

Anybus[®] Managed Layer 2 PoE Switch

USER MANUAL

SCM-1202-186

Version 1.0

Publication date 2021-12-07



Important User Information

Disclaimer

The information in this document is for informational purposes only. Please inform HMS Networks of any inaccuracies or omissions found in this document. HMS Networks disclaims any responsibility or liability for any errors that may appear in this document.

HMS Networks reserves the right to modify its products in line with its policy of continuous product development. The information in this document shall therefore not be construed as a commitment on the part of HMS Networks and is subject to change without notice. HMS Networks makes no commitment to update or keep current the information in this document.

The data, examples and illustrations found in this document are included for illustrative purposes and are only intended to help improve understanding of the functionality and handling of the product. In view of the wide range of possible applications of the product, and because of the many variables and requirements associated with any particular implementation, HMS Networks cannot assume responsibility or liability for actual use based on the data, examples or illustrations included in this document nor for any damages incurred during installation of the product. Those responsible for the use of the product must acquire sufficient knowledge in order to ensure that the product is used correctly in their specific application and that the application meets all performance and safety requirements including any applicable laws, regulations, codes and standards. Further, HMS Networks will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features or functional side effects found outside the documented scope of the product. The effects caused by any direct or indirect use of such aspects of the product are undefined and may include e.g. compatibility issues and stability issues.

Copyright © 2021 HMS Networks

Contact Information

Postal address:
Box 4126
300 04 Halmstad, Sweden

E-Mail: info@hms.se

Table of Contents

1. Safety	1
2. Overview	2
3. Preparation	3
3.1. Support and Resources	3
4. Installation	4
4.1. Hardware Layout	4
4.1.1. Hardware Dimensions	4
4.1.2. Front Side	5
4.1.3. Bottom Side	5
4.2. DIN Rail Mounting	6
4.3. Connecting Ground Screw	6
4.4. Connecting Digital Input Wires	7
4.5. Connecting Digital Output Wires	7
4.6. Connecting to Ethernet	7
4.7. Connecting to a Fiber Network	8
4.8. Connecting Power Wires	8
4.9. Diagnostic Console and Reset Button	8
4.10. PoE (Power over Ethernet)	9
4.10.1. PoE Power Input	9
4.10.2. PoE Power Output	9
4.10.3. PoE Basic Configuration	9
5. Configuration	11
5.1. Before You Begin Configuration	11
5.2. Accessing the Web Management Interface	11
5.2.1. Web Interface Overview	11
5.2.2. Saving the Configuration	11
5.2.3. Logging out from the Web Interface	12
5.3. System	12
5.4. Green Ethernet	15
5.5. Thermal Protection	16
5.6. Ports	17
5.7. Security	19
5.7.1. HTTPS	19
5.7.2. Networks	25
5.7.3. Network Access Server (NAS)	26
5.7.4. ACL	28
5.7.5. RADIUS Server Configuration	37
5.8. Aggregation	39
5.9. Loop Protection	43
5.10. Spanning Tree	44
5.11. IPMC	46
5.12. LLDP	47
5.13. PoE	49
5.14. MAC Table	50
5.15. VLAN	53
5.16. Private VLANs	55
5.17. QoS	56
5.18. Mirroring	58

6. Monitor	61
6.1. System	61
6.1.1. System Information	61
6.1.2. LED Status	61
6.1.3. CPU Load	62
6.1.4. IP Status	62
6.1.5. Routing Information Base	62
6.1.6. Log	63
6.1.7. Relay Output Status	64
6.2. Green Ethernet	64
6.3. Thermal Protection	65
6.4. Ports	65
6.4.1. State	65
6.4.2. Port Statistics Overview	65
6.4.3. QoS Statistics	66
6.4.4. QoS Control List (QCL)	66
6.4.5. Detailed Statistics	67
6.5. Security	68
6.5.1. Access Management Statistics	68
6.6. Aggregation	68
6.7. Loop Protection	69
6.8. Spanning Tree	69
6.8.1. STP Bridge Status	69
6.8.2. Port Status	70
6.8.3. Port Statistics	71
6.9. IPMC	71
6.9.1. IGMP Snooping Status	71
6.9.2. Group Information	72
6.10. LLDP	72
6.10.1. LLDP Neighbor Information	72
6.10.2. LLDP Neighbors EEE Information	73
6.10.3. Port Statistics	74
6.11. MAC Address	75
6.12. VLANs	76
6.12.1. Membership	76
6.12.2. Ports (VLANs)	76
6.13. PoE	77
6.13.1. LLDP Power Over Ethernet Neighbor	79
7. Diagnostics	81
7.1. Ping (IPv4)	81
7.2. Traceroute (IPv4)	83
8. Maintenance	85
8.1. Rebooting the Switch	85
8.2. Factory Default	85
8.3. Software	85
8.4. Configuration Files	85

1. Safety

Intended Use

The intended use of this equipment is as a communication interface and gateway. The equipment receives and transmits data on various physical levels and connection types.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

General Safety



CAUTION

This equipment emits RF energy in the ISM (Industrial, Scientific, Medical) band. Make sure that all medical devices used in proximity to this equipment meet appropriate susceptibility specifications for this type of RF energy.



CAUTION

This equipment contains parts that can be damaged by electrostatic discharge (ESD). Use ESD prevention measures to avoid damage.



CAUTION

Minimum temperature rating of the cable to be connected to the field wiring terminals, 90 °C.



CAUTION

Use copper wire only for field wiring terminals.



CAUTION

This equipment is recommended for use in both industrial and domestic environments. For industrial environments it is mandatory to use the functional earth connection to comply with immunity requirements. For domestic environments the functional earth must be used if a shielded Ethernet cable is used, in order to meet emission requirements.



CAUTION

Ensure that the power supply is turned off before connecting it to the equipment.



IMPORTANT

Using the wrong type of power supply can damage the equipment. Ensure that the power supply is connected properly and of the recommended type.

2. Overview

The Anybus Managed L2 PoE Switch is designed for industrial environments which requires high quality fiber communication, such as industrial automation or road traffic control.

Major Features

- 10-port Full Gigabit Ethernet, including 2 100/1000M SFP ports and 8 10/100/1000M RJ45 ports
- Advanced Management Features: Flow Control, Port Trunk/802.3ad LACP, VLAN, Private VLAN, Shared VLAN, Class of Service, Traffic Prioritize, Rate Control, Port Mirror, IGMP Snooping v2, Port classification, Port policing, Port scheduler, Port shaping, QoS control list, WRED, Port Security, ACL, Loop Protection
- Advanced Security System: IEEE 802.1X/RADIUS, Management IP, Management VLAN, SSL
- Redundancy Technology: Rapid Spanning Tree Protocol (RSTP)
- Excellent heat dissipation design for operating in -40 ~ +75° C environments
- IEC 61000-6-2/4 Heavy Industrial Environment

3. Preparation

3.1. Support and Resources

For additional documentation and software downloads, FAQs, troubleshooting guides and technical support, please visit www.anybus.com/support.

**NOTE**

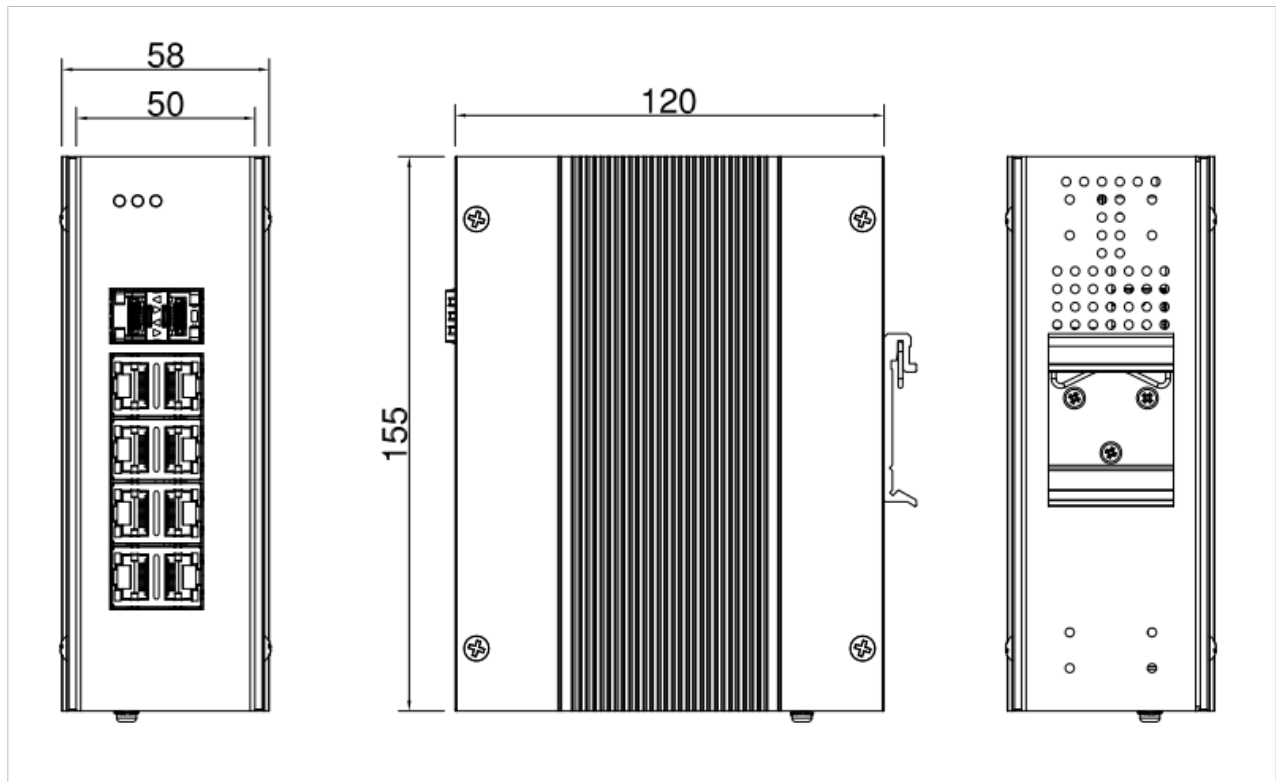
Have the product article number available, to search for the specific product page. You find the product article number on the product cover.

4. Installation

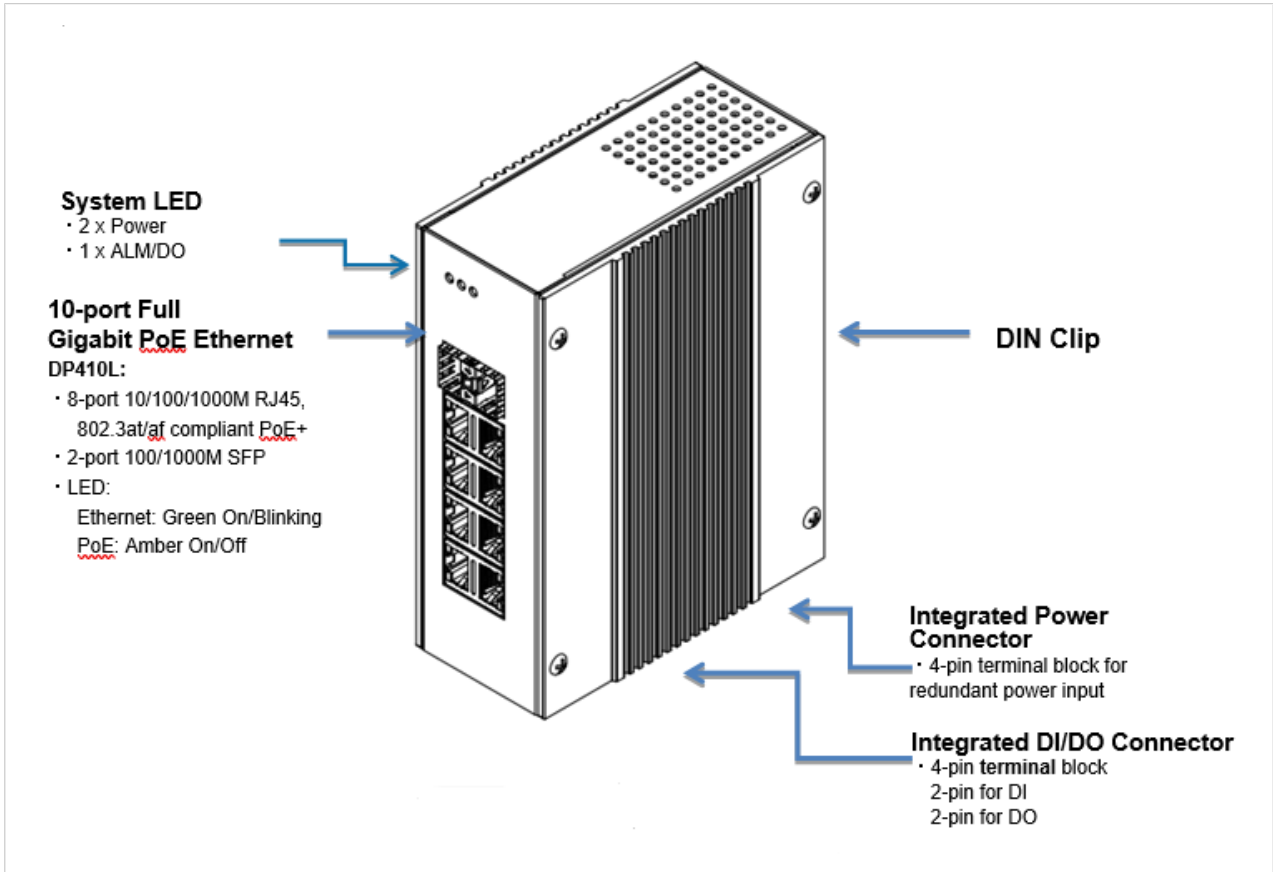
4.1. Hardware Layout

4.1.1. Hardware Dimensions

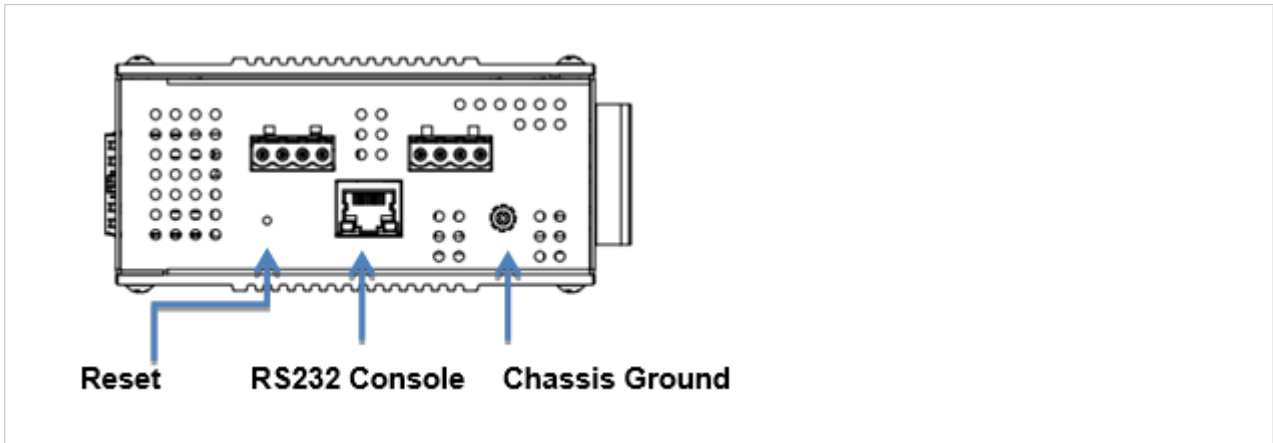
Dimensions: 50 x 155 x 120 (W x H x D) / without DIN Rail Clip



4.1.2. Front Side



4.1.3. Bottom Side

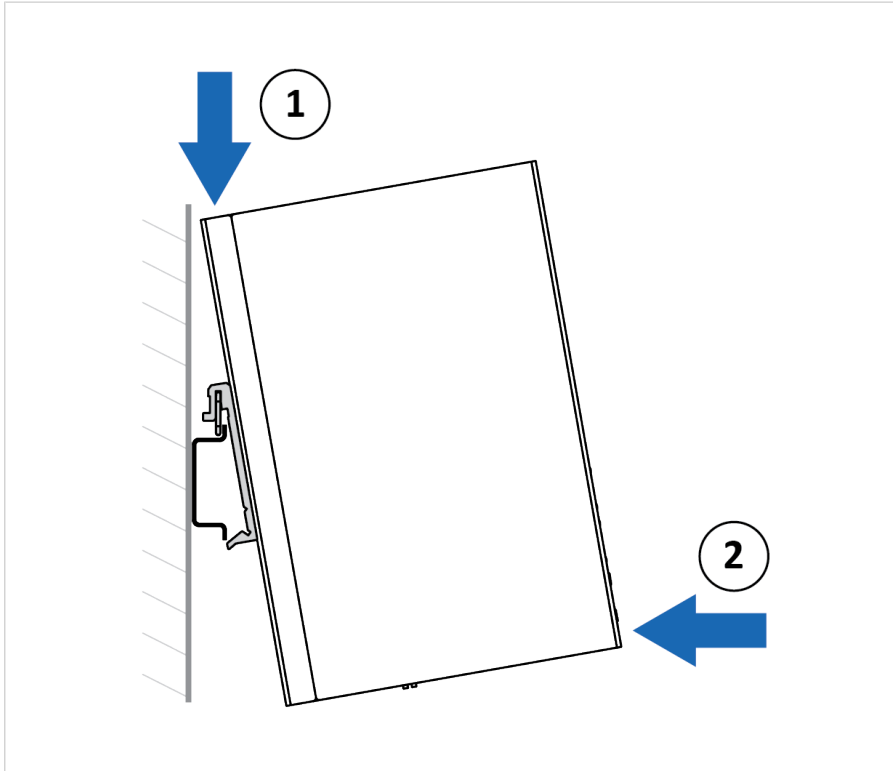


4.2. DIN Rail Mounting



NOTE

Mount the switch on a DIN rail in accordance with the EN 50022 standard.



Mount the switch on a DIN rail:

1. Insert the upper end of the DIN rail clip into the DIN rail.
2. Push the bottom of the DIN rail clip into the DIN rail.

4.3. Connecting Ground Screw



NOTE

To avoid system damage, the equipment should be connected to ground.

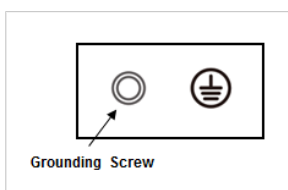


Figure 1. Grounding Screw

1. Establish a direct connection between the ground screw and the grounding surface prior to connecting devices.

4.4. Connecting Digital Input Wires

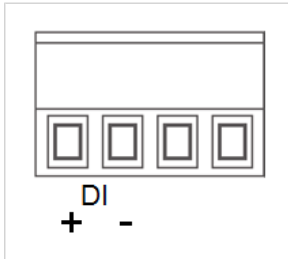
The Digital Input comes with photo-coupler isolation.



NOTE

The Digital High accepts 11 - 30 VDC.

The Digital Low accepts 0 - 10 VDC.



Connect the switch to Digital Input (DI):

1. Insert the wires into the 2-pin DI + and DI - contacts on the terminal block connector.
2. Tighten the wire-clamp screws.

4.5. Connecting Digital Output Wires

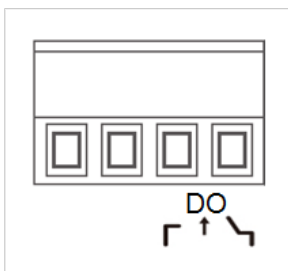
The relay output of the 2-pin terminal block connector are used to detect user-configured events.

When a user-configured event is triggered, the two wires attached to the fault contacts, form a close circuit. The fault circuit remains opened until a user-configured event occur.



NOTE

The relay contact supports 0.5 A current, DC 24 V. Do not exceed these voltage and current limits.



Connect the switch to Digital Output (DO):

1. Insert the wires into the 2-pin DO contact on the terminal block connector.
2. Tighten the wire-clamp screws.

4.6. Connecting to Ethernet

Connect the switch to a Ethernet network.

All eight available Ethernet ports are 802.3af/at PoE compliant. Each port can deliver up to 30 W, with a total PoE power budget of 120 W at 24 V input.

4.7. Connecting to a Fiber Network

Connect the switch to a fiber network via an SFP port.

The two available SFP ports are found above the eight Ethernet ports on the front of the product.

4.8. Connecting Power Wires



CAUTION

Ensure that the power supply is turned off before connecting it to the equipment.



IMPORTANT

Using the wrong type of power supply can damage the equipment. Ensure that the power supply is connected properly and of the recommended type.

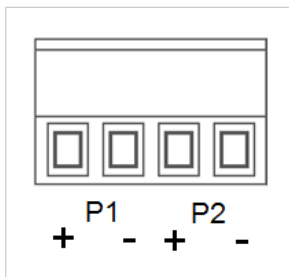


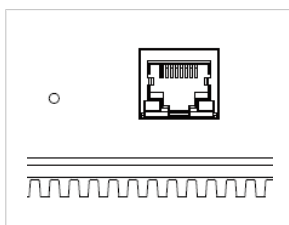
Figure 2. Power Connector

Connect the switch to power:

1. **Connecting to main power supply P1:** Insert the positive and negative wires into the P1+ and P1- contacts on the 4 pin terminal block.
2. **Connecting to redundant power supply P2:** Insert the positive and negative wires into the P2+ and P2- contacts on the 4 pin terminal block
3. Tighten the wire-clamp screws.
4. Connect the power wires to a DC switching type power supply.

4.9. Diagnostic Console and Reset Button

The switch provides a reset button and a diagnostic console connector.



For the RS232 Diagnostic Console, the default baud rate settings are 115,200, N, 8, 1.

The reset button makes it possible to reset the switch or reload factory defaults (> 7 sec).

4.10. PoE (Power over Ethernet)

The Managed L2 PoE switch comes equipped with eight 802.3af/at PoE ports. It accepts 24 V power input, and the available input voltage ranges from 12-57 V.

For the PoE ports, each port can deliver up to 30 W power with a total PoE power budget of 120 W at 24 V input.



NOTE

Considering the voltage lost when using long distance Ethernet cables, or the voltage used when using booster PoE, it is recommended to set PSU voltage input to 54 V.

4.10.1. PoE Power Input

With the Booster PoE design, the switch can support low voltage input and still deliver 54 VDC output to the power device (PD). The switch typically supports 24 VDC input (range of 10 - 57 VDC). The compliant power budget of the 10 - 18 V input is different from that of 19.2 - 57 V input, so ensure that the power budget is enough before installing. For better power efficiency, we recommend higher voltage input.

Table 1.

Power Input	10 - 18 VDC : 8.27 A	19.2 - 54 VDC : 7.31 A	55/56/57 VDC : 2.5 A
PoE Output	54 VDC : 60 W	54 VDC : 120 W	55/56/57 VDC : 120 W



NOTE

For 12 V battery systems, the system accepts 9.6 V input for a short period and lower power consumption. The 9.6 V is the lower design limit of the switch. It is not recommended to use 9.6 V for longer periods.

4.10.2. PoE Power Output

Every PoE device has a delivering PoE power restriction. The switch supports a maximum of 120 W at 24 V (19.2 - 57 V) input, and 60 W at 12 V (10 - 18 V) input. Make sure the power budget is enough for the power request of the PoE powered devices.

The PoE port budget is compliant with IEEE 802.3af/at standard. The maximum available current in 802.3af is 350 mA, and the maximum available current in 802.3at is 600 mA.



NOTE

If the system PoE consumption exceeds the system budget control, the PoE system will turn off low priority port PoE functions, until the consumption is smaller than the system budget. The port priority settings can be configured via the configuration interfaces.

4.10.3. PoE Basic Configuration

In the Web management interface, go to Configuration and select PoE to inspect and configure the PoE port settings.

See [PoE \(page 49\)](#) for more information.

Under normal circumstances, the 802.3af/at compliant Powered Device (PD) will be automatically detected. The only actions that are needed are to allocate enough Power Budget for the switch ports, and enable the PoE feature for all ports or specific ports.

The simplest scenario is to keep the default settings and enable PoE+ (802.3af/at) for all ports. The PoE+ stands for the 802.3at version, which is backward compatible with 802.3af PoE.

The following image shows the Power Over Ethernet Configuration screen. Select "PoE+" at the top of the column of the PoE mode, and then click the button "Submit".

Power Over Ethernet Configuration

Reserved Power determined by	<input checked="" type="radio"/> Class	<input type="radio"/> Allocation	<input type="radio"/> LLDP-MED
Power Management Mode	<input checked="" type="radio"/> Actual Consumption	<input type="radio"/> Reserved Power	
Capacitor Detection	<input checked="" type="radio"/> Disabled	<input type="radio"/> Enabled	

PoE Power Supply Configuration

Primary Power Supply [W]	120
---------------------------------	-----

PoE Port Configuration

Port	PoE Mode	Priority	Maximum Power [W]
*	PoE+ ▼	<> ▼	0
1	PoE+ ▼	Low ▼	0
2	PoE+ ▼	Low ▼	0
3	PoE+ ▼	Low ▼	0
4	PoE+ ▼	Low ▼	0
5	PoE+ ▼	Low ▼	0
6	PoE+ ▼	Low ▼	0
7	PoE+ ▼	Low ▼	0
8	PoE+ ▼	Low ▼	0

After clicking "Submit", the PoE+/PoE ports are enabled. They will detect available PDs and deliver power according to the settings.

5. Configuration

5.1. Before You Begin Configuration

The switch is configured through web management.

You can also configure the switch through console management, Telnet management or SSH management.



NOTE

The switch default IP address is `http://192.168.10.1/`.



NOTE

The default switch login user name and password is **admin**.

5.2. Accessing the Web Management Interface

Prepare for configuring the switch settings via the web management interface.

Before You Begin

- Connect the switch to your computer.
- Connect the switch to power.
- To link your computer with the switch, make sure that the IP address of the computer is located in the same subnet as the switch default IP address.

Access the web management interface:

1. In your browser, type `http://192.168.10.1` (or the IP address of the switch) and press Enter.
 - The web-based management interface login screen appears.
2. In the login screen, enter user name and password (default values are **admin**, **admin**).
3. Click OK.
 - The web-based management interface welcome page appears.

5.2.1. Web Interface Overview

5.2.2. Saving the Configuration



NOTE

Unsaved settings will be lost when the switch is powered off or restarted.

- To apply changes made on a configuration page/tab, click Submit at the bottom of the page.
- To cancel the changes, click Reset.
Some pages have additional buttons that are described in the respective sections in this manual.
- To save changed settings permanently, select Maintenance -> Configuration -> Save Startup-config -> Save Configuration.
The recent changes will otherwise be discarded if the switch is rebooted.

5.2.3. Logging out from the Web Interface

To manually logout from the system:

1. In the web interface top menu, click the Logout icon.
2. To confirm, click Yes.

5.3. System

This section shows basic information about the switch, to make it easier to identify on the network.

System Information Configuration

System Contact	<input type="text"/>
System Name	<input type="text"/>
System Location	<input type="text"/>
System Timezone Offset (minutes)	<input type="text" value="0"/>

Table 2. Information

Item	Description
System Contact	Contact person information for this managed node. The allowed string length is 0 to 255; allowed content is the ASCII characters from 32 to 126.
System Name	An admin assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
System Location	The physical location of this node. The allowed string length is 0 to 255; allowed content is the ASCII characters from 32 to 126.
System Timezone Offset (minutes)	Provide the timezone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -1439 to 1439 minutes.

IP Configuration

The IP Configuration page allows the user to configure the device IP Address and set it according to the interface and VLAN. The second section describes IP Routes, where the user can configure the routing.

IP Configuration

IP Interfaces

Delete	VLAN	Enable	DHCPv4				Hostname	Fallback	Current Lease	IPv4	
			Type	IfMac	ASCII	HEX				Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	Auto	Port 1				1		192.168.10.1	24

IP Routes

Delete	Network	Mask Length	Gateway	Distance(IPv4) / Next Hop VLAN(IPv6)
<input type="checkbox"/>	0.0.0.0	0	192.168.1.1	5

Basic IP settings, control IP interfaces and IP routes. The maximum number of interfaces supported is 8 and the maximum number of routes is 32.

Table 3. IP Interfaces

Item	Description
Delete	Select this option to delete an existing IP interface.
VLAN	The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface.
IPv4 DHCP Enabled	Enable the DHCPv4 client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol.
IPv4 DHCP Client Identifier Type	The type of DHCP client identifier. User can choose Auto, ifmac, ASCII, and HEX.
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 host name of the 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 uses 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 shows the current interface address, as provided by the DHCP server.
IPv4 Address	The IPv4 address of the interface in dotted decimal notation. If DHCP is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.
IPv4 Mask	The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for a IPv4 address. If DHCP is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fallback address is desired.

Table 4. IP Routes

Item	Description
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. A default route can use the value 0.0.0.0.
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. 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.
Distance (only for IPv4)	The distance value of route entry is used to provide the priority information of the routing protocols to routers. When there are two or more different routing protocols are involved and have the same destination, the distance value can be used to select the best path.
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.

LOG

Configure System Log on this page.

System Log Configuration

Server Mode	Disabled ▼
Server Address	<input type="text"/>
Syslog Level	Informational ▼

Table 5. System Log Configuration

Item	Description
Server Mode	Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are: Enabled: Enable server mode operation. Disabled: Disable server mode operation.
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(6).

RELAY OUTPUT

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

Relay Output Configuration

Port Link Failure									
1	2	3	4	5	6	7	8	9	10
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Table 6. Relay Output Configuration

Item	Description
Port Link Failure	A check box is provided for each port of a Port Link Failure. When checked, port link failure will trigger relay status to "on". When unchecked, port link failure will not trigger relay status to "on". By default, port link failure is disabled on all ports.

5.4. Green Ethernet

Green Ethernet, or Energy-Efficient Ethernet (EEE) is a power saving option that reduces power usage when there is low or no traffic utilization.

Port Power Savings Configuration

Optimize EEE for Latency ▾

Port Configuration

Port	ActiPHY	PerfectReach	EEE	EEE Urgent Queues									
				1	2	3	4	5	6	7	8		
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Table 7. EEE Optimization

Item	Description
Optimize EEE for	The switch can be set to optimize EEE for either best power saving or least traffic latency.

Table 8. Port Configuration

Item	Description
Port	The switch port number of the logical 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 a short moment in order to determine if a 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 is not started at once as transmit data is available for a port, but the data 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 latency for specific frames, by mapping the frames to a specific queue (done with QOS) and marking the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and latency will be reduced to the wakeup time.
EEE Urgent Queues	Queues set here 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.

5.5. Thermal Protection

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 ▼

This page allows the user to inspect and configure the current setting 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.

Temperature settings for groups

- The temperature at which the ports with the corresponding group will be turned off. Temperatures between 0 and 255 C are supported.

Port groups

- The group the port belongs to. Four groups are supported.

5.6. Ports

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

Port Configuration															Refresh	
Port	Link	Current	Speed Configured	Adv Duplex		Adv speed			Flow Control			PFC		Maximum Frame Size	Excessive Collision Mode	Frame Length Check
				Fdx	Hdx	10M	100M	1G	Enable	Curr Rx	Curr Tx	Enable	Priority			
*		<>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				0-7	10240	<>	<input type="checkbox"/>
1	Down	Auto		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
2	1Gfdx	Auto		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
3	Down	SFP_Auto_AMS		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
4	Down	SFP_Auto_AMS		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240	Discard	<input type="checkbox"/>
5	Down	Auto		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240		<input type="checkbox"/>
6	Down	Auto		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240		<input type="checkbox"/>
7	Down	Auto		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240		<input type="checkbox"/>
8	Down	Auto		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240		<input type="checkbox"/>
9	Down	Auto		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240		<input type="checkbox"/>
10	Down	Auto		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	0-7	10240		<input type="checkbox"/>

Submit Reset

Table 9. Port Configuration

Item	Description
Port	The logical port number.
Link	The current link state. Green indicates that the link is up and red that it is down.
Current Link Speed	The current link speed of the port.
Configured Link Speed	<p>Selects any available link speed for the given switch port. Only speeds supported by the specific port are shown.</p> <p>Possible choices are:</p> <ul style="list-style-type: none"> Disabled - Disables the switch port operation. Auto - Port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner. 10 Mbps HDX - Forces the cu port in 10 Mbps half-duplex mode. 10 Mbps FDX - Forces the cu port in 10 Mbps full duplex mode. 100 Mbps HDX - Forces the cu port in 100 Mbps half-duplex mode. 100 Mbps FDX - Forces the cu port in 100 Mbps full duplex mode. 1 Gbps FDX - Forces the port in 1 Gbps full duplex. SFP_Auto_AMS - Automatically determines the speed of the SFP. Note: There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFPs might not be detectable. The port is set in AMS mode. Cu port is set in Auto mode. 100-FX - SFP port in 100-FX speed. Cu port disabled. 1000-X - SFP port in 1000-X speed. Cu port disabled. Ports in AMS mode with 1000-X speed has Cu port preferred. Ports in AMS mode with 100-FX speed has Cu port preferred.
Advertise Duplex	When duplex is set to Auto, i.e auto negotiation, the port will only advertise the specified duplex as either Fdx or Hdx to the link partner. By default the port will advertise all the supported duplexes if the Duplex is Auto.
Advertise Speed	When Speed is set to 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 the port will advertise all the supported speeds if speed is set to Auto.
Flow Control	<p>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.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>NOTE</p> <p>The 100FX standard doesn't support Auto Negotiation, so when in 100FX mode the flow control capabilities will always be shown as "disabled".</p> </div>
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, a 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 Flow control 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.

Item	Description
Excessive Collision Mode	Configure port transmit collision behavior. Discard: Discard frame after 16 collisions (default). Restart: Restart back off algorithm after 16 collisions.
Frame Length Check	Configures if frames with incorrect frame length in the EtherType/Length field shall be dropped. An Ethernet frame contains a field EtherType which can be used to indicate the frame payload size (in bytes) for values of 1535 and below. If the EtherType/Length field is above 1535, it indicates that the field is used as an EtherType (indicating which protocol is encapsulated in the payload of the frame). If "frame length check" is enabled, frames with payload size less than 1536 bytes are dropped, if the EtherType/Length field doesn't match the actually payload length. If "frame length check" is disabled, frames are not dropped due to frame length mismatch. Note: No drop counters count frames dropped due to frame length mismatch.

5.7. Security

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

System Password

Old Password	<input style="width: 90%;" type="password" value="....."/>
New Password	<input style="width: 90%;" type="password"/>
Confirm New Password	<input style="width: 90%;" type="password"/>

Table 10. Switch Password

Item	Description
Old Password	Enter the current system password. If this is incorrect, the new password will not be set.
New Password	The system password. The allowed string length is 0 to 31, and the allowed content is the ASCII characters from 32 to 126.
Confirm New Password	The new password must be entered twice to catch typing errors.

Authentication Method Configuration

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

Authentication Method Configuration

Client	Methods	
console	local ▼	no ▼
http	local ▼	no ▼

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

Table 11. Authentication Method Configuration

Item	Description
Client	The management client for which the configuration below applies.
Methods	<p>Method can be set to one of the following values:</p> <ul style="list-style-type: none"> 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. <p>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.</p>

5.7.1. HTTPS

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

HTTPS Configuration Refresh

Mode	Disabled ▼
Automatic Redirect	Disabled ▼
Certificate Maintain	None ▼
Certificate Status	Switch secure HTTP certificate is presented

Table 12. HTTPS Configuration

Item	Description
Mode	Indicates the HTTPS mode operation. Possible modes are: <ul style="list-style-type: none"> Enabled: Enable HTTPS mode operation Disabled: Disable HTTPS mode operation
Automatic Redirect	Indicates 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 by browser. You need to initialize the HTTPS connection manually for this case. Possible modes are: <ul style="list-style-type: none"> Enabled: Enable HTTPS redirect mode operation Disabled: Disable HTTPS redirect mode operation
Certificate Maintain	The certificate maintenance section. Possible operations are: <ul style="list-style-type: none"> 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 Status	Display the current status of the switch certificate. Possible statuses are: <ul style="list-style-type: none"> Switch secure HTTP certificate is presented Switch secure HTTP certificate is not presented Switch secure HTTP certificate is generating....

5.7.1.1. Access Management Configuration

Configure the access management table on this page. 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.

Possible modes of the Access Management Configuration are:

- Enabled: Enable access management mode operation.
- Disabled: Disable access management mode operation.

Table 13. Access Management Table

Item	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the access management entry.
Start IP address	The start IP unicast address for the access management entry.
End IP address	The end IP unicast address for the access management entry.
HTTP/HTTPS	Indicates that the host can access the switch from HTTP/HTTPS interface if the host IP address matches the IP address range provided in the entry.
SNMP	Indicates that the host can access the switch from SNMP interface if the host IP address matches the IP address range provided in the entry.

5.7.1.2. SNMP System Configuration

Configure SNMP on this page.

SNMP System Configuration

Mode	Enabled ▾
Engine ID	8000b80a030200c14b3ab4

Table 14. SNMP System Configuration

Item	Description
Mode	Indicates the SNMP mode operation. Possible modes are: <ul style="list-style-type: none"> • <i>Enabled</i>: Enable SNMP mode operation. • <i>Disabled</i>: 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.

5.7.1.3. SNMP Trap Configuration

Configure SNMP traps on this page.

Trap Configuration

Trap Destination Configurations

Delete	Name	Enable	Version	Destination Address	Destination Port
<input type="button" value="Add New Entry"/>					
<input type="button" value="Submit"/> <input type="button" value="Reset"/>					

Table 15. SNMP Trap Destination Configurations

Item	Description
Name	Indicates the trap destination's name.
Enable	Indicates the trap destination mode operation. Possible modes are: <ul style="list-style-type: none"> • <i>Enabled</i>: Enable SNMP trap mode operation. • <i>Disabled</i>: Disable SNMP trap mode operation.
Version	Indicates the SNMP trap supported version. Possible versions are: <ul style="list-style-type: none"> • <i>SNMPv1</i>: Set SNMP trap supported version 1. • <i>SNMPv2c</i>: Set SNMP trap supported version 2c. • <i>SNMPv3</i>: 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').
Destination Port	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.

5.7.1.4. SNMP Trap Source Configurations

This page provides SNMP trap source configurations. A trap is sent for the given trap source if at least one filter with filter type included matches the filter, and no filters with filter type excluded matches.

Table 16. SNMP Trap Source Configuration

Item	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Name	Indicates the name for the entry.

Item	Description
Type	The filter type for the entry. Possible types are: <ul style="list-style-type: none"> <i>included</i>: An optional flag to indicate a trap is sent for the given trap source is matched. <i>excluded</i>: 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 kind of the trap name. For example, ifIndex is the subset OID of linkUp and linkDown. A valid subset OID is one or more digital numbers (0-4294967295) or asterisk (*), which are separated by dots (.). The first character must not begin with asterisk (*) and the maximum of OID count must not exceed 128.

5.7.1.5. SNMPv3 Community Configuration

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

SNMPv3 Community Configuration

Delete	Community name	Community secret	Source IP	Source Prefix
<input type="checkbox"/>	public	public	0.0.0.0	0
<input type="checkbox"/>	private	private	0.0.0.0	0

Table 17. SNMPv3 Community Configuration

Item	Description
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.

5.7.1.6. SNMPv3 User Configuration

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

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	8000b80a030200c14b3ab4	WoMaster	Auth, Priv	MD5	DES

Table 18. SNMPv3 User Configuration

Item	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with the 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: <ul style="list-style-type: none"> <i>NoAuth, NoPriv</i>: No authentication and no privacy.

Item	Description
	<ul style="list-style-type: none"> • <i>Auth, NoPriv</i>: Authentication and no privacy. • <i>Auth, Priv</i>: Authentication and privacy. <p>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.</p>
Authentication Protocol	<p>Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:</p> <ul style="list-style-type: none"> • <i>None</i>: No authentication protocol. • <i>MD5</i>: An optional flag to indicate that this user uses MD5 authentication protocol. • <i>SHA</i>: An optional flag to indicate that this user uses SHA authentication protocol. <p>The security level value cannot be modified if the entry already exists. Ensure that the value is set correctly.</p>
Authentication Password	<p>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.</p>
Privacy Protocol	<p>Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:</p> <ul style="list-style-type: none"> • <i>None</i>: No privacy protocol. • <i>DES</i>: An optional flag to indicate that this user uses DES authentication protocol. • <i>AES</i>: An optional flag to indicate that this user uses AES authentication protocol.
Privacy Password	<p>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.</p>

5.7.1.7. SNMPv3 Group Configuration

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

SNMPv3 Group Configuration

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

Table 19. SNMPv3 Group Configuration

Item	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Security Model	<p>Indicates the security model that this entry should belong to. Possible security models are:</p> <ul style="list-style-type: none"> • <i>v1</i>: Reserved for SNMPv1. • <i>v2c</i>: Reserved for SNMPv2c. • <i>usm</i>: 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.

5.7.1.8. SNMPv3 View Configuration

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

SNMPv3 View Configuration

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

Table 20. SNMPv3 View Configuration

Item	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
View Type	Indicates the view type that this entry should belong to. Possible view types are: <ul style="list-style-type: none"> <i>included</i>: An optional flag to indicate that this view subtree should be included. <i>excluded</i>: 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 (*).

5.7.1.9. SNMPv3 Access Configuration

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

SNMPv3 Access Configuration

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

Table 21. SNMPv3 Access Configuration

Item	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: <ul style="list-style-type: none"> <i>any</i>: Any security model accepted (v1 v2c usm). <i>v1</i>: Reserved for SNMPv1. <i>v2c</i>: Reserved for SNMPv2c. <i>usm</i>: User-based Security Model (USM).
Security Level	Indicates the security model that this entry should belong to. Possible security models are: <ul style="list-style-type: none"> <i>NoAuth, NoPriv</i>: No authentication and no privacy. <i>Auth, NoPriv</i>: Authentication and no privacy. <i>Auth, Priv</i>: 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.

5.7.2. Networks

5.7.2.1. Port Security

This page allows you to configure the Port Security global and per-port settings. 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 four different described below.

Port Security Configuration

Global Configuration

Aging Enabled	<input type="checkbox"/>
Aging Period	<input type="text" value="3600"/> seconds
Hold Time	<input type="text" value="300"/> seconds

Port Configuration

Port	Mode	Limit	Violation Mode	Violation Limit	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

The Port Security configuration consists of two sections, a global and a per-port.

Table 22. Global Configuration

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

Table 23. Port Configuration

Item	Description
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. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

Item	Description
Violation Mode	<p>If Limit is reached, the switch can take one of the following actions:</p> <ul style="list-style-type: none"> • <i>Protect</i>: Do not allow more than Limit MAC addresses on the port, but take no further action. • <i>Restrict</i>: 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. • <i>Shutdown</i>: 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 reopen the port: <ol style="list-style-type: none"> 1. In the "Configuration->Ports" page's "Configured" column, first disable the port, then restore the original mode. 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 <i>Restrict</i> .
State	<p>This column shows the current Port Security state of the port. The state takes one of four values:</p> <ul style="list-style-type: none"> • <i>Disabled</i>: Port Security is disabled on the port. • <i>Ready</i>: The limit is not yet reached. This can be shown for all violation modes. • <i>Limit Reached</i>: Indicates that the limit is reached on this port. This can be shown for all violation modes. • <i>Shutdown</i>: Indicates that the port is shut down by Port Security. This state can only be shown if violation mode is set to <i>Shutdown</i>.

5.7.3. Network Access Server (NAS)

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings. The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Configuration→Security→AAA" page.

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

Network Access Server Configuration

System Configuration

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

Port Configuration


Port	Admin State	Port State	Restart	
1	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize
9	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize
10	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize

Table 24. System Configuration

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

Item	Description
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 MAC-Based Auth, i.e. modes using the Port Security functionality to secure MAC addresses. 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. 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 MAC-Based Auth, i.e. modes using the Port Security functionality to secure MAC addresses. If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. 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.

Table 25. Port Configuration

Item	Description
Port	The port number for which the configuration below applies.
Admin State	<p>If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:</p> <ul style="list-style-type: none"> <i>Force Authorized:</i> 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. <i>Force Unauthorized:</i> 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. <i>802.1X:</i> 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 switches are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and 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. <div style="border: 1px solid gray; padding: 10px; margin-top: 10px;"> <p> NOTE Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.</p> </div>

Item	Description
	<ul style="list-style-type: none"> MAC-based Auth.: Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using 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 port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.
Port State	<p>The current state of the port. It can take one of the following values:</p> <ul style="list-style-type: none"> 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	<p>Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect.</p> <ul style="list-style-type: none"> 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.



5.7.4. ACL

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

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	5595
3	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	2189
5	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
7	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0

Table 26. ACL Ports Configuration

Item	Description
Port	The logical port for the settings contained in the same row.
Policy ID	Select the policy to apply to this port. The allowed values are 0 through 63. The default value is 0.
Action	Select whether forwarding is permitted (<i>Permit</i>) or denied (<i>Deny</i>). The default value is "Permit".

Item	Description
Rate Limiter ID	Select which rate limiter to apply on this port. The allowed values are <i>Disabled</i> or the values 1 through 16. The default value is "Disabled".
Port Redirect	Select which port frames are redirected on. The allowed values are <i>Disabled</i> 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: <ul style="list-style-type: none"> • <i>Enabled</i>: Frames received on the port are mirrored. • <i>Disabled</i>: Frames received on the port are not mirrored. <p>The default value is "Disabled".</p>
Logging	Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC. The allowed values are: <ul style="list-style-type: none"> • <i>Enabled</i>: Frames received on the port are stored in the System Log. • <i>Disabled</i>: Frames received on the port are not logged. <p>The default value is "Disabled".</p> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;">  <p>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.</p> </div>
Shutdown	Specify the port shut down operation of this port. The allowed values are: <ul style="list-style-type: none"> • <i>Enabled</i>: If a frame is received on the port, the port will be disabled. • <i>Disabled</i>: Port shut down is disabled. <p>The default value is "Disabled".</p> <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;">  <p>NOTE The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).</p> </div>
State	Specify the port state of this port. The allowed values are: <ul style="list-style-type: none"> • <i>Enabled</i>: To reopen ports by changing the volatile port configuration of the ACL user module. • <i>Disabled</i>: To close ports by changing the volatile port configuration of the ACL user module. <p>The default value is "Enabled".</p>
Counter	Counts the number of frames that match this ACE.

Rate Limiter

Configure the rate limiter for the ACL of the switch.

ACL Rate Limiter Configuration

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

Submit Reset

Table 27. ACL Rate Limiter Configuration

Item	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row and its range is 1 to 16.
Rate	The valid rate is 0 - 99, 100, 200, 300, ...,1092000 in pps or 0, 100, 200, 300, ..., 1000000 in kbps.
Unit	Specify the rate unit. The allowed values are: <ul style="list-style-type: none"> • <i>pps</i>: packets per second. • <i>kbps</i>: Kbits per second.

5.7.4.1. 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 128 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.

Access Control List Configuration

Auto-refresh Refresh Clear Remove All

ACE	Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter
1	9	Any	Any	Permit	Disabled	Disabled	Disabled	0

Table 28. Access Control List Configuration

Item	Description
ACE	Indicates the ACE ID.
Ingress Port	Indicates the ingress port of the ACE. Possible values are: <ul style="list-style-type: none"> • <i>All</i>: The ACE will match all ingress ports. • <i>Port</i>: The ACE will match a specific ingress port.
Policy/Bitmask	Indicates the policy number and bitmask of the ACE.
Frame Type	Indicates the frame type of the ACE. Possible values are: <ul style="list-style-type: none"> • <i>Any</i>: The ACE will match any frame type. • <i>EType</i>: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. • <i>ARP</i>: The ACE will match ARP/RARP frames. • <i>IPv4</i>: The ACE will match all IPv4 frames.

Item	Description
	<ul style="list-style-type: none"> • <i>IPv4/ICMP</i>: The ACE will match IPv4 frames with ICMP protocol. • <i>IPv4/UDP</i>: The ACE will match IPv4 frames with UDP protocol. • <i>IPv4/TCP</i>: The ACE will match IPv4 frames with TCP protocol. • <i>IPv4/Other</i>: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. • <i>IPv6</i>: The ACE will match all IPv6 standard frames.
Action	Indicates the forwarding action of the ACE. <ul style="list-style-type: none"> • <i>Permit</i>: Frames matching the ACE may be forwarded and learned. • <i>Deny</i>: Frames matching the ACE are dropped. • <i>Filter</i>: 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 <i>Disabled</i> 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: <ul style="list-style-type: none"> • <i>Enabled</i>: Frames received on the port are mirrored. • <i>Disabled</i>: Frames received on the port are not mirrored. The default value is "Disabled".
Counter	The counter indicates the number of times the ACE was hit by a frame.
Modification Buttons	You can modify each ACE (Access Control Entry) in the table using the buttons on the right.

ACE Configuration

Configure an ACE (Access Control Entry) on this page. An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected. A frame that hits this ACE matches the configuration that is defined here.

ACE Configuration

Second Lookup	Disabled ▾	Action	Permit ▾
Ingress Port	All Port 1 Port 2 Port 3 Port 4	Rate Limiter	Disabled ▾
Policy Filter	Any ▾	Mirror	Disabled ▾
Frame Type	Any ▾	Logging	Disabled ▾
		Shutdown	Disabled ▾
		Counter	0

VLAN Parameters

802.1Q Tagged	Any ▾
VLAN ID Filter	Any ▾
Tag Priority	0 ▾

Table 29. ACE (Access Control Entry) Configuration

Item	Description
Ingress Port	Select the ingress port for which this ACE applies. <ul style="list-style-type: none"> • <i>All</i>: The ACE applies to all ports.



Item	Description
	<ul style="list-style-type: none"> • <i>Port n</i>: The ACE applies to this port number, where n is the number of the switch port.
Policy Filter	<p>Specify the policy number filter for this ACE.</p> <ul style="list-style-type: none"> • <i>Any</i>: No policy filter is specified. (policy filter status is "don't-care".) • <i>Specific</i>: 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 63.
Policy Bitmask	When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0x3f. 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	<p>Select the frame type for this ACE. These frame types are mutually exclusive.</p> <ul style="list-style-type: none"> • <i>Any</i>: Any frame can match this ACE. • <i>Ethernet Type</i>: 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). • <i>ARP</i>: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with Ethernet type. • <i>IPv4</i>: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with Ethernet type. • <i>IPv6</i>: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.
Action	<p>Specify the action to take with a frame that hits this ACE.</p> <ul style="list-style-type: none"> • <i>Permit</i>: The frame that hits this ACE is granted permission for the ACE operation. • <i>Deny</i>: The frame that hits this ACE is dropped. • <i>Filter</i>: Frames matching the ACE are filtered.
Rate Limiter	Specify the rate limiter in number of base units. The allowed range is 1 to 16. <i>Disabled</i> indicates that the rate limiter operation is disabled.
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. <i>Disabled</i> 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	<p>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:</p> <ul style="list-style-type: none"> • <i>Enabled</i>: Frames received on the port are mirrored. • <i>Disabled</i>: Frames received on the port are not mirrored. <p>The default value is "Disabled".</p>
Logging	<p>Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information. The allowed values are:</p> <ul style="list-style-type: none"> • <i>Enabled</i>: Frames matching the ACE are stored in the System Log. • <i>Disabled</i>: Frames matching the ACE are not logged. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  <p>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.</p> </div>
Shutdown	<p>Specify the port shutdown operation of the ACE. The allowed values are:</p> <ul style="list-style-type: none"> • <i>Enabled</i>: If a frame matches the ACE, the ingress port will be disabled. • <i>Disabled</i>: Port shut down is disabled for the ACE. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  <p>NOTE The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).</p> </div>
Counter	The counter indicates the number of times the ACE was hit by a frame.

Table 30. MAC Parameters

Item	Description
SMAC Filter	<p>(Only displayed when the frame type is Ethernet Type or ARP.) Specify the source MAC filter for this ACE.</p> <ul style="list-style-type: none"> • <i>Any</i>: No SMAC filter is specified. (SMAC filter status is "don't-care".)

Item	Description
	<ul style="list-style-type: none"> • <i>Specific</i>: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering a 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 "xxxxxxxxxx" (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. <ul style="list-style-type: none"> • <i>Any</i>: No DMAC filter is specified. (DMAC filter status is "don't-care".) • <i>MC</i>: Frame must be multicast. • <i>BC</i>: Frame must be broadcast. • <i>UC</i>: Frame must be unicast. • <i>Specific</i>: 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 "xxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.

Table 31. VLAN Parameters

Item	Description
802.1Q Tagged	Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are: <ul style="list-style-type: none"> • <i>Any</i>: Any value is allowed ("don't-care"). • <i>Enabled</i>: Tagged frame only. • <i>Disabled</i>: Untagged frame only. • The default value is "Any".
VLAN ID Filter	Specify the VLAN ID filter for this ACE. <ul style="list-style-type: none"> • <i>Any</i>: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".) • <i>Specific</i>: 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".)

Table 32. ARP Parameters

Item	Description
ARP/RARP	Specify the available ARP/RARP opcode (OP) flag for this ACE. <ul style="list-style-type: none"> • <i>Any</i>: No ARP/RARP OP flag is specified. (OP is "don't-care".) • <i>ARP</i>: Frame must have ARP opcode set to ARP. • <i>RARP</i>: Frame must have RARP opcode set to RARP. • <i>Other</i>: Frame has unknown ARP/RARP Opcode flag.
Request/Reply	Specify the available Request/Reply opcode (OP) flag for this ACE. <ul style="list-style-type: none"> • <i>Any</i>: No Request/Reply OP flag is specified. (OP is "don't-care".) • <i>Request</i>: Frame must have ARP Request or RARP Request OP flag set. • <i>Reply</i>: Frame must have ARP Reply or RARP Reply OP flag.
Sender IP Filter	Specify the sender IP filter for this ACE. <ul style="list-style-type: none"> • <i>Any</i>: No sender IP filter is specified. (Sender IP filter is "don't-care".) • <i>Host</i>: Sender IP filter is set to Host. Specify the sender IP address in the Sender IP Address field that appears. • <i>Network</i>: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the Sender IP Address and Sender IP 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. <ul style="list-style-type: none"> • <i>Any</i>: No target IP filter is specified. (Target IP filter is "don't-care".) • <i>Host</i>: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears.

Item	Description
	<ul style="list-style-type: none"> • <i>Network</i>: 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.
ARP Sender MAC Match	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. <ul style="list-style-type: none"> • <i>0</i>: ARP frames where SHA is not equal to the SMAC address. • <i>1</i>: ARP frames where SHA is equal to the SMAC address. • <i>Any</i>: Any value is allowed ("don't-care").
RARP Target MAC Match	Specify whether frames can hit the action according to their target hardware address field (THA) settings. <ul style="list-style-type: none"> • <i>0</i>: RARP frames where THA is not equal to the target MAC address. • <i>1</i>: RARP frames where THA is equal to the target MAC address. • <i>Any</i>: 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. <ul style="list-style-type: none"> • <i>0</i>: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04). • <i>1</i>: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04). • <i>Any</i>: 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. <ul style="list-style-type: none"> • <i>0</i>: ARP/RARP frames where the HLD is not equal to Ethernet (1). • <i>1</i>: ARP/RARP frames where the HLD is equal to Ethernet (1). • <i>Any</i>: 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. <ul style="list-style-type: none"> • <i>0</i>: ARP/RARP frames where the PRO is not equal to IP (0x800). • <i>1</i>: ARP/RARP frames where the PRO is equal to IP (0x800). • <i>Any</i>: Any value is allowed ("don't-care").

Table 33. IP Parameters

Item	Description
IP Protocol Filter	Specify the IP protocol filter for this ACE. <ul style="list-style-type: none"> • <i>Any</i>: No IP protocol filter is specified ("don't-care"). • <i>Specific</i>: 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. • <i>ICMP</i>: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file. • <i>UDP</i>: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file. • <i>TCP</i>: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.
IP Protocol Value	When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value.
IP TTL	Specify the Time-to-Live settings for this ACE. <ul style="list-style-type: none"> • <i>zero</i>: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry. • <i>non-zero</i>: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry. • <i>Any</i>: 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. <ul style="list-style-type: none"> • <i>No</i>: 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. • <i>Yes</i>: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry. • <i>Any</i>: Any value is allowed ("don't-care").
IP Option	Specify the options flag setting for this ACE. <ul style="list-style-type: none"> • <i>No</i>: IPv4 frames where the options flag is set must not be able to match this entry. • <i>Yes</i>: IPv4 frames where the options flag is set must be able to match this entry. • <i>Any</i>: Any value is allowed ("don't-care").

Item	Description
SIP Filter	Specify the source IP filter for this ACE. <ul style="list-style-type: none"> <i>Any</i>: No source IP filter is specified. (Source IP filter is "don't-care".) <i>Host</i>: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears. <i>Network</i>: 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. <ul style="list-style-type: none"> <i>Any</i>: No destination IP filter is specified. (Destination IP filter is "don't-care".) <i>Host</i>: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears. <i>Network</i>: 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.

Table 34. IPv6 Parameters

Item	Description
Next Header Filter	Specify the IPv6 next header filter for this ACE. <ul style="list-style-type: none"> <i>Any</i>: No IPv6 next header filter is specified ("don't-care"). <i>Specific</i>: 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. <i>ICMP</i>: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file. <i>UDP</i>: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file. <i>TCP</i>: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.
Next Header Value	When "Specific" is selected for the IPv6 next header value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IPv6 protocol value.
SIP Filter	Specify the source IPv6 filter for this ACE. <ul style="list-style-type: none"> <i>Any</i>: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".) <i>Specific</i>: 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	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	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 0xFFFFF0 (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. <ul style="list-style-type: none"> <i>zero</i>: IPv6 frames with a hop limit field greater than zero must not be able to match this entry. <i>non-zero</i>: IPv6 frames with a hop limit field greater than zero must be able to match this entry. <i>Any</i>: Any value is allowed ("don't-care").

Table 35. ICMP Parameters

Item	Description
ICMP Type Filter	Specify the ICMP filter for this ACE. <ul style="list-style-type: none"> <i>Any</i>: No ICMP filter is specified (ICMP filter status is "don't-care"). <i>Specific</i>: 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.

Item	Description
ICMP Code Filter	Specify the ICMP codefilter for this ACE. <ul style="list-style-type: none"> • <i>Any</i>: No ICMP code filter is specified (ICMP code filter status is "don't-care"). • <i>Specific</i>: 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.

Table 36. TCP/UDP Parameters

Item	Description
TCP/UDP Source Filter	Specify the TCP/UDP source filter for this ACE. <ul style="list-style-type: none"> • <i>Any</i>: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care"). • <i>Specific</i>: 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. • <i>Range</i>: 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.
TCP/UDP Source 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.
TCP/UDP Source 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. A frame that hits this ACE matches this TCP/UDP source value.
TCP/UDP Destination Filter	Specify the TCP/UDP destination filter for this ACE. <ul style="list-style-type: none"> • <i>Any</i>: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care"). • <i>Specific</i>: 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. • <i>Range</i>: 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.
TCP/UDP Destination Number	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.
TCP/UDP Destination 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. A frame that hits this ACE matches this TCP/UDP destination value.
TCP FIN	Specify the TCP "No more data from sender" (FIN) value for this ACE. <ul style="list-style-type: none"> • 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. • <i>Any</i>: Any value is allowed ("don't-care").
TCP SYN	Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. <ul style="list-style-type: none"> • 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. • <i>Any</i>: Any value is allowed ("don't-care").
TCP RST	Specify the TCP "Reset the connection" (RST) value for this ACE. <ul style="list-style-type: none"> • 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. • <i>Any</i>: Any value is allowed ("don't-care").
TCP PSH	Specify the TCP "Push Function" (PSH) value for this ACE. <ul style="list-style-type: none"> • 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. • <i>Any</i>: Any value is allowed ("don't-care").
TCP ACK	Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE. <ul style="list-style-type: none"> • 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. • <i>Any</i>: Any value is allowed ("don't-care").
TCP URG	Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE. <ul style="list-style-type: none"> • 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. • <i>Any</i>: Any value is allowed ("don't-care").

Table 37. Ethernet Type Parameters

Item	Description
EtherType Filter	Specify the Ethernet type filter for this ACE. <ul style="list-style-type: none"> 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.

5.7.5. RADIUS Server 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	Yes ▼	
Key	<input type="text"/>	
NAS-IP-Address	<input type="text"/>	
NAS-Identifier	<input type="text"/>	

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Change Secret Key
<input type="checkbox"/>	192.168.10.100	1812	1813	30	30	<input type="checkbox"/>

Table 38. Global Configuration

Item	Description
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.
Retransmit	Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered 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, you can change the secret key - up to 63 characters long - shared between the RADIUS server and the switch.
NAS-IP-Address (Attribute 4)	The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
NAS-Identifier (Attribute 32)	The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Table 39. Server Configuration

Item	Description
Delete	To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.
Hostname	The IPv4/IPv6 address of the RADIUS server.
Auth Port	The UDP port to use on the RADIUS server for authentication. Set to 0 to disable authentication.

Item	Description
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 selected, you can change the setting and it will override the global key. Leaving it blank will use the global key.

5.8. Aggregation

This section provides examples on how to configure Link Aggregation Control Protocol (LACP)/AGGR using the Command Line Interface (CLI). The commands apply to an enhanced version of the LACP.

LACP Enhancement Features

The following sections describe various LACP enhancement features.

Aggregation Groups

To create an aggregation, a group type must be chosen on the interfaces that are participating in the group. This can be LACP active, LACP passive, or statically created aggregation “On”. No looping occurs even though the parallel links have links and have not formed an aggregation. Spanning tree is not needed for this but can be enabled to avoid loops between groups. LACP active initiates the LACP frames to partner. LACP passive does not initiate the LACP frames to partner, but answers if requested. “On” is a statically created aggregation without LACP.

Bundle Max

If there any exist suitable link partner, each LACP group automatically forms an aggregation for all of its members. The number of members can be restricted by setting the max bundle value to a number less than the number of group members. When the numbers of members who have formed aggregation reach the specified value, the remaining ports are set to standby and do not forward any frames. If an active member goes down, then a standby member will take over. The priority assignment controls to which member goes active/standby.

Revertive/Non-Revertive

The LACP group can be configured to be revertive (default) or non-revertive. When a higher priority port which is in active/standby comes back up, it becomes active again and the current active port (if it has lower priority) goes into standby, unless the group is configured to be non-revertive. In non-revertive mode, if a port comes back up, nothing changes and the traffic is not disturbed.



NOTE

Each time a link changes, the traffic is halted until the new aggregation (key) is fully set up.

1:1 Active (Standby) LACP

To achieve 1:1 active/standby configuration, create a group with two ports and configure one of the ports as bundle max. One of the ports, with higher priority, actively forwards traffic while the other remains in standby mode. The port, in standby mode, does not forward any frames other than BPDUs. The LACP state of the standby port is in no sync state. If the active port goes down, the standby port takes over. When the failed port becomes operational, it takes over the frame forwarding (unless configured not to - non-revertive) operation.

LACP State Information

The states of the LACP protocol (partner and actor) are visible through show lacp neighbor detail and show lacp internal detail commands.

CLI

The CLI syntax (for configuration and status) follows the Cisco IOS port-channel style. At Anybus, port-channel is called aggregation.

ICLI Commands

The following sections describe the implementation of the previously discussed LACP features through ICLI commands.

Creating an Aggregation Group

The following snippet shows how to create an active LACP group with ports Gig 1/1-2 as members.

```
# conf t
(config)#
interface GigabitEthernet 1/1-2
(config-if)#
  aggregation group 1 mode ?
  active      Active LACP
  on          Static aggregation
  passive     Passive LACP
<cr>
(config-if)# aggregation group 1 mode active

Active can be replaced with passive and on.
```

Showing the Status of an Aggregation Group

The following snippet shows the status of the active LACP group, created in the previous chapter.

```
# show aggregation
Aggr ID   Name      Type           Speed      Configured   Aggregated
-----   ----     -
1         LLAG1    LACP_ACTIVE    Undefined  Gi 1/1-2    none
Show the internal configuration and status.

# show lacp internal
Port      State     Key           Priority
-----   ----     -
Gi 1/1    Down     1             32768
Gi 1/2    Down     1             32768
```

Where...

- *Port*: is the local port.
- *State*: indicates if a partner is seen and an aggregation created.
- *Key*: is used as a term in the 802.1D standard. Here it equals the group id.
- *Priority*: is used for active/standby purpose.

Showing the Detailed Status of an Aggregation Group

The following snippet shows the detailed status of the aggregation group.

```
# show lacp neighbor details
Port          : The local port
State         : The active/inactive state of this port
Aggr ID       : The group id of this aggregation
Partner Key   : The aggr key of the partner
Partner Port  : The port of the partner
Partner Port Prio : The partner port priority
[Activ Timeou Aggrege Synchro Collect Distrib Defau Expired]:
Booleans. The LACP protocol state seen from the link partner.

# show lacp internal details
Port          : The local port
State         : The active/inactive state of this port
Key           : The key of this port, same as group id.
```

```
Priority           : The LACP priority of this port
[Activ Timeou Aggrege Synchro Collect Distrib Defau Expired]:
Booleans. The LACP protocol state seen from the actor (the local unit).
```

Statistics

The following snippet shows the statistics of the aggregation group.

```
# show lacp      statistics
Port           Rx Frames   Tx Frames      Rx Unknown     Rx Illegal
-----
Gi 1/1         2572          14067          0               0
Gi 1/2         2572          14068          0               0
```

System ID

The following snippet shows the system ID. The system ID is the combination of the priority and the MAC address.

```
(config)# lacp system-priority ?
 <1-65535>      Priority value, lower means higher priority
# show lacp system-id
System ID: 32768 - 00:01:c1:00:f6:90
```

Port LACP Commands

The following snippet shows how to configure LACP for each port.

```
# conf t
(config)# interface GigabitEthernet 1/1-2
(config-if)# lacp ?
port-priority      timeout          <cr>
```

Where...

- *Port-priority* - the LACP priority for the port.
- *Timeout* - fast or slow protocol timeout.

Group LACP Commands

The following snippet shows how to perform an additional configuration of LACP based groups.

```
# conf t
(config)# interface llag 1
(config-llag)# lacp ?
failover
max-bundle
```

- *failover* - revertive (default) /non-revertive.
- *max-bundle* - max size of the aggregation (1-max). All the default ports in the group can aggregate.

Forwarding Mode of the Aggregation

The forwarding distribution of the traffic can be affected by changing the aggregation mode. This is a global parameter and affects all aggregations. These mode parameters can be combined.

**NOTE**

Any change in the aggregation mode stops all forwarding until the key is fully setup.

```
config)# aggregation mode ?
    dmac      Destination MAC affects the distribution
    ip        IP address affects the distribution
    port      IP port affects the distribution
    smac      Source MAC affects the distribution
(config)# aggregation mode ?
aggregation mode { [ smac ] [ dmac ] [ ip ] [ port ] }
(config)# aggregation mode smac dmac
(config)# end
#
```

Delete an Aggregation Group

The following snippet shows how to delete an aggregation group.

```
#conf t
(config)# no interface llag 1
(config)#
```

5.9. Loop Protection

The switch supports a loop elimination function that is based on per port or system configure. It prevents communication looping caused by RSTP and Ring if the ring topology changes. The following figure shows the Loop Protection page.

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

Submit Reset

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

Table 40. General Settings

Item	Description
Enable Loop Protection	Controls whether loop protection is enabled (as a whole).
Transmission Time	The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds. Default value is 5 seconds.
Shutdown Time	The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart). Default value is 180 seconds.

Table 41. Port Configuration

Item	Description
Port	The switch port number of the port.
Enable	Controls whether loop protection is enabled on this switch port.
Action	Configures the action performed when a loop is detected on a port. Valid values are <i>Shutdown Port</i> , <i>Shutdown Port and Log</i> or <i>Log Only</i> .
Tx Mode	Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

5.10. Spanning Tree

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	RSTP
Bridge Priority	32768
Hello Time	2
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	

Table 42. Basic Settings

Item	Description
Protocol Version	The RSTP / STP protocol version setting. Valid values are <i>RSTP</i> and <i>STP</i> .
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.
Hello Time	The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds, default is 2 seconds.
	<div style="display: flex; align-items: center;"> <div> <p>NOTE</p> <p>Changing this parameter from the default value is not recommended, and may have adverse effects on your network.</p> </div> </div>
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 $\leq (FwdDelay-1)*2$.
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.

Table 43. Advanced Settings

Item	Description
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 (24 hours).

Port Configuration

This page allows the user to inspect and configure the current STP CIST port configuration. 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 Role	TCN	BPDU Guard	Point-to-point
-	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True

CIST Normal Port Configuration

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

Submit Reset

Table 44. Port Configuration

Item	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls whether STP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The Autosetting 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 Monitor > Spanning Tree > STP Detailed Bridge Status.
AdminEdge	Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).
AutoEdge	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDUs are received on the port or not.
Restricted Role	If enabled, causes the port not to be selected as Root Port for the CIST, 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 <i>Root Guard</i> .
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 BPDUs. 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.

5.11. IPMC

Basic Configuration

This page provides IGMP Snooping related configuration.

IGMP Snooping Configuration

Global Configuration

Snooping Enabled

Unregistered IPMCv4 Flooding Enabled

Port Related Configuration

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

Table 45. IGMP Snooping Configuration

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

VLAN Configuration

Navigating the IGMP Snooping VLAN Table

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

IGMP Snooping VLAN Table Columns

IGMP Snooping VLAN Configuration

Start from VLAN with entries per page.

VLAN ID	Snooping Enabled	Querier Election	Querier Address
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0.0.0.0

For IGMP VLAN interface creation, you need to enter the IP configuration page to setup the IP interface first. *System -> IP -> Add IP interface.*

Table 46. IGMP Snooping VLAN Configuration

Item	Description
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enabled	Enable the per-VLAN IGMP Snooping. Up to 8 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.

5.12. LLDP

LLDP is an IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

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

Interface	Mode	Trap	Optional TLVs				
			Port Descr	Sys Name	Sys Descr	Sys Capa	Mgmt Addr
	<>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/1	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/2	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/3	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/4	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/5	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/6	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/7	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/8	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/9	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GigabitEthernet 1/10	Disabled	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Submit Reset

Table 47. LLDP Parameters

Item	Description
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.

Table 48. LLDP Interface Configuration

Item	Description
Interface	The switch interface name of the logical LLDP interface.
Mode	Select LLDP mode. <ul style="list-style-type: none">• <i>Rx only</i>: The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.• <i>Tx only</i>: The switch will drop LLDP information received from neighbors, but will send out LLDP information.• <i>Disabled</i>: The switch will not send out LLDP information, and will drop LLDP information received from neighbors.• <i>Enabled</i>: The switch will send out LLDP information, and will analyze LLDP information received from neighbors.
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.

5.13. PoE

Power Over Ethernet Configuration

Reserved Power determined by	<input type="radio"/> Class <input checked="" type="radio"/> Allocation <input type="radio"/> LLDP-MED
Power Management Mode	<input checked="" type="radio"/> Actual Consumption <input type="radio"/> Reserved Power
Capacitor Detection	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled

PoE Power Supply Configuration

Primary Power Supply [W]	120
---------------------------------	-----

PoE Port Configuration

Port	PoE Mode	Priority	Maximum Power [W]
*	<> ▼	<> ▼	20
1	PoE+ ▼	Critical ▼	20
2	PoE+ ▼	Critical ▼	20
3	PoE+ ▼	High ▼	10
4	PoE+ ▼	High ▼	10
5	PoE+ ▼	Low ▼	10
6	PoE+ ▼	Low ▼	10
7	PoE+ ▼	Low ▼	10
8	PoE+ ▼	Low ▼	10

Table 49. Power Over Ethernet Configuration

Item	Description
Reserved Power determined by	<p>There are three modes for configuring how the ports/PDs may reserve power.</p> <ul style="list-style-type: none"> Class mode: In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts. In this mode, the Maximum Power fields have no effect. Allocated mode: In this mode the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields. LLDP-MED mode: This mode is similar to the Class mode except that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode. Both ends of the switch and PD must support LLDP information detection, otherwise it will not work. The PD devices rarely support LLDP information detection, you need to check with the supplier before using it. In this mode the Maximum Power fields have no effect. <p>For all modes: If a port uses more power than the reserved power for the port, the port is shut down.</p>
Power Management Mode	<p>There are two modes for configuring when to shut down the ports:</p> <ul style="list-style-type: none"> Actual Consumption: In this mode, the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down. Reserved Power: In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.


Item	Description
Capacitor Detection	<p>Controls capacitor detection for legacy PD devices.</p> <p><i>Disabled:</i> This feature is disabled.</p> <p><i>Enabled:</i> This feature is enabled.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>NOTE The capacitor-type PD device may be an old style powered device or only available for proprietary applications of few brands. Even the PoE chipset support capacitor detection, it may still not interoperate well. We recommend that you connect the 802.3af/at compliant PD to the switch.</p> </div>

Table 50. PoE Power Supply Configuration


Item	Description
Primary Power Supply (Power Budget)	<p>To be able to determine the amount of power the PD may use, it must be defined what amount of power a power source can deliver. Valid values of 24 V (19.2 - 57 V) input is in the range 1 - 120 W. Valid values of 12 V (10 - 18 V) input is in the range 1 - 60 W. More than 120 W is not allowed by the web GUI.</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>NOTE When configuring the power budget, user must pay attention to the maximum limit for 12 V input is 60 W. The web GUI do not alarm for this setup.</p> </div>

Table 51. Port Configuration

Item	Description
Port	This is the physical port number for this row.
PoE Mode	<p>The PoE Mode represents the PoE operating mode for the port.</p> <ul style="list-style-type: none"> • <i>Disabled:</i> PoE disabled for the port. • <i>PoE:</i> Enables PoE IEEE 802.3af (Class 4 PDs limited to 15.4W). • <i>PoE+:</i> Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 30W).
Priority	<p>The Priority represents the ports priority. There are three levels of power priority named Low, High and Critical.</p> <p>The priority is used in the case where the remote devices requires more power than the power supply can deliver. In this case the port with the lowest priority will be turned off, starting from the port with the highest port number.</p>
Maximum Power	<p>The Maximum Power value contains a numerical value that indicates the maximum power in Watt that can be delivered to a remote device.</p> <p>The maximum allowed value is 30 W.</p>

5.14. MAC Table

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

MAC Address Table Configuration

Aging Configuration

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

MAC Table Learning

	Port Members									
	1	2	3	4	5	6	7	8	9	10
Auto	●	●	●	●	●	●	●	●	●	●
Disable	○	○	○	○	○	○	○	○	○	○
Secure	○	○	○	○	○	○	○	○	○	○

VLAN Learning Configuration

Learning-disabled VLANs	
-------------------------	--

Static MAC Table Configuration

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

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 5000 timesseconds. The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by selecting the Disable automatic aging checkbox.

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:

Table 52. MAC Table Learning

Item	Description
Auto	Learning is done automatically as soon as a frame with unknown SMAC is received.
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped.

NOTE
 Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

VLAN Learning Configuration

Item	Description
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 learnt. By the 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. 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.

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.

Table 53. Static MAC Table Configuration

Item	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.
Adding a New Static Entry	Click to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Submit".

5.15. VLAN

Configuration

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
Ethertype for Custom S-ports	88A8

Port VLAN Configuration



Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	☑	<>	<>	1	
1	Access	1	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	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag All	1	

Table 54. Global VLAN Configuration

Item	Description
Allowed Access VLANs	This field shows the allowed Access VLANs, i.e. it only affects ports configured as Access ports. Ports in other modes are members of the VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.
Ethertype for Custom 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.

Table 55. Port VLAN Configuration

Item	Description
Port	This is the logical port number of this row.
Mode	<p>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.</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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

Item	Description
	<ul style="list-style-type: none"> • <i>Hybrid</i>: 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: <ul style="list-style-type: none"> – 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	<p>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.</p>
Port Type	<p>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.</p> <p><i>Unaware</i>: 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.</p> <p><i>C-Port</i>: 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.</p> <p><i>S-Port</i>: 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.</p> <div data-bbox="336 898 1401 1126" style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p> NOTE</p> <p>If the S-port is configured to accept Tagged and Untagged frames (see Ingress Acceptance below), frames with a C-tag are treated like frames with an S-tag.</p> <p>If the S-port is configured to accept Untagged Only frames, S-tagged frames will be discarded (except for priority S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID.</p> </div> <p><i>S-Custom-Port</i>: 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.</p> <div data-bbox="336 1285 1401 1509" style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p> NOTE</p> <p>If the custom S-port is configured to accept Tagged and Untagged frames (see Ingress Acceptance below), frames with a C-tag are treated like frames with a custom S-tag. If the Custom S-port is configured to accept Untagged Only frames, custom S-tagged frames will be discarded (except for priority custom S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID.</p> </div>
Ingress Filtering	<p>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.</p>
Ingress Acceptance	<p>Hybrid ports allow for changing the type of frames that are accepted on ingress.</p> <ul style="list-style-type: none"> • <i>Tagged and Untagged</i>: Both tagged and untagged frames are accepted. See Port Type for a description of when a frame is considered tagged. • <i>Tagged Only</i>: Only frames tagged with the corresponding Port Type tag are accepted on ingress. • <i>Untagged Only</i>: Only untagged frames are accepted on ingress. See Port Type for a description of when a frame is considered untagged.
Egress Tagging	<p>Ports in Trunk and Hybrid mode may control the tagging of frames on egress.</p> <ul style="list-style-type: none"> • <i>Untag Port VLAN</i>: Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag. • <i>Tag All</i>: All frames, whether classified to the Port VLAN or not, are transmitted with a tag. • <i>Untag All</i>: 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.

Item	Description
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.

SVL (Shared VLAN Learning)

Shared VLAN Learning allows for frames initially classified to a particular VLAN (based on Port VLAN ID or VLAN tag information) be bridged on a shared VLAN. In SVL two or more VLANs are grouped to share common source address information in the MAC table. The common entry in the MAC table is identified by a Filter ID (FID). SVL is useful for configuration of more complex, asymmetrical cross-VLAN traffic patterns, like E-TREE (Rooted-Multipoint) and Multi-netted Server. The alternative VLAN learning mode is IVL. The default VLAN learning mode is IVL and not all switches support SVL. In Independent VLAN Learning, every VLAN uses its own logical source address table as opposed to SVL where two or more VLANs share the same part of the MAC address table.

Shared VLAN Learning Configuration

Delete	FID	VLANs
Delete	1	1,2
Delete	2	3

This page allows for controlling SVL configuration on the switch. 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.

Table 56. Shared VLAN Learning Configuration

Item	Description
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 63.
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.

5.16. Private VLANs

This switch also has private VLAN functions; it helps to resolve the primary VLAN ID shortage, client ports' isolation and network security issues. A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains, allowing User to isolate the ports on the switch from each other. A subdomain consists of a primary VLAN and one or more secondary VLANs. All VLANs in a private VLAN domain share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another. The secondary VLANs may either be isolated VLANs or community VLANs. A host on an isolated VLAN can only communicate with the associated promiscuous port in its primary VLAN. Hosts on community VLANs can communicate among themselves and with their associated promiscuous port but not with ports in other community VLANs.

Membership

Private VLAN Membership Configuration Auto-refresh Refresh

Delete	PVLAN ID	Port Members													
<input type="checkbox"/>	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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.

Table 57. Private VLAN Membership Configuration

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

Port Isolation

This page is used for enabling or disabling port isolation on ports in a Private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Port Isolation Configuration Auto-refresh Refresh

Port Number
1 <input type="checkbox"/>
2 <input type="checkbox"/>
3 <input type="checkbox"/>
4 <input type="checkbox"/>
5 <input type="checkbox"/>
6 <input type="checkbox"/>
7 <input type="checkbox"/>
8 <input type="checkbox"/>
9 <input type="checkbox"/>
10 <input type="checkbox"/>

Table 58. Port Isolation Configuration

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

5.17. QoS

QoS is a mechanism for providing different priorities to different applications, users, or data flows, or to guarantee a certain level of performance for a data flow.

All incoming frames are classified into a Class of Service (CoS), which is used in the queue system when the assigning resources, in the arbitration from ingress to egress queues and in the egress scheduler when selecting the next frame for transmission.

There is a one-to-one mapping between the terms CoS, QoS class, queue, and priority. A CoS of zero has the lowest priority.

Bandwidth control in the queues can be done by using policers or shapers.

Apart from shapers and policers, different scheduling mechanisms can be configured based on how the different priority queues in the QoS system are handled.

Weighted Random Early Detection (WRED) can be configured globally to avoid congestion and drop the Yellow Frames (frames with DPL greater than zero) when the queues are filled.

The storm policers of the devices can be used at a global level to control the amount of flooded frames. It is also possible to configure per-port storm policers.

QoS Classification

QoS is classified as:

- Basic QoS - This enables predefined schemes for handling CoS, Drop Precedence Level (DPL), Priority Code Points (PCP), Drop Eligible Indicator (DEI), Class of Service ID (CoSID), and Differentiated Service Code Points (DSCP).
- CoS and DPL classification based on PCP and DEI for tagged frames. The mapping table from PCP and DEI to CoS and DPL is programmable per port.
- CoS and DPL classification based on DSCP values.
- DSCP translation.
- DSCP remarking based on CoS.
- Per-port CoS and DPL configuration for untagged and non-IP Frames.
- Per-port CoSID configuration. CoSID is a value that can be used as a selector in Egress Maps and Ethernet Services. It does not relate to CoS in any way.
- General classification using an Ingress Map.
- General remarking using an Egress Map.
- Advanced QoS - This uses the QoS Control Lists (QCLs), which provides a flexible classification.
- Higher layer protocol fields (Layer 2 through Layer 4) for rule matching.
- Actions include reclassification of CoS, DPL, PCP, DEI, DSCP, and ACL policy values. It is also possible to reclassify by using an Ingress Map.

Policers

Policers limit the bandwidth of received frames exceeding the configurable rates. Policers can be configured at queue level or at a port level. There is also a provision to add policers at the EVC level, although this provision is not discussed in this document.

Shapers

Egress traffic shaping can be achieved using bandwidth shapers. Shapers can be configured at queue level or at a port level.

Scheduling Algorithm

Two types of scheduling are possible on the device at a port level:

- Strict Priority: All queues follow strict priority scheduling.
- Deficit Weighted Round Robin (DWRR): Scheduling is based on the weights configured for each queue. Configuration is present to select the number of queues which can be under DWRR. It is possible to include from two to all eight queues in DWRR mode.

When the number of queues selected for DWRR is less than eight then the lowest priority queues are put in DWRR and higher priority queues are put in Strict Priority. For example, if number of Queues is two for DWRR then Queue 0 and Queue 1 are set in DWRR mode, and the remaining Queues 2 to 7 are set in Strict Priority.

Weighted Random Early Detection (WRED)

Congestion can be avoided in the queue system by enabling and configuring the Weighted Random Early Detection (WRED) function. WRED can discard frames with DPL greater than zero.

There are three separate WRED groups, and each port belongs to one of these groups.

Configuration includes enabling WRED per group, queue, and DPL and setting the minimum and maximum Threshold. Minimum threshold is the queue fills level at which the WRED starts discarding the Frames. Maximum threshold can be configured as either Drop Probability or Fill Level. When the unit is Drop Probability, the mentioned threshold would be the Drop Probability with the queue fill level is just about 100%. When the unit is Fill Level, then it represents the queue fill level where Drop Probability is 100%.

Storm Policing

Storm policers restrict the amount of flooded frames (frames coming with SMAC which are not learnt earlier) entering the device. The configurations are global per-device and not per-port. Storm policers can be applied separately on Unicast, Multicast, or Broadcast packets.

It is also possible to configure per-port storm policers. Port storm policers can be applied separately on Unicast, Broadcast, and flooded (unknown) packets.

Ingress Map

An Ingress Map is a mapping table created to classify values at ingress such as, CoS, DPL, PCP, DEI, DSCP, and CoSID based on the key values in the packet (PCP, PCP/DEI, DSCP, or PCP/DEI/DSCP).

In order to use an Ingress Map, it must first be created and configured. Configuration consists of the following parameters:

- *Key*: Which part of the packet to use for lookup.
- *Actions*: Which kinds of values to classify.
- *Mappings*: The actual value to use for classification for each value of the key.

A specific Ingress Map can be associated with one or more ports, QCEs, or EVCs/ECES. Using an Ingress Map will always take precedence over other kinds of port-based classification.

5.18. Mirroring

Session ID	Mode	Type	VLAN ID	Reflector Port
1	Enabled	Mirror	-	-

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 to a destination port where a network analyzer can be attached to analyze the network traffic. Remote Mirroring is an extended function of Mirroring. It can extend the destination port in another switch. In this way, the administrator can analyze the network traffic on the other switches.

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

Mirror & RMirror Configuration

Global Settings

Session ID	1
Mode	Enabled
Type	Mirror
VLAN ID	200
ReflectorPort	Port 1

Source VLAN(s) Configuration

VLAN ID	1
---------	---

Port Configuration

Port	Source	Destination
*	<>	<input type="checkbox"/>
Port 1	Disabled	<input type="checkbox"/>
Port 2	Disabled	<input type="checkbox"/>
Port 3	Disabled	<input type="checkbox"/>
Port 4	Disabled	<input type="checkbox"/>
Port 5	Disabled	<input type="checkbox"/>
Port 6	Disabled	<input type="checkbox"/>
Port 7	Disabled	<input type="checkbox"/>
Port 8	Disabled	<input type="checkbox"/>
Port 9	Disabled	<input type="checkbox"/>
Port 10	Disabled	<input type="checkbox"/>
CPU	Disabled	<input type="checkbox"/>

Table 59. Global Settings

Item	Description
Session	Select session id to configure.
Mode	Enable/Disable the mirror or Remote Mirroring function.
Type	Select switch type. <ul style="list-style-type: none"> <i>Mirror</i>: The switch is running on mirror mode. The source port(s) and destination port are located on this switch. <i>RMirror Source</i>: The switch is a source node for monitor flow. The source port(s), reflector port are located on this switch. <i>RMirror Destination</i>: 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.
ReflectorPort	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.
	<div style="display: flex; align-items: center;"> <div> <p>NOTE</p> <p>The reflector port needs to select only on Sourceswitch type.</p> </div> </div>
	<div style="display: flex; align-items: center;"> <div> <p>NOTE</p> <p>The reflector port needs to disable MAC Table learning and STP.</p> </div> </div>
	<div style="display: flex; align-items: center;"> <div> <p>NOTE</p> <p>The reflector port only support pure copper ports.</p> </div> </div>

Source VLAN(s) Configuration

The switch can support VLAN-based Mirroring. If you want to monitor some VLANs on the switch, you can set the selected VLANs on this field.





NOTE

The Mirroring session shall have either ports or VLANs as sources, but not both.

Remote Mirroring Port Configuration

The following table is used for port role selecting.

Table 60. Port Configuration

Item	Description
Port	The logical port for the settings contained in the same row.
Source	<p>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.</p> <ul style="list-style-type: none"> • <i>Disabled</i>: Neither frames transmitted nor frames received are mirrored. • <i>Both</i>: Frames received and frames transmitted are mirrored on the Destination port. • <i>Rx only</i>: Frames received on this port are mirrored on the Destination port. Frames transmitted are not mirrored. • <i>Tx only</i>: Frames transmitted on this port are mirrored on the Destination port. Frames received are not mirrored.
Destination	<p>Select destination port.</p> <p>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.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  <p>NOTE On mirror mode, the device only supports one destination port.</p> </div> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">  <p>NOTE The destination port needs to disable MAC Table learning.</p> </div>

6. Monitor

6.1. System

6.1.1. System Information

The switch system information is provided here.

System Information
Auto-refresh [Refresh](#)

System	
Contact Name	switch
Contact Location	
Hardware	
MAC Address	02-00-c1-dc-33-dd
Time	
System Date	2018-01-01T00:21:25+00:00
System Uptime	0d 00:21:46
Software	
Software Version	v0.9.8-1539939663
Software Date	2018-10-19T02:01:03-07:00
Acknowledgments	Details

Table 61. System Information

Item	Description
Contact	The system contact configured in Configuration System Information System Contact.
Name	The system name configured in Configuration System Information System Name.
Location	The system location configured in Configuration System Information System Location.
MAC Address	The MAC Address of this switch.
System Date	The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.
System Uptime	The period of time that the device has been operational.
Software Version	The software version of this switch.
Software Date	The date when the switch software was produced.

6.1.2. LED Status

The switch system LED status is provided here.

System LED Status
Auto-refresh [Refresh](#) [Clear](#)

Clear Type	All
Description	System LED: green, solid, normal indication.

Table 62. System LED Status

Item	Description
Clear Type	The types of system LED status clearing. Possible values are:
Description	The description of system LED. <ul style="list-style-type: none"> All: Clear all error status of the system LED and back to normal indication. Fatal: Clear fatal error status of the system LED. Software: Clear generic software error status of the system LED.

6.1.3. CPU Load

This page displays the CPU load, using an SVG graph. The load is measured as averaged over the last 100 ms, 1 sec 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.

6.1.4. 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 neighbor cache (ARP cache) status.

IP Interfaces
Auto-refresh Refresh

Interface	Type	Address	Status
VLAN1	LINK	02-00-c1-dc-33-dd	<UP BROADCAST MULTICAST>
VLAN1	IPv4	192.168.10.1/24	

IPv6 Routes

Network	Gateway	Status

Neighbour cache

IP Address	Link Address
192.168.10.11	VLAN1:70-8b-cd-03-b5-67

IP Interfaces

Table 63. IP Interfaces

Item	Description
Interface	The name of the interface.
Type	The address type of the entry. This may be LINK or IPv4.
Address	The current address of the interface (of the given type).
Status	The status flags of the interface (and/or address).

IPv6 Routes

Table 64. IPv6 Routes

Item	Description
Network	The destination IPv6 network or host address of this route.
Gateway	The gateway address of this route.
Status	The status flags of the route.

Neighbour Cache

Table 65. Neighbour Cache

Item	Description
IP Address	The IP address of the entry.
Link Address	The Link (MAC) address for which a binding to the IP address given exist.

6.1.5. Routing Information Base

This is IPv4 route entry table. It is used to provide the route entries status information

Routing Information Base 1 - 1 of 1 entry Auto-refresh Refresh << >>

Start from Network / Protocol NextHop with entries per page.

Codes: C - connected, S - static, O - OSPF, * - selected route, D - DHCP installed route

Protocol	Network/Prefix	NextHop	Distance	Metric	Interface	Uptime (hh:mm:ss)	State
C *	192.168.10.0/24	-	-	-	VLAN 1	-	Active

Navigating the Routing Information Base 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 Network" 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.

Table 66. Routing Information Base

Item	Description
Protocol	The protocol of the route. <ul style="list-style-type: none"> <i>DHCP</i>: The route is created by DHCP. <i>Connected</i>: The destination network is connected directly. <i>Static</i>: The route is created by user. <i>OSPF</i>: The route is created by OSPF.
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 until the route is created. The unit is in seconds.
State	Indicate if the destination network is reachable or not.

6.1.6. Log

The switch system log information is provided here.

System Log Information Auto-refresh Refresh Clear << >>

Level
 Clear Level

The total number of entries is 5 for the given level.

Start from ID with entries per page.

ID	Level	Time	Message
1	Informational	2018-01-01T00:00:03+00:00	SYS-BOOTING: Switch just made a cold boot.
2	Notice	2018-01-01T00:00:03+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
3	Notice	2018-01-01T00:00:03+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
4	Notice	2018-01-01T00:00:05+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/4, changed state to up.
5	Notice	2018-01-01T00:00:09+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.

Navigating the System Log Information Table

Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table. The "Level" input field is used to filter the display system log entries.

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

Table 67. System Log Information

Item	Description
ID	The ID of the system log entry.
Level	The level of the system log entry. <ul style="list-style-type: none"> • <i>Info</i>: The system log entry is belonged information level. • <i>Warning</i>: The system log entry is belonged warning level. • <i>Error</i>: The system log entry is belonged error level.
Time	The time of the system log entry.
Message	The detail message of the system log entry.

6.1.7. Relay Output Status

This page displays the relay output status of the ports of the switch.

Relay Output Status

Relay Status	off									
Port	1	2	3	4	5	6	7	8	9	10
Relay Trigger by	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Auto-refresh

Table 68. Relay Output Status

Item	Description
Relay Status	The switch relay status.
Port	The switch port number of the logical port.
Relay Trigger by	The current relay status "on" trigger by which ports.

6.2. Green Ethernet

This page provides the current status for EEE (Energy-Efficient Ethernet).

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	●	✗	✗	✗	✗	✗	✗

Auto-refresh

Table 69. Port Power Savings Status

Item	Description
Local Port	This is the logical port number for this row.
Link	Shows if the link is up for the port (green = link up, red = link down).
EEE Cap	Shows if the port is EEE capable.
EEE Enable	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 μSec.
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.

6.3. Thermal Protection

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

Thermal Protection Status Auto-refresh Refresh

Thermal Protection Port Status

Port	Temperature	Port status
1	55 °C	Port link operating normally
2	55 °C	Port link operating normally
3	55 °C	Port link operating normally
4	55 °C	Port link operating normally
5	0 °C	Port link operating normally
6	0 °C	Port link operating normally
7	0 °C	Port link operating normally
8	0 °C	Port link operating normally
9	0 °C	Port link operating normally
10	0 °C	Port link operating normally

Table 70. Thermal Protection Port Status


Item	Description
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.

6.4. Ports

6.4.1. State

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

Port State Overview Auto-refresh Refresh



The port states are illustrated as follows:

- *Gray port*: disabled
- *Black port*: down
- *Green or yellow port*: link

6.4.2. Port Statistics Overview

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

Port Statistics Overview Auto-refresh Refresh Clear

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	6101	5252	1407045	1915000	0	0	0	0	3763
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0

The displayed counters are:

Table 71. Port Statistics Overview

Item	Description
Port	The logical port for the settings contained in the same row.
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions per port.
Drops	The number of frames discarded due to ingress or egress congestion.
Filtered	The number of received frames filtered by the forwarding process.

6.4.3. QoS Statistics

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

Queuing Counters Auto-refresh [Refresh](#) [Clear](#)

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7		
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	
1	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
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	6240	2910	0	0	0	0	0	0	0	0	0	0	0	0	0	2491	0
5	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
7	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
9	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

The displayed counters are:

Table 72. Queuing Counters

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

6.4.4. QoS Control List (QCL)

This page shows the QCL status by different QCL users.

QoS Control List Status Combined Auto-refresh [Resolve Conflict](#) [Refresh](#)

User	QCE	Port	Frame Type	Action						Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	
No entries										

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 1024 on each switch.

Table 73. QoS Control List Status

Item	Description
User	Indicates the QCL user.
QCE	Indicates the QCE ID.
Port	Indicates the list of ports configured with the QCE.

Item	Description
Frame Type	Indicates the type of frame. Possible values are: <ul style="list-style-type: none"> • <i>Any</i>: Match any frame type. • <i>Ethernet</i>: Match EtherType frames. • <i>LLC</i>: Match (LLC) frames. • <i>SNAP</i>: Match (SNAP) frames. • <i>IPv4</i>: Match IPv4 frames. • <i>IPv6</i>: 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: <ul style="list-style-type: none"> • <i>CoS</i>: Classify Class of Service. • <i>DPL</i>: Classify Drop Precedence Level. • <i>DSCP</i>: Classify DSCP value. • <i>PCP</i>: Classify PCP value. • <i>DEI</i>: Classify DEI value. • <i>Policy</i>: Classify ACL Policy number.
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.

6.4.5. Detailed Statistics

This page provides detailed traffic statistics for a specific switch port.

Detailed Port Statistics Port 1 Port 1 | Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

Use the port select box to select which switch port details to display. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

Table 74. Receive Total and Transmit Total

Item	Description
Rx and Tx Packets	The number of received and transmitted (good and bad) packets.
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
Rx and Tx Unicast	The number of received and transmitted (good and bad) unicast packets.
Rx and Tx Multicast	The number of received and transmitted (good and bad) multicast packets.
Rx and Tx Broadcast	The number of received and transmitted (good and bad) broadcast packets.
Rx and Tx Pause	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

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.

Table 75. Receive Error Counters

Item	Description
Rx Drops	The number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short ¹ frames received with valid CRC.
Rx Oversize	The number of long ² frames received with valid CRC.
Rx Fragments	The number of short ¹ frames received with invalid CRC.
Rx Jabber	The number of long ² frames received with invalid CRC.
Rx Filtered	The number of received frames filtered by the forwarding process.

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

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

Table 76. Transmit Error Counters

Item	Description
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.

6.5. Security

6.5.1. Access Management Statistics

This page provides statistics for access management.

Access Management Statistics			
Interface	Received Packets	Allowed Packets	Discarded Packets
HTTP	0	0	0
HTTPS	0	0	0
SNMP	0	0	0

Auto-refresh Refresh Clear

Table 77. Access Management Statistics

Item	Description
Interface	The interface type through which the remote host can access the switch.
Received Packets	Number of received packets from the interface when access management mode is enabled.
Allowed Packets	Number of allowed packets from the interface when access management mode is enabled.
Discarded Packets	Number of discarded packets from the interface when access management mode is enabled.

6.6. Aggregation

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

Aggregation Status

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

Table 78. Aggregation Status

Item	Description
Aggr ID	The Aggregation ID associated with this aggregation instance.
Name	Name of the Aggregation group ID.
Type	Type of the Aggregation group (Static or LACP).
Speed	Speed of the Aggregation group.
Configured Ports	Configured member ports of the Aggregation group.
Aggregated Ports	Aggregated member ports of the Aggregation group.

6.7. Loop Protection

This page displays the loop protection port status 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	Log Only	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Up	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	0	Down	-	-
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Down	-	-
10	Shutdown	Enabled	0	Down	-	-

Table 79. Loop Protection Status

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

6.8. Spanning Tree

6.8.1. STP Bridge Status

This page provides detailed information on a single STP bridge instance, along with port state for all active ports associated.

STP Detailed Bridge Status Auto-refresh Refresh

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	32768.02-00-C1-6F-61-F1
Root ID	32768.02-00-C1-6F-61-F1
Root Cost	0
Root Port	-
Regional Root	32768.02-00-C1-6F-61-F1
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	17
Topology Change Last	0d 01:18:59

CIST Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point-to-Point	Uptime
4	128:004	DesignatedPort	Forwarding	20000	Yes	Yes	0d 00:10:47

The page contains two tables with the following information:

Table 80. STP Bridge Status

Item	Description
Bridge Instance	The Bridge instance - <i>CIST, MST1, ...</i>
Bridge ID	The Bridge ID of this Bridge instance.
Root ID	The Bridge ID of the currently elected root bridge.
Root Port	The switch port currently assigned the root port role.
Root Cost	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Regional Root	The Bridge ID of the currently elected regional root bridge, inside the MSTP region of this bridge. (For the CIST instance only).
Internal Root Cost	The Regional Root Path Cost. For the Regional Root Bridge this is zero. For all other CIST instances in the same MSTP region, it is the sum of the Internal Port Path Costs on the least cost path to the Internal Root Bridge. (For the CIST instance only).
Topology Flag	The current state of the Topology Change Flag of this Bridge instance.
Topology Change Count	The number of times where the topology change flag has been set (during a one-second interval).
Topology Change Last	The time passed since the Topology Flag was last set.

Table 81. CIST Ports & Aggregations State

Item	Description
Port	The switch port number of the logical STP port.
Port ID	The port ID as used by the STP protocol. This is the priority part and the logical port index of the bridge port.
Role	The current STP port role. The port role can be one of the following values: <ul style="list-style-type: none"> • <i>AlternatePort</i> • <i>BackupPortRootPort</i> • <i>DesignatedPort</i>
State	The current STP port state. The port state can be one of the following values: <ul style="list-style-type: none"> • <i>Discarding</i> • <i>LearningForwarding</i>
Path Cost	The current STP port path cost. This will either be a value computed from the <i>Auto</i> setting, or any explicitly configured value.
Edge	The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop.
Point-to-Point	The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transit to STP state.
Uptime	The time since the bridge port was last initialized.

6.8.2. Port Status

This page displays the STP CIST port status for physical ports of the switch.

STP Port Status Auto-refresh Refresh

Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	DesignatedPort	Forwarding	0d 00:12:59
5	Disabled	Discarding	-
6	Disabled	Discarding	-
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	Disabled	Discarding	-

Table 82. STP Port Status

Item	Description
Port	The switch port number of the logical STP port.
CIST Role	The current STP port role of the CIST port. The port role can be one of the following values: <i>AlternatePortBackupPort RootPort DesignatedPortDisabled</i> .
CIST State	The current STP port state of the CIST port. The port state can be one of the following values: <i>DiscardingLearning Forwarding</i> .
Uptime	The time since the bridge port was last initialized.

6.8.3. Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch.

STP Statistics Auto-refresh Refresh Clear

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
4	0	429	0	0	0	0	0	0	0	0

Table 83. STP Statistics

Item	Description
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.

6.9. IPMC

6.9.1. IGMP Snooping 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
1	-	-	-	-	-	-	-	-	-
2	Static	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-

Router Port

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

Table 84. IGMP Snooping Status

Item	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	Working Querier Version currently.
Host Version	Working Host Version currently.
Querier Status	Shows the Querier status is <i>ACTIVE</i> or <i>IDLE</i> . <i>DISABLE</i> means that the specific interface is administratively disabled.
Querier Transmitted	The number of Transmitted Queries.
Querier Received	The number of Received Queries.
V1 Reports Received	The number of Received V1 Reports.
V2 Reports Received	The number of Received V2 Reports.
V3 Reports Received	The number of Received V3 Reports.
V2 Leaves Received	The number of Received V2 Leaves.
Router Port	Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. <i>Static</i> : the specific port is configured to be a router port. <i>Dynamic</i> : the specific port is learnt to be a router port. <i>Both</i> : 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.

6.9.2. Group Information

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

IGMP Snooping Group Information Auto-refresh Refresh |<< >>

Start from VLAN and group address with entries per page.

VLAN ID	Groups	Port Members
1	2	3 4 5 6 7 8 9 10
<i>No more entries</i>		

Navigating the IGMP Group Table

Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP Group Table. Clicking the 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 button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

Table 85. IGMP Group Table

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

6.10. LLDP

6.10.1. LLDP Neighbor Information

This page provides a status overview for all LLDP neighbors.

LLDP Neighbor Information Auto-refresh Refresh

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

The displayed table contains a row for each interface on which an LLDP neighbor is detected.

The columns hold the following information:

Table 86. LLDP Neighbor Information

Item	Description
Local Interface	The interface on which the LLDP frame was received.
Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames.
Port ID	The Port ID is the identification of the neighbor port.
Port Description	Port Description is the port description advertised by the neighbor unit.
System Name	System Name is the name advertised by the neighbor unit.
System Capabilities	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: <ol style="list-style-type: none"> 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved <p>When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).</p>
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.

6.10.2. LLDP Neighbors EEE Information

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.

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 1/4	EEE not enabled for this interface							

LLDP Neighbors EEE Information Table

The displayed table contains a row for each interface. If the interface does not support EEE, then it displays as "EEE not supported for this interface". If EEE is not enabled on a particular interface, then it displays as "EEE not enabled for this interface". If the link partner doesn't support EEE, then it displays as "Link partner is not EEE capable".

The columns hold the following information:

Table 87. LLDP Neighbors EEE Information

Item	Description
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 receives 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 partner 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. <ul style="list-style-type: none"> • <i>Red</i>: Switch and link partner have not agreed on wakeup times. • <i>Green</i>: Switch and link partner have agreed on wakeup times.

6.10.3. Port Statistics

This page provides an overview of all LLDP traffic.

LLDP Global Counters

Global Counters	
Clear global counters	<input checked="" type="checkbox"/>
Neighbor entries were last changed	2018-01-01T04:05:48+00:00 (258 secs. ago)
Total Neighbors Entries Added	1
Total Neighbors Entries Deleted	1
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	1

Auto-refresh

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	<input checked="" type="checkbox"/>
GigabitEthernet 1/2	43	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/3	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/4	82	1	0	0	0	0	2	1	<input checked="" type="checkbox"/>
GigabitEthernet 1/5	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/6	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/7	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/8	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/9	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>
GigabitEthernet 1/10	0	0	0	0	0	0	0	0	<input checked="" type="checkbox"/>

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.

Table 88. Global Counters

Item	Description
Clear global counters	If checked the global counters are cleared when Clear is pressed.
Neighbor entries were last changed	It 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.

Item	Description
Total Neighbors Entries Ages Out	Shows the number of entries deleted due to Time-To-Live expiring.

Table 89. Local Counters

Item	Description
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.

6.11. MAC Address

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.

MAC Address Table Auto-refresh Refresh Clear << >>

Start from VLAN and MAC address with entries per page.

Type	VLAN	MAC Address	Port Members																	
			CPU	1	2	3	4	5	6	7	8	9	10							
Static	1	02-00-C1-6F-61-F1	✓																	
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-6F-61-F1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic	1	70-8B-CD-03-B5-67	✓																	
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.

Navigating the MAC Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table. The "Start from MAC address" and "VLAN" input fields allow the user to select the starting point in the MAC Table. Clicking the 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 Refresh a button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

Table 90. MAC Address Table

Item	Description
Type	Indicates whether the entry is a static or a dynamic entry.
MAC Address	The MAC address of the entry.
VLAN	The VLAN ID of the entry.
Port Members	The ports those are members of the entry.

6.12. VLANs

6.12.1. Membership

This page provides an overview of membership status of VLAN users.

VLAN Membership Status for Combined users Combined ▾ Auto-refresh Refresh

Start from VLAN with entries per page. << >>

VLAN ID	Port Members									
	1	2	3	4	5	6	7	8	9	10
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Various internal software modules may use VLAN services to configure VLAN memberships on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.

Table 91. VLAN Membership Status for Combined Users

Item	Description
VLAN ID	VLAN ID for which the Port members are displayed.
Port Members	<p>A row of check boxes for each port is displayed for each VLAN ID.</p> <p>If a port is included in a VLAN, the following image will be displayed: ✓</p> <p>If a port is in the forbidden port list, the following image will be displayed: ✗</p> <p>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.</p>

6.12.2. Ports (VLANs)

This page provides VLAN Port Status.

VLAN Port Status for Combined users Combined ▾ Auto-refresh Refresh

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

Various internal software modules may use VLAN services to configure VLAN port configuration on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware. If a given software modules hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table.

Table 92. VLAN Port Status

Item	Description
Port	The logical port for the settings contained in the same row.
Port Type	Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.
Ingress Filtering	Shows whether a given user wants ingress filtering enabled or not. The field is empty if not overridden by the selected user.
Frame Type	Shows the acceptable frame types (All, Tagged, 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	It 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.

6.13. PoE

This page allows the user to inspect the current status for all PoE ports.

Power Over Ethernet Status							
Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	2	7 [W]	7 [W]	3.1 [W]	58 [mA]	Critical	PoE turned ON
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Critical	No PD detected
3	-	0 [W]	0 [W]	0 [W]	0 [mA]	High	No PD detected
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	High	No PD detected
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	2	7 [W]	7 [W]	3.1 [W]	59 [mA]	Low	PoE turned ON
8	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		14 [W]	14 [W]	6.2 [W]	117 [mA]		

Table 93. Power Over Ethernet Status

Item	Description
Local Port	This is the logical port number for this row.
PD Class	Each PD is classified according to a class that defines the maximum power the PD will use. The PD Class shows the PDs class. Five classes are defined: <ul style="list-style-type: none"> • Class 0: Max. power 15.4 W • Class 1: Max. power 4.0 W • Class 2: Max. power 7.0 W • Class 3: Max. power 15.4 W • Class 4: Max. power 30.0 W
Power Requested	The Power Requested shows the requested amount of power the PD wants to be reserved.
Power Allocated	The Power Allocated shows the amount of power the switch has allocated for the PD.

Item	Description
Power Used	The Power Used shows how much power the PD currently is using.
Current Used	The Power Used shows how much current the PD currently is using.
Priority	The Priority shows the port's priority configured by the user.
Port Status	<p>The Port Status shows the port's status. The status can be one of the following values:</p> <ul style="list-style-type: none">• <i>PoE not available - No PoE chip found</i>: PoE not supported for the port.• <i>PoE turned OFF - PoE disabled</i>: PoE is disabled by user.• <i>PoE turned OFF - Power budget exceeded</i>: The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.• <i>No PD detected</i>: No PD detected for the port.• <i>PoE turned OFF - PD overload</i>: The PD has requested or used more power than the port can deliver, and is powered down.• <i>PoE turned OFF</i>: PD is off.• <i>Invalid PD</i>: PD detected, but is not working correctly.

Example 1. After selected Reserved Power/Allocation, the statuses will be...

Power Requested is configured.

Power Over Ethernet Status

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	20 [W]	0 [W]	0 [W]	0 [mA]	Critical	No PD detected
2	-	20 [W]	0 [W]	0 [W]	0 [mA]	Critical	No PD detected
3	-	10 [W]	0 [W]	0 [W]	0 [mA]	High	No PD detected
4	-	10 [W]	0 [W]	0 [W]	0 [mA]	High	No PD detected
5	-	10 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	-	10 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	-	10 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
8	-	10 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		100 [W]	0 [W]	0 [W]	0 [mA]		

Power is allocated.

Power Over Ethernet Status

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	2	20 [W]	20 [W]	2.9 [W]	50 [mA]	Critical	PoE turned ON
2	-	20 [W]	0 [W]	0 [W]	0 [mA]	Critical	No PD detected
3	-	10 [W]	0 [W]	0 [W]	0 [mA]	High	No PD detected
4	-	10 [W]	0 [W]	0 [W]	0 [mA]	High	No PD detected
5	-	10 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
6	-	10 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
7	2	10 [W]	10 [W]	3 [W]	58 [mA]	Low	PoE turned ON
8	-	10 [W]	0 [W]	0 [W]	0 [mA]	Low	No PD detected
Total		100 [W]	30 [W]	5.9 [W]	108 [mA]		

If you disable the PoE, you will see PoE turned OFF-PoE disabled.

Power Over Ethernet Status

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	-	0 [W]	0 [W]	0 [W]	0 [mA]	Critical	PoE turned OFF - PoE disabled
2	-	0 [W]	0 [W]	0 [W]	0 [mA]	Critical	PoE turned OFF - PoE disabled
3	-	0 [W]	0 [W]	0 [W]	0 [mA]	High	PoE turned OFF - PoE disabled
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	High	PoE turned OFF - PoE disabled
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
6	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
7	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
8	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
Total		0 [W]	0 [W]	0 [W]	0 [mA]		

6.13.1. LLDP Power Over Ethernet Neighbor

This page provides a status overview for all LLDP PoE neighbors. This is applied while both Switch and PD are configured as PoE LLDP information detection. The displayed table contains a row for each interface on which an LLDP PoE neighbor is detected.

LLDP Neighbor Power Over Ethernet Information

Local Interface	Power Type	Power Source	Power Priority	Maximum Power
No PoE neighbor information found				

Table 94. LLDP Neighbor Power Over Ethernet Information

Item	Description
Local Interface	The interface for this switch on which the LLDP frame was received.
Power Type	The Power Type represents whether the device is a Power Sourcing Entity (PSE) or Power Device (PD). If the Power Type is unknown it is represented as <i>Reserved</i> .
Power Source	The Power Source represents the power source being utilized by a PSE or PD device. If the device is a PSE device it can either run on its Primary Power Source or its Backup Power Source. If it is unknown whether the PSE device is using its Primary Power Source or its Backup Power Source it is indicated as <i>Unknown</i> . If the device is a PD device it can either run on its local power supply or it can use the PSE as power source. It can also use both its local power supply and the PSE. If it is unknown what power supply the PD device is using it is indicated as <i>Unknown</i> .
Power Priority	Power Priority represents the priority of the PD device, or the power priority associated with the PSE type device's interface that is sourcing the power. There are three levels of power priority: <i>Critical</i> , <i>High</i> and <i>Low</i> . If the power priority is unknown it is indicated as <i>Unknown</i> .
Maximum Power	The Maximum Power Value contains a numerical value that indicates the maximum power in watts required by a PD device from a PSE device, or the minimum power a PSE device is capable of sourcing over a maximum length cable based on its current configuration. The maximum allowed value is 102.3 W. If the device indicates value higher than 102.3 W, it is represented as "reserved".

7. Diagnostics

The switch provides several ways for the user to monitor the switch status or diagnostic functions to check problems related to the switch.

7.1. Ping (IPv4)

Ping is a utility that sends packets over a network to a specific host, in order to generate a response. Ping uses Internet Control Message Protocol (ICMP) packets.

Ping (IPv4)


Fill in the parameters as needed and press "Start" to initiate the Ping session.

Hostname or IP Address	<input style="width: 90%;" type="text"/>	
Payload Size	<input style="width: 90%;" type="text" value="56"/>	bytes
Payload Data Pattern	<input style="width: 90%;" type="text" value="0"/>	(single byte value; integer or hex with prefix '0x')
Packet Count	<input style="width: 90%;" type="text" value="5"/>	packets
TTL Value	<input style="width: 90%;" type="text" value="64"/>	
VID for Source Interface	<input style="width: 90%;" type="text"/>	
Source Port Number	<input style="width: 90%;" type="text"/>	
IP Address for Source Interface	<input style="width: 90%;" type="text"/>	
Quiet (only print result)	<input type="checkbox"/>	



This page allows you to send ICMP (IPv4) PING packets to troubleshoot IP connectivity issues. You can configure the following parameters:

Table 95. PING Parameters

Item	Description
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 (TTL) 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.

Item	Description
Source Port Number	<p>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.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;">  <p>NOTE You may only specify either the Source Port Number or the IP address for the source interface.</p> </div>
Address for Source Interface	<p>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.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;">  <p>NOTE You may only specify either the VID or the IP Address for the source interface.</p> </div>
Quiet (only print result)	<p>Checking this option will not print the result of each ping request, but only show the final result. After pressing Start, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon the 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 will refresh automatically until responses to all packets are received, or until a timeout occurs.</p> <p>The output from the command will look like the following:</p> <pre> 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 </pre>

7.2. 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	<input type="text"/>		
DSCP Value	<input type="text" value="0"/>		
Number of Probes Per Hop	<input type="text" value="3"/>		packets
Response Timeout	<input type="text" value="3"/>		seconds
First TTL Value	<input type="text" value="1"/>		
Max TTL Value	<input type="text" value="30"/>		
VID for Source Interface	<input type="text"/>		
IP Address for Source Interface	<input type="text"/>		
Use ICMP instead of UDP	<input type="checkbox"/>		
Print Numeric Addresses	<input type="checkbox"/>		

You can configure the following parameters for the test:

Table 96. Traceroute Parameters

Item	Description
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. <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> NOTE You may only specify either the VID or the IP Address for the source interface. </div>
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. <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> NOTE You may only specify either the VID or the IP Address for the source interface. </div>
Use ICMP instead of UDP	By default the traceroute command will use UDP. Selecting this option forces it to use ICMP ECHO packets instead.

Item	Description
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.

8. Maintenance

8.1. Rebooting the Switch

This function allows user to restart the device. Click on Restart from the menus. Restart device main screen, to do confirmation request. Click Yes, then the switch will restart immediately.

8.2. Factory Default

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

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



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.

8.3. Software

This page facilitates an update of the firmware controlling the switch. Click *Choose File*, select a software image on the computer 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.



IMPORTANT

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.

8.4. 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 memory 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.

This page is intentionally left blank.

This page is intentionally left blank.

This page is intentionally left blank.