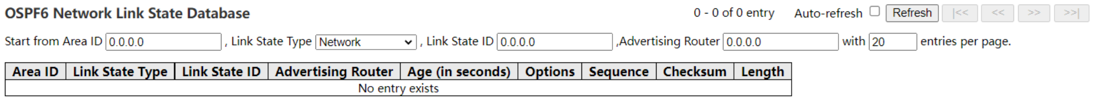
Length

The Length in bytes of the LSA.

Router Link Count

The link count of the LSA. The field is significant only when the link state type is 'Router Link State' (Type 1).

[Network]



OSPF6 Network Link State Database

0 - 0 of 0 entry Auto-refresh □ Refresh |<< << >> >>|

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 ,Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length
No entry exists								

OSPF6 Network Link State Database

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 "Start from Area ID" input field allows 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Area ID

The OSPF6 area ID of the link state advertisement.

Link State Type

The type of the link state advertisement.

Link State ID

The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router

The advertising router ID which originated the LSA.

Age

The time in seconds since the LSA was originated.

Options

The OSPF6 option field which is present in OSPF6 hello packets, which enables OSPF6 routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF6 routers.

Sequence

The LS sequence number of the LSA.

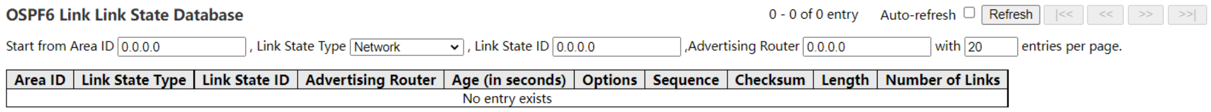
Checksum

The checksum of the LSA contents.

Length

The Length in bytes of the LSA.

[Link]



OSPF6 Link Link State Database

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 ,Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Number of Links
No entry exists									

OSPF6 Link Link State Database

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 "Start from Area ID" input field allows 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Area ID

The OSPF6 area ID of the link state advertisement.

Link State Type

The type of the link state advertisement.

Link State ID

The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router

The advertising router ID which originated the LSA.

Age

The time in seconds since the LSA was originated.

Options

The OSPF6 option field which is present in OSPF6 hello packets, which enables OSPF6 routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF6 routers.

Sequence

The LS sequence number of the LSA.

Checksum

The checksum of the LSA contents.

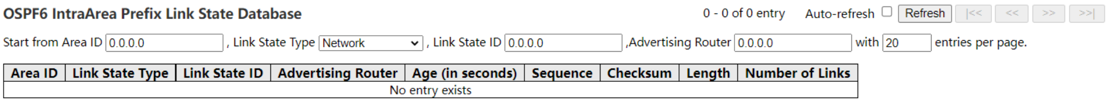
Length

The Length in bytes of the LSA.

Number of Links

The count of the LSA.

[IntraArea Prefix]



OSPF6 IntraArea Prefix Link State Database

0 - 0 of 0 entry Auto-refresh □

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 ,Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Sequence	Checksum	Length	Number of Links
No entry exists								

OSPF6 IntraArea Prefix Link State Database

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 "Start from Area ID" input field allows 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Area ID

The OSPF6 area ID of the link state advertisement.

Link State Type

The type of the link state advertisement.

Link State ID

The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router

The advertising router ID which originated the LSA.

Age

The time in seconds since the LSA was originated.

Sequence

The LS sequence number of the LSA.

Checksum

The checksum of the LSA contents.

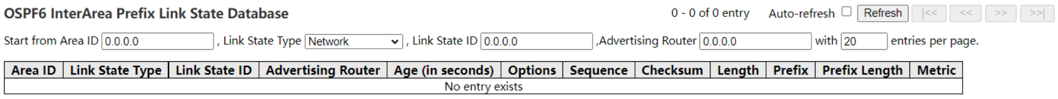
Length

The Length in bytes of the LSA.

Number of Links

The count of the Prefixes.

[InterArea Prefix]



OSPF6 InterArea Prefix Link State Database

0 - 0 of 0 entry Auto-refresh ☐ Refresh |<< << >> >>|

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 ,Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Prefix	Prefix Length	Metric
No entry exists											

OSPF6 InterArea Prefix Link State Database

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 "Start from Area ID" input field allows 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Area ID

The OSPF6 area ID of the link state advertisement.

Link State Type

The type of the link state advertisement.

Link State ID

The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router

The advertising router ID which originated the LSA.

Age

The time in seconds since the LSA was originated.

Options

The OSPF6 option field which is present in OSPF6 hello packets, which enables OSPF6 routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF6 routers.

Sequence

The LS sequence number of the LSA.

Checksum

The checksum of the LSA contents.

Length

The Length in bytes of the LSA.

Prefix

IPv6 network address.

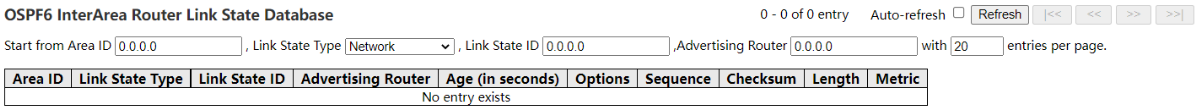
Prefix Length

IPv6 network mask length.

Metric

User specified metric for this summary route. The field is significant only when the link state type is 'Inter_Area Prefix/Router Link State' (Type 3, 4).

[InterArea Router]



OSPF6 InterArea Router Link State Database

0 - 0 of 0 entry Auto-refresh □

Start from Area ID 0.0.0.0 , Link State Type Network , Link State ID 0.0.0.0 ,Advertising Router 0.0.0.0 with 20 entries per page.

Area ID	Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Metric
No entry exists									

OSPF6 InterArea Router Link State Database

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 "Start from Area ID" input field allows 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Area ID

The OSPF6 area ID of the link state advertisement.

Link State Type

The type of the link state advertisement.

Link State ID

The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router

The advertising router ID which originated the LSA.

Age

The time in seconds since the LSA was originated.

Options

The OSPF6 option field which is present in OSPF6 hello packets, which enables OSPF6 routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF6 routers.

Sequence

The LS sequence number of the LSA.

Checksum

The checksum of the LSA contents.

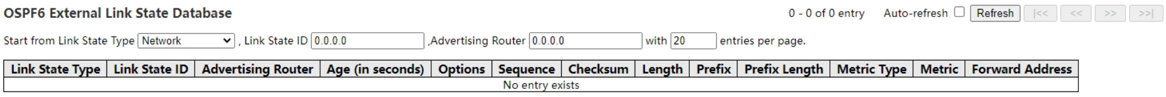
Length

The Length in bytes of the LSA.

Metric

User specified metric for this summary route. The field is significant only when the link state type is 'Summary/ASBR Summary Link State' (Type 3, 4).

[External]



OSPF6 External Link State Database

0 - 0 of 0 entry Auto-refresh ☐ Refresh |<< << >> >>|

Start from Link State Type Network , Link State ID 0.0.0.0 ,Advertising Router 0.0.0.0 with 20 entries per page.

Link State Type	Link State ID	Advertising Router	Age (in seconds)	Options	Sequence	Checksum	Length	Prefix	Prefix Length	Metric Type	Metric	Forward Address
No entry exists												

OSPF6 External Link State Database

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 "Start from Link State Type" input field allows 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Link State Type

The type of the link state advertisement.

Link State ID

The OSPF6 link state ID. It identifies the piece of the routing domain that is being described by the LSA.

Advertising Router

The advertising router ID which originated the LSA.

Age

The time in seconds since the LSA was originated.

Options

The OSPF6 option field which is present in OSPF6 hello packets, which enables OSPF6 routers to support (or not support) optional capabilities, and to communicate their capability level to other OSPF6 routers.

Sequence

The LS sequence number of the LSA.

Checksum

The checksum of the LSA contents.

Length

The Length in bytes of the LSA.

Prefix

IPv6 network address.

Prefix Length

IPv6 network mask length.

Metric Type

The External type of the LSA. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

Metric

User specified metric for this summary route. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

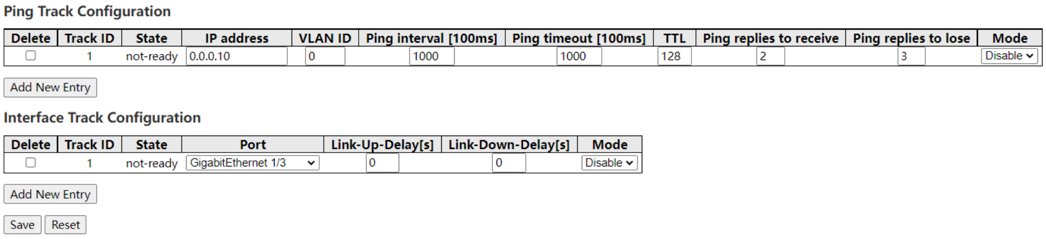
Forward Address

The IP address of forward address. The field is significant only when the link state type is 'External/NSSA External Link State' (Type 5, 7).

6.7. Tracking

[Routing > Tracking]

[Configuration]



Ping Track Configuration

Delete	Track ID	State	IP address	VLAN ID	Ping interval [100ms]	Ping timeout [100ms]	TTL	Ping replies to receive	Ping replies to lose	Mode
□	1	not-ready	0.0.0.10	0	1000	1000	128	2	3	Disable

Add New Entry

Interface Track Configuration

Delete	Track ID	State	Port	Link-Up-Delay[s]	Link-Down-Delay[s]	Mode
□	1	not-ready	GigabitEthernet 1/3	0	0	Disable

Add New Entry

Save Reset

Track Configuration

You can configure Track settings. Click on "Add New Entry" on this page to add Track information. Then click the "Save" button to save the configuration. After checking, click "Delete" on the left side of the configuration display area to delete the corresponding Track configuration.

Delete

Select this option to delete an existing Track.

Track ID

Ping tracking index.

State

tracking instance state.

up: tracked object state is up.
down: tracked object state is down.

not-ready: tracked object state is not ready.

IP address

Set the address of the router to be monitored.

VLAN ID

VLAN interface number.

Ping interval [100ms]

Set the number of milliseconds between the pings to the target router address.

Ping timeout [100ms]

Set the timeout in milliseconds for a ping reply.

TTL

Set the time to live for a ping request packet.

Ping replies to receive

Set the number of consecutive ping successes until the tracked object is considered to be up.

Ping replies to lose

Set the number of consecutive ping misses until the tracked object is considered to be down.

Mode

tracking instance mode.

Disable: Deactivate a tracking instance.

Enable: Activate a tracking instance.

Interface Track Configuration

Delete

Select this option to delete an existing Track.

Track ID

Interface tracking index.

State

tracking instance state.

up: tracked object state is up.

down: tracked object state is down.

not-ready: tracked object state is not ready.

Port

Ethernet interface.

Link-Up-Delay[s]

Set the linkup-delay of the interface tracking instance.

Link-Down-Delay[s]

Set the linkdown-delay of the interface tracking.

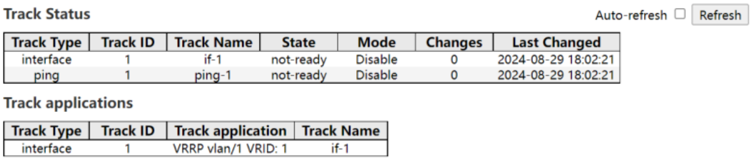
Mode

tracking instance mode.

Disable: Deactivate a tracking instance.

Enable: Activate a tracking instance.

[Status]



Track Status

Track Type	Track ID	Track Name	State	Mode	Changes	Last Changed
interface	1	if-1	not-ready	Disable	0	2024-08-29 18:02:21
ping	1	ping-1	not-ready	Disable	0	2024-08-29 18:02:21

Track applications

Track Type	Track ID	Track application	Track Name
interface	1	VRRP vlan/1 VRID: 1	if-1

Track Status

Track Type

Track instance type.

Track ID

Track instance ID.

Track Name

Track instance name.

State

tracking instance state.

up: tracked object state is up.

down: tracked object state is down.

not-ready: tracked object state is not ready.

Mode

tracking instance mode.

Disable: Deactivate a tracking instance.

Enable: Activate a tracking instance.

Changes

Number of state changes.

Last Changed

Time of last change.

Track applications

Track Type

Track instance type.

Track ID

Track instance ID.

Track application

The applications subscribing to track objects.

Track Name

Track instance name.

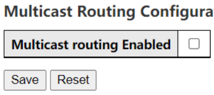
6.8. Multicast Routing

6.8.1. Global

[Routing > Multicast routing > Global]

[Configuration]

This page provides multicast routing configuration.



Multicast Routing Configuration

Multicast routing Enabled	□

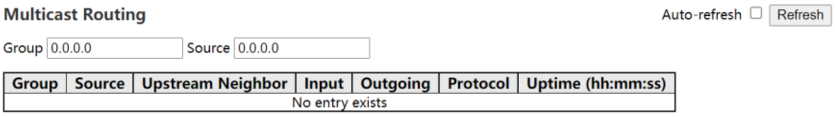
Multicast Routing Configuration

Multicast routing Enabled

The multicast routing function was enabled or disabled. Procedure Multicast routing is a routing protocol used to transmit multicast data in a network. Multicast data is data that is sent simultaneously to a group of recipients. Unlike unicast and broadcast, multicast data is sent only to predetermined multicast group members.

[Statistics]

This page provides multicast route status information.



Multicast Routing

Auto-refresh □

Group 0.0.0.0 Source 0.0.0.0

Group	Source	Upstream Neighbor	Input	Outgoing	Protocol	Uptime (hh:mm:ss)
No entry exists						

Multicast Routing

Group

The destination address of a multicast communication, identifying a set of recipients.

Source

The address of the sender of the multicast communication. The source address identifies the source of a packet.

Upstream Neighbor

In multicast routing, it refers to the interface or neighbor node that transfers multicast packets from one network node to another. An upstream neighbor is a node or interface that is close to the source address in the packet transmission direction.

Input

The network interface that receives multicast packets is also called the receiving interface.

Outgoing

The network interface that transmit multicast packets is also called the transmit interface.

Protocol

A specific communication Protocol that supports Multicast routing, such as Protocol Independent Multicast (PIM) or Internet Group Management Protocol (IGMP).

Uptime (hh:mm:ss)

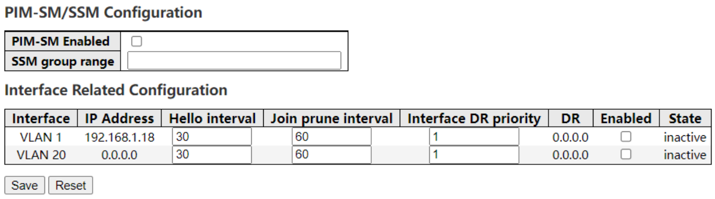
Running time of multicast routing protocol.

6.8.2. PIM

PIM-SM/SSM

[Routing > Multicast routing > PIM > PIM-SM/SSM]

On this page, you can configure PIM-SM/SSM and the pim interface.



PIM-SM/SSM Configuration

PIM-SM Enabled	□
SSM group range	

Interface Related Configuration

Interface	IP Address	Hello interval	Join prune interval	Interface DR priority	DR	Enabled	State
VLAN 1	192.168.1.18	30	60	1	0.0.0.0	□	inactive
VLAN 20	0.0.0.0	30	60	1	0.0.0.0	□	inactive

PIM-SM/SSM Configuration

PIM-SM Enabled

enable/disable PIM-SM.

SSM group range

Specify the multicast group name. You can configure the SSM group address range by specifying the prefix list.

Interface Related Configuration

Interface

The interface for configuring pim services is displayed.

IP Address

The IP address of the current interface is displayed.

Hello interval

Specifies the pim hello message interval, a type of control message used to establish and maintain neighbor relationships.

Join prune interval

The join message is used to notify the PIM router to join a specific multicast group.

Interface DR priority

Specify the interface DR Priority. The router with a higher DR Priority is selected as the DR.

DR

The address of the DR Elected by the current PIM is displayed. 0.0.0.0 indicates that there is no DR.

Enabled

The pim function was enabled or disabled on the interface.

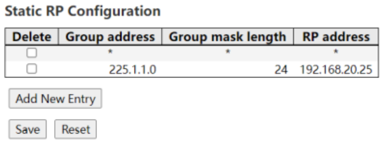
State

Displays the status of the current pim service interface.

Static RP Configuration

[Routing > Multicast routing > PIM > Static RP Configuration]

This page provides Static RP configuration.



Static RP Configuration

Delete	Group address	Group mask length	RP address
□	*	*	*
□	225.1.1.0	24	192.168.20.25

Static RP Configuration

Delete

Delete Static RP configuration.

Group address

Specifies the scope of the multicast group.

Group mask length

Specifies the mask length of the multicast group.

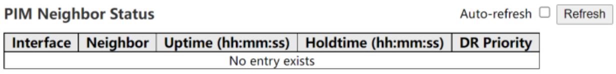
RP address

Specifies the IP address of the Static RP.

Neighbor

[Routing > Multicast routing > PIM > Neighbor]

This page provides the status of the PIM neighbor.



PIM Neighbor Status

Interface	Neighbor	Uptime (hh:mm:ss)	Holdtime (hh:mm:ss)	DR Priority
No entry exists				

PIM Neighbor Status

Interface

An interface that runs the pim protocol for receiving and sending multicast packets.

Neighbor

IP address of the PIM neighbor connected to the current interface, which indicates the IP address of the neighbor router on the current interface.

Uptime (hh:mm:ss)

Running time of the PIM protocol.

Holdtime (hh:mm:ss)

Interval for sending Hello messages by the PIM neighbor router. Hello messages are used to maintain connection status and routing information between neighbors.

DR Priority

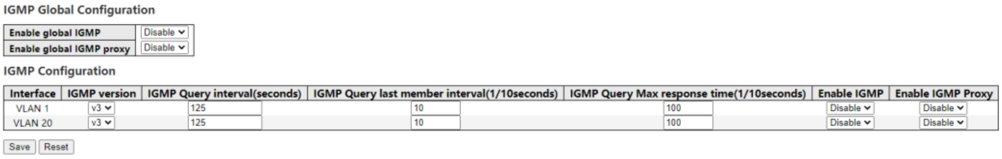
Designated Router (DR) priority: In PIM-SM (Sparse Mode), it refers to the priority value used to select a DR Among multiple routers. In the multicast group, the DR Is responsible for maintaining the multicast tree of the multicast group and forwarding data to related interfaces.

6.8.3. IGMP

[Routing > Multicast routing > IGMP]

[Configuration]

This page provides igmp configuration.



IGMP Global Configuration

Enable global IGMP	Disable
Enable global IGMP proxy	Disable

IGMP Configuration

Interface	IGMP version	IGMP Query interval(seconds)	IGMP Query last member interval(1/10seconds)	IGMP Query Max response time(1/10seconds)	Enable IGMP	Enable IGMP Proxy
VLAN 1	v3	125	10	100	Disable	Disable
VLAN 20	v3	125	10	100	Disable	Disable

IGMP Global Configuration

Enable global IGMP protocol

Enable/Disable igmp.

Enable global IGMP proxy

Enable/Disable igmp proxy.

IGMP Configuration

Interface

The interface for configuring igmp services is displayed.

IGMP protocol version

Specifies the version of IGMP protocol being used. IGMPv2 is the most commonly used version, but IGMPv3 can also be selected to support more features and security.

IGMP Query interval(seconds)

Specifies the time interval (in seconds) between each IGMP Query message. Query messages are sent from IGMP routers to hosts to check if hosts are still interested in a particular group. A shorter query interval can detect host changes more promptly but also increases network traffic.

IGMP Query last member interval (1/10 seconds)

Specifies the time interval (in seconds) for sending query messages after not receiving any member reports. This parameter is used to send query messages after a host leaves a group to confirm if there are other hosts still interested in that group.

IGMP Query Max response time (1/10 seconds)

Specifies the maximum time that hosts wait after receiving a query message to send a member report. If a host doesn't send a member report within this time, it will be considered no longer interested in the group. This parameter is used to coordinate the response time of hosts to query messages and avoid network congestion.

Enable igmp

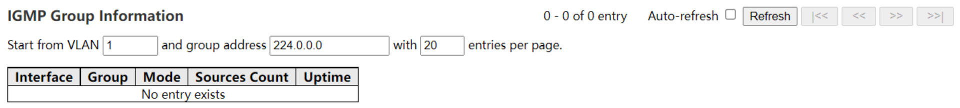
Enable/Disable interface igmp protocol.

Enable igmp proxy

Enable/Disable interface igmp proxy.

[Groups Information]

This page provides igmp groups status information.



IGMP Group Information

0 - 0 of 0 entry Auto-refresh □ Refresh |<< << >> >>|

Start from VLAN 1 and group address 224.0.0.0 with 20 entries per page.

Interface	Group	Mode	Sources Count	Uptime
No entry exists				

IGMP Group Information

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 "Start from VLAN" input field allows 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Interface

Indicates the interface to which the multicast group belongs.

Group

IP address of the multicast group.

Mode

The mode of the multicast group. There are three modes available:

Exclude: indicates that only the specified source can be added to the multicast group.

Include: indicates that all sources except the specified source can be added to the multicast group.

Isolated: indicates that only a specified source can send multicast data to this multicast group.

Sources Count

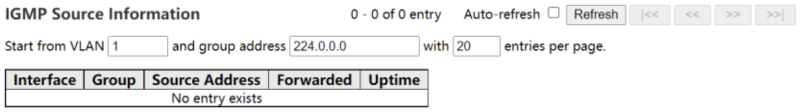
The number of sources in a multicast group.

Uptime

Running time of the multicast group.

[Sources Information]

This page provides igmp sources status information.



IGMP Source Information 0 - 0 of 0 entry

Start from VLAN 1 and group address 224.0.0.0 with 20 entries per page.

Interface	Group	Source Address	Forwarded	Uptime
No entry exists				

IGMP Source Information

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 "Start from VLAN" input field allows 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 Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

Interface

Indicates the interface to which the multicast group belongs.

Group

IP address of the multicast group.

Source Address

IGMP source address, that is, the IP address of the host that initiates the IGMP request.

Forwarded

Whether to forward packets from the source address: By default, the received packets from the source address are forwarded to other network devices. If the device does not allow packets from the source address to be forwarded, the value is displayed as "false".

Uptime

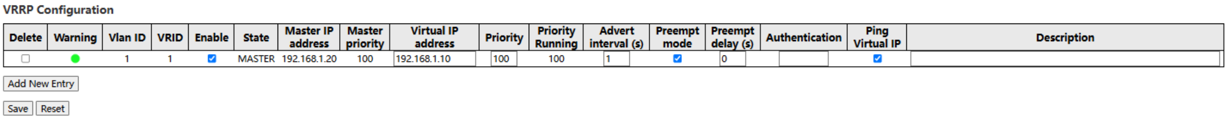
The time since the device received the packet from the source address for the last time. This value can be used to understand how active the source address is.

6.9. L3-Redundancy

6.9.1. VRRP

Configuration

[Routing > L3-Redundancy > VRRP > Configuration]



VRRP Configuration

Delete	Warning	Vlan ID	VRID	Enable	State	Master IP address	Master priority	Virtual IP address	Priority	Priority Running	Advert interval (s)	Preempt mode	Preempt delay (s)	Authentication	Ping Virtual IP	Description
□	●	1	1	☑	MASTER	192.168.1.20	100	192.168.1.10	100	100	1	☑	0		☑	

VRRP Configuration

You can configure VRRP basic settings. Click on "Add New Entry" on this page to add VRRP information. Then click the "Save" button to save the configuration. After checking, click "Delete" on the left side of the configuration display area to delete the corresponding VRRP configuration.

Delete

Select this option to delete an existing VRRP.

Warning

Priority change will have no effect while interface is vrrp address owner.

Vlan ID

Specifies the VLAN-based router interface.

VRID

Specifies the Virtual Router Identifier. Valid values are between 1 and 255.

Enable

Activates/deactivates the VRRP instance specified in this row.

- marked (default setting)

  The VRRP instance is enabled.

- unmarked

  The VRRP instance is disabled.

State

Displays the VRRP state.

- INIT

  VRRP is in the initialization phase, the function is inactive, or the master router is still unnamed.

- BACKUP

  The router sees the possibility of becoming the master router.

- MASTER

  The router is the master router.

Master IP address

Displays the IP address to which the virtual router sends advertisements.

Master priority

Displays the priority to which the virtual router sends advertisements.

Virtual IP address

Specifies the virtual IP address in the subnet of the primary IP address on the interface.

Priority

Specifies the VRRP priority value. The router with the higher priority value takes over the master router role. If the virtual router IP address is the same as the IP address of a router interface, then the router is the IP address owner. If an IP address owner exists, then VRRP assigns the IP address owner the VRRP priority 255 and declares the router as the master router. Valid values are between 1 and 254 (default setting: 100).

Priority Running

Displays the priority of the virtual router. The value differs from Priority if tracked objects are down or the virtual router is the IP address owner.

Advert interval (s)

Specifies the interval for sending out advertisement messages as the master router. Valid values are between 1 and 255 (default setting: 1).

Preempt mode

Activates/deactivates the preempt mode. This setting specifies if this router, as a backup router, takes over the master router role when the master router has a lower VRRP priority.

- marked (default setting)

  When you enable the preempt mode, this router takes the master router role from a router with a lower VRRP priority without waiting for an election.

- unmarked

  When you disable the Preempt mode, this router assumes the role of a backup router and listens for master router advertisements. After the master down interval expires, without receiving advertisements from the master router, this router participates in the master router election process.

Preempt delay (s)

Specifies the pre-empt delay time in seconds. With the pre-empt mode activated and in collaboration with VRRP tracking, a reassignment of the master router role is possible. However, dynamic routing procedures take a certain amount of time to react to route changes and to refill routing tables. To help avoid the loss of packets during this time, the device lets you specify a pre-empt delay. The delay lets the dynamic routing procedure fill the routing tables before reassignment of the master router role. Valid values are between 0 and 255 (default setting: 0).

Authentication

Specifies the authentication string. The authentication string contains a maximum of 8 characters.

Ping Virtual IP

Activates/deactivates the ping to the virtual IP of the VRRP group. You use the VRRP ping for connectivity analyses. The prerequisite for allowing the device to answer ping requests from the interfaces is that you activate the function globally. In the Routing > IP> IP Configuration, mark the Send Echo Reply checkbox.

- marked (default setting)

The device answers ICMP ping requests.

- unmarked

The device ignores ICMP ping requests.

Description

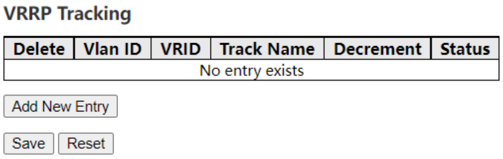
Specifies the description string. The description string contains a maximum of 64 characters.

Include English letters, digits, and common symbols and space.

Note : The same VLAN interface supports the maximum number of VRRP is 2.

Tracking

[Routing > L3-Redundancy > VRRP > Tracking]



VRRP Tracking

Delete	Vlan ID	VRID	Track Name	Decrement	Status
No entry exists					

VRRP Tracking

You can configure VRRP Tracking settings. Click on "Add New Entry" on this page to add VRRP information. Then click the "Save" button to save the configuration. After checking, click "Delete" on the left side of the configuration display area to delete the corresponding VRRP Tracking configuration.

Delete

Select this option to delete an existing VRRP Tracking.

Vlan ID

Select the router interface number of the virtual router.

VRID

Select the virtual router ID for this virtual router. Valid values are between 1 and 255.

Track name

Displays the name of the tracking object to which the virtual router is linked. If the result for a tracking object is negative, then the VRRP instance reduces the priority of the virtual router. The tracking object is negative for example, if the monitored interface is inactive or the monitored router cannot be reached.

Decrement

Specifies the value by which the VRRP instance reduces the priority of the virtual router when the monitoring result is negative. Valid values are between 1 and 254 (default setting: 20).

Status

Displays the monitoring result of the tracking object.

- UP

  The monitoring result is positive.

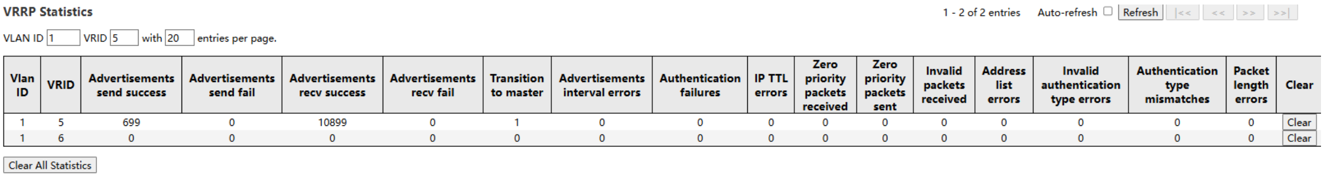
- DOWN

  The monitoring result is negative.

Statistics

[Routing > L3-Redundancy > VRRP > Statistics]

This page can display the number of counters that count events related to VRRP functionality. Click on "Clear" on this page to clear statistical data. Click on “Clear Alll Statistics” on this page to clear all statistical data.



VRRP Statistics

1 - 2 of 2 entries Auto-refresh □ Refresh |<< << >> >>|

VLAN ID 1 VRID 5 with 20 entries per page.

Vlan ID	VRID	Advertisements send success	Advertisements send fail	Advertisements recv success	Advertisements recv fail	Transition to master	Advertisements interval errors	Authentication failures	IP TTL errors	Zero priority packets received	Zero priority packets sent	Invalid packets received	Address list errors	Invalid authentication type errors	Authentication type mismatches	Packet length errors	Clear
1	5	699	0	10899	0	1	0	0	0	0	0	0	0	0	0	0	Clear
1	6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Clear

Clear All Statistics

VRRP Statistics

Advertisements send success

Displays the number of VRRP advertisements sended success.

Advertisements send fail

Displays the number of VRRP advertisements sended fail.

Advertisements recv success

Displays the number of VRRP advertisements received success.

Advertisements recv fail

Displays the number of VRRP advertisements received fail.

Transition to master

Displays the number of VRRP router transition to master state.

Advertisements interval errors

Displays the number of VRRP advertisements received by the router outside the advertisement interval. The value lets you determine if the routers have the same advertise interval specified across the virtual router instance.

Authentication failures

Displays the number of VRRP advertisements received with authentication errors.

IP TTL errors

Displays the number of VRRP advertisements received with an IP TTL not equal to 255.

Zero priority packets received

Displays the number of VRRP advertisements received with priority 0.

Zero priority packets sent

Displays the number of VRRP advertisements that the device sent with priority 0.

Invalid packets received

Displays the number of invalid VRRP advertisements received.

Address list errors

Displays the number of VRRP advertisements received for which the address list does not match the address list configured locally for the virtual router.

Invalid authentication type errors

Displays the number of VRRP advertisements received with an invalid authentication type.

Authentication type mismatches

Displays the number of VRRP advertisements received with an incorrect authentication type.

Packet length errors

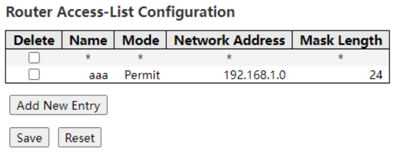
Displays the number of VRRP advertisements received with an incorrect packet length.

Clear

Clear a single VRRP statistic.

6.10. Access-list

[Routing > Access-list]



Router Access-List Configuration

Delete	Name	Mode	Network Address	Mask Length
□	*	*	*	*
□	aaa	Permit	192.168.1.0	24

Router Access-List Configuration

Delete

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

Name

Access-list name.

Mode

The access right mode of the access-list entry.

Network Address

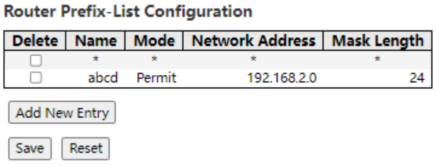
IPv4 network address.

Mask Length

IPv4 network mask length.

6.11. Prefix-list

[Routing > Prefix-list]



Router Prefix-List Configuration

Delete	Name	Mode	Network Address	Mask Length
□	*	*	*	*
□	abcd	Permit	192.168.2.0	24

Router Prefix-List Configuration

Delete

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

Name

Prefix-list name.

Mode

The access right mode of the prefix-list entry.

Network Address

IPv4 network address.

Mask Length

IPv4 network mask length.

7. Diagnostics

The menu contains the following dialogs:

Status Configuration
System
Ports
LLDP
Loop Protection
SFlow
DDMI
UDLD
Ping
Traceroute
Copper Cable Test

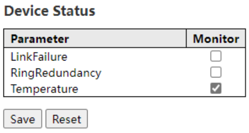
7.1. Status Configuration

7.1.1. Device Status

[Diagnostics > Status Configuration > Device Status]

[Configuration]

On this page, you can configure the device status.



Device Status

Parameter	Monitor
LinkFailure	□
RingRedundancy	□
Temperature	☑

Device Status

Parameters

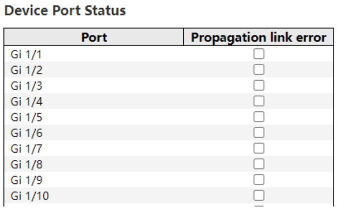
This section is used to display the configuration items for the device status. The content of parameters may vary depending on the device.

Monitor

Use the checkbox to control whether the device status configuration items are monitored.

[Port]

On this page, you can configure the port status feature within the device status.



Device Port Status

Port	Propagation link error
Gi 1/1	□
Gi 1/2	□
Gi 1/3	□
Gi 1/4	□
Gi 1/5	□
Gi 1/6	□
Gi 1/7	□
Gi 1/8	□
Gi 1/9	□
Gi 1/10	□

Device Port Status

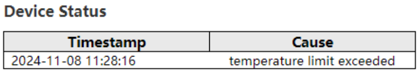
Port

Used to display all ports of the device status.

Propagation Link Errors

Use the checkbox to control whether the device port configuration items monitor the propagation link errors option.

[Status]



Device Status

Timestamp	Cause
2024-11-08 11:28:16	temperature limit exceeded

Device Status

Timestamp

Used to display the time when this alert item occurred.

Cause

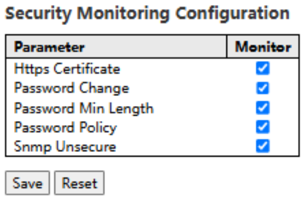
Used to display the specific content of the alert item.

7.1.2. Security Status

[Diagnostics > Status Configuration > Security Status]

[Configuration]

On this page, you can configure the device security status.



Security Monitoring Configuration

Parameter	Monitor
Https Certificate	☑
Password Change	☑
Password Min Length	☑
Password Policy	☑
Snmp Unsecure	☑

Security Monitoring Configuration

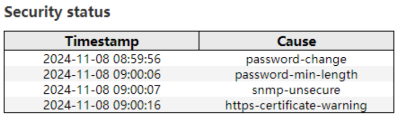
Parameters

Used to display the configuration items for the device security status. The content of parameters may vary depending on the device.

Monitor

Use the checkbox to control whether the device status configuration items are monitored.

[Status]



Security status

Timestamp	Cause
2024-11-08 08:59:56	password-change
2024-11-08 09:00:06	password-min-length
2024-11-08 09:00:07	snmp-unsecure
2024-11-08 09:00:16	https-certificate-warning

Security status

Timestamp

Used to display the time when this alert item occurred.

Cause

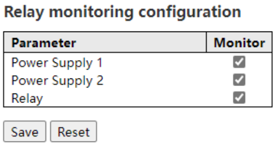
Check Item Used to display the specific content of the alert item.

7.1.3. Relay Status

[Diagnostics > Status Configuration > Relay Status]

[Configuration]

On this page, you can configure the device Relay status.



Relay monitoring configuration

Parameter	Monitor
Power Supply 1	☑
Power Supply 2	☑
Relay	☑

Relay monitoring configuration

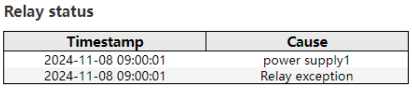
Parameters

Used to display the configuration items for the device Relay status. The content of parameters may vary depending on the device.

Monitor

Use the checkbox to control whether the device status configuration items are monitored.

[Status]



Relay status

Timestamp	Cause
2024-11-08 09:00:01	power supply1
2024-11-08 09:00:01	Relay exception

Relay status

Timestamp

Used to display the time when this alert item occurred.

Cause

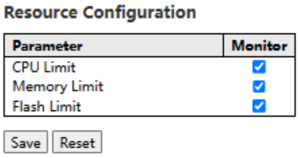
Check Item Used to display the specific content of the alert item.

7.1.4. Resource Status

[Diagnostics > Status Configuration > Resource Status]

[Configuration]

On this page, you can configure the device Resource status.



Resource Configuration

Parameter	Monitor
CPU Limit	☑
Memory Limit	☑
Flash Limit	☑

Resource Configuration

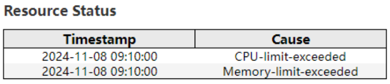
Parameters

Used to display the configuration items for the device Resource status. The content of parameters may vary depending on the device.

Monitor

Use the checkbox to control whether the device status configuration items are monitored.

[Status]



Resource Status

Timestamp	Cause
2024-11-08 09:10:00	CPU-limit-exceeded
2024-11-08 09:10:00	Memory-limit-exceeded

Resource Status

Timestamp

Used to display the time when this alert item occurred.

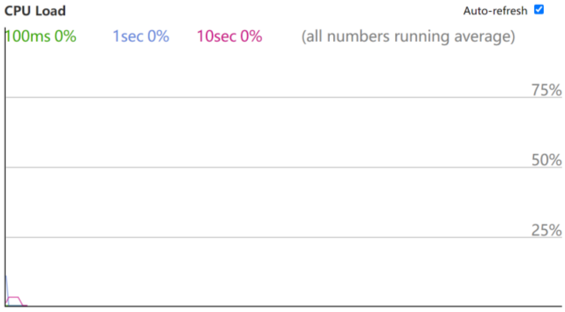
Cause

Check Item Used to display the specific content of the alert item.

7.2. System

7.2.1. CPU Load

[Diagnostics > System > CPU Load]



CPU Load

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.

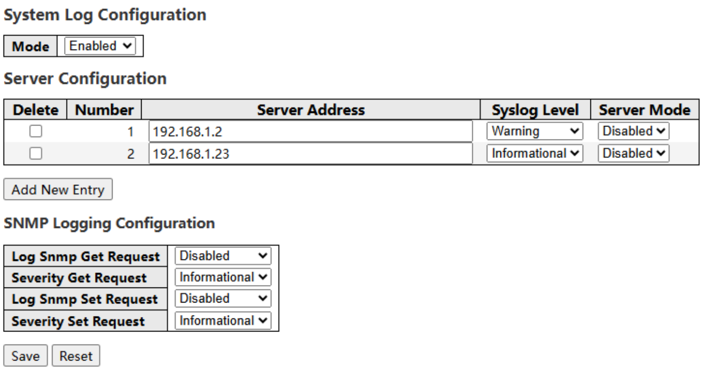
In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.

7.2.2. Log

[Diagnostics > System > Log]

[configuration]

On this page, you can configure the System Log.



System Log Configuration

Mode	Enabled

Server Configuration

Delete	Number	Server Address	Syslog Level	Server Mode
□	1	192.168.1.2	Warning	Disabled
□	2	192.168.1.23	Informational	Disabled

SNMP Logging Configuration

Log Snmp Get Request	Disabled
Severity Get Request	Informational
Log Snmp Set Request	Disabled
Severity Set Request	Informational

System Log Configuration

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.

Delete

Clear this server's configuration.

Number

Display the server's serial number.

Server Address

Indicates the IPv4 host address of syslog server. If the switch provide DNS feature, it also can be a domain name.

Syslog Level

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

Error: Send the specific messages which severity code is less or equal than Error (3).

Warning: Send the specific messages which severity code is less or equal than Warning (4).

Notice: Send the specific messages which severity code is less or equal than Notice (5).

Informational: Send the specific messages which severity code is less or equal than Informational.

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.

SNMP Logging Configuration

Log Snmp Get Request

Enables/disables the logging of SNMP Get requests.

Severity Get Request

Specifies the severity of the event that the device registers for SNMP Get requests.

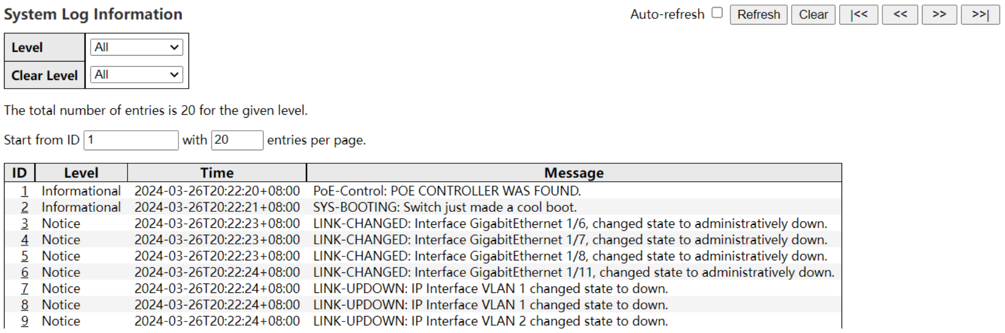
Log Snmp Set Request

Enables/disables the logging of SNMP Set requests.

Severity Set Request

Specifies the severity of the event that the device registers for SNMP Set requests.

[Status]



System Log Information

Level	All
Clear Level	All

The total number of entries is 20 for the given level.

Start from ID 1 with 20 entries per page.

ID	Level	Time	Message
1	Informational	2024-03-26T20:22:20+08:00	PoE-Control: POE CONTROLLER WAS FOUND.
2	Informational	2024-03-26T20:22:21+08:00	SYS-BOOTING: Switch just made a cool boot.
3	Notice	2024-03-26T20:22:23+08:00	LINK-CHANGED: Interface GigabitEthernet 1/6, changed state to administratively down.
4	Notice	2024-03-26T20:22:23+08:00	LINK-CHANGED: Interface GigabitEthernet 1/7, changed state to administratively down.
5	Notice	2024-03-26T20:22:23+08:00	LINK-CHANGED: Interface GigabitEthernet 1/8, changed state to administratively down.
6	Notice	2024-03-26T20:22:24+08:00	LINK-CHANGED: Interface GigabitEthernet 1/11, changed state to administratively down.
7	Notice	2024-03-26T20:22:24+08:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to down.
8	Notice	2024-03-26T20:22:24+08:00	LINK-UPDOWN: IP Interface VLAN 1 changed state to down.
9	Notice	2024-03-26T20:22:24+08:00	LINK-UPDOWN: IP Interface VLAN 2 changed state to down.

System Log Information

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 **Clear** button.

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 **Refresh** 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.

ID

The identification of the system log entry.

Level

The level of the system log entry.

Informational: The system log entry is belonged to information level.

Warning: The system log entry is belonged to warning level.

Error: The system log entry is belonged to error level.

Notice: The system log entry is belonged to notice level.

All: The system log entry is belonged to all level.

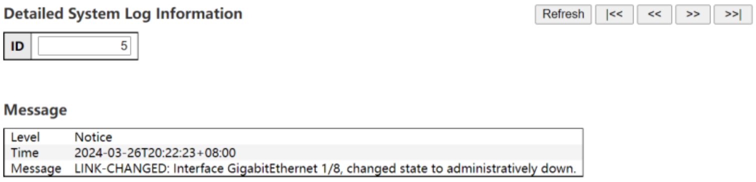
Time

The occurred time of the system log entry.

Message

The detail message of the system log entry.

If you click on the ID in the navigation bar, the page appears as shown as below:



Detailed System Log Information

ID 5

Message

Level	Notice
Time	2024-03-26T20:22:23+08:00
Message	LINK-CHANGED: Interface GigabitEthernet 1/8, changed state to administratively down.

Detailed System Log Information

This option displays detailed log information of the switch system.

Level

The severity level of the system log entry.

ID

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

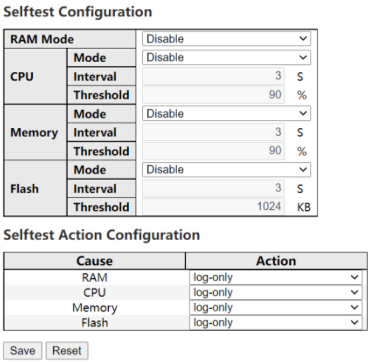
Message

The detailed message of the system log entry.

7.2.3. Selftest

[Diagnostics > System > Selftest]

On this page, you can configure the Selftest.



Selftest Configuration

RAM Mode		Disable	
CPU	Mode	Disable	
	Interval	3	s
	Threshold	90	%
Memory	Mode	Disable	
	Interval	3	s
	Threshold	90	%
Flash	Mode	Disable	
	Interval	3	s
	Threshold	1024	KB

Selftest Action Configuration

Cause	Action
RAM	log-only
CPU	log-only
Memory	log-only
Flash	log-only

Selftest Configuration

RAM Mode

Enable or disable the RAM selftest on cold start of the device. When disabled the device booting time is reduced.

CPU Mode

Enable or disable the CPU self-test feature of the device.

CPU Interval

Configure the value of the CPU self-test interval. The unit is in seconds.

CPU Threshold

Configure the value of the rising threshold for the CPU self-test. The unit is in percentage.

Memory Mode

Enable or disable the memory self-test feature of the device.

Memory Interval

Configure the value of the memory self-test interval. The unit is in seconds.

Memory Threshold

Configure the value of the rising threshold for the memory self-test. The unit is in percentage.

Flash Mode

Enable or disable the flash self-test feature of the device.

Flash Interval

Configure the value of the flash self-test interval. The unit is in seconds.

Flash Threshold

Configure the value of the falling threshold for the flash self-test. The unit is in KB.

Selftest Action Configuration

Cause

The selftest component:

Ramtest, CPU, Memory, Flash.

Action

Configure the action that a selftest component should take.

log-only: Write a message to the logging file.

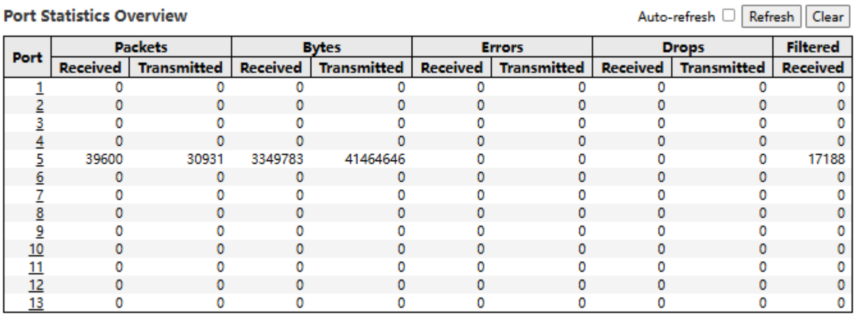
send-trap: Send a trap to the management station.

7.3. Ports

7.3.1. Traffic Overview

[Diagnostics > Ports > Traffic Overview]

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



Port Statistics Overview

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	39600	30931	3349783	41464646	0	0	0	0	17188
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0

Port Traffic Overview

Port

The logical port for the settings contained in the same row.

Packets

The number of received and transmitted packets per port.

Bytes

The number of received and transmitted bytes per port.

Errors

The number of frames received in error and the number of incomplete transmissions per port.

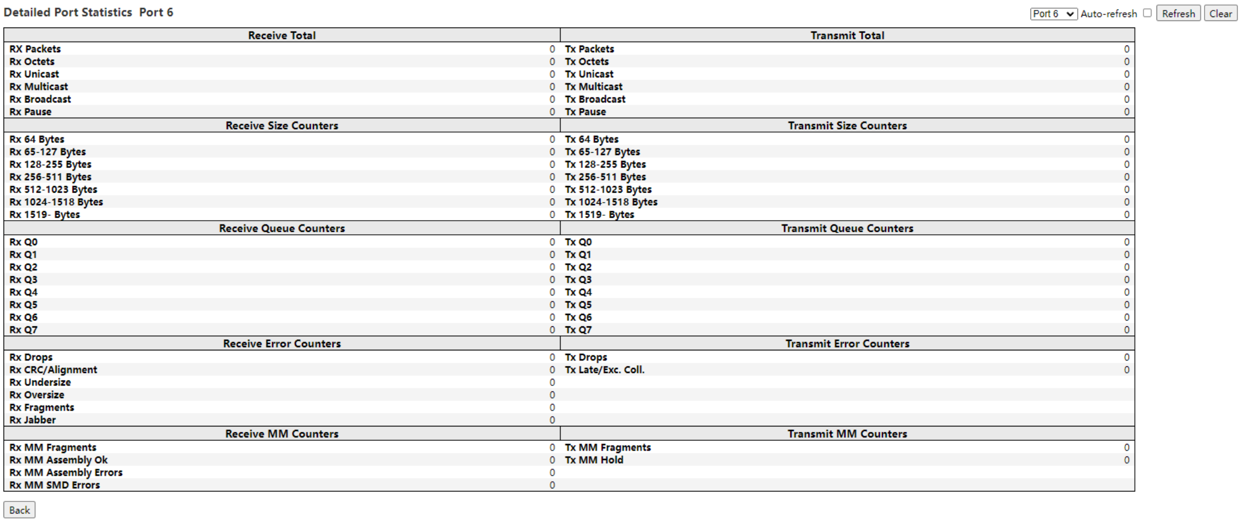
Drops

The number of frames discarded due to ingress or egress congestion.

Filtered

STP blocked packet reception count.

Click port to display details.



Detailed Port Statistics Port 6

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 1024-1518 Bytes	0	Tx 1024-1518 Bytes	0
Rx 1519- Bytes	0	Tx 1519- 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 MM Counters		**Transmit MM Counters**	
Rx MM Fragments	0	Tx MM Fragments	0
Rx MM Assembly Ok	0	Tx MM Hold	0
Rx MM Assembly Errors	0		
Rx MM SMD Errors	0		

Detailed Port Statistics Port

This option 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, the error counters for receive and transmit, and the MM counters for receive and transmit.

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 and bad) packets split into categories based on 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 ingress 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.

Short frames are frames that are smaller than 64 bytes.

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

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.

Receive MM Counters

Rx MM Fragments: A count of received MAC frame fragments.

Rx MM Assembly Ok: A count of MAC frames that were successfully reassembled and delivered to MAC.

Rx MM Assembly Errors: A count of MAC frames with reassembly errors. The counter is incremented when the ASSEMBLY_ERROR state of the Receive Processing State Diagram is entered.

Rx MM SMD Errors: A count of received MAC frames / MAC frame fragments rejected due to unknown SMD value or arriving with an SMD-C when no frame is in progress. The counter is incremented each time the BAD_FRAG state of the Receive Processing State Diagram is entered.

Transmit MM Counters

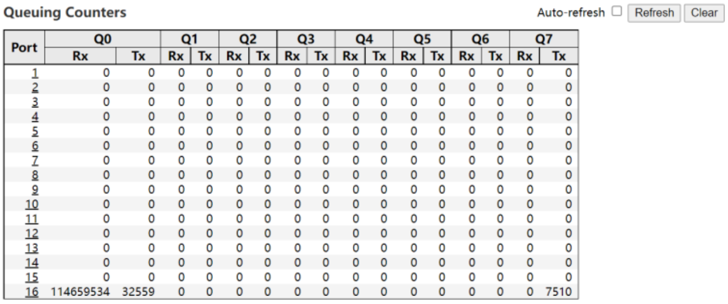
Tx MM Fragments: A count of transmitted MAC frame fragments.

Tx MM Hold: A count of times MM_CTL.request(HOLD) primitive assertion caused preemption of a preemptable MAC frame.

7.3.2. QoS Statistics

[Diagnostics > Ports > QoS Statistics]

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



Queuing Counters

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	114659534	32559	0	0	0	0	0	0	0	0	0	0	0	0	0	7510

Queuing Counters

Port

The logical port for the settings contained in the same row.

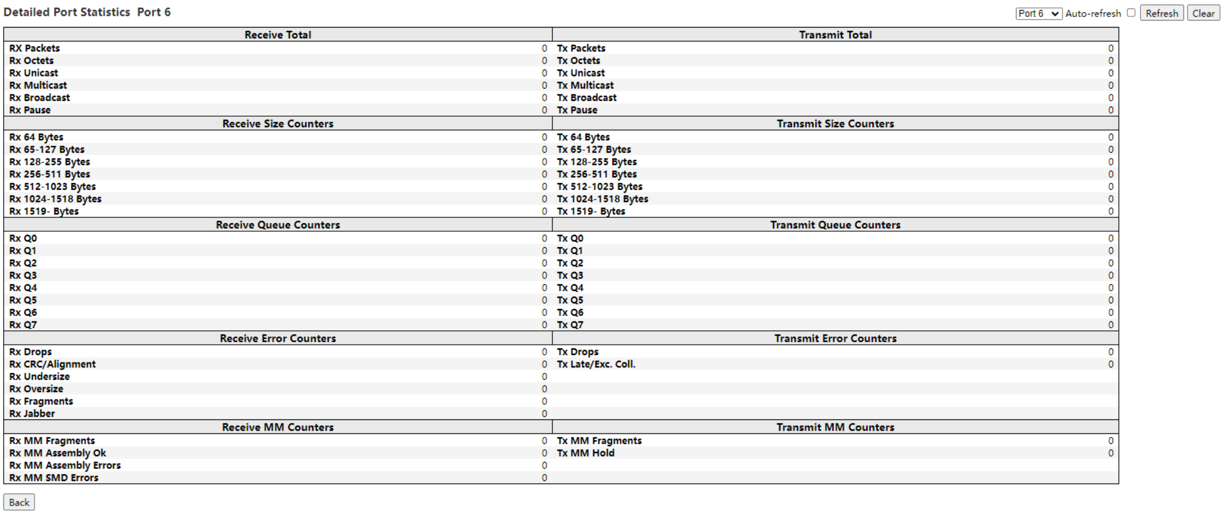
Qn

There are 8 QoS queues per port. Q0 is the lowest priority queue.

Rx/Tx

The number of received and transmitted packets per queue.

Click port to display details.



Detailed Port Statistics Port 6

Port 6 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 1024-1518 Bytes	0	Tx 1024-1518 Bytes	0
Rx 1519- Bytes	0	Tx 1519- 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 MM Counters		**Transmit MM Counters**	
Rx MM Fragments	0	Tx MM Fragments	0
Rx MM Assembly Ok	0	Tx MM Hold	0
Rx MM Assembly Errors	0		
Rx MM SMD Errors	0		

Detailed Port Statistics Port #

This option 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, the error counters for receive and transmit, and the MM counters for receive and transmit.

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 and bad) packets split into categories based on 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 ingress 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.

Short frames are frames that are smaller than 64 bytes.

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

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.

Receive MM Counters

Rx MM Fragments: A count of received MAC frame fragments.

Rx MM Assembly Ok: A count of MAC frames that were successfully reassembled and delivered to MAC.

Rx MM Assembly Errors: A count of MAC frames with reassembly errors. The counter is incremented when the ASSEMBLY_ERROR state of the Receive Processing State Diagram is entered.

Rx MM SMD Errors: A count of received MAC frames / MAC frame fragments rejected due to unknown SMD value or arriving with an SMD-C when no frame is in progress. The counter is incremented each time the BAD_FRAG state of the Receive Processing State Diagram is entered.

Transmit MM Counters

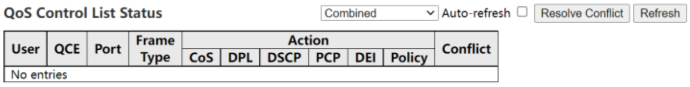
Tx MM Fragments: A count of transmitted MAC frame fragments.

Tx MM Hold: A count of times MM_CTL.request(HOLD) primitive assertion caused preemption of a preemptable MAC frame.

7.3.3. QCL Status

[Diagnostics > Ports > 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.



QoS Control List Status

User	QCE	Port	Frame Type	Action						Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	
No entries										

The parameters in the upper right drop-down menu are:

1. Combined
2. Static
3. Voice VLAN
4. DHCPv6 Snooping
5. IPv6 Source Guard
6. conflict

QoS Control List Status

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.

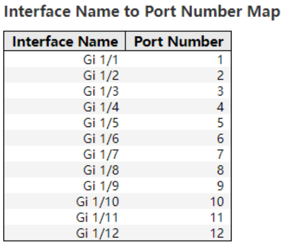
Ingress Map: Classify Ingress Map ID.

Conflict

Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

7.3.4. Name Map

[Diagnostics > Ports > Name Map]



Interface Name to Port Number Map

Interface Name	Port Number
Gi 1/1	1
Gi 1/2	2
Gi 1/3	3
Gi 1/4	4
Gi 1/5	5
Gi 1/6	6
Gi 1/7	7
Gi 1/8	8
Gi 1/9	9
Gi 1/10	10
Gi 1/11	11
Gi 1/12	12

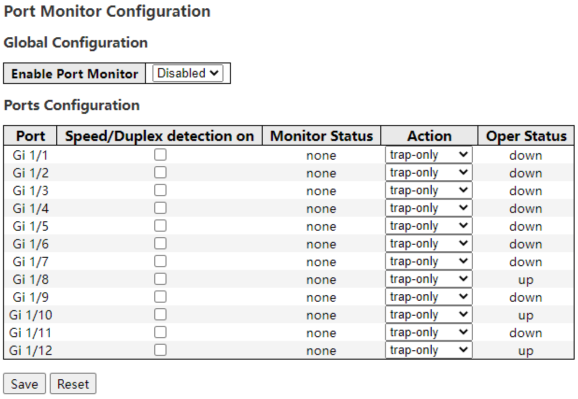
Many Web pages use a port number to express an interface, whereas CLI uses interface names. The table on this page provides a means to convert from one to the other.

7.3.5. Ports Monitor

Global

[Diagnostics > Ports > Ports Monitor > Global]

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



Port Monitor Configuration

Global Configuration

Enable Port Monitor	Disabled

Ports Configuration

Port	Speed/Duplex detection on	Monitor Status	Action	Oper Status
Gi 1/1	☐	none	trap-only	down
Gi 1/2	☐	none	trap-only	down
Gi 1/3	☐	none	trap-only	down
Gi 1/4	☐	none	trap-only	down
Gi 1/5	☐	none	trap-only	down
Gi 1/6	☐	none	trap-only	down
Gi 1/7	☐	none	trap-only	down
Gi 1/8	☐	none	trap-only	up
Gi 1/9	☐	none	trap-only	down
Gi 1/10	☐	none	trap-only	up
Gi 1/11	☐	none	trap-only	down
Gi 1/12	☐	none	trap-only	up

Port Monitor Configuration

Global Configuration

Enable Port Monitor

Enables/disables the Port Monitor function globally.

Ports Configuration

Port

This is the physical port number for this row.

Speed/Duplex detection on

Activates/deactivates the monitoring of the link speed and duplex mode on the port.
Possible values:

- Enabled

  Monitoring is active.

  – The “Port Monitor” function monitors the link speed and duplex mode on the port.

  – If the device detects an unpermitted combination of link speed and duplex mode, then the device executes the action specified in the “Action” column.

  – On the “Speed/Duplex detection” list, specify the parameters to be monitored.
- Disabled(default setting)

  Monitoring is inactive.

Monitor Status

Displays the monitored parameter that led to the action on the port.

Possible values:

- none

  No monitored parameter.

  The device does not carry out any action.

- speed-duplex

  Impermissible combination of speed and duplex mode detected.

Action

Specifies the action that the device carries out if the Port Monitor function detects that the parameters have been exceeded.

Valid values are trap-only and port-disable.

Oper Status

Displays the operating state of the port.

Possible values:

- up

  The port is enabled.

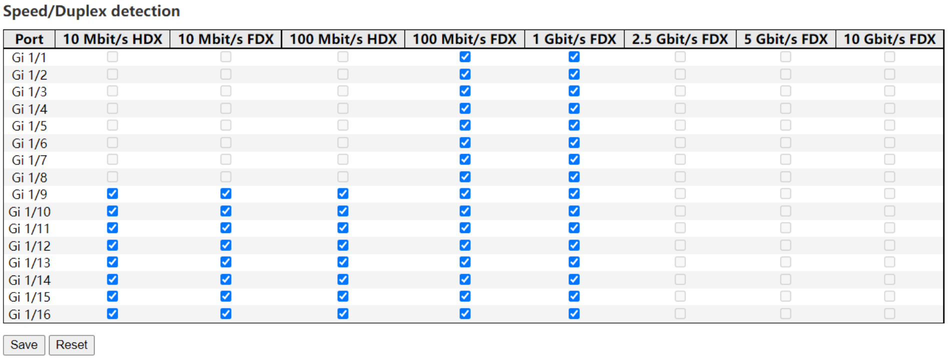
- down

  The port is disabled.

Speed/Duplex detection

[Diagnostics > Ports > Ports Monitor > Speed/Duplex detection]

This page allows the user to inspect the current Ports Monitor speed-duplex configurations, and possibly change them as well.



Speed/Duplex detection

Port	10 Mbit/s HDX	10 Mbit/s FDX	100 Mbit/s HDX	100 Mbit/s FDX	1 Gbit/s FDX	2.5 Gbit/s FDX	5 Gbit/s FDX	10 Gbit/s FDX
Gi 1/1	□	□	□	☑	☑	□	□	□
Gi 1/2	□	□	□	☑	☑	□	□	□
Gi 1/3	□	□	□	☑	☑	□	□	□
Gi 1/4	□	□	□	☑	☑	□	□	□
Gi 1/5	□	□	□	☑	☑	□	□	□
Gi 1/6	□	□	□	☑	☑	□	□	□
Gi 1/7	□	□	□	☑	☑	□	□	□
Gi 1/8	□	□	□	☑	☑	□	□	□
Gi 1/9	☑	☑	☑	☑	☑	□	□	□
Gi 1/10	☑	☑	☑	☑	☑	□	□	□
Gi 1/11	☑	☑	☑	☑	☑	□	□	□
Gi 1/12	☑	☑	☑	☑	☑	□	□	□
Gi 1/13	☑	☑	☑	☑	☑	□	□	□
Gi 1/14	☑	☑	☑	☑	☑	□	□	□
Gi 1/15	☑	☑	☑	☑	☑	□	□	□
Gi 1/16	☑	☑	☑	☑	☑	□	□	□

Speed/Duplex detection

Port

This is the logical port number for this row.

10 Mbit/s HDX

Activates/deactivates the port monitor to accept a half-duplex and 10 Mbit/s data rate combination on the port.

Possible values:

- marked

  The port monitor takes into consideration the speed and duplex combination.

- unmarked

  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the “Global” tab.

10 Mbit/s FDX

Activates/deactivates the port monitor to accept a full-duplex and 10 Mbit/s data rate combination on the port.

Possible values:

- marked

  The port monitor takes into consideration the speed and duplex combination.

- unmarked

  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the “Global” tab.

100 Mbit/s HDX

Activates/deactivates the port monitor to accept a half-duplex and 100 Mbit/s data rate combination on the port.

Possible values:

- marked

  The port monitor takes into consideration the speed and duplex combination.

- unmarked

  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the “Global” tab.

100 Mbit/s FDX

Activates/deactivates the port monitor to accept a full-duplex and 100 Mbit/s data rate combination on the port.

Possible values:

- marked

  The port monitor takes into consideration the speed and duplex combination.

- unmarked

  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the “Global” tab.

1 Gbit/s FDX

Activates/deactivates the port monitor to accept a full-duplex and 1 Gbit/s data rate combination on the port.

Possible values:

- marked

  The port monitor takes into consideration the speed and duplex combination.

- unmarked

  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the “Global” tab.

2.5 Gbit/s FDX

Activates/deactivates the port monitor to accept a full-duplex and 2.5 Gbit/s data rate combination on the port.

Possible values:

- marked

  The port monitor takes into consideration the speed and duplex combination.

- unmarked

  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the “Global” tab.

5 Gbit/s FDX

Activates/deactivates the port monitor to accept a full-duplex and 5 Gbit/s data rate combination on the port.

Possible values:

- marked

  The port monitor takes into consideration the speed and duplex combination.

- unmarked

  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the “Global” tab.

10 Gbit/s FDX

Activates/deactivates the port monitor to accept a full-duplex and 10 Gbit/s data rate combination on the port.

Possible values:

- marked

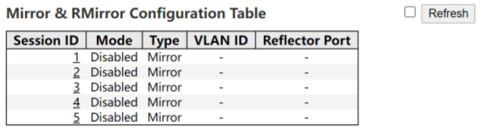
  The port monitor takes into consideration the speed and duplex combination.

- unmarked

  If the port monitor detects the speed and duplex combination on the port, then the device executes the action specified in the “Global” tab.

7.3.6. Mirroring

[Diagnostics > Ports > Mirroring]



Mirror & RMirror Configuration Table

□ Refresh

Session ID	Mode	Type	VLAN ID	Reflector Port
1	Disabled	Mirror	-	-
2	Disabled	Mirror	-	-
3	Disabled	Mirror	-	-
4	Disabled	Mirror	-	-
5	Disabled	Mirror	-	-

Mirror & RMirror Configuration Table

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.

Session ID

Select session id to configure.

Mode

Select switch mode.

Disabled: To **Disabled** the mirror or Remote Mirroring function.

Enabled: To **Enabled** the mirror or Remote Mirroring function.

Type

Three types of mirrors.

Mirror

The switch is running on mirror mode.

The source port(s) and destination port are located on this switch.

RMirror source

The switch is a source node for monitor flow.

The source port(s), reflector port are located on this switch.

RMirror destination

The switch is an end node for monitor flow.

The destination port(s) is located on this switch.

VLAN ID

The VLAN ID points out where the monitor packet will copy to. The default VLAN ID is 200.When performing CPU port mirroring, please do not configure the interface vlan for that VLAN.

Reflector Port

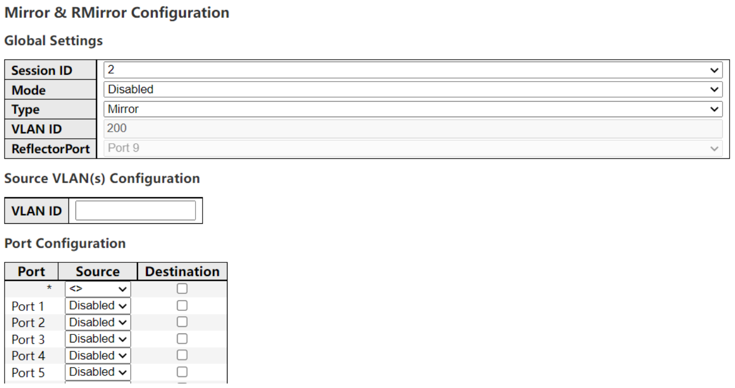
The **reflector port** is a method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until the Remote Mirroring is disabled.
In the stacking mode, you need to select switch ID to select the correct device.
If you shut down a port, it cannot be a candidate for **reflector port**.
If you shut down the port which is a **reflector port**, the remote mirror function cannot work.

Note1: The reflector port needs to select only on Source switch type.

Note2: The reflector port needs to disable MAC Table learning and STP.

Note3: The reflector port only supports pure copper ports except for management ports.

Click on the conversation ID to open the hidden interface, as shown in the following screenshot:



Mirror & RMirror Configuration

Global Settings

Session ID	2
Mode	Disabled
Type	Mirror
VLAN ID	200
ReflectorPort	Port 9

Source VLAN(s) Configuration

VLAN ID	

Port Configuration

Port	Source	Destination
*	<>	□
Port 1	Disabled	□
Port 2	Disabled	□
Port 3	Disabled	□
Port 4	Disabled	□
Port 5	Disabled	□

Source VLAN(s) Configuration

The switch can supports VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field.

Note1: The Mirroring session shall have either ports or VLANs as sources, but not both.

Port Configuration

Port

The physical port to which the settings in the same row are applied.

Source

Select mirror mode.

Disabled: Neither frames transmitted nor frames received are mirrored.

Both: Frames received and frames transmitted are mirrored on the **Destination port**.

Rx only: Frames received on this port are mirrored on the **Destination port**. Frames transmitted are not mirrored.

Tx only: Frames transmitted on this port are mirrored on the **Destination port**. Frames received are not mirrored.

Destination

Select destination port.

This checkbox is designed for mirror or Remote Mirroring.

The **destination port** is a switched port that you receive a copy of traffic from the source port.

Note1: On mirror mode, the device only supports one destination port.

Note2: The destination port needs to disable MAC Table learning.

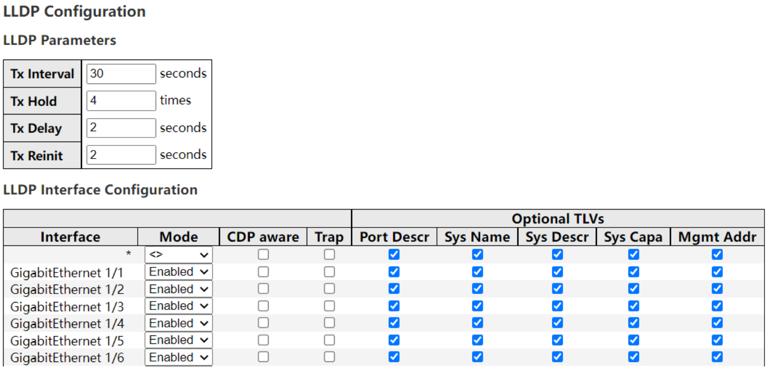
7.4. LLDP

7.4.1. LLDP

[Diagnostics > LLDP > LLDP]

[Configuration]

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



LLDP Configuration

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**	**Trap**	**Port Descr**	**Sys Name**	**Sys Descr**	**Sys Capa**	**Mgmt Addr**
*	<>	□	□	☑	☑	☑	☑	☑
GigabitEthernet 1/1	Enabled	□	□	☑	☑	☑	☑	☑
GigabitEthernet 1/2	Enabled	□	□	☑	☑	☑	☑	☑
GigabitEthernet 1/3	Enabled	□	□	☑	☑	☑	☑	☑
GigabitEthernet 1/4	Enabled	□	□	☑	☑	☑	☑	☑
GigabitEthernet 1/5	Enabled	□	□	☑	☑	☑	☑	☑
GigabitEthernet 1/6	Enabled	□	□	☑	☑	☑	☑	☑

LLDP Parameters

Tx 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.

LLDP Interface Configuration

Interface

LLDP Physical Interface Name.

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.

Trap

Whether to send a trap.

Port Descr

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.

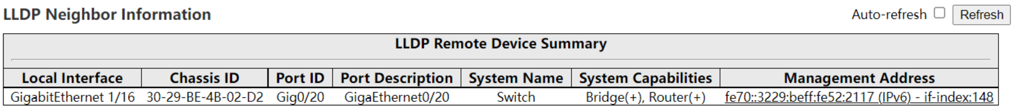
Sys Capa

Optional TLV: When checked the "system capability" is included in LLDP information transmitted.

Mgmt Addr

Optional TLV: When checked the "management address" is included in LLDP information transmitted.

[Status]



LLDP Neighbor Information

LLDP Remote Device Summary

Local Interface	Chassis ID	Port ID	Port Description	System Name	System Capabilities	Management Address
GigabitEthernet 1/16	30-29-BE-4B-02-D2	Gig0/20	GigaEthernet0/20	Switch	Bridge(+), Router(+)	fe70::3229:beff:fe52:2117 (IPv6) - if-index:148

LLDP Neighbor 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:

1. Other

2. Repeater

3. Bridge

4. WLAN Access Point

5. Router

6. Telephone

7. DOCSIS cable device

8. Station only

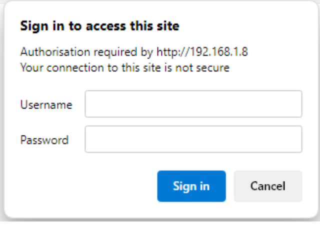
9. Reserved

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. Click to be redirected to the neighbor's device login page.

Clicking the management address redirects to the following page:



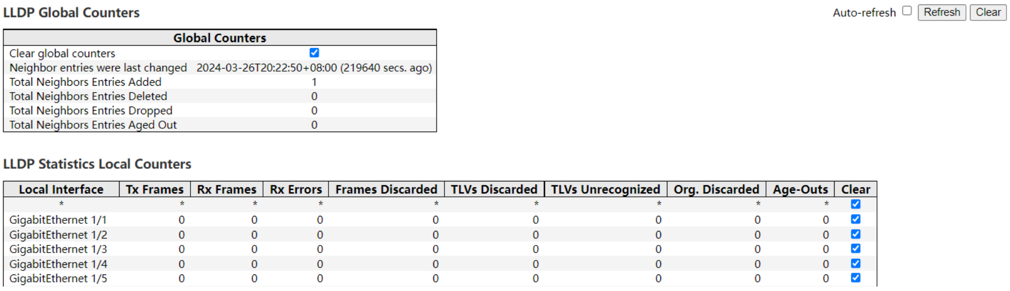
Sign in to access this site

Authorisation required by http://192.168.1.8
Your connection to this site is not secure

Username	
Password	

[Port Statistics]

This page provides an overview of all LLDP traffic.



LLDP Global Counters

Global Counters	
Clear global counters	☑
Neighbor entries were last changed	2024-03-26T20:22:50+08:00 (219640 secs. ago)
Total Neighbors Entries Added	1
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Interface	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs	Clear
*	*	*	*	*	*	*	*	*	☑
GigabitEthernet 1/1	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/2	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/3	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/4	0	0	0	0	0	0	0	0	☑
GigabitEthernet 1/5	0	0	0	0	0	0	0	0	☑

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.

LLDP Global Counters

Clear global counters

If checked the global counters are cleared when clear is pressed.

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.

LLDP Statistics Local Counters

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

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

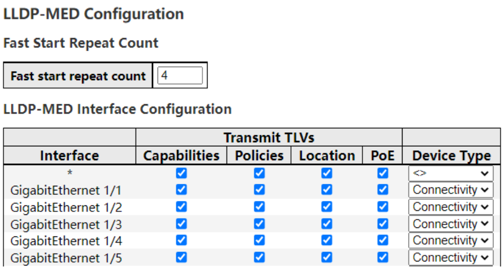
If checked the counters for the specific interface are cleared when clear is pressed.

7.4.2. LLDP-MED

[Diagnostics > LLDP > LLDP-MED]

[Configuration]

This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.



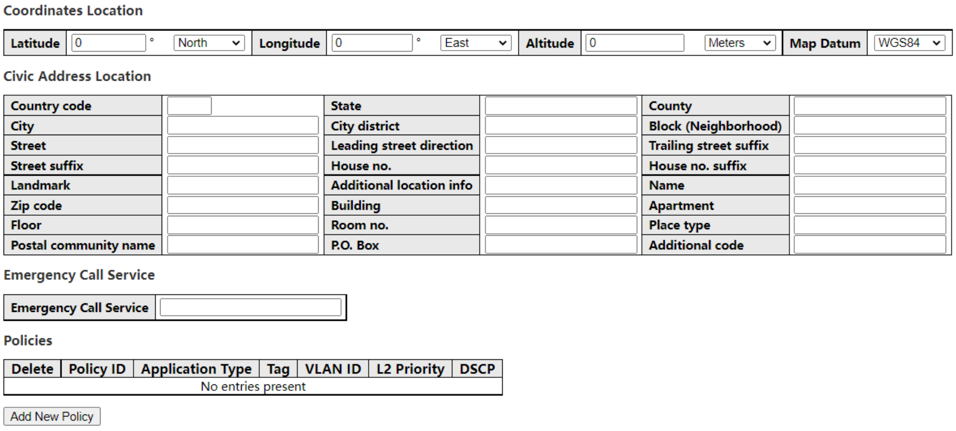
LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count	4

LLDP-MED Interface Configuration

	Transmit TLVs				
Interface	Capabilities	Policies	Location	PoE	Device Type
*	☑	☑	☑	☑	<>
GigabitEthernet 1/1	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/2	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/3	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/4	☑	☑	☑	☑	Connectivity
GigabitEthernet 1/5	☑	☑	☑	☑	Connectivity



Coordinates Location

Latitude	0 °	North	Longitude	0 °	East	Altitude	0	Meters	Map Datum	WGS84

Civic Address Location

Country code		State		County	
City		City district		Block (Neighborhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community name		P.O. Box		Additional code	

Emergency Call Service

Emergency Call Service	

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
No entries present						

Fast start repeat count

Fast start repeat count

Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated interface. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors.

Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.

LLDP Interface Configuration

It is possible to select which LLDP-MED information that shall be transmitted to the neighbors. When the checkbox is checked the information is included in the frame transmitted to the neighbor.

Interface

The interface name to which the configuration applies.

Transmit TLVs - Capabilities

When checked the switch's capabilities is included in LLDP-MED information transmitted.

Transmit TLVs - Policies

When checked the configured policies for the interface is included in LLDP-MED information transmitted.

Transmit TLVs - Location

When checked the configured location information for the switch is included in LLDP-MED information transmitted.

Transmit TLVs - PoE

When checked the configured PoE (Power Over Ethernet) information for the interface is included in LLDP-MED information transmitted.

Device Type

Any LLDP-MED Device is operating as a specific type of LLDP-MED Device, which may be either a Network Connectivity Device or a specific Class of Endpoint Device, as defined below:

A Network Connectivity Device is a LLDP-MED Device that provides access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices.

An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies :

1. LAN Switch/Router

2. IEEE 802.1 Bridge

3. IEEE 802.3 Repeater (included for historical reasons)

4. IEEE 802.11 Wireless Access Point

5. Any device that supports the IEEE 802.1AB and MED extensions that can relay IEEE 802 frames via any method.

An Endpoint Device a LLDP-MED Device that sits at the network edge and provides some aspect of IP communications service, based on IEEE 802 LAN technology.

The main difference between a Network Connectivity Device and an Endpoint Device is that only an Endpoint Device can start the LLDP-MED information exchange.

Even though a switch always should be a Network Connectivity Device, it is possible to configure it to act as an Endpoint Device, and thereby start the LLDP-MED information exchange (In the case where two Network Connectivity Devices are connected together).

Coordinates Location

Latitude

Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits.

It is possible to specify the direction to either North of the equator or South of the equator.

Longitude

Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits.

It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

Altitude

Altitude SHOULD be normalized to within -2097151.9 to 2097151.9 with a maximum of 1 digits.

It is possible to select between two altitude types (floors or meters).

Meters: Representing meters of Altitude defined by the vertical datum specified.

Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

Map Datum

The Map Datum is used for the coordinates given in these options:

WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.

NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).

NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.

Civic Address Location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). The total number of characters for the combined civic address information must not exceed 250 characters.

A couple of notes to the limitation of 250 characters.

1) If more than one civic address location is used, each of the additional civic address locations will use 2 extra characters in addtion to the civic address location text.

2) The 2 letter country code is not part of the 250 characters limitation.

Country code

The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

State

National subdivisions (state, canton, region, province, prefecture).

County

County, parish, gun (Japan), district.

City

City, township, shi (Japan) - Example: Copenhagen.

City district

City division, borough, city district, ward, chou (Japan).

Block (Neighborhood)

Neighborhood, block.

Street

Street - Example: Poppelvej.

Leading street direction

Leading street direction - Example: N.

Trailing street suffix

Trailing street suffix - Example: SW.

Street suffix

Street suffix - Example: Ave, Platz.

House no.

House number - Example: 21.

House no. Suffix

House number suffix - Example: A, 1/2.

Landmark

Landmark or vanity address - Example: Columbia University.

Additional location info

Additional location info - Example: South Wing.

Name

Name (residence and office occupant) - Example: Flemming Jahn.

Zip code

Postal/zip code - Example: 2791.

Building

Building (structure) - Example: Low Library.

Apartment

Unit (Apartment, suite) - Example: Apt 42.

Floor

Floor - Example: 4.

Room no.

Room number - Example: 450F.

Place type

Place type - Example: Office.

Postal community name

Postal community name - Example: Leonia.

P.O. Box

Post office box (P.O. BOX) - Example: 12345.

Additional code

Additional code - Example: 1320300003.

Emergency Call Service

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Emergency Call Service

Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Policies

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

1. Layer 2 VLAN ID (IEEE 802.1Q-2003)

2. Layer 2 priority value (IEEE 802.1D-2004)

3. Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

1. Voice

2. Guest Voice

3. Softphone Voice

4. Video Conferencing

5. Streaming Video

6. Control/Signalling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Delete

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

Policy ID

ID for the policy. This is auto generated and shall be used when selecting the policies that shall be mapped to the specific interfaces.

Application Type

Intended use of the application types:
1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
2. Voice Signalling (conditional) - for use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.
3. Guest Voice - support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
4. Guest Voice Signalling (conditional) - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.
5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.
6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

8. Video Signalling (conditional) - for use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.

Tag

Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN. Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.

Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

VLAN ID

VLAN identifier (VID) for the interface as defined in IEEE 802.1Q-2003.

L2 Priority

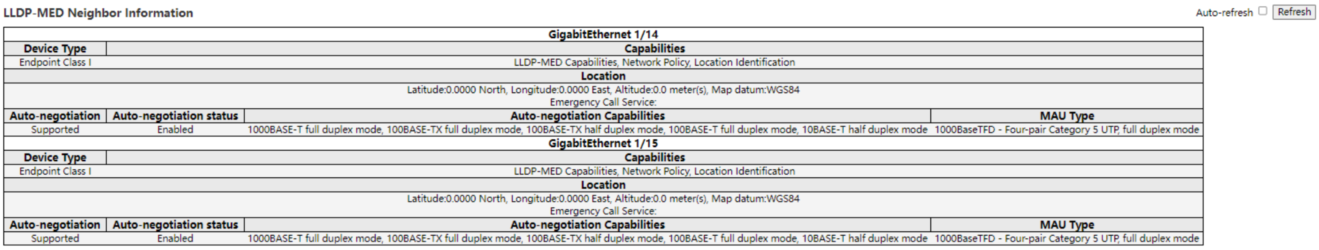
L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

DSCP

DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

[Status]

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each interface on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED.



LLDP-MED Neighbor Information

Auto-refresh □ Refresh

<table>
<tr><th colspan="4">GigabitEthernet 1/14</th></tr>
<tr><th>Device Type</th><th colspan="3">Capabilities</th></tr>
<tr><td>Endpoint Class I</td><td colspan="3">LLDP-MED Capabilities, Network Policy, Location Identification</td></tr>
<tr><th colspan="4">Location</th></tr>
<tr><td colspan="4">Latitude:0.0000 North, Longitude:0.0000 East, Altitude:0.0 meter(s), Map datum:WGS84
Emergency Call Service:</td></tr>
<tr><th>Auto-negotiation</th><th>Auto-negotiation status</th><th>Auto-negotiation Capabilities</th><th>MAU Type</th></tr>
<tr><td>Supported</td><td>Enabled</td><td>1000BASE-T full duplex mode, 100BASE-TX full duplex mode, 100BASE-TX half duplex mode, 100BASE-T full duplex mode, 10BASE-T half duplex mode</td><td>1000BaseTFD - Four-pair Category 5 UTP, full duplex mode</td></tr>
<tr><th colspan="4">GigabitEthernet 1/15</th></tr>
<tr><th>Device Type</th><th colspan="3">Capabilities</th></tr>
<tr><td>Endpoint Class I</td><td colspan="3">LLDP-MED Capabilities, Network Policy, Location Identification</td></tr>
<tr><th colspan="4">Location</th></tr>
<tr><td colspan="4">Latitude:0.0000 North, Longitude:0.0000 East, Altitude:0.0 meter(s), Map datum:WGS84
Emergency Call Service:</td></tr>
<tr><th>Auto-negotiation</th><th>Auto-negotiation status</th><th>Auto-negotiation Capabilities</th><th>MAU Type</th></tr>
<tr><td>Supported</td><td>Enabled</td><td>1000BASE-T full duplex mode, 100BASE-TX full duplex mode, 100BASE-TX half duplex mode, 100BASE-T full duplex mode, 10BASE-T half duplex mode</td><td>1000BaseTFD - Four-pair Category 5 UTP, full duplex mode</td></tr>
</table>

LLDP-MED Neighbor Information

Interface

The interface on which the LLDP frame was received.

Device Type

LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

LLDP-MED Network Connectivity Device Definition

LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

1. LAN Switch/Router

2. IEEE 802.1 Bridge

3. IEEE 802.3 Repeater (included for historical reasons)

4. IEEE 802.11 Wireless Access Point

5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method

LLDP-MED Endpoint Device Definition

LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework.

Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following.

Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example will any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

LLDP-MED Generic Endpoint (Class I)

The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057.

Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED Media Endpoint (Class II)

The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar.

Discovery services defined in this class include media-type-specific network layer policy discovery.

LLDP-MED Communication Endpoint (Class III)

The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user.

Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, inventory management.

LLDP-MED Capabilities

LLDP-MED Capabilities describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are:

1. LLDP-MED capabilities

2. Network Policy

3. Location Identification

4. Extended Power via MDI - PSE

5. Extended Power via MDI - PD

6. Inventory

7. Reserved

Application Type

Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.

1. Voice - for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

2. Voice Signalling - for use in network topologies that require a different policy for the voice signalling than for the voice media.

3. Guest Voice - to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

4. Guest Voice Signalling - for use in network topologies that require a different policy for the guest voice signalling than for the guest voice media.

5. Softphone Voice - for use by softphone applications on typical data centric devices, such as PCs or laptops.

6. Video Conferencing - for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

7. Streaming Video - for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

8. Video Signalling - for use in network topologies that require a separate policy for the video signalling than for the video media.

Policy

Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown.

Unknown: The network policy for the specified application type is currently unknown.

Defined: The network policy is defined (known).

TAG

TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged.

Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.

Tagged: The device is using the IEEE 802.1Q tagged frame format.

VLAN ID

VLAN ID is the VLAN identifier (VID) for the interface as defined in IEEE 802.1Q-2003. A value of 1 through 4095 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress interface is used instead.

Priority

Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).

DSCP

DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).

Auto-negotiation

Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.

Auto-negotiation status

Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined the operational MAU type field value rather than by auto-negotiation.

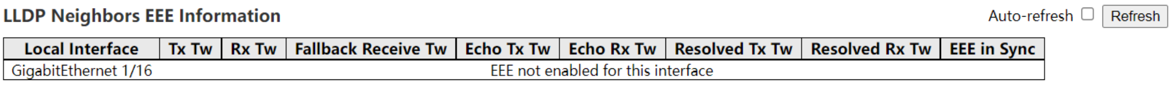
Auto-negotiation Capabilities

Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

7.4.3. EEE

[Diagnostics > LLDP > EEE]

This page provides an overview of EEE information exchanged by LLDP.



LLDP Neighbors EEE Information

Auto-refresh □ Refresh

Local Interface	Tx Tw	Rx Tw	Fallback Receive Tw	Echo Tx Tw	Echo Rx Tw	Resolved Tx Tw	Resolved Rx Tw	EEE in Sync
GigabitEthernet 1/16	EEE not enabled for this interface							

By using EEE power savings can be achieved at the expense of traffic latency. This latency occurs due to that the circuits EEE turn off to save power, need time to boot up before sending traffic over the link. This time is called "wakeup time". To achieve minimal latency, devices can use LLDP to exchange information about their respective tx and rx "wakeup time ", as a way to agree upon the minimum wakeup time they need.

LLDP Neighbors EEE Information

Local Interface

The interface at which LLDP frames are received or transmitted.

Tx Tw

The link partner's maximum time that transmit path can hold-off sending data after deassertion of LPI.

Rx Tw

The link partner's time that receiver would like the transmitter to hold-off to allow time for the receiver to wake from sleep.

Fallback Receive Tw

The link partner's fallback receive Tw.

A receiving link partner may inform the transmitter of an alternate desired Tw_sys_tx. Since a receiving link partner is likely to have discrete levels for savings, this provides the transmitter with additional information that it may use for a more efficient allocation. Systems that do not implement this option default the value to be the same as that of the Receive Tw_sys_tx.

Echo Tx Tw

The link partner's Echo Tx Tw value.

The respective echo values shall be defined as the local link partners reflection (echo) of the remote link partners respective values. When a local link partner receives its echoed values from the remote link partner, it can determine whether or not the remote link partner has received, registered and processed its most recent values. For example, if the local link partner receives echoed parameters that do not match the values in its local MIB, then the local link partner infers that the remote link partners request was based on stale information.

Echo Rx Tw

The link partner's Echo Rx Tw value.

Resolved Tx Tw

The resolved Tx Tw for this link. Note : NOT the link partner.

The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

Resolved Rx Tw

The resolved Rx Tw for this link. Note : NOT the link partner.

The resolved value that is the actual "tx wakeup time " used for this link (based on EEE information exchanged via LLDP).

EEE in Sync

Shows whether the switch and the link partner have agreed on wake times.

Red - Switch and link partner have not agreed on wakeup times.

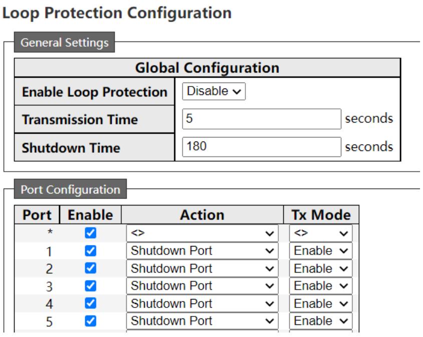
Green - Switch and link partner have agreed on wakeup times.

7.5. Loop Protection

[Diagnostics > Loop Protection]

[Configuration]

This page allows the user to configure the current Loop Protection.



Loop Protection Configuration

General Settings

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

Port Configuration

Port	Enable	Action	Tx Mode
*	☑	<>	<>
1	☑	Shutdown Port	Enable
2	☑	Shutdown Port	Enable
3	☑	Shutdown Port	Enable
4	☑	Shutdown Port	Enable
5	☑	Shutdown Port	Enable

Loop Protection Configuration

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. Default value is 180 seconds.

Port Configuration

Enable

Controls whether loop protection is enabled on this switch port.

Action

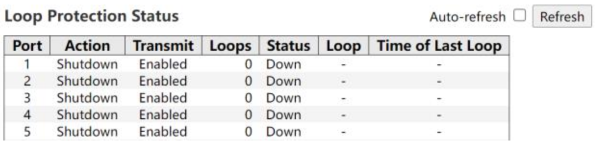
Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port and Log or Log Only.

Tx Mode

Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

[Status]

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



Loop Protection Status

Auto-refresh □ Refresh

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Down	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-

Loop Protection Status

Port

The switch port number of the physical 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

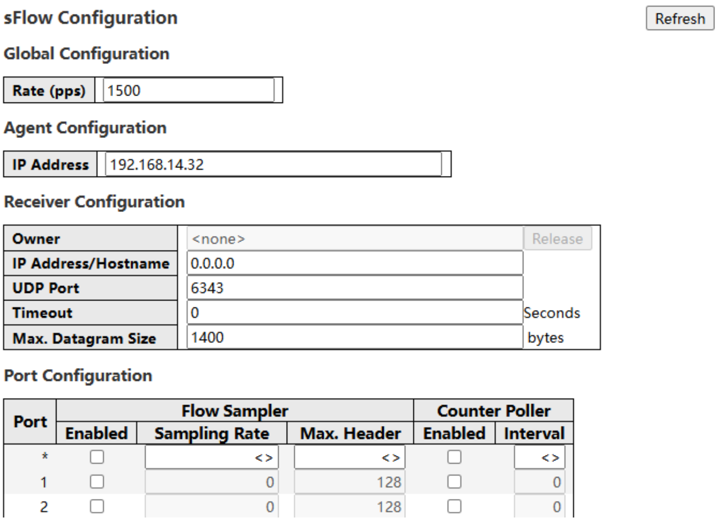
The time of the last loop event detected.

7.6. SFlow

[Diagnostics > SFlow]

[Configuration]

This page allows for configuring sFlow. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.



sFlow Configuration

Global Configuration

Rate (pps)	1500

Agent Configuration

IP Address	192.168.14.32

Receiver Configuration

Owner	<none>	Release
IP Address/Hostname	0.0.0.0	
UDP Port	6343	
Timeout	0	Seconds
Max. Datagram Size	1400	bytes

Port Configuration

Port	Flow Sampler			Counter Poller	
	Enabled	Sampling Rate	Max. Header	Enabled	Interval
*	□	<>	<>	□	<>
1	□	0	128	□	0
2	□	0	128	□	0

sFlow Configuration

sFlow configuration is not persisted to non-volatile memory, which means that a reboot will disable sFlow sampling.

Global Configuration

Rate (pps)

The maximum rate at which sFlow sampled packets are sent to the control plane, measured in packets per second (pps), is defined to prevent CPU overload from compromising device stability.

Agent Configuration

IP Address

The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time.

Both IPv4 and IPv6 addresses are supported.

Receiver Configuration

Owner

Basically, sFlow can be configured in two ways: Through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:
• If sFlow is currently unconfigured/unclaimed, Owner contains **<none>**.
• If sFlow is currently configured through Web or CLI, Owner contains **<Configured through local management>**.
• If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.
If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid inadvertent reconfiguration.

The button Release allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).

IP Address/Hostname

The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.

UDP Port

The UDP port on which the sFlow receiver listens to sFlow datagrams. The default port (6343) is used.

Timeout

The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings. Valid range is 0 to 2147483647 seconds.

Max. Datagram Size

The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

Port Configuration

Port

The port number for which the configuration below applies.

Flow Sampler Enabled

Enables/disables flow sampling on this port.

Flow Sampler Sampling Rate

The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port.

Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field. Valid range depends on the chip capability.

Flow Sampler Max. Header

The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes.

To have room for any frame, the maximum datagram size should be roughly 100 bytes larger than the maximum header size. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.

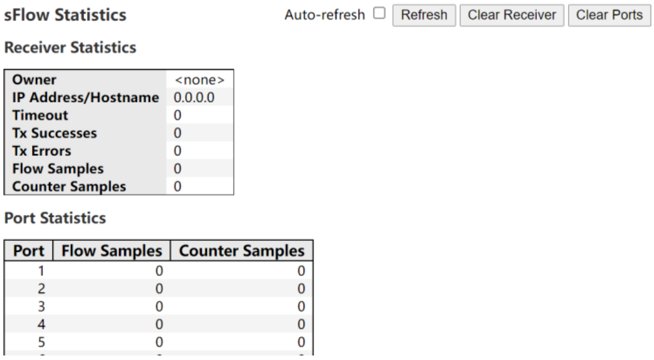
Counter Poller Enabled

Enables/disables counter polling on this port.

Counter Poller Interval

With counter polling enabled, this specifies the interval - in seconds - between counter poller samples. Valid range is 1 to 3600 seconds.

[Satus]



sFlow Statistics

Receiver Statistics

Owner	<none>
IP Address/Hostname	0.0.0.0
Timeout	0
Tx Successes	0
Tx Errors	0
Flow Samples	0
Counter Samples	0

Port Statistics

Port	Flow Samples	Counter Samples
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0

sFlow Statistics

Receiver Statistics

Owner

This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:

- If sFlow is currently unconfigured/unclaimed, Owner contains <**none**>.
- If sFlow is currently configured through Web or CLI, Owner contains <**Configured through local management**>.
- If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.

IP Address/Hostname

The IP address or hostname of the sFlow receiver.

Timeout

The number of seconds remaining before sampling stops and the current sFlow owner is released.

Tx Successes

The number of UDP datagrams successfully sent to the sFlow receiver.

Tx Errors

The number of UDP datagrams that has failed transmission. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics → Ping).

Flow Samples

The total number of flow samples sent to the sFlow receiver.

Counter Samples

The total number of counter samples sent to the sFlow receiver.

Port Statistics

Port

The port number for which the following statistics applies.

Flow Samples

The number of flow samples sent to the sFlow receiver originating from this port.

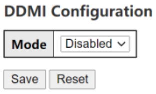
Counter Samples

The total number of counter samples sent to the sFlow receiver originating from this port.

7.7. DDMI

[Diagnostics > DDMI]

Configure DDMI on this page.



DDMI Configuration

Mode	Disabled

DDMI Configuration

Mode

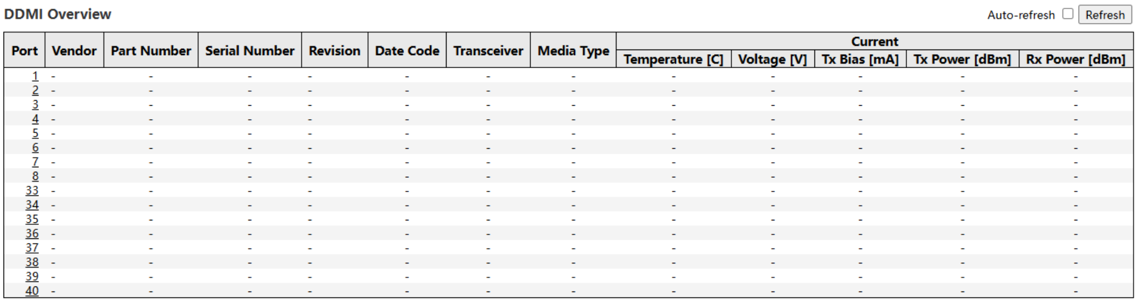
Indicates the DDMI mode operation. Possible modes are:

Enabled: Enable DDMI mode operation.

Disabled: Disable DDMI mode operation.

[Overview]

Display DDMI overview information on this page.



DDMI Overview

Port	Vendor	Part Number	Serial Number	Revision	Date Code	Transceiver	Media Type	Current				
								Temperature [C]	Voltage [V]	Tx Bias [mA]	Tx Power [dBm]	Rx Power [dBm]
1	-	-	-	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-	-	-	-
33	-	-	-	-	-	-	-	-	-	-	-	-
34	-	-	-	-	-	-	-	-	-	-	-	-
35	-	-	-	-	-	-	-	-	-	-	-	-
36	-	-	-	-	-	-	-	-	-	-	-	-
37	-	-	-	-	-	-	-	-	-	-	-	-
38	-	-	-	-	-	-	-	-	-	-	-	-
39	-	-	-	-	-	-	-	-	-	-	-	-
40	-	-	-	-	-	-	-	-	-	-	-	-

DDMI Overview

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 Revision level for part number provided by vendor.

Date Code

Indicates Date code Vendor's manufacturing date code.

Transceiver

Indicates Transceiver compatibility.

Media Type

Indicates SFP interface media type.

Current Temperature

Indicates the current temperature value of SFP transceiver.

Current Voltage

Indicates the current voltage value of SFP transceiver.

Current Tx Bias

Indicates the current Tx Bias value of SFP transceiver.

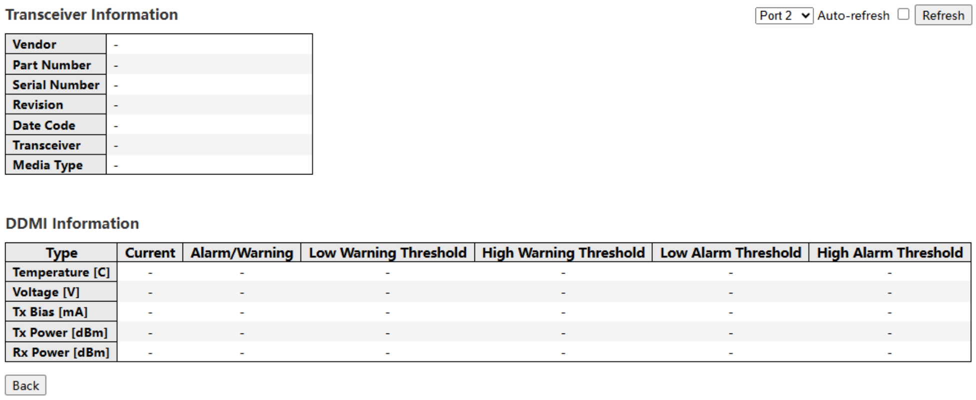
Current Tx Power

Indicates the current Tx Power value of SFP transceiver.

Current Rx Power

Indicates the current Rx Power value of SFP transceiver.

If you click on Port in the navigation bar, the page appears as shown as below:



Transceiver Information

Vendor	-
Part Number	-
Serial Number	-
Revision	-
Date Code	-
Transceiver	-
Media Type	-

DDMI Information

Type	Current	Alarm/Warning	Low Warning Threshold	High Warning Threshold	Low Alarm Threshold	High Alarm Threshold
Temperature [C]	-	-	-	-	-	-
Voltage [V]	-	-	-	-	-	-
Tx Bias [mA]	-	-	-	-	-	-
Tx Power [dBm]	-	-	-	-	-	-
Rx Power [dBm]	-	-	-	-	-	-

Display DDMI detailed information on this page.

Transceiver Information

Display transceiver information on this page.

Vendor

Indicates SFP vendor name.

Part Number

Indicates Part number provided by SFP vendor.

Serial Number

Indicates Serial number provided by vendor.

Revision

Indicates Revision level for part number provided by vendor.

Date Code

Indicates Vendor's manufacturing date code.

Transceiver

Indicates SFP Transceiver compatibility.

Media Type

Indicates SFP interface media type.

DDMI Information

Display DDMI information on this page.

Current

The current value of temperature, voltage, TX bias, TX power, and RX power.

Alarm/Warning

Indicates whether there is an alarm or warning.

Low Warning Threshold

The low warning threshold value of temperature, voltage, TX bias, TX power, and RX power.

High Warning Threshold

The high warning threshold value of temperature, voltage, TX bias, TX power, and RX power.

Low Alarm Threshold

The low alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.

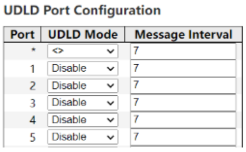
High Alarm Threshold

The high alarm threshold value of temperature, voltage, TX bias, TX power, and RX power.

7.8. UDLD

[Diagnostics > UDLD]

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



UDLD Port Configuration

Port	UDLD Mode	Message Interval
*	<>	7
1	Disable	7
2	Disable	7
3	Disable	7
4	Disable	7
5	Disable	7

UDLD Port Configuration

Port

Port number of the switch.

UDLD Mode

Configures the UDLD mode on a port. Valid values are **Disable**, **Normal** and **Aggressive**. Default mode is Disable.

Disable

In disabled mode, UDLD functionality doesn't exists on port.

Normal

In normal mode, if the link state of the port was determined to be unidirectional, it will not affect the port state.

Aggressive

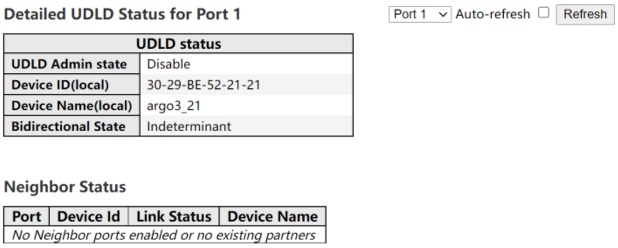
In aggressive mode, unidirectional detected ports will get shutdown. To bring back the ports up, need to disable UDLD on that port.

Message Interval

Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from 7 to 90 seconds(Default value is 7 seconds)(Currently default time interval is supported, due to lack of detailed information in RFC 5171).

[Status]

This page displays the UDLD status of the ports.



Detailed UDLD Status for Port 1

UDLD status	
UDLD Admin state	Disable
Device ID(local)	30-29-BE-52-21-21
Device Name(local)	argo3_21
Bidirectional State	Indeterminant

Neighbor Status

Port	Device Id	Link Status	Device Name
No Neighbor ports enabled or no existing partners			

Detailed UDLD Status for Port

UDLD Admin State

The current port state of the logical port, *Enabled* if any of the state(*Normal, Aggressive*) is Enabled.

Device ID(local)

The ID of Device.

Device Name(local)

Name of the Device.

Bidirectional State

The current state of the port.

Neighbor Status

Port

The current port of neighbour device.

Device ID

The current ID of neighbour device.

Link Status

The current link status of neighbour port.

Device Name

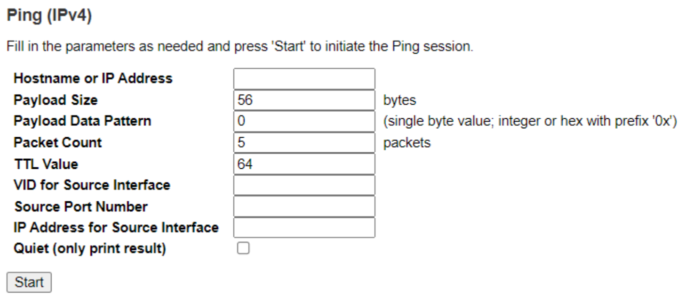
Name of the Neighbour Device.

7.9. Ping

[Diagnostics > Ping]

[IPv4]

This page allows you to issue ICMP (IPv4) PING packets to troubleshoot IP connectivity issues.



Ping (IPv4)

Fill in the parameters as needed and press 'Start' to initiate the Ping session.

Hostname or IP Address		
Payload Size	56	bytes
Payload Data Pattern	0	(single byte value; integer or hex with prefix '0x')
Packet Count	5	packets
TTL Value	64	
VID for Source Interface		
Source Port Number		
IP Address for Source Interface		
Quiet (only print result)	□	

Ping (IPv4)

Hostname or IP Address

The address of the destination host, either as a symbolic hostname or an IP Address.

Payload Size

Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.

Payload Data Pattern

Determines the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

Packet Count

Determines the number of PING requests sent. The default value is 5. The valid range is 1-60.

TTL Value

Determines the Time-To-Live field value in the IPv4 header. The default value is 64. The valid range is 1-255.

VID for Source Interface

This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

Source Port Number

This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration.

Address for Source Interface

This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

Quiet (only print result)

Checking this option will not print the result of each ping request but will only show the final result.

After you press ‘Start’, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

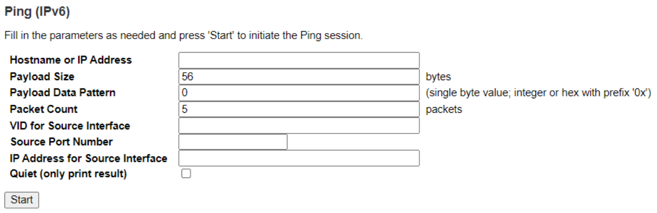
The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

The output from the command will look like the following:

```
PING 172.16.1.1 (172.16.1.1) from 172.16.1.10: 56 data bytes

64 bytes from 172.16.1.1: seq=0 ttl=64 time=2.034 ms

64 bytes from 172.16.1.1: seq=1 ttl=64 time=1.729 ms

64 bytes from 172.16.1.1: seq=2 ttl=64 time=1.954 ms

64 bytes from 172.16.1.1: seq=3 ttl=64 time=1.699 ms

64 bytes from 172.16.1.1: seq=4 ttl=64 time=1.916 ms


--- 172.16.1.1 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 1.699/1.866/2.034 ms
```

[IPv6]

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.



Ping (IPv6)

Fill in the parameters as needed and press 'Start' to initiate the Ping session.

Hostname or IP Address		
Payload Size	56	bytes
Payload Data Pattern	0	(single byte value; integer or hex with prefix '0x')
Packet Count	5	packets
VID for Source Interface		
Source Port Number		
IP Address for Source Interface		
Quiet (only print result)	□	

Ping (IPv6)

Hostname or IP Address

The address of the destination host, either as a symbolic hostname or an IP Address.

Payload Size

Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.

Payload Data Pattern

Determines the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

Packet Count

Determines the number of PING requests sent. The default value is 5. The valid range is 1-60.

VID for Source Interface

This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

Source Port Number

This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the Source Port Number or the IP Address for the source interface.

Address for Source Interface

This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

Quiet (only print result)

Checking this option will not print the result of each ping request but will only show the final result.

After you press ‘start’, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

The output from the command will look like the following:

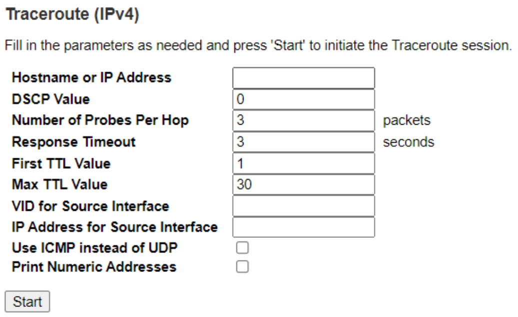
```
PING 2001::01 (2001::1) from 2001::3: 56 data bytes
64 bytes from 2001::1: seq=0 ttl=64 time=2.118 ms
64 bytes from 2001::1: seq=1 ttl=64 time=2.009 ms
64 bytes from 2001::1: seq=2 ttl=64 time=1.852 ms
64 bytes from 2001::1: seq=3 ttl=64 time=2.869 ms
64 bytes from 2001::1: seq=4 ttl=64 time=1.845 ms

--- 2001::01 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.845/2.138/2.869 ms
```

7.10. Traceroute

[Diagnostics > Traceroute]

[IPv4]

This page allows you to perform a traceroute test over IPv4 towards a remote host. traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network.



Traceroute (IPv4)

Fill in the parameters as needed and press 'Start' to initiate the Traceroute session.

Hostname or IP Address		
DSCP Value	0	
Number of Probes Per Hop	3	packets
Response Timeout	3	seconds
First TTL Value	1	
Max TTL Value	30	
VID for Source Interface		
IP Address for Source Interface		
Use ICMP instead of UDP	☐	
Print Numeric Addresses	☐	

Traceroute (IPv4)

You can configure the following parameters for the test:

Hostname or IP Address

The destination IP Address.

DSCP Value

This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-63.

Number of Probes Per Hop

Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.

Response Timeout

Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.

First TTL Value

Determines the value of the Time-To-Live (TTL) field in the IPv4 header in the first packet sent. The default number is 1. The valid range is 1-30.

Max TTL Value

Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1-255.

VID for Source Interface

This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

Address for Source Interface

This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

Use ICMP instead of UDP

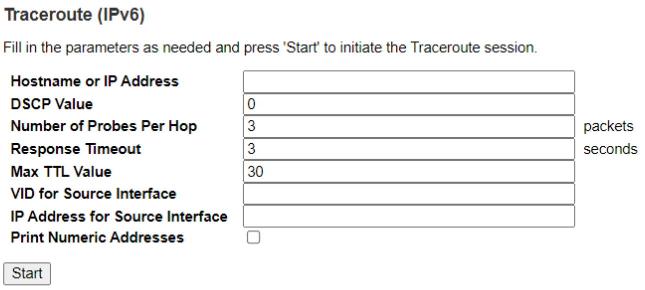
By default the **traceroute** command will use UDP datagrams. Selecting this option forces it to use ICMP ECHO packets instead.

Print Numeric Addresses

By default the **traceroute** command will print out hop information using a reverse DNS lookup for the acquired host ip addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the **traceroute** command to print numeric IP addresses instead.

[IPv6]

This page allows you to perform a traceroute test over IPv6 towards a remote host. traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv6 network.



Traceroute (IPv6)

Fill in the parameters as needed and press 'Start' to initiate the Traceroute session.

Hostname or IP Address		
DSCP Value	0	
Number of Probes Per Hop	3	packets
Response Timeout	3	seconds
Max TTL Value	30	
VID for Source Interface		
IP Address for Source Interface		
Print Numeric Addresses	□	

Traceroute (IPv6)

You can configure the following parameters for the test:

Hostname or IP Address

The destination IP Address.

DSCP Value

This value is used for the DSCP value in the IPv6 header. The default value is 0. The valid range is 0-255.

Number of Probes Per Hop

Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.

Response Timeout

Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.

Max TTL Value

Determines the maximum value of the Time-To-Live (TTL) field in the IPv6 header. If this value is reached before the specified remote host is reached the test stops. The default number is 255. The valid range is 1-255.

VID for Source Interface

This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

Address for Source Interface

This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

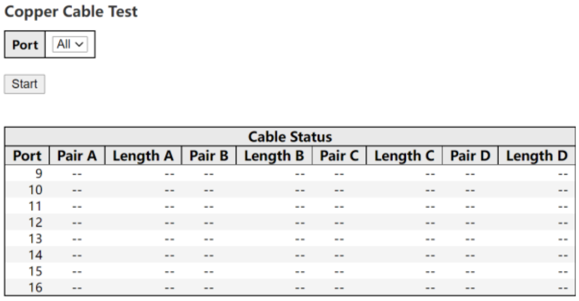
Print Numeric Addresses

By default the **traceroute** command will print out hop information using a reverse DNS lookup for the acquired host ip addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the **traceroute** command to print numeric IP addresses instead.

7.11. Copper Cable Test

[Diagnostics > Copper Cable Test]

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



Copper Cable Test

Port: All

Cable Status								
Port	Pair A	Length A	Pair B	Length B	Pair C	Length C	Pair D	Length D
9	--	--	--	--	--	--	--	--
10	--	--	--	--	--	--	--	--
11	--	--	--	--	--	--	--	--
12	--	--	--	--	--	--	--	--
13	--	--	--	--	--	--	--	--
14	--	--	--	--	--	--	--	--
15	--	--	--	--	--	--	--	--
16	--	--	--	--	--	--	--	--

Copper Cable Test

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

Port

The port where you are requesting Cable Test Cable Diagnostics.

Port

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

The length (in meters) of the cable pair. The resolution is 3 meters.

8. OAM

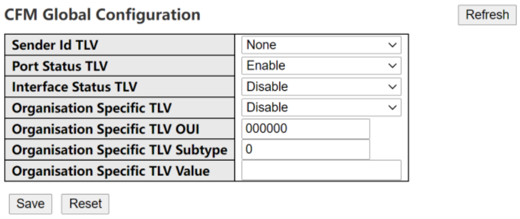
The menu contains the following dialogs:
CFM
Link OAM

8.1. CFM

8.1.1. Global

[OAM > CFM > Global]

On this page, you can configure the CFM Global parameters.



CFM Global Configuration

Sender Id TLV	None
Port Status TLV	Enable
Interface Status TLV	Disable
Organisation Specific TLV	Disable
Organisation Specific TLV OUI	000000
Organisation Specific TLV Subtype	0
Organisation Specific TLV Value	

CFM Global Configuration

Sender Id TLV

Choose whether and what to use as Sender ID TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.

None: The sender ID is empty.

Chassis: Set the chassis ID as the sender ID.

Manage: Set the management address as the sender ID.

ChassisManage: Set the chassis ID and management address as the sender ID.

Port Status TLV

Choose whether to send Port Status TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.

Enable: Send Port Status TLVs in CCMs generated by this switch.

Disable: Do not send Port Status TLVs in CCMs generated by this switch.

Interface Status TLV

Choose whether to send Interface Status TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.

Enable: Send Interface Status TLVs in CCMs generated by this switch.

Disable: Do not Send Interface Status TLVs in CCMs generated by this switch.

Organization Specific TLV

Choose whether to send Organization Specific TLVs in CCMs generated by this switch. Can be overridden by Domain and Service level configuration.

Enable: Send Organization Specific TLVs in CCMs generated by this switch.

Disable: Do not send Organization Specific TLVs in CCMs generated by this switch.

Organization Specific TLV OUI

This is the three-bytes OUI transmitted with the Organization-Specific TLVs. Enter as 6 characters 0-9, a-f.

Organization Specific TLV Subtype

This is the subtype transmitted with the Organization-Specific TLV. Can be any value in range [0; 255].

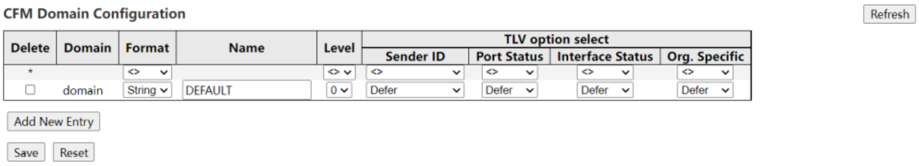
Organization Specific TLV Value

This is the value transmitted in the Organization-Specific TLVs. Value is a printable character string of length 0-63.

8.1.2. Domain

[OAM > CFM > Domain]

On this page, you can configure the CFM Domain parameters.



CFM Domain Configuration

Refresh

Delete	Domain	Format	Name	Level	TLV option select			
					Sender ID	Port Status	Interface Status	Org. Specific
*		<>		<>	<>	<>	<>	<>
□	domain	String	DEFAULT	0	Defer	Defer	Defer	Defer

Add New Entry

Save Reset

CFM Domain Configuration

Delete

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

Domain

Name of Domain. Value is a single word which begins with an alphabetic letter A-Z or a-z with length 1-15.

Format

Select the MD name format. To mimic Y.1731 MEG IDs, use type None.

None: The MD name format is empty.

String: The MD name format is string.

Name

The contents of this pamameter depends on the value of the format member.

If format is None: Name is not used, but will be set to all-zeros behind the scenes. This format is typically used by Y.1731-kind-of-PDUs.

If format is String: Name must contain a string from 1 to 43 characters long.

Level

MD/MEG level of this domain. Valid values are restricted to 0 - 7.

About leak prevention

Leak prevention is about discarding OAM PDUs with MEG levels lower than the MEP they hit when the OAM PDUs are ingressing the port on which the MEP resides, and to discard OAM PDUs with MEG levels at or lower than the MEP's when the OAM PDUs are ingressing other ports.

There are two categories of architectures, when it comes to leak-prevention: Those that use Shared MEG level and those that use Independent MEG level:

Shared MEG level

On Shared MEG level architectures, Port Down MEPs always perform level filtering no matter which VLAN ID (VID) OAM PDUs get classified to, unless the same port has a VLAN MEP on the VID in question. So if you have a Port MEP in VID X and a VLAN MEP in VID Y, an OAM frame arriving on the port and gets classified to VID X or VID Z will be handled/level-filtered by the Port MEP, whereas an OAM frame ingressing the port in VID Y will be handled by the VLAN MEP. Likewise, if the switch has a Port MEP on VID X on Port X and an OAM frame ingresses on VID Y on Port Y, it is subject to level filtering before egressing Port X, unless Port X also has a VLAN MEP on VID Y, in which case the VLAN MEP will take care of level-filtering the OAM PDU.

On Shared MEG level architectures, all Port MEPs must have the same MEG level and any VLAN MEP must have a MEG level higher than the Port MEPs' MEG level.

Independent MEG level

On Independent MEG level architectures, Port Down MEPs never perform level filtering on frames not classified to the MEP's VID. So if you have a Port MEP on VID X and a VLAN MEP on VID Y and an OAM frame ingresses any port on VID Z, it is not subject to handling/level-filtering by any of the two MEPs.

This switch exhibits Independent MEG level

TLV option select

Sender Id: Default Sender ID TLV format to be used in CCMs generated by this Domain (may be overridden in service).

None: Do not include Sender ID TLVs.

Chassis: Enable Sender ID TLV and send Chassis ID (MAC Address).

Manage: Enable Sender ID TLV and send Management address (IPv4 Address).

ChassisManage: Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).

Defer: Let the global configuration decide if Sender ID TLVs shall be included (may be overridden in service).

Port Status: Include or exclude Port Status TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).

Disable: Do not include Port Status TLVs.

Enable: Include Port Status TLVs.

Defer: Let the global configuration decide if Port Status TLVs shall be included (may be overridden in Service).

Interface Status: Include or exclude Interface Status TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).

Disable: Do not include Interface Status TLVs.

Enable: Include Interface Status TLVs.

Defer: Let the global configuration decide if Interface Status TLVs shall be included (may be overridden in Service).

Org. Specific: Exclude Organization-Specific TLV in CCMs generated by this Domain or let higher level determine (may be overridden in Service).

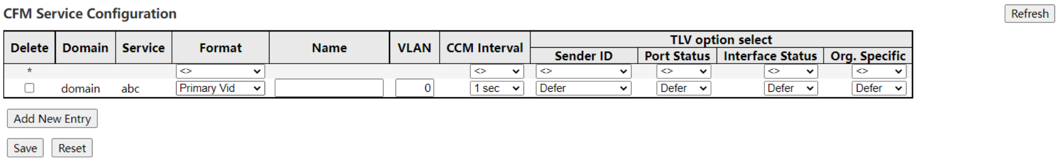
Disable: Do not include Organization-Specific TLVs.

Defer: Let the global configuration decide if Organization-Specific TLVs shall be included (may be overridden in Service).

8.1.3. Service

[OAM > CFM > Service]

On this page, you can configure the CFM Service parameters.



CFM Service Configuration

Delete	Domain	Service	Format	Name	VLAN	CCM Interval	TLV option select			
							Sender ID	Port Status	Interface Status	Org. Specific
*			<>			<>	<>	<>	<>	<>
□	domain	abc	Primary Vid		0	1 sec	Defer	Defer	Defer	Defer

CFM Service Configuration

Delete

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

Domain

Name of Domain under which this Service resides.

Service

Name of Service. Value is a single word which begins with an alphabetic letter A-Z or a-z with length 1-15.

Format

Select the short Service name format. This decides how the value of the Name parameter will be interpreted. To mimic Y.1731 MEG IDs, create an MD instance with an empty name and use Y1731 ICC or Y1731 ICC CC. Possible values are:

String

Two Octets

Y1731 ICC

Y1731 ICC CC

Primary Vid

Look under **Name** for explanation.

Name

The contents of this parameter depends on the value of the format member. Besides the limitations explained for each of them, the following applies in general:

If the Domain Format is **None**, the size of this cannot exceed 45 bytes.If the Domain Format is not **None**, the size of this cannot exceed 44 bytes.

If **Format** is **String**, the following applies:

length must be in range [1; 44]

Contents must be in range [32; 126]

If **Format** is Two Octets, the following applies: **Name**[0] and **Name**[1] will both be interpreted as unsigned 8-bit integers (allowing a range of [0; 255]). **Name**[0] will be placed in the PDU before **Name**[1].The remaining available bytes in name will not be used.

If **Format** is **Y1731 ICC**, the following applies: length must be 13. Contents must be in range [a-z,A-Z,0-9]

Y.1731 specifies that it is a concatenation of ICC (ITU Carrier Code) and UMC (Unique MEG ID Code):

ICC: 1-6 bytes

UMC: 7-12 bytes

In principle UMC can be any value in range [1; 127], but this API does not allow for specifying length of ICC, so the underlying code doesn't know where ICC ends and UMC starts.

The Domain Format must be **None**.

If Format is **Y1731 ICC CC**, the following applies: length must be 15. First 2 chars (CC): Must be amongst [A-Z].

Next 1-6 chars (ICC): Must be amongst [a-z,A-Z,0-9]

Next 7-12 chars (UMC): Must be amongst [a-z,A-Z,0-9]

There may be ONE (slash) present in name[3-7]

The Domain format must be **None**.

VLAN

The MA's primary VID. A primary VID of 0 means that all MEPs created within this MA will be created as port MEPs (interface MEPs). There can only be one port MEP per interface. A given port MEP may still be created with tags, if that MEP's VLAN is non-zero. A non-zero primary VID means that all MEPs created within this MA will be created as VLAN MEPs. A given MEP may be configured with another VLAN than the MA's primary VID, but it is impossible to have untagged VLAN MEPs.

CCM Interval

The CCM rate of all MEPs bound to this Service.

TLV option select

Sender Id: Default Sender ID TLV format to be used in CCMs generated by this Service.

None: Do not include Sender ID TLVs.

Chassis: Enable Sender ID TLV and send Chassis ID (MAC Address).

Manage: Enable Sender ID TLV and send Management address (IPv4 Address).

ChassisManage: Enable Sender ID TLV and send both Chassis ID (MAC Address) and Management Address (IPv4 Address).

Defer: Let the Domain configuration decide if Sender ID TLVs shall be included.

Port Status: Include or exclude Port Status TLV in CCMs generated by this Service or let higher level determine.

Disable: Do not include Port Status TLVs.

Enable: Include Port Status TLVs.

Defer: Let the Domain configuration decide if Port Status TLVs shall be included.

Interface Status: Include or exclude Interface Status TLV in CCMs generated by this Service or let higher level determine.

Disable: Do not include Interface Status TLVs.

Enable: Include Interface Status TLVs.

Defer: Let the Domain configuration decide if Interface Status TLVs shall be included.

Org. Specific: Exclude Organization-Specific TLV in CCMs generated by this Service or let higher level determine.

Disable: Do not include Organization-Specific TLVs.

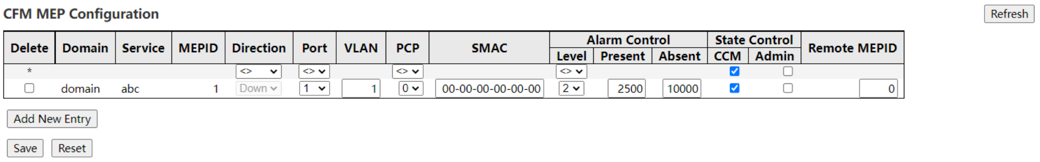
Defer: Let the Domain configuration decide if Organization-Specific TLVs shall be included.

8.1.4. MEP

[OAM > CFM > MEP]

[Configuration]

On this page, you can configure the CFM MEP parameters.



CFM MEP Configuration

Delete	Domain	Service	MEPID	Direction	Port	VLAN	PCP	SMAC	Alarm Control			State Control		Remote MEPID
									Level	Present	Absent	CCM	Admin	
*				<>	<>		<>		<>			☑	□	
□	domain	abc	1	Down	1	1	0	00-00-00-00-00-00	2	2500	10000	☑	□	0

CFM MEP Configuration

Delete

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

Domain

Name of Domain under which this MEP resides.

Service

Name of Service under which this MEP resides.

MEPID

The identification of this MEP. Must be an integer [1..8091].

Direction

Set whether this MEP is an Up- or a Down-MEP.

Port

Port on which this MEP resides.

VLAN

VLAN ID, Use the value 0 to indicate untagged traffic (implies a port MEP).

PCP

Choose PCP value in PDUs' VLAN tag. Not used if untagged.

SMAC

Set a Source MAC address to be used in CCM PDUs originating at this MEP. Must be a unicast address. Format is XX:XX:XX:XX:XX:XX. If all-zeros, the switch port's MAC address will be used instead.

Alarm Control

Level: If a defect is detected with a priority higher than this level, a fault alarm notification will be generated.

Valid range is [1; 6] with 1 indicating that any defect will cause a fault alarm and 6 indicating that no defect can cause a fault alarm. See 802.1Q-2018, clause 20.9.5, LowestAlarmPri.
The possible defects and their priorities are:

Short name Description	Priority
DefRDICCM Remote Defect Indication	1
DefMACstatus MAC Status	2
DefRemoteCCM Remote CCM	3
DefErrorCCM Error CCM Received	4
DefXconCCM Cross Connect CCM Received	5

Present: The time in milliseconds that defects must be present before a fault alarm notification is issued. Default is 2500 ms.

Absent: The time in milliseconds that defects must be absent before a fault alarm notification is reset. Default is 10000 ms.

State Control

CCM: Enable or disable generation of continuity-check messages (CCMs).

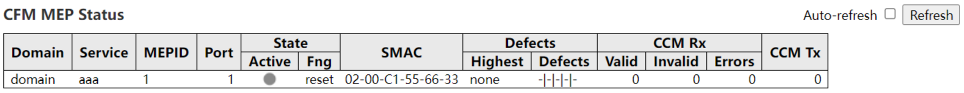
Admin: Enable or disable this MEP. When this MEP is enabled, it will check received/missing CCMs and can raise defects.

Remote MEPID

Specify the Remote MEP that this MEP is expected to receive CCM PDUs from. Must be an integer [0..8091] where 0 means undefined. The value of Remote MEPID must be different from the value of MEPID.

[Status]

Monitor CFM Status on this page.



CFM MEP Status

Domain	Service	MEPID	Port	State		SMAC	Defects		CCM Rx			CCM Tx
				Active	Fng		Highest	Defects	Valid	Invalid	Errors	
domain	aaa	1	1	●	reset	02-00-C1-55-66-33	none	-|-|-|-|-	0	0	0	0

CFM MEP Status

Domain

Name of Domain under which this MEP resides.

Service

Name of Service under which this MEP resides.

MEPID

The identification of this MEP.

Port

Port on which this MEP resides.

State

Active Operational state of the MEP.

- ● OFF: This indicates that the MEP Admin State is disabled.
- ● DOWN: The MEP Admin State is enabled, but an error state exists.
- ● UP: The MEP Admin State is enabled, and no errors and defects exists.

Fng: Holds the current state of the Fault Notification Generator State Machine. Values will be one of the following:

State	Description.
reset	No defect has been present since reset timer expired or the State Machine was last reset.
defect	A defect is present, but not for a long enough time to be reported.
reportDefect	A transient state during which the defect is reported.
defectReported	A defect is present, and some defect has been reported.
defectClearing	No defect is present, but the ResetTime timer has not yet expired.

SMAC

This MEP's MAC address.

Defects

Highest : Highest priority defect that has been present since the MEP's fault notification generator state machine was last in the reset state.

Defects: A MEP can detect and report a number of defects, and multiple defects can be present at the same time. This is indicated the following letter code.

Code	Defect	Description
-	Defect not present	Defect not present
R	someRDIdefect	RDI received from at least one remote MEP
M	someMACstatusDefect	Received Port Status TLV != psUp or Interface Status TLV != isUp
C	someRMEPCCMdefect	Valid CCM is not received within 3.5 times CCM interval from at least one remote MEP
E	errorCCMdefect	Received CCM from an unknown remote MEP-ID or CCM interval mismatch
X	xconCCMdefect	Received CCM with an MD/MEG level smaller than configured or wrong MAID/MEGID (cross-connect)

CCM Rx

Valid: Total number of CCMs that hit this MEP and passed the validation test.

Invalid: Total number of CCMs that hit this MEP and didn't pass the validation test.

Errors: Total number of out-of-sequence errors seen from RMEPs.

CCM Tx

Total number of CCM PDUs transmitted by this MEP.

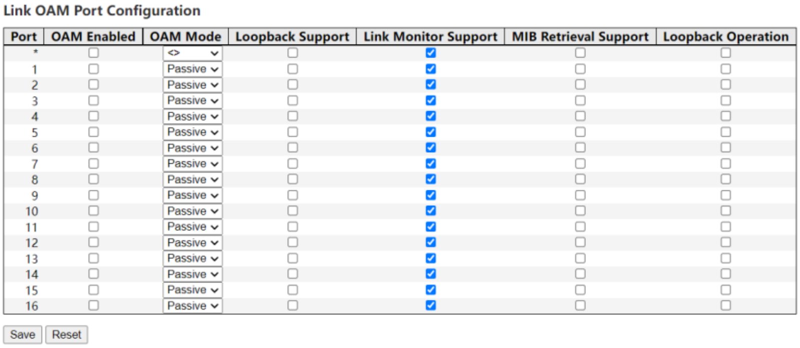
8.2. Link OAM

8.2.1. Port

[OAM > Link OAM > Port]

[Configuration]

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



Link OAM Port Configuration

Port	OAM Enabled	OAM Mode	Loopback Support	Link Monitor Support	MIB Retrieval Support	Loopback Operation
*	□	<>	□	☑	□	□
1	□	Passive	□	☑	□	□
2	□	Passive	□	☑	□	□
3	□	Passive	□	☑	□	□
4	□	Passive	□	☑	□	□
5	□	Passive	□	☑	□	□
6	□	Passive	□	☑	□	□
7	□	Passive	□	☑	□	□
8	□	Passive	□	☑	□	□
9	□	Passive	□	☑	□	□
10	□	Passive	□	☑	□	□
11	□	Passive	□	☑	□	□
12	□	Passive	□	☑	□	□
13	□	Passive	□	☑	□	□
14	□	Passive	□	☑	□	□
15	□	Passive	□	☑	□	□
16	□	Passive	□	☑	□	□

Link OAM Port Configuration

Port

The switch port number.

OAM Enabled

Controls whether Link OAM is enabled on this switch port. Enabling Link OAM provides the network operators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions.

OAM Mode

Configures the OAM Mode as Active or Passive. The default mode is Passive.

Active mode

DTE's configured in Active mode initiate the exchange of Information OAMPDUs as defined by the Discovery process. Once the Discovery process completes, Active DTE's are permitted to send any OAMPDU while connected to a remote OAM peer entity in Active mode. Active DTE's operate in a limited respect if the remote OAM entity is operating in Passive mode. Active devices should not respond to OAM remote loopback commands and variable requests from a Passive peer.

Passive mode

DTE's configured in Passive mode do not initiate the Discovery process. Passive DTE's react to the initiation of the Discovery process by the remote DTE. This eliminates the possibility of passive to passive links. Passive DTE's shall not send Variable Request or Loopback Control OAMPDUs.

Loopback Support

Controls whether the loopback support is enabled for the switch port. Link OAM remote loopback can be used for fault localization and link performance testing. Enabling the loopback support will allow the DTE to execute the remote loopback command that helps in the fault detection.

Link Monitor Support

Controls whether the Link Monitor support is enabled for the switch port. On enabling the Link Monitor support, the DTE supports event notification that permits the inclusion of diagnostic information.

MIB Retrieval Support

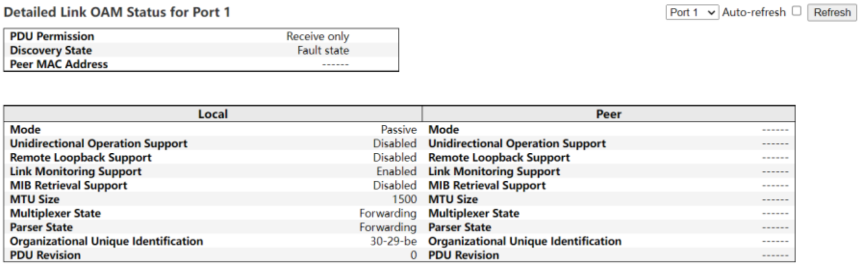
Controls whether the MIB Retrieval Support is enabled for the switch port. On enabling the MIB retrieval support, the DTE supports polling of various Link OAM based MIB variables' contents.

Loopback Operation

If the Loopback support is enabled, enabling this field will start a loopback operation for the port.

[Status]

This page provides Link OAM configuration operational status.



Detailed Link OAM Status for Port 1

PDU Permission	Receive only
Discovery State	Fault state
Peer MAC Address	------

Local		Peer	
Mode	Passive	Mode	------
Unidirectional Operation Support	Disabled	Unidirectional Operation Support	------
Remote Loopback Support	Disabled	Remote Loopback Support	------
Link Monitoring Support	Enabled	Link Monitoring Support	------
MIB Retrieval Support	Disabled	MIB Retrieval Support	------
MTU Size	1500	MTU Size	------
Multiplexer State	Forwarding	Multiplexer State	------
Parser State	Forwarding	Parser State	------
Organizational Unique Identification	30-29-be	Organizational Unique Identification	------
PDU Revision	0	PDU Revision	------

The displayed fields shows the active configuration status for the selected port.

Detailed Link OAM Status for Port

PDU Permission

This field is available only for the Local DTE. It displays the current permission rules set for the local DTE. Possible values are "Link fault","Receive only", "Information exchange only", "ANY".

Discovery State

Displays the current state of the discovery process. Possible states are Fault state, Active state, Passive state, SEND_LOCAL_REMOTE_STATE, SEND_LOCAL_REMOTE_OK_STATE, SEND_ANY_STATE.

Peer MAC Address

The MAC address of the neighbor's device.

Link OAM Port Configuration Status

Mode

The Mode in which the Link OAM is operating, Active or Passive.

Unidirectional Operation Support

This feature is not available to be configured by the user. The status of this configuration is retrieved from the PHY.

Remote Loopback Support

If status is enabled, DTE is capable of OAM remote loopback mode.

Link Monitoring Support

If status is enabled, DTE supports interpreting Link Events.

MIB Retrieval Support

If status is enabled, DTE supports sending Variable Response OAMPDUs.

MTU Size

It represents the largest OAMPDU, in octets, supported by the DTE. This value is compared to the remote’s Maximum PDU Size and the smaller of the two is used.

Multiplexer State

When in forwarding state, the Device is forwarding non-OAMPDUs to the lower sublayer. In case of discarding, the device discards all the non-OAMPDU's.

Parser State

When in forwarding state, Device is forwarding non-OAMPDUs to higher sublayer. When in loopback, Device is looping back non-OAMPDUs to the lower sublayer. When in discarding state, Device is discarding non-OAMPDUs.

Organizational Unique Identification

24-bit Organizationally Unique Identifier of the vendor.

PDU Revision

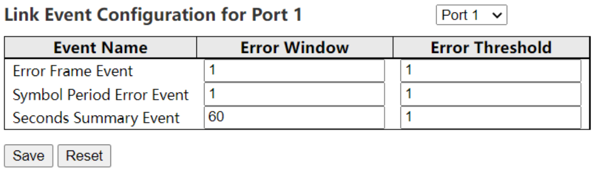
It indicates the current revision of the Information TLV. The value of this field shall start at zero and be incremented each time something in the Information TLV changes. Upon reception of an Information TLV from a peer, an OAM client may use this field to decide if it needs to be processed (an Information TLV that is identical to the previous Information TLV doesn't need to be parsed as nothing in it has changed).

8.2.2. Event

[OAM > Link OAM > Event]

[Configuration]

This page allows the user to inspect the current Link OAM Link Event configurations, and change them as well.



Link Event Configuration for Port 1

Event Name	Error Window	Error Threshold
Error Frame Event	1	1
Symbol Period Error Event	1	1
Seconds Summary Event	60	1

Link Event Configuration for Port #

Event Name

Name of the Link Event which is being configured.

Error Frame Event：The Errored Frame Event counts the number of errored frames detected during the specified period. The period is specified by a time interval (Window in order of 1 sec). This event is generated if the errored frame count is equal to or greater than the specified threshold for that period (Period Threshold). Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Error Frame Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '1'.

Symbol Peroid Error Event：The Errored Symbol Period Event counts the number of symbol errors that occurred during the specified period. The period is specified by the number of symbols that can be received in a time interval on the underlying physical layer. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period. Error Window for 'Symbol Period Error Event' must be an integer value between 1-60 and its default value is '1'. Whereas Error Threshold must be between 0-4294967295 and its default value is '1'.

Seconds Summary Event：the Errored Frame Seconds Summary Event TLV counts the number of errored frame seconds that occurred during the specified period. The period is specified by a time interval. This event is generated if the number of errored frame seconds is equal to or greater than the specified threshold for that period. An errored frame second is a one second interval wherein at least one frame error was detected. Errored frames are frames that had transmission errors as detected at the Media Access Control sublayer. Error Window for 'Seconds Summary Event' must be an integer value between 10-900 and its default value is '60'. Whereas Error Threshold must be between 1-900 and its default value is '1'.

Error window

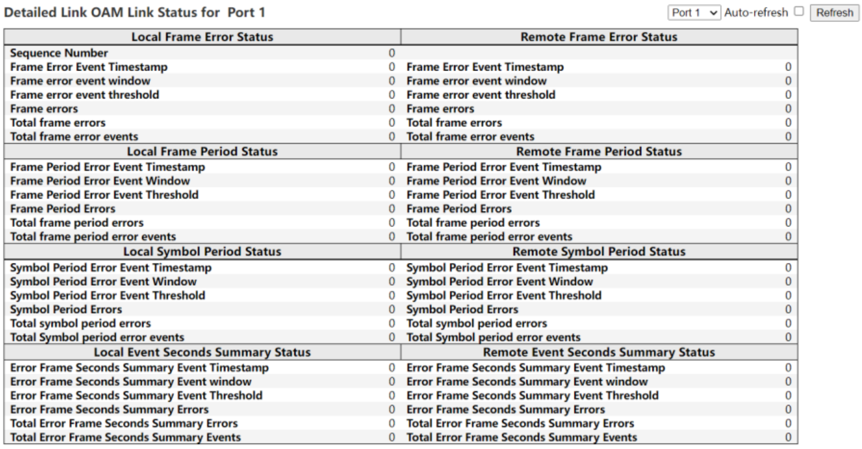
Represents the window period in the order of 1 sec for the observation of various link events.

Loopback Support

Represents the threshold value for the window period for the appropriate Link event so as to notify the peer of this error.

[Status]

This page displays detailed information about the current OAM link state.



Detailed Link OAM Link Status for Port 1

Local Frame Error Status		Remote Frame Error Status	
Sequence Number	0		
Frame Error Event Timestamp	0	Frame Error Event Timestamp	0
Frame error event window	0	Frame error event window	0
Frame error event threshold	0	Frame error event threshold	0
Frame errors	0	Frame errors	0
Total frame errors	0	Total frame errors	0
Total frame error events	0	Total frame error events	0
Local Frame Period Status		**Remote Frame Period Status**	
Frame Period Error Event Timestamp	0	Frame Period Error Event Timestamp	0
Frame Period Error Event Window	0	Frame Period Error Event Window	0
Frame Period Error Event Threshold	0	Frame Period Error Event Threshold	0
Frame Period Errors	0	Frame Period Errors	0
Total frame period errors	0	Total frame period errors	0
Total frame period error events	0	Total frame period error events	0
Local Symbol Period Status		**Remote Symbol Period Status**	
Symbol Period Error Event Timestamp	0	Symbol Period Error Event Timestamp	0
Symbol Period Error Event Window	0	Symbol Period Error Event Window	0
Symbol Period Error Event Threshold	0	Symbol Period Error Event Threshold	0
Symbol Period Errors	0	Symbol Period Errors	0
Total symbol period errors	0	Total symbol period errors	0
Total Symbol period error events	0	Total Symbol period error events	0
Local Event Seconds Summary Status		**Remote Event Seconds Summary Status**	
Error Frame Seconds Summary Event Timestamp	0	Error Frame Seconds Summary Event Timestamp	0
Error Frame Seconds Summary Event window	0	Error Frame Seconds Summary Event window	0
Error Frame Seconds Summary Event Threshold	0	Error Frame Seconds Summary Event Threshold	0
Error Frame Seconds Summary Errors	0	Error Frame Seconds Summary Errors	0
Total Error Frame Seconds Summary Errors	0	Total Error Frame Seconds Summary Errors	0
Total Error Frame Seconds Summary Events	0	Total Error Frame Seconds Summary Events	0

The left pane displays the Event status for the Local OAM unit while the right pane displays the status for the Peer for the respective port.

Detailed Link OAM Link Status for Port

Port

The switch port number.

Sequence Number

This two-octet field indicates the total number of events occurred at the remote end.

Frame Error Event Timestamp

This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Frame error event window

This two-octet field indicates the duration of the period in terms of 100 ms intervals. 1) The default value is one second. 2) The lower bound is one second. 3) The upper bound is one minute.

Frame error event threshold

This four-octet field indicates the number of detected errored frames in the period is required to be equal to or greater than in order for the event to be generated. 1) The default value is one frame error. 2) The lower bound is zero frame errors. 3) The upper bound is unspecified.

Frame errors

This four-octet field indicates the number of detected errored frames in the period.

Total frame errors

This eight-octet field indicates the sum of errored frames that have been detected since the OAM sublayer was reset.

Total frame error events

This four-octet field indicates the number of Errored Frame Event TLVs that have been generated since the OAM sublayer was reset.

Frame Period Error Event Timestamp

This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Frame Period Error Event Window

This four-octet field indicates the duration of period in terms of frames.

Frame Period Error Event Threshold

This four-octet field indicates the number of errored frames in the period is required to be equal to or greater than in order for the event to be generated.

Frame Period Errors

This four-octet field indicates the number of frame errors in the period.

Total frame period errors

This eight-octet field indicates the sum of frame errors that have been detected since the OAM sublayer was reset.

Total frame period error events

This four-octet field indicates the number of Errored Frame Period Event TLVs that have been generated since the OAM sublayer was reset.

Symbol Period Error Event Timestamp

This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals.

Symbol Period Error Event Window

This eight-octet field indicates the number of symbols in the period.

Symbol Period Error Event Threshold

This eight-octet field indicates the number of errored symbols in the period is required to be equal to or greater than in order for the event to be generated.

Symbol Period Errors

This eight-octet field indicates the number of symbol errors in the period.

Total symbol period errors

This eight-octet field indicates the sum of symbol errors since the OAM sublayer was reset.

Total Symbol period error events

This four-octet field indicates the number of Errored Symbol Period Event TLVs that have been generated since the OAM sublayer was reset.

Error Frame Seconds Summary Event Timestamp

This two-octet field indicates the time reference when the event was generated, in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

Error Frame Seconds Summary Event Window

This two-octet field indicates the duration of the period in terms of 100 ms intervals, encoded as a 16-bit unsigned integer.

Error Frame Seconds Summary Event Threshold

This two-octet field indicates the number of errored frame seconds in the period is required to be equal to or greater than in order for the event to be generated, encoded as a 16-bit unsigned integer.

Error Frame Seconds Summary Errors

This two-octet field indicates the number of errored frame seconds in the period, encoded as a 16-bit unsigned integer.

Total Error Frame Seconds Summary Errors

This four-octet field indicates the sum of errored frame seconds that have been detected since the OAM sublayer was reset.

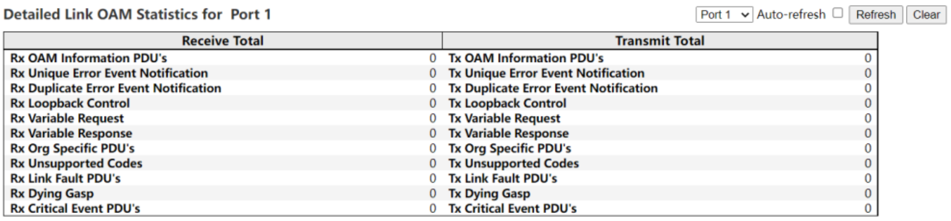
Total Error Frame Seconds Summary Events

This four-octet field indicates the number of Errored Frame Seconds Summary Event TLVs that have been generated since the OAM sublayer was reset, encoded as a 32bit unsigned integer.

8.2.3. Statistics

[OAM > Link OAM > Statistics]

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



Detailed Link OAM Statistics for Port 1

Receive Total		Transmit Total	
Rx OAM Information PDU's	0	Tx OAM Information PDU's	0
Rx Unique Error Event Notification	0	Tx Unique Error Event Notification	0
Rx Duplicate Error Event Notification	0	Tx Duplicate Error Event Notification	0
Rx Loopback Control	0	Tx Loopback Control	0
Rx Variable Request	0	Tx Variable Request	0
Rx Variable Response	0	Tx Variable Response	0
Rx Org Specific PDU's	0	Tx Org Specific PDU's	0
Rx Unsupported Codes	0	Tx Unsupported Codes	0
Rx Link Fault PDU's	0	Tx Link Fault PDU's	0
Rx Dying Gasp	0	Tx Dying Gasp	0
Rx Critical Event PDU's	0	Tx Critical Event PDU's	0

The displayed counters represent the total number of OAM frames received and transmitted for the selected port. Discontinuities of these counter can occur at re-initialization of the management system.

Detailed Link OAM Statistics for Port #

Rx and Tx OAM Information PDU's

The number of received and transmitted OAM Information PDU's. Discontinuities of this counter can occur at re-initialization of the management system.

Rx and Tx Unique Error Event Notification

A count of the number of unique Event OAMPDUs received and transmitted on this interface. Event Notifications may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. Duplicate Event Notification transmissions are counted by Duplicate Event Notification counters for Tx and Rx respectively. A unique Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is distinct from the previously transmitted Event Notification OAMPDU Sequence Number.

Rx and Tx Duplicate Error Event Notification

A count of the number of duplicate Event OAMPDUs received and transmitted on this interface. Event Notification OAMPDUs may be sent in duplicate to increase the probability of successfully being received, given the possibility that a frame may be lost in transit. A duplicate Event Notification OAMPDU is indicated as an Event Notification OAMPDU with a Sequence Number field that is identical to the previously transmitted Event Notification OAMPDU Sequence Number.

Rx and Tx Loopback Control

A count of the number of Loopback Control OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Request

A count of the number of Variable Request OAMPDUs received and transmitted on this interface.

Rx and Tx Variable Response

A count of the number of Variable Response OAMPDUs received and transmitted on this interface.

Rx and Tx Org Specific PDU's

A count of the number of Organization Specific OAMPDUs transmitted on this interface.

Rx and Tx Unsupported Codes

A count of the number of OAMPDUs transmitted on this interface with an unsupported op-code.

Rx and Tx Link fault PDU's

A count of the number of Link fault PDU's received and transmitted on this interface.

Rx and Tx Dying Gasp

A count of the number of Dying Gasp events received and transmitted on this interface.

Rx and Tx Critical Event PDU's

A count of the number of Critical event PDU's received and transmitted on this interface.

9. TCN

The menu contains the following dialogs:

TTDP Config

TRDP Config

TTDP Status

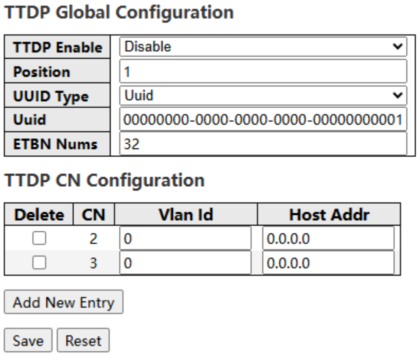
ETBN Status

Flow Statistics

9.1. TTDP Config

[TCN > TTDP Config]

Configuration



TTDP Global Configuration

TTDP Enable	Disable
Position	1
UUID Type	Uuid
Uuid	00000000-0000-0000-0000-000000000001
ETBN Nums	32

TTDP CN Configuration

Delete	CN	Vlan Id	Host Addr
□	2	0	0.0.0.0
□	3	0	0.0.0.0

TTDP Global Configuration

TTDP Enable

Indicates whether the TTDP feature is enabled. Once enabled, configuration settings on the TTDP Configuration page and TTDP Port page cannot be modified.

Position

Represents the static location information of the ETBN within the grouped subnet. The value ranges from 0 to 32, where 0 is the default value.

UUID Type

The numerical type that represents the TTDP composition identifier, where Cst String refers to generating a Uuid using a string, and Uuid is a string with a specific format.

Uuid

Represents the composition identifier for TTDP. When the Uuid type is Cst String, it consists of 3 to 20 visible characters (excluding spaces). When the Uuid type is Uuid, it is a 36-character hexadecimal string in the format (xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx).

ETBN Nums

Specifies the number of ETBNs in the grouped subnet. The value ranges from 1 to 32.

TTDP CN Configuration

Delete

This field indicates whether to delete the TTDP composition network configuration.

CN

This field represents the set of composition networks in the composition network information. The valid range is from 1 to 32.

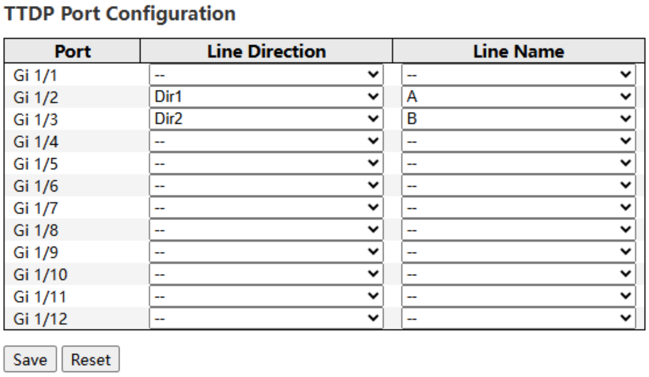
Vlan Id

This field indicates the VLAN where the composition network is located. The valid range is 0 to 4095.

Host Addr

This field indicates the host address where the composition network is located. The valid range is from 0.0.0.0 to 255.255.255.255.

Port



TTDP Port Configuration

Port	Line Direction	Line Name
Gi 1/1	--	--
Gi 1/2	Dir1	A
Gi 1/3	Dir2	B
Gi 1/4	--	--
Gi 1/5	--	--
Gi 1/6	--	--
Gi 1/7	--	--
Gi 1/8	--	--
Gi 1/9	--	--
Gi 1/10	--	--
Gi 1/11	--	--
Gi 1/12	--	--

TTDP Port Configuration

Port

This field indicates the physical port number of the device.

Line Direction

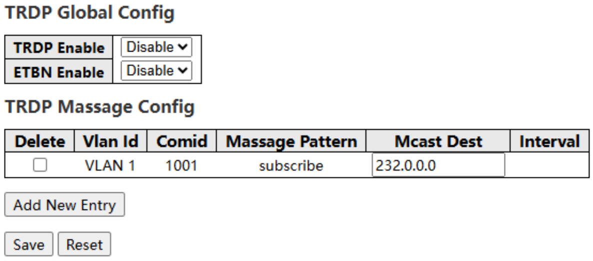
This field indicates the direction of the TTDP line: Line 1 or Line 2.

Line Name

This field indicates the name of the TTDP line, which can be A, B, C, or D.

9.2. TRDP Config

[TCN > TRDP Config]



TRDP Global Config

TRDP Enable	Disable
ETBN Enable	Disable

TRDP Massage Config

Delete	Vlan Id	Comid	Massage Pattern	Mcast Dest	Interval
□	VLAN 1	1001	subscribe	232.0.0.0	

TDRP Global Config

TRDP Enable

Indicates whether to enable the TRDP function for TCN. Enabling means turning on the TRDP function, while disabling means turning off the TRDP function.

ETBN Enable

Indicates whether to enable the ETBN role for TRDP. Enabling means activating this role, while disabling means deactivating this role.

TRDP Massage Config

Delete

Delete TRDP PD message configuration.

Vlan Id

This field indicates the VLAN where the TRDP PD message is located. The valid range is VLAN 1 to VLAN 4095. If the configured VLAN does not have an IP interface assigned, the configuration will fail.

Comid

Indicates the comid of the TRDP PD message. The comid configuration range is from 1001 to 65535.

Massage pattern

Indicates the mode of the TRDP PD message. Two PD message modes are available: the first is publish mode, and the second is subscribe mode. When in publish mode, the time interval can be configured; when in subscribe mode, the time interval cannot be configured.

Mcast Dest

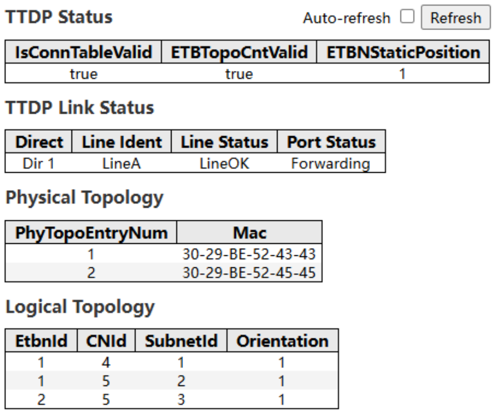
Indicates the multicast destination address to which the TRDP PD message is sent. The valid range is 224.0.0.0 to 239.255.255.255.

Interval

Indicates the sending interval of the TRDP PD subscribed message. When the message mode is publish mode, the interval can be configured and the valid range is 1000 to 65535 milliseconds. When the message mode is subscribe mode, the interval cannot be configured.

9.3. TTDP Status

[TCN > TTDP Status]



TTDP Status

IsConnTableValid	ETBTopoCntValid	ETBNStaticPosition
true	true	1

TTDP Link Status

Direct	Line Ident	Line Status	Port Status
Dir 1	LineA	LineOK	Forwarding

Physical Topology

PhyTopoEntryNum	Mac
1	30-29-BE-52-43-43
2	30-29-BE-52-45-45

Logical Topology

EtbnId	CNId	SubnetId	Orientation
1	4	1	1
1	5	2	1
2	5	3	1

TTDP Status

IsConnTableValid

Indicates whether the TTDP link table is valid. Valid is true, invalid is false.

ETBTopoCntValid

Indicates whether the ETBN topology is valid. Valid is true; invalid is false.

ETBN StaticPosition

Indicates the static position of the ETBN.

TTDP Link Status

Direct

Indicates the direction of the TTDP link status table.

Line Ident

Indicates the line direction of the TTDP link status table. The line directions are A, B, C, and D.

Line Status

Indicates the line status of the TTDP link status table.

Port Status

Indicates the port status of the TTDP link status table.

Physical Topology

PhyTopoEntryNum

Indicates the How many entries are there in the physical topology table.

Mac

Indicates the MAC address stored in the physical topology table.

Logical Topology

EtbnId

Indicates the ETBN ID in the logical topology.

CNId

Indicates the composition network ID in the logical topology.

SubnetId

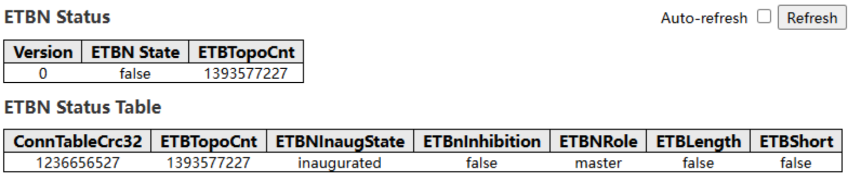
Indicates the subnet ID in the logical topology.

Orientation

Indicates the direction of each entry in the logical topology table.

9.4. ETBN Status

[TCN > ETBN Status]



ETBN Status

Version	ETBN State	ETBTopoCnt
0	false	1393577227

ETBN Status Table

ConnTableCrc32	ETBTopoCnt	ETBNInaugState	ETBnInhibition	ETBNRole	ETBLength	ETBShort
1236656527	1393577227	inaugurated	false	master	false	false

ETBN Status

Version

Indicates the version of the ETBN.

ETBN State

Indicates whether the ETBN status is enabled.

ETBTopoCnt

Indicates the ETB topology sum.

ETBN Status Table

ConnTableCrc32

Indicates the CRC value of the ETB link table.

ETBTopoCnt

Indicates whether the ETBN topology is stable. If the topology sum remains unchanged, it means the topology is stable; if the topology sum changes, it indicates that the ETBN network is unstable.

ETBNInaugState

Indicates whether the ETBN is started.

ETBnInhibition

Indicates whether ETBN suppression is enabled.True means enabled, false means disabled.

ETBNRole

Indicates whether the ETBN role is configured.

ETBLength

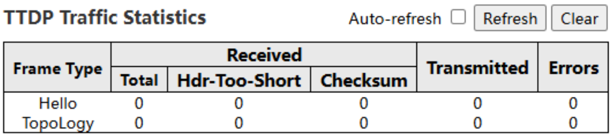
Indicates whether the ETB is extended.

ETBShort

Indicates whether the ETB is shortened.

9.5. Flow Statistics

[TCN > Flow Statistics]



TTDP Traffic Statistics

Frame Type	Received			Transmitted	Errors
	Total	Hdr-Too-Short	Checksum		
Hello	0	0	0	0	0
TopoLogy	0	0	0	0	0

TTDP Traffic Statistics

Frame Type

Indicates the type of frame received by TTDP: Hello frame or Topology frame.

Received Total

Indicates the total amount of data received for each frame type.

Received Hdr-Too-Short

Indicates the number of undersized frames received for each frame type.

Received Checksum

Indicates the number of frames with checksum errors received for each frame type.

Transmitted

Indicates the number of data frames sent for each frame type.

Errors

Indicates the number of error packets received for each frame type.

10. Advanced

The menu contains the following dialogs:

DHCPv4
DHCPv6
DNS
UPnP
File Management

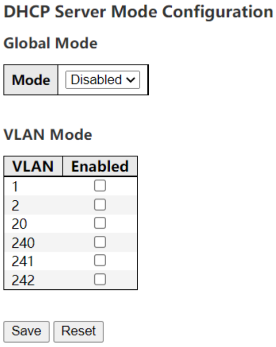
10.1. DHCPv4

10.1.1. Server

Mode

[Advanced > DHCPv4 > Server > Mode]

This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN.



DHCP Server Mode Configuration

Global Mode

Mode	Disabled

VLAN Mode

VLAN	Enabled
1	□
2	□
20	□
240	□
241	□
242	□

DHCP Server Mode Configuration

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 pre system.

VLAN Mode

Configure operation mode to enable/disable DHCP server per VLAN.

VLAN

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.

1. press Add VLAN Range to add a new VLAN range.

2. input the VLAN range that you want to disable.

3. choose Mode to be Disabled.

4. press Save to apply the change.

Then, you will see the disabled VLAN range is removed from the DHCP Server mode configuration page.

Enabled

Indicate the operation mode per VLAN. Possible modes are:

Enabled: Enable DHCP server per VLAN.

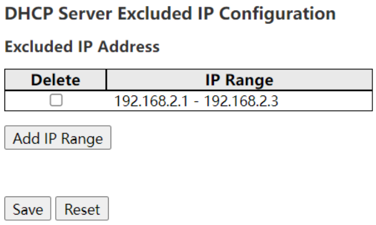
Disabled: Disable DHCP server per VLAN.

Excluded IP

[Advanced > DHCPv4 > Server > Excluded IP]

[Configuration]

This page configures excluded IP addresses. DHCP server will not allocate these excluded IP addresses to DHCP client.



DHCP Server Excluded IP Configuration

Excluded IP Address

Delete	IP Range
□	192.168.2.1 - 192.168.2.3

DHCP Server Excluded IP Configuration

Excluded IP Address

Configure excluded IP addresses.

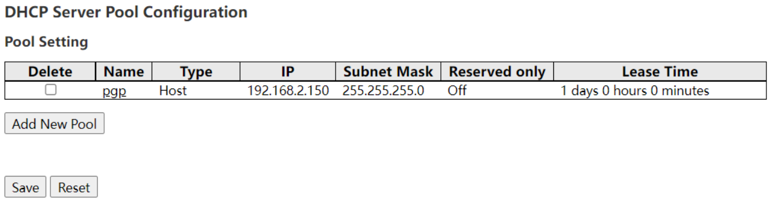
IP Range

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.

Pool

[Advanced > DHCPv4 > Server > Pool]

This page manages DHCP pools. According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client.



DHCP Server Pool Configuration

Pool Setting

Delete	Name	Type	IP	Subnet Mask	Reserved only	Lease Time
□	pgp	Host	192.168.2.150	255.255.255.0	Off	1 days 0 hours 0 minutes

DHCP Server Pool Configuration

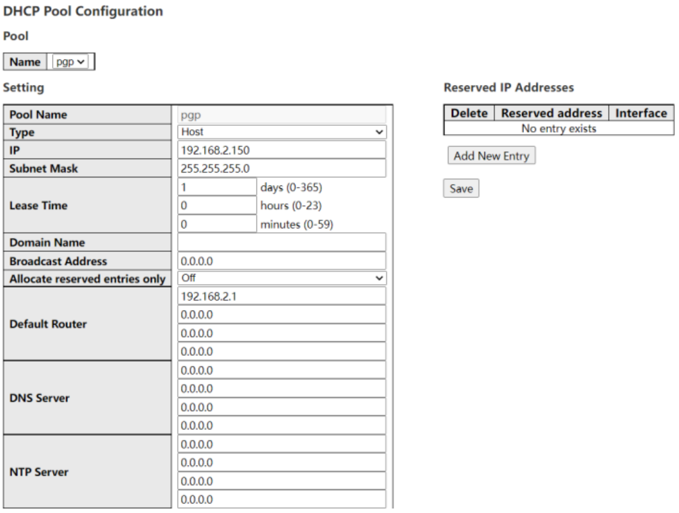
Pool Setting

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.



DHCP Pool Configuration

Pool

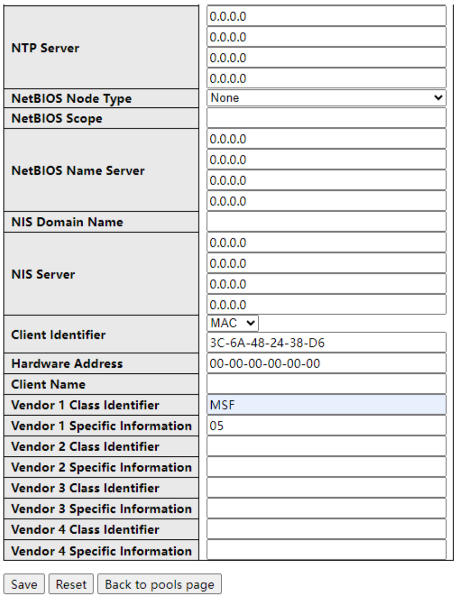
Name: pgp

Setting

Pool Name	pgp
Type	Host
IP	192.168.2.150
Subnet Mask	255.255.255.0
Lease Time	1 days (0-365) 0 hours (0-23) 0 minutes (0-59)
Domain Name	
Broadcast Address	0.0.0.0
Allocate reserved entries only	Off
Default Router	192.168.2.1 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 0.0.0.0

Reserved IP Addresses

Delete	Reserved address	Interface
No entry exists		



NTP Server	0.0.0.0 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	MAC 3C-6A-48-24-38-D6
Hardware Address	00-00-00-00-00-00
Client Name	
Vendor 1 Class Identifier	MSF
Vendor 1 Specific Information	05
Vendor 2 Class Identifier	
Vendor 2 Specific Information	
Vendor 3 Class Identifier	
Vendor 3 Specific Information	
Vendor 4 Class Identifier	
Vendor 4 Specific Information	

DHCP Pool Configuration

Pool

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.

Setting

Pool Name

Address Pool Name.

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.

Domain Name

DHCP Domain Name.

Broadcast Address

Configure Broadcast Address.

Allocate reserved entries only

If enabled, the IP address pool entered in the reservation entry table can be restricted to available addresses.

Default Router

Configure Default Route.

DNS Server

Configure DNS Server.

NTP Server

Configure NTP Server.

NetBIOS Node Type

Set NetBIOS node type. The types are: None, B-node (Broadcast node), P-node (Peer-to-peer node), M-node (Mixed node), H-node (Hybrid node).

NetBIOS Scope

Set NetBIOS Scope ID, limited to 32 characters.

NetBIOS Name Server

Specify an IP address as the NetBIOS name server.

NIS Domain Name

Set NIS Server Domain Name.

NIS Server

Set NIS Server Address.

Client Identifier

The client identifier can be set as a name, limited to 64 characters, or as a MAC address format.

Hardware Address

Client MAC Address.

Client Name

Client Hostname, limited to 32 characters.

Vendor # Class Identifier

Vendor Class Identifier, limited to 64 characters.

Vendor # Specific Information

64 octets of hexadecimal values (0x...).

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.

Reserved Only

If on, Ip addresses optainable from the pool are limited to those entered into the reserved entries table.

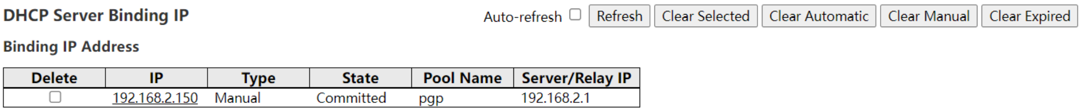
Lease Time

Display lease time of the pool.

Binding

[Advanced > DHCPv4 > Server > Binding]

This page displays bindings generated for DHCP clients.



DHCP Server Binding IP

Binding IP Address

Delete	IP	Type	State	Pool Name	Server/Relay IP
□	192.168.2.150	Manual	Committed	pgp	192.168.2.1

DHCP Server Binding IP

Binding IP Address

Display all bindings.

IP

IP address allocated to DHCP client.

Type

Type of binding. Possible types are Automatic, Manual, Expired.

State

State of binding. Possible states are Committed, Allocated, Expired.

Pool Name

The pool that generates the binding.

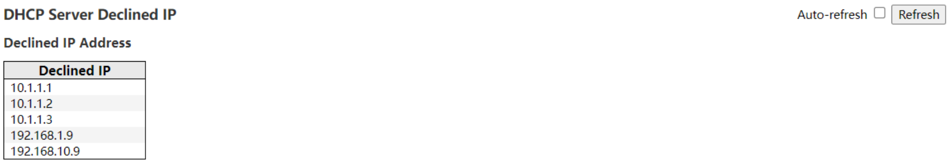
Server/Relay IP

Either IP address of dhcp server or, in case of relayed binding, IP address of relay agent through which binding was negotiated.

Declined IP

[Advanced > DHCPv4 > Server > Declined IP]

This page displays declined IP addresses.



DHCP Server Declined IP

Declined IP Address

Declined IP
10.1.1.1
10.1.1.2
10.1.1.3
192.168.1.9
192.168.10.9

DHCP Server Declined IP

Declined IP Addresses

Display IP addresses declined by DHCP client.

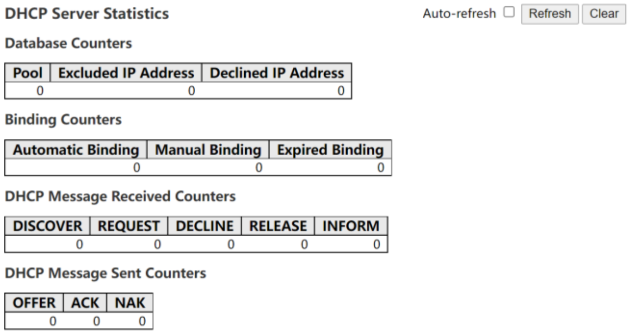
Declined IP

List of IP addresses declined.

Statistics

[Advanced > DHCPv4 > Server > Statistics]

This page displays the database counters and the number of DHCP messages sent and received by DHCP server.



DHCP Server Statistics

Database Counters

Pool	Excluded IP Address	Declined IP Address
0	0	0

Binding Counters

Automatic Binding	Manual Binding	Expired Binding
0	0	0

DHCP Message Received Counters

DISCOVER	REQUEST	DECLINE	RELEASE	INFORM
0	0	0	0	0

DHCP Message Sent Counters

OFFER	ACK	NAK
0	0	0

DHCP Server Statistics

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 declined IP addresses.

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

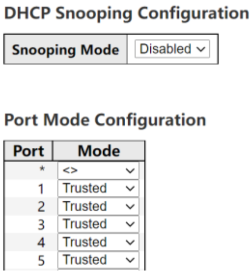
Number of DHCP NAK messages sent.

10.1.2. Snooping

[Advanced > DHCPv4 > Snooping]

[Configuration]

On this page, you can configure Snooping Mode and Port Mode.



DHCP Snooping Configuration

Snooping Mode	Disabled

Port Mode Configuration

Port	Mode
*	<>
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted

DHCP snooping Configuration

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

Mode

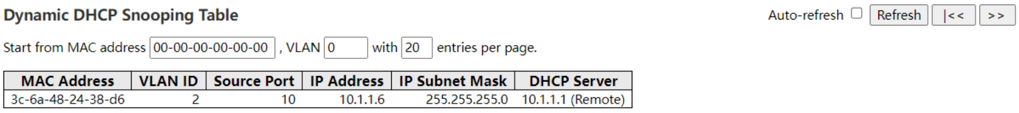
Indicates the DHCP snooping port mode. Possible port modes are:

Trusted: Configures the port as trusted source of the DHCP messages.

Untrusted: Configures the port as untrusted source of the DHCP messages.

[Snooping Table]

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

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
3c-6a-48-24-38-d6	2	10	10.1.1.6	255.255.255.0	10.1.1.1 (Remote)

Dynamic 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 **"|<<"** button to start over.

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.

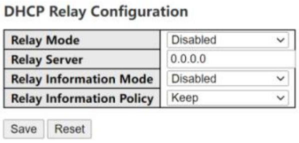
DHCP Server Address

DHCP Server address of the entry.

10.1.3. Relay

[Advanced > DHCPv4 > Relay]

[Configuration]



DHCP Relay Configuration

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

DHCP 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.

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 equals 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.

Disabled: 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:

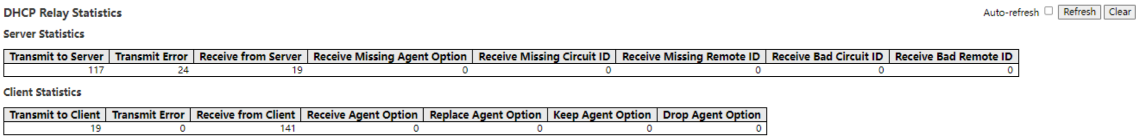
Replace: Replace the original relay information when a DHCP message that already contains it is received.

Keep: Keep the original relay information when a DHCP message that already contains it is received.

Drop: Drop the package when a DHCP message that already contains relay information is received.

[Relay Statistics]

This page provides statistics for DHCP relay.



DHCP Relay Statistics

Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
117	24	19	0	0	0	0	0

Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
19	0	141	0	0	0	0

DHCP Relay Statistics

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 client.

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.

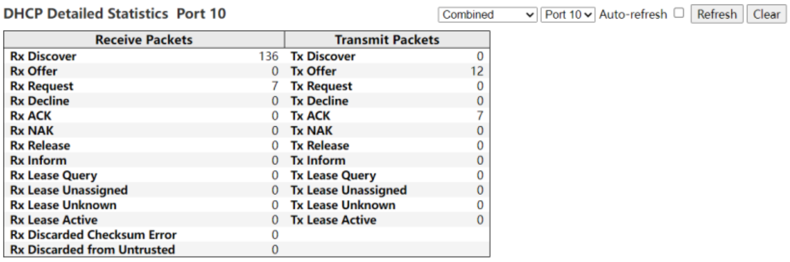
Drop Agent Option

The number of packets that were dropped which were received with relay agent information.

10.1.4. Detailed Statistics

[Advanced > DHCPv4 > Detailed Statistics]

This page provides statistics for DHCP snooping.



DHCP Detailed Statistics Port 10

Receive Packets		Transmit Packets	
Rx Discover	136	Tx Discover	0
Rx Offer	0	Tx Offer	12
Rx Request	7	Tx Request	0
Rx Decline	0	Tx Decline	0
Rx ACK	0	Tx ACK	7
Rx NAK	0	Tx NAK	0
Rx Release	0	Tx Release	0
Rx Inform	0	Tx Inform	0
Rx Lease Query	0	Tx Lease Query	0
Rx Lease Unassigned	0	Tx Lease Unassigned	0
Rx Lease Unknown	0	Tx Lease Unknown	0
Rx Lease Active	0	Tx Lease Active	0
Rx Discarded Checksum Error	0		
Rx Discarded from Untrusted	0		

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.

DHCP Detailed Statistics Port #

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 packets coming from untrusted port.

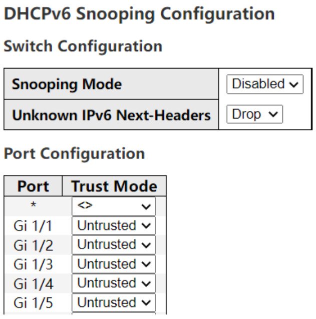
10.2. DHCPv6

10.2.1. Snooping

[Advanced > DHCPv6 > Snooping]

[Configuration]

Configure DHCPv6 (aka. DHCP over IPv6) Snooping on this page.



DHCPv6 Snooping Configuration

Switch Configuration

Snooping Mode	Disabled
Unknown IPv6 Next-Headers	Drop

Port Configuration

Port	Trust Mode
*	<>
Gi 1/1	Untrusted
Gi 1/2	Untrusted
Gi 1/3	Untrusted
Gi 1/4	Untrusted
Gi 1/5	Untrusted

DHCPv6 Snooping Configuration

Switch Configuration

Snooping Mode

Indicates the DHCPv6 snooping mode operation.

Possible modes are:

Enabled: Enable DHCPv6 snooping mode operation. When DHCPv6 snooping mode operation is enabled, the DHCPv6 client request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.

Disabled: Disable DHCP snooping mode operation.

Unknown IPv6 Next-Headers

Indicates how Unknown IPv6 Next-Header values should be treated. The switch needs to parse all IPv6 packets to a DHCPv6 client to determine if it is in fact a DHCPv6 message. If an unknown IPv6 extension header is encountered the parsing cannot continue. See RFC 7610, section 5, item 3 for details.

Possible options are:

Drop: Drop packets with unknown IPv6 extension headers. This is the most secure option but may result in traffic disruptions.

Allow: Allow packets with unknown IPv6 extension headers. This is a less secure option but prevents traffic disruptions.

Port Mode Configuration

Trust Mode

Indicates the DHCPv6 snooping port mode.

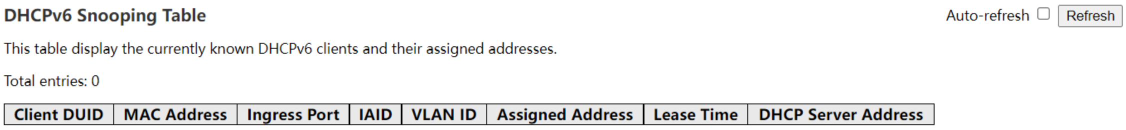
Possible port modes are:

Trusted: Configures the port as trusted source of the DHCPv6 messages.

Untrusted: Configures the port as untrusted source of the DHCPv6 messages.

[Snooping Table]

This page displays the content of the current DHCPv6 snooping table.



DHCPv6 Snooping Table

This table display the currently known DHCPv6 clients and their assigned addresses.

Total entries: 0

Client DUID	MAC Address	Ingress Port	IAID	VLAN ID	Assigned Address	Lease Time	DHCP Server Address

DHCPv6 snooping table

Client DUID

The DHCP Unique Identifier (DUID) for the client. DHCPv6 uses this value to uniquely identify a client host instead of just using the MAC address of one of its interface ports (as DHCPv4 does).

MAC Address

The MAC address for the client interface port that sent the DHCPv6 message.

Ingress Port

The local port on the snooping switch where client messages are received.

IAID

Each client may contain multiple interfaces and may request addresses for each of these in the same DHCPv6 message. The Identity Association ID (IAID) value uniquely identifies the interface in the scope of the client.

VLAN ID

The VLAN ID which is used by the client messages.

Assigned Address

The address assigned to the interface identified by the IAID value.

Lease Time

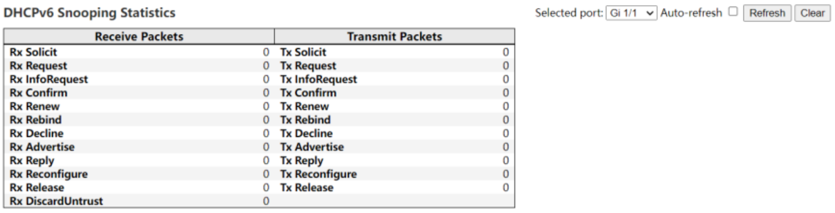
The lease time associated with the assigned address in seconds.

DHCP Server Address

The IPv6 address of the DHCP server which assigned the address to the client.

[Snooping Statistics]

This page provides statistics for DHCPv6 snooping.



DHCPv6 Snooping Statistics

Selected port: Gi 1/1 Auto-refresh □

Receive Packets		Transmit Packets	
Rx Solicit	0	Tx Solicit	0
Rx Request	0	Tx Request	0
Rx InfoRequest	0	Tx InfoRequest	0
Rx Confirm	0	Tx Confirm	0
Rx Renew	0	Tx Renew	0
Rx Rebind	0	Tx Rebind	0
Rx Decline	0	Tx Decline	0
Rx Advertise	0	Tx Advertise	0
Rx Reply	0	Tx Reply	0
Rx Reconfigure	0	Tx Reconfigure	0
Rx Release	0	Tx Release	0
Rx DiscardUntrust	0		

DHCPv6 Snooping Statistics

General Receive and Transmit Packets

The page contains both RX and TX counters for all known DHCPv6 message types.

Please refer to RFC 3315 for details on the various DHCPv6 message types.

Untrusted Discards

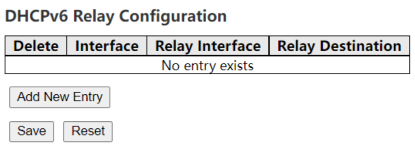
The DiscardUntrust counter indicate the number of received DHCP server packets that has been discarded due to the port being untrusted.

10.2.2. Relay

[Advanced > DHCPv6 > Relay]

[Configuration]

This is a page to configure Dhcp6_Relay for a specific vlan.



DHCPv6 Relay Configuration

Delete	Interface	Relay Interface	Relay Destination
No entry exists			

DHCPv6 Relay configuration

Interface

Interface identification.

Relay Interface

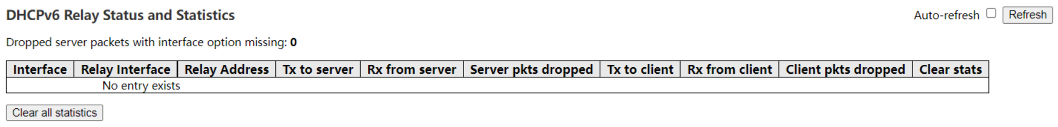
Interface identification. The id of the interface used for relaying.

Relay Destination

An Ipv6 address represented as human readable text as specified in RFC5952. The IPv6 address of the DHCPv6 server that requests shall be relayed to. The default value 'ff05::1:3' mans 'any DHCP server'.

[Relay Statistics]

This page shows current, configured relay agents and their statistics.



DHCPv6 Relay Status and Statistics

Auto-refresh □ Refresh

Dropped server packets with interface option missing: 0

Interface	Relay Interface	Relay Address	Tx to server	Rx from server	Server pkts dropped	Tx to client	Rx from client	Client pkts dropped	Clear stats
No entry exists									

DHCPv6 Relay Status and Statistics

Interface

Interface identification. The id of the interface that receives client requests.

Relay Interface

Interface identification. The id of the interface used for relaying.

Relay Address

An Ipv6 address represented as human readable text as specified in RFC5952. The IPv6 address that requests shall be relayed to. The default value 'ff05::1:3' means 'any DHCPv6 server'.

Tx to server

Integer number. Number of packets relayed to server.

Rx from server

Integer number. Number of packets received from server.

Server pkts dropped

Integer number. Number of packets from server that relay agent drops.

Tx to client

Integer number. Number of packets sent to client.

Rx from client

Integer number. Number of packets received from client.

Client pkts dropped

Integer number. Number of packets from client that relay agent drops.

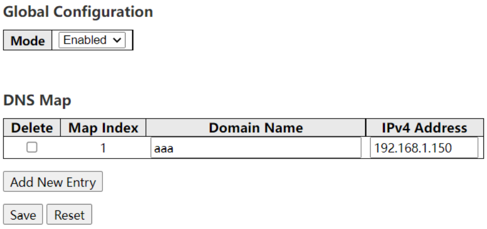
Clear stats

Clear: Resets all statistics counters of relevant entry to zero.

10.3. DNS

10.3.1. Configuration

[Advanced > DNS > Configuration]



Global Configuration

Mode	Enabled

DNS Map

Delete	Map Index	Domain Name	IPv4 Address
□	1	aaa	192.168.1.150

Global Configuration

Mode

Indicates the IP DNS mapping switch.

Possible modes are:

Enabled: Enable IP DNS mapping.

Disabled: Disable IP DNS mapping.

DNS Map

Delete

Delete the entry for mapping DNS domain names to IP addresses.

Map Index

Index of DNS map item.

Domain Name

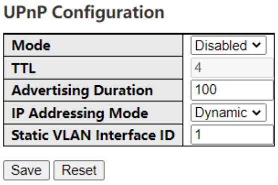
Domain name of DNS map item.

IPv4 Address

IPv4 address of DNS map item.

10.4. UPnP

[Advanced > UPnP]



UPnP Configuration

Mode	Disabled
TTL	4
Advertising Duration	100
IP Addressing Mode	Dynamic
Static VLAN Interface ID	1

UPnP Configuration

Configure UPnP on this page.

Mode

Indicates the UPnP operation mode. Possible modes are:

Enabled: Enable UPnP mode operation.

Disabled: Disable UPnP mode operation.

When the mode is enabled, two ACEs are added automatically to trap UPNP related packets to CPU. The ACEs are automatically removed when the mode is disabled.

TTL

The TTL value is used by UPnP to send SSDP advertisement messages. Read only now.

Advertising Duration

The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive an SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400. Specified in seconds.

IP Addressing Mode

IP addressing mode provides two ways to determine IP address assignment:

Dynamic: Default selection for UPnP. UPnP module helps users choosing the IP address of the switch device. It finds the first available system IP address.

Static: User specifies the IP interface VLAN for choosing the IP address of the switch device.

Static VLAN Interface ID

The index of the specific IP VLAN interface. It will only be applied when IP Addressing Mode is Static. Valid configurable values ranges from 1 to 4095. Default value is 1.

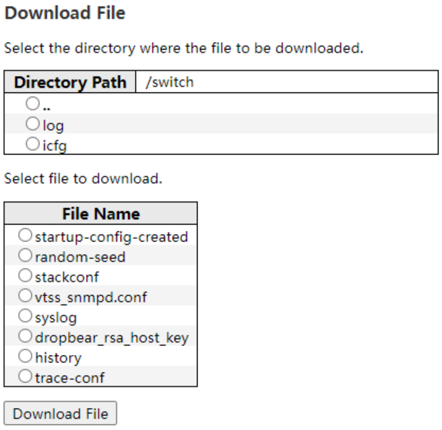
10.5. File Management

File management on the device: Upload, Download, Delete.

The files are stored in flash on the switch.

10.5.1. Download

[Advanced > File Management > Download]



Download File

Select the directory where the file to be downloaded.

Directory Path	/switch
○ ..	
○ log	
○ icfg	

Select file to download.

File Name
○ startup-config-created
○ random-seed
○ stackconf
○ vtss_snmpd.conf
○ syslog
○ dropbear_rsa_host_key
○ history
○ trace-conf

Download File

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

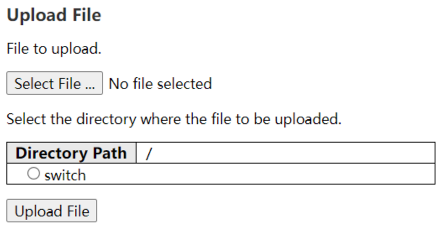
Select the directory where the file to be downloaded **Directory Path**, switch is path.

Select file to download **File Name**.

Then click Download File.

10.5.2. Upload

[Advanced > File Management > Upload]



Upload File

File to upload.

Select File ... No file selected

Select the directory where the file to be uploaded.

Directory Path	/
○ switch	

Upload File

It is possible to upload a file from the web browser to all the files on the switch.

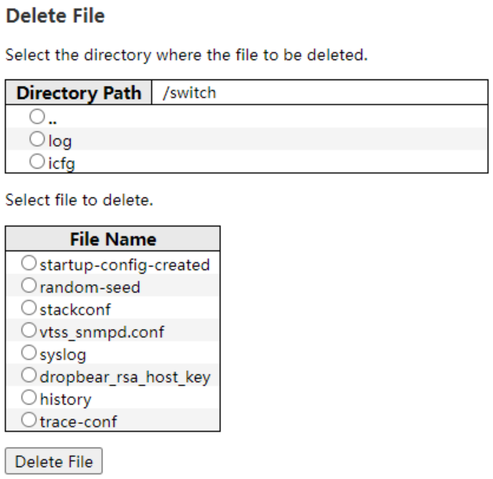
Select file to download **Select File**.

Select the directory where the file to be downloaded **Directory Path**, switch is path.

Then click Upload File.

10.5.3. Delete

[Advanced > File Management > Delete]



Delete File

Select the directory where the file to be deleted.

Directory Path	/switch
○ ..	
○ log	
○ icfg	

Select file to delete.

File Name
○ startup-config-created
○ random-seed
○ stackconf
○ vtss_snmpd.conf
○ syslog
○ dropbear_rsa_host_key
○ history
○ trace-conf

Delete File

It is possible to delete any of the writable files stored in flash on the switch.

Select the directory where the file to be downloaded **Directory Path**, switch is path.

Select file to delete **File Name**.

Then click Delete File.

11. Help

11.1. About

TNM4000-TA11T08G20GT Switch

Version CENTAURI V3.1

11.2. Technical support

Technical questions

For technical questions, please contact any dealer in your area or contact our company directly.
You can find the addresses of our partners on the Internet.
The company website provides a list of local telephone numbers and email addresses for technical support.
Also includes a free knowledge base and a software download section.

Technical Documents

The current manuals and operating instructions for the company's products are available on the Internet.

Customer Innovation Center

The Customer Innovation Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
  You find the training courses on technology and products currently available on the Internet.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Customer Innovation Center, you decide against any compromise in any case. Our client-customized package leaves you free to choose the service components you want to use.