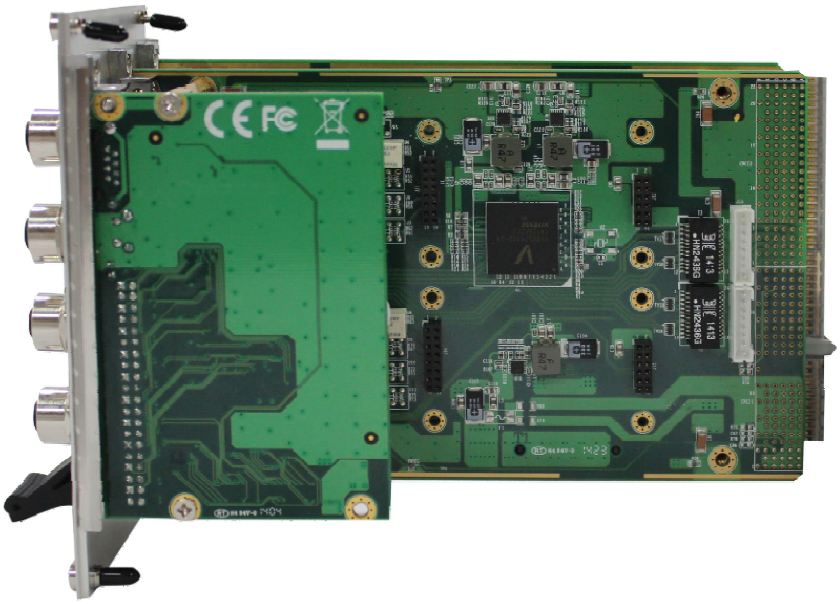


CPGS-9160-M12 Series

Industrial 3U CompactPCI Managed Gigabit Ethernet Switch

User Manual

Version 1.0

September, 2016

COPYRIGHT NOTICE

TRADEMARKS

ORing is a registered trademark of ORing Industrial Networking Corp.
All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

Product(s) associated with this publication complies/comply with all applicable regulations. Please refer to the Technical Specifications section for more details.

WARRANTY

ORing warrants that all ORing products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). ORing will repair or replace products found by ORing to be defective within this warranty period, with shipment expenses apportioned by ORing and the distributor. This warranty does not cover product modifications or repairs done by persons other than ORing-approved personnel, and this warranty does not apply to ORing products that are misused, abused, improperly installed, or damaged by accidents.
Please refer to the Technical Specifications section for the actual warranty period(s) of the product(s) associated with this publication.

DISCLAIMER

Information in this publication is intended to be accurate. ORing shall not be responsible for its use or infringements on third-parties as a result of its use. There may occasionally be unintentional errors on this publication. ORing reserves the right to revise the contents of this publication without notice.

CONTACT INFORMATION

ORing Industrial Networking Corp.
3F., NO.542-2.JhongJheng Rd, Sindian District , New Taipei City 23148, Taiwan, R.O.C.
Tel: + 886 2 2918 1066 // Fax: + 886 2 2918 2368
Website: www.oring-networking.com

Technical Support
E-mail: support@oring-networking.com

Sales Contact
E-mail: sales@oring-networking.com (Headquarters)
sales@oring-networking.com.cn (China)

Table of Content

Getting Started

1.1 About the CPGS-9160-M12

ORing's CPGS-9160-M12 is a compact Ethernet switch with a highly integrated 3U Compact PCI card form factor. Featuring 8x10/100/1000Base-T(X) in CompactPCI sockets and 8x10/100/1000Base-T(X) ports in M12 connectors, the switch is fully compliant with the EN50155 standard, and is ideal for harsh industrial applications, such as factory automation, vehicle, and railway applications. The M12 connectors make the card a perfect fit for rolling stock applications. With complete support for Ethernet redundancy protocols such as O-Ring (recovery time < 30ms over 250 units of connection) and MSTP (RSTP/STP compatible), the switch can protect your mission-critical applications from network interruptions or temporary malfunctions with its fast recovery technology. Featuring a wide operating temperature from -40°C to 70°C, the device can be managed centrally and conveniently via Open-Vision, web browsers, Telnet and console (CLI) configuration, making it one of the most reliable choices for power substation and rolling stock applications. Since the switch card is hot swappable, you do not need to turn off the system power during installation.

1.2 Software Features

- Supports MSTP/RSTP/STP (IEEE 802.1s/w/D) for Ethernet redundancy
- Supports standard IEC 62439-2 MRP (Media Redundancy Protocol) function
- Supports IPV6 new internet protocol version
- Support Modbus TCP protocol
- Supports IEEE 802.3az Energy-Efficient Ethernet technology
- Supports HTTPS/SSH protocols to enhance network security
- Supports SMTP client
- Supports IP-based bandwidth management
- Supports application-based QoS management
- Supports Device Binding security function
- Supports DOS/DDOS auto prevention
- Supports 9.6K Bytes Jumbo frame
- Supports multiple notifications for incidents
- IGMP v2/v3 (IGMP snooping support) for filtering multicast traffic
- Supports SNMP v1/v2c/v3 & RMON & 802.1Q VLAN network management
- Supports management via Web-based interfaces, Telnet, Console (CLI), and Windows utility (Open-Vision)
- Supports LLDP protocol

1.3 Hardware Features

- Features a 3U and 8HP CompactPCI form factor with hot swapping ability
- PICMG 2.0 compatible
- 8x10/100/1000Base-T(X) ports for connecting to other CompactPCI sockets and 8x10/100/1000Base-T(X) ports in M12 connectors
- 1 x console port (RJ-45)
- EN51055 compliance and M12 connectors for reliable operation against environmental disturbances
- Operating Temperature: -40 to 70ºC
- Storage Temperature: -40 to 85ºC
- Operating Humidity: 5% to 95%, non-condensing
- Dimensions: 81.7 (W) x 209 (D) x 130.7 (H)mm

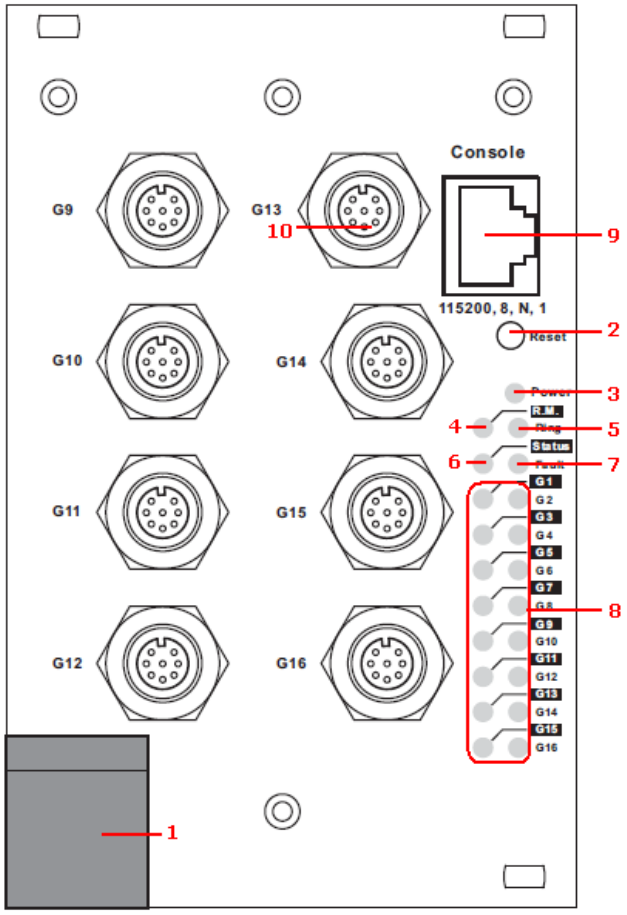
Hardware Overview

2.1 Front Panel

2.1.1 Ports and Connectors

The device provides the following ports on the front panel.

Port	Description
10/100/1000 Fast Ethernet ports	Six 10/100/1000 Base-T(X) Fast Ethernet ports supporting auto-negotiation. Default settings as below: Speed: auto Duplex: auto Flow control: disable
Console port	One console port for with RS-232 to RJ-45 connector
Reset button	
Ejection lever	



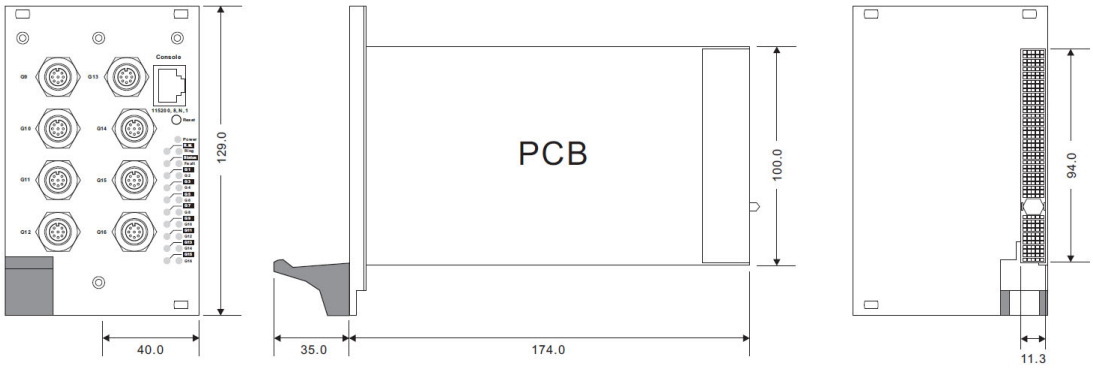
1. Ejection lever
2. Reset button
3. Power status LED
4. R.M. status LED
5. Ring status LED
6. System status LED
7. Fault LED
8. Port status LEDs
9. Console port
10. Ethernet ports

2.1.2 LEDs

LED	Color	Status	Description
Power	Green	On	Power is on
R.M	Green	On	Port is operated as Ring Master.
Ring	Green	On	Port is operated in Ring mode
Status	Green	On	Ethernet link is on
Fault	Amber	On	An error has occurred
10/100/1000Base-T(X) port			
LNK/ACT	Green	On	Port is linked
		Blinking	Transmitting data

Hardware Installation

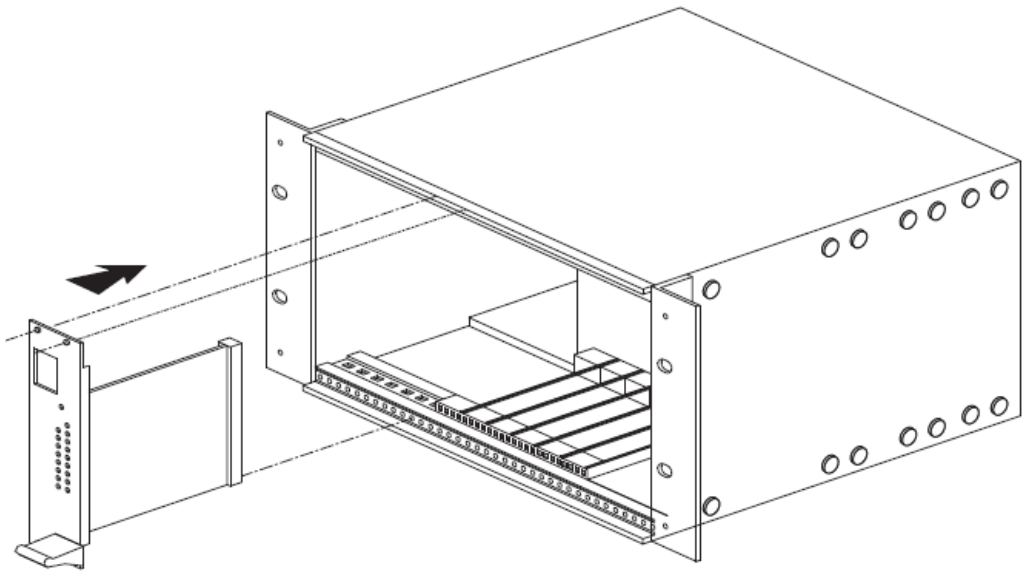
3.1 Installation



Measurement (Unit = mm)

Follow the steps below to install the card to the CPCI chassis.

1. Remove the metal cover plate on the back of an available CPCI slot.
2. Insert the card into the slot and use the bracket screws to secure it firmly in place.
3. Connect the card to the desired network devices.



ATTENTION

PCI Express cards, like all computer equipment, can be severely damaged by static electricity. Be sure that you are properly grounded before opening your computer case or touching your PCI Express card. It is recommended that you wear an anti-static strap when installing any computer component. If an anti-static strap is unavailable, discharge yourself of any static electricity build-up by touching a large grounded metal surface (such as the computer case) for several seconds.

Be careful to handle the PCI Express card by its edges and not the connectors or other components on the cards. Avoid rocking the card from side to side and or forcing the card into the slot. When the card is installed, pull on it gently to check it is properly connected.

Always shut down the computer before opening it to avoid damaging its internal components or the components you are installing. Do not open the computer or attempt to install items inside it while it is on.

Do not turn on the computer unless all of its internal and external parts are in place and it is closed. Operating the computer when it is open or missing parts can damage it or cause injury.

3.2 Connection

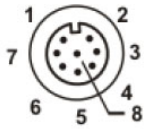
3.2.1 Cables

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

The device uses M12 or RJ45 connectors for network connection. Please refer to the following table for cable specifications.

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328 ft)	8-pin female M12 A-coding connector
100BASE-TX	Cat. 5 100-ohm UTP	UTP 100 m (328 ft)	8-pin female M12 A-coding connector
1000BASE-T	Cat. 5e, 6	UTP 100 m (328ft)	8-pin female M12 A-coding connector

M12/8P Pin Definition



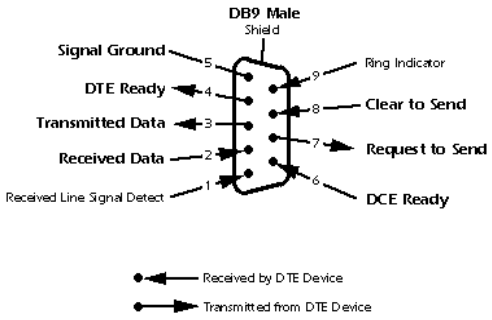
10/100Base-T(X)	
PIN No.	Description
#6	TD+
#4	TD-
#5	RD+
#8	RD-

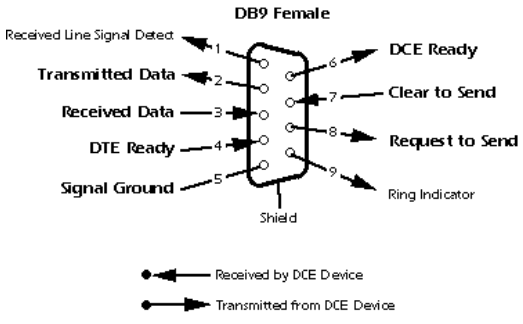
1000Base-T	
PIN No.	Description
#1	BI_DC+
#2	BI_DD+
#3	BI_DD-
#4	BI_DA-
#5	BI_DB+
#6	BI_DA+
#7	BI_DC-
#8	BI_DB-

RS-232 Console Port Wiring

The device can be managed via console ports using a RS-232 cable which can be found in the package. You can connect the port to a PC via the RS-232 cable with a DB-9 female connector. The DB-9 female connector of the RS-232 cable should be connected the PC while the other end of the cable (RJ-45 connector) should be connected to the console port of the switch.

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





Backplane Pin Definition

The device is equipped with eight Gigabit ports in CompactPCI sockets. The table below provides information of each pin on the backplane of the card. Please refer to the table for the pin assignment of each port.

25	GND	5V				5V	GND	
24	GND		5V				GND	
23	GND				5V		GND	
22	GND		GND				GND	
21	GND				GND		GND	
20	GND		GND				GND	
19	GND				GND		GND	
18	GND		GND				GND	
17	GND				GND		GND	
16	GND		GND				GND	
15	GND				GND		GND	
14	KEY AREA							J1
13								
12								
11	GND				GND		GND	
10	GND		GND				GND	
9	GND				GND		GND	
8	GND		GND				GND	
7	GND				GND		GND	
6	GND		GND				GND	
5	GND				GND		GND	
4	GND		HEALTHY#				GND	
3	GND				5V		GND	
2	GND		5V				GND	
1	GND	5V				5V	GND	
Pin	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	

22	GND		STxD	GND		SRxD	GND	
21	GND			GND			GND	
20	GND	LED5_0	LED5_1	GND	LED7_0	LED7_1	GND	
19	GND	LED4_0	LED4_1	GND	LED6_0	LED6_1	GND	
18	GND	LED1_0	LED1_1	GND	LED3_0	LED4_1	GND	J2
17	GND	LED0_0	LED0_1	GND	LED2_0	LED2_1	GND	
16	GND	P7_A_P	P7_A_N	GND	P7_C_P	P7_C_N	GND	
15	GND	P7_B_P	P7_B_N	GND	P7_D_P	P7_D_N	GND	
14	GND	P6_A_P	P6_A_N	GND	P6_C_P	P6_C_N	GND	

13	GND	P6_B_P	P6_B_N	GND	P6_D_P	P6_D_N	GND	
12	GND	P5_A_P	P5_A_N	GND	P5_C_P	P5_C_N	GND	
11	GND	P5_B_P	P5_B_N	GND	P5_D_P	P5_D_N	GND	
10	GND	P4_A_P	P4_A_N	GND	P4_C_P	P4_C_N	GND	
9	GND	P4_B_P	P4_B_N	GND	P4_D_P	P4_D_N	GND	
8	GND	P3_A_P	P3_A_N	GND	P3_C_P	P3_C_N	GND	
7	GND	P3_B_P	P3_B_N	GND	P3_D_P	P3_D_N	GND	
6	GND	P2_A_P	P2_A_N	GND	P2_C_P	P2_C_N	GND	
5	GND	P2_B_P	P2_B_N	GND	P2_D_P	P2_D_N	GND	
4	GND	P1_A_P	P1_A_N	GND	P1_C_P	P1_C_N	GND	
3	GND	P1_B_P	P1_B_N	GND	P1_D_P	P1_D_N	GND	
2	GND	P0_A_P	P0_A_N	GND	P0_C_P	P0_C_N	GND	
1	GND	P0_B_P	P0_B_N	GND	P0_D_P	P0_D_N	GND	
Pin	**Z**	**A**	**B**	**C**	**D**	**E**	**F**	

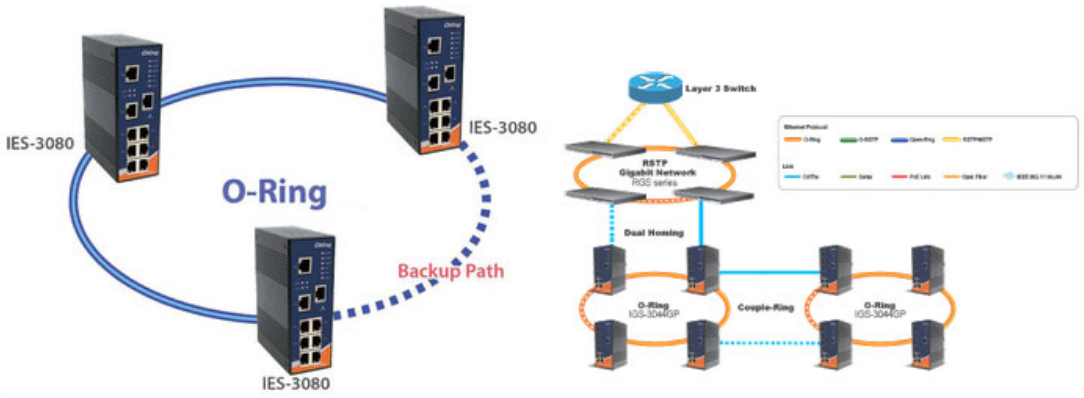
Redundancy

Redundancy for minimized system downtime is one of the most important concerns for industrial networking devices. Hence, ORing has developed proprietary redundancy technologies including O-Ring and Open-Ring featuring faster recovery time than existing redundancy technologies widely used in commercial applications, such as STP, RSTP, and MSTP. ORing's proprietary redundancy technologies not only support different networking topologies, but also assure the reliability of the network.

4.1 O-Ring

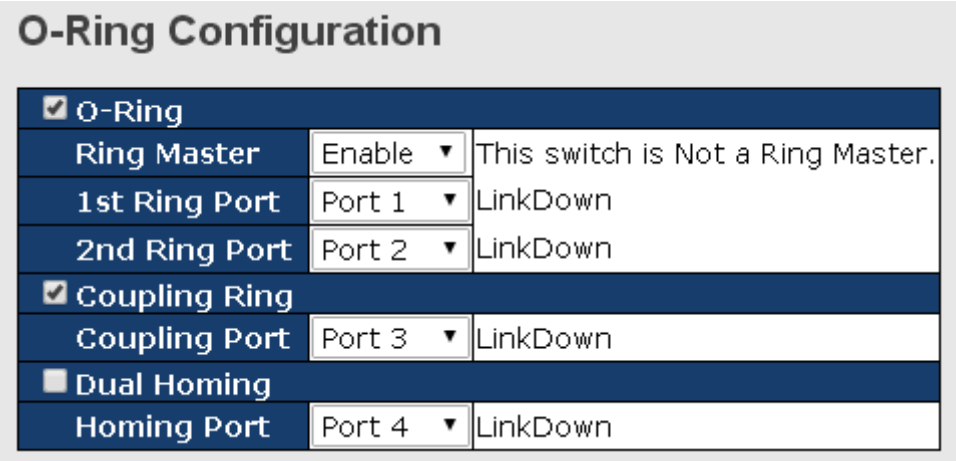
4.1.1 Introduction

O-Ring is ORing's proprietary redundant ring technology, with recovery time of less than 30 milliseconds (in full-duplex Gigabit operation) or 10 milliseconds (in full-duplex Fast Ethernet operation) and up to 250 nodes. The ring protocols identify one switch as the master of the network, and then automatically block packets from traveling through any of the network's redundant loops. In the event that one branch of the ring gets disconnected from the rest of the network, the protocol automatically readjusts the ring so that the part of the network that was disconnected can reestablish contact with the rest of the network. The O-Ring redundant ring technology can protect mission-critical applications from network interruptions or temporary malfunction with its fast recover technology.



4.1.2 Configurations

O-Ring supports three ring topologies: **Ring Master**, **Coupling Ring**, and **Dual Homing**. You can configure the settings in the interface below.



Label	Description
Redundant Ring	Check to enable O-Ring topology.
Ring Master	Only one ring master is allowed in a ring. However, if more than one switches are set to enable **Ring Master**, the switch with the lowest MAC address will be the active ring master and the others will be backup masters.
1st Ring Port	The primary port when the switch is ring master
2nd Ring Port	The backup port when the switch is ring master
Coupling Ring	Check to enable **Coupling Ring**. **Coupling Ring** can divide a big ring into two smaller rings to avoid network topology changes affecting all switches. It is a good method for connecting two rings.
Coupling Port	Ports for connecting multiple rings. A coupling ring needs four switches to build an active and a backup link. Links formed by the coupling ports will run in active/backup mode.
Dual Homing	Check to enable **Dual Homing**. When **Dual Homing** is enabled, the ring will be connected to normal switches through two RSTP links (ex: backbone Switch). The two links work in active/backup mode, and connect each ring to the normal switches in RSTP mode.
Apply	Click to apply the configurations.

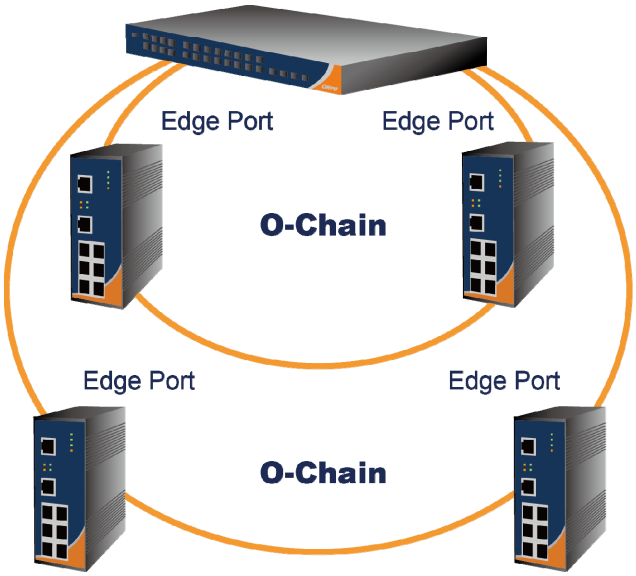
Note: due to heavy computing loading, setting one switch as ring master and coupling ring at the same time is not recommended.

4.2 O-Chain

4.2.1 Introduction

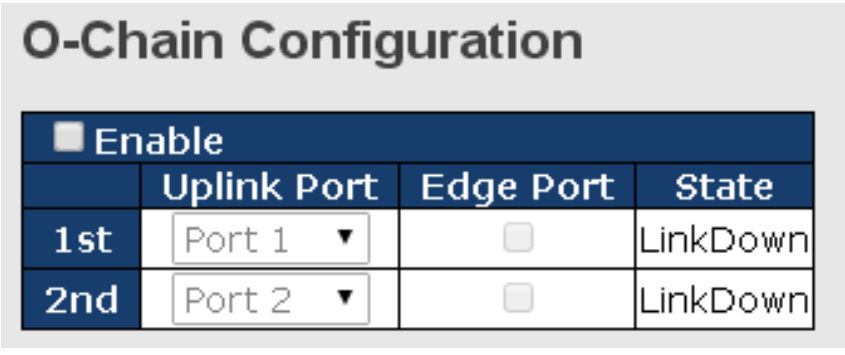
O-Chain is ORing's revolutionary network redundancy technology which enhances network redundancy for any backbone networks, providing ease-of-use and maximum fault-recovery swiftness, flexibility, compatibility, and cost-effectiveness in a set of network redundancy topologies. The self-healing Ethernet technology designed for distributed and complex industrial networks enables the network to recover in less than 30 milliseconds (in full-duplex Gigabit operation) or 10 milliseconds (in full-duplex Fast Ethernet operation) for up to 250 switches if at any time a segment of the chain fails.

O-Chain allows multiple redundant rings of different redundancy protocols to join and function together as a large and the most robust network topologies. It can create multiple redundant networks beyond the limitations of current redundant ring technologies.



4.2.2 Configurations

O-Chain is very easy to configure and manage. Only one edge port of the edge switch needs to be defined. Other switches beside them just need to have O-Chain enabled.

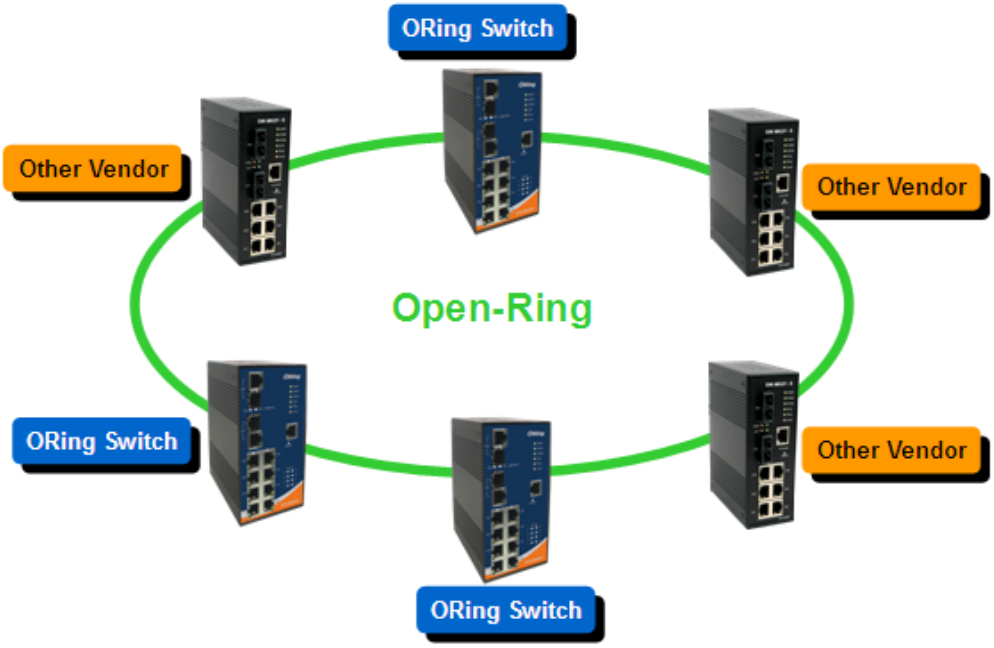


Label	Description
Enable	Check to enable O-Chain function
1st Ring Port	The first port connecting to the ring
2nd Ring Port	The second port connecting to the ring
Edge Port	An O-Chain topology must begin with edge ports. The ports with a smaller switch MAC address will serve as the backup link and RM LED will light up.

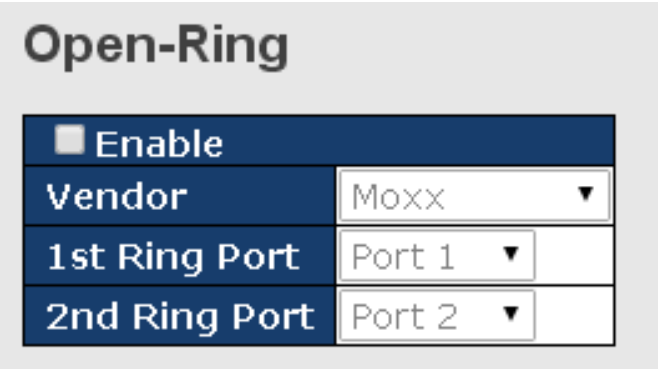
4.3 Open-Ring

4.3.1 Introduction

Open-Ring is a technology developed by ORing to enhance ORing switches' interoperability with other vendors' products. With this technology, you can add any ORing switches to the network based on other ring technologies.



4.3.2 Configurations



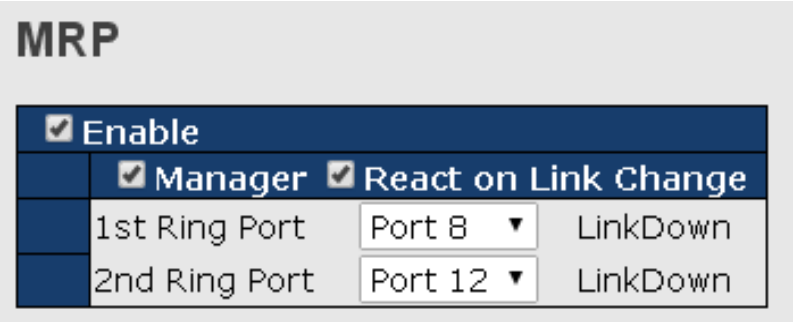
Label	Description
Enable	Check to enable Open-Ring topology
Vendor	Choose the venders that you want to join in their rings
1st Ring Port	The first port to connect to the ring
2nd Ring Port	The second port to connect to the ring

4.3 MRP

4.3.1 Introduction

MRP (Media Redundancy Protocol) is an industry standard for high-availability Ethernet networks. MRP allowing Ethernet switches in ring configuration to recover from failure rapidly to ensure seamless data transmission. A MRP ring (IEC 62439) can support up to 50 devices and will enable a back-up link in 80ms (adjustable to max. 200ms/500ms).

4.3.2 Configurations



Label	Description
Enable	Enables the MRP function
Manager	Every MRP topology needs a MRP manager. One MRP topology can only have a Manager. If two or more switches are set to be Manager, the MRP topology will fail.
React on Link Change (Advanced mode)	Faster mode. Enabling this function will cause MRP topology to converge more rapidly. This function only can be set in MRP manager switch.
1st Ring Port	Chooses the port which connects to the MRP ring
2nd Ring Port	Chooses the port which connects to the MRP ring

4.4 MSTP

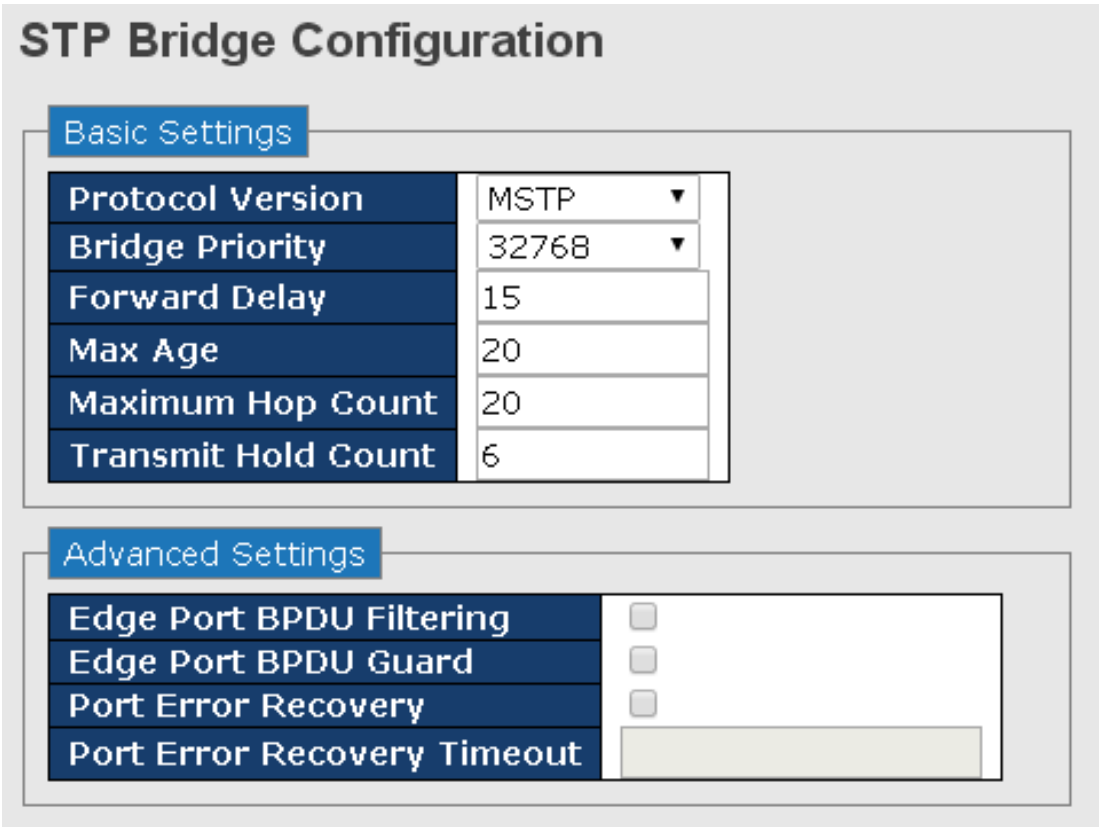
STP (Spanning Tree Protocol), and its advanced versions RSTP (Rapid Spanning Tree

Protocol) and MSTP (Multiple Spanning Tree Protocol), are designed to prevent network loops and provide network redundancy. Network loops occur frequently in large networks as when two or more paths run to the same destination, broadcast packets may get in to an infinite loop and hence causing congestion in the network. STP can identify the best path to the destination, and block all other paths. The blocked links will stay connected but inactive. When the best path fails, the blocked links will be activated. Compared to STP which recovers a link in 30 to 50 seconds, RSTP can shorten the time to 5 to 6 seconds.

Since the recovery time of STP and RSTP takes seconds, which is unacceptable in some industrial applications, MSTP was developed. The technology supports multiple spanning trees within a network by grouping and mapping multiple VLANs into different spanning-tree instances, known as MSTIs, to form individual MST regions. Each switch is assigned to an MST region. Hence, each MST region consists of one or more MSTP switches with the same VLANs, at least one MST instance, and the same MST region name. Therefore, switches can use different paths in the network to effectively balance loads.

4.4.1 Bridge Status

This page shows the status for all STP bridge instance.



Label	Description
Protocol Version	Select Spanning Tree type , support STP / RSTP / MSTP
Bridge Priority	A value used to identify the root bridge. The bridge with the lowest value has the highest priority and is selected as the root. If the value changes, you must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule
Forwarding Delay	The time of a port waits before changing from RSTP learning and listening states to forwarding state. The valid value is between 4 through 30.
Max Age	The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. The valid value is between 6 and 40.
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 of 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.
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).

NOTE: the calculation of the MAX Age, Hello Time, and Forward Delay Time is as follows:

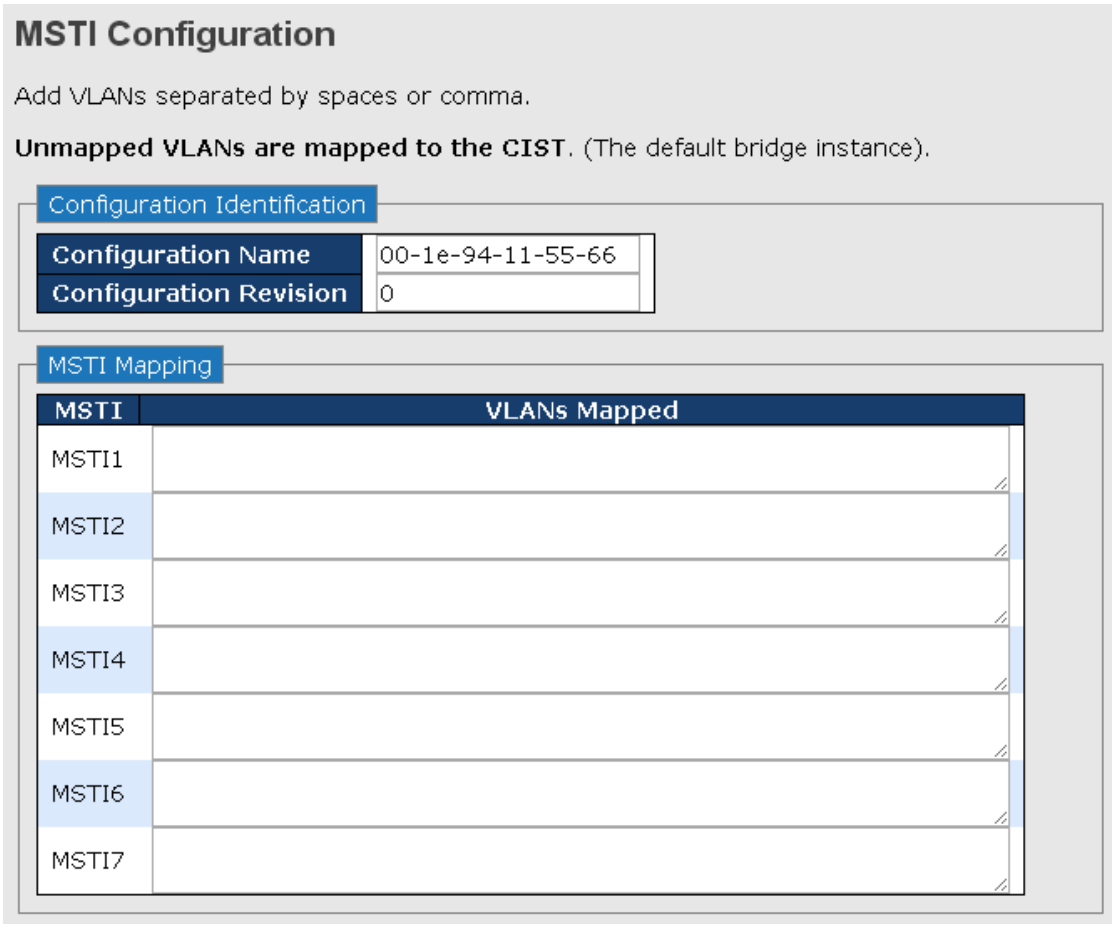
2 x (Forward Delay Time value –1) > = Max Age value >= 2 x (Hello Time value +1)

4.4.1 MSTI Mapping

This page allows you to examine and adjust the configuration of STP MSTI. This function will

map VLANs to a specific MSTP instance. .

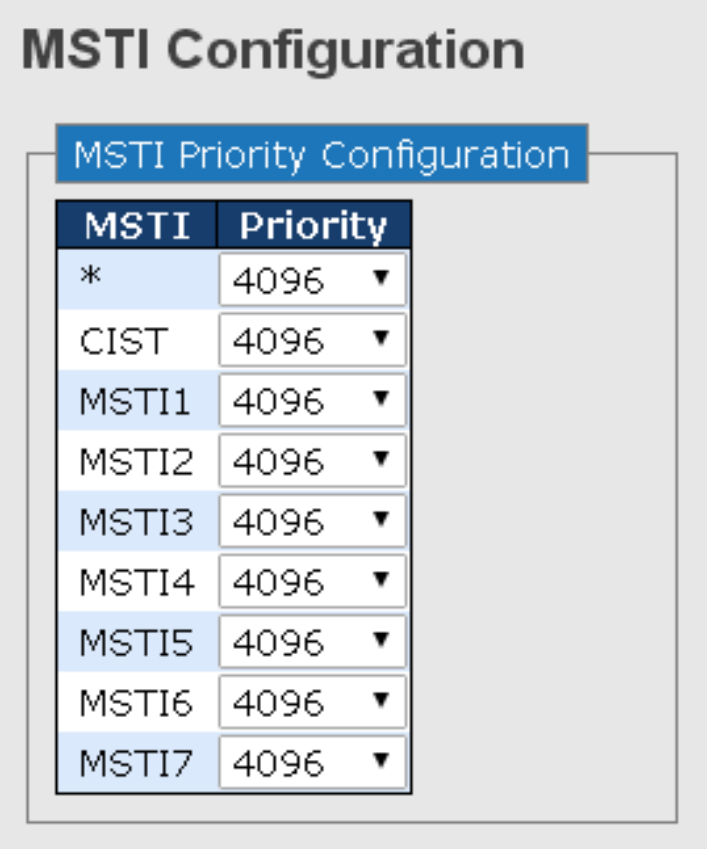
This page allows you to examine and adjust the configuration of STP MSTI. This function will map VLANs to a specific MSTP instance. .



Label	Description
Configuration Name	The name for this MSTI. Maximum characters allowed are 32. The default name is the switch's MAC address.
Configuration Revision	The revision for this MSTI.
MSTI 1-7	Instance identifier to configure. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. (Range: 1-7)
VLANs Mapped	VLANs to assign to this MST instance. Note that the VLANs must be separated with comma and/or space and one VLAN can only be mapped to one MSTI. (Range: 1-4094)

4.1.2 MSTI Priorities

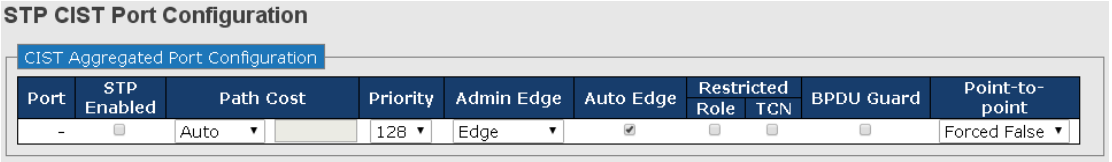
You can configure the bridge priority for the CIST and any configured MSTI. Remember that RSTP will look up each MST Instance as a single bridge node.

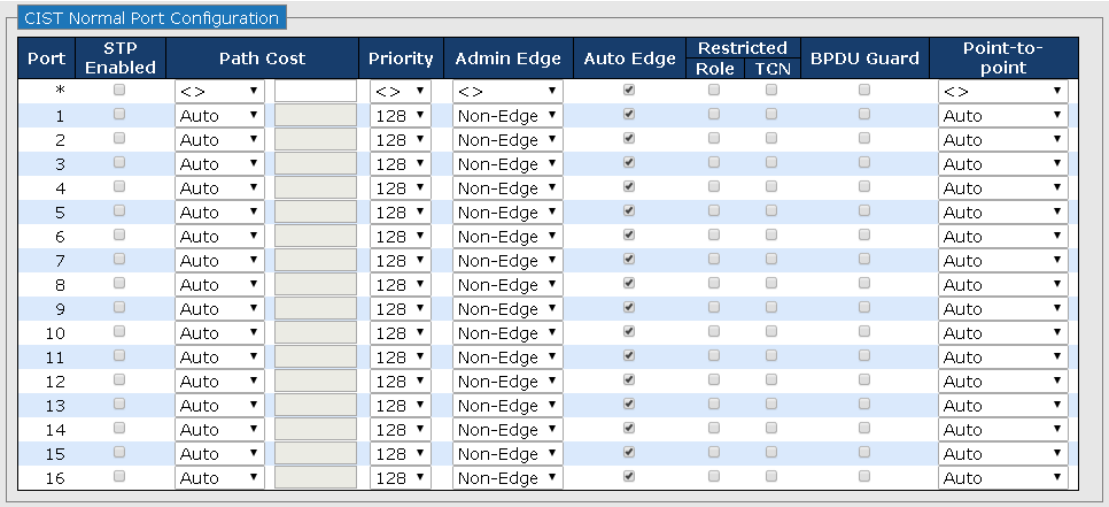


Label	Description
MSTI	Instance identifier to configure.
Priority	The priority of a spanning tree instance.

4.1.3 CIST Ports

This page allows you to configure CIST ports including physical and aggregated ports.





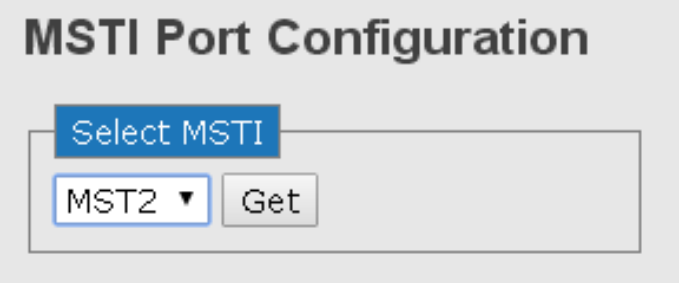
Label	Description
Port	The port identifier
STP Enabled	Check to enable STP Function
Path Cost	This parameter allows you to control the path cost for each port. **Auto** will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. **Specific** will allow you to enter a user-defined value.
Path Cost Value (1-200000000)	If you choose Specific from the drop-down list, you can specify a value ranging from 1 to 200000000. As STA determines the best path between devices based on path cost, lower values are suggested for ports attached to faster media, and higher values for ports with slower media.
Priority	Specify the priority for a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (usually with the lowest value) will be used as an active link in the Spanning Tree. In this way, a port with higher priority is less likely to be blocked if the Spanning Tree Algorithm discovers network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
Admin Edge	When an interface is attached to a LAN segment at the end of a bridged LAN or to an end node, you can enable this function so forwarding loops can pass directly through to the spanning tree forwarding state. Since end nodes cannot cause forwarding loops, enabling this function allows for quicker convergence for

	devices such as workstations or servers. The current forwarding database will be retained to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events. The spanning tree will not initiate reconfiguration when the interface changes state. It also overcomes other STA-related timeout problems. Keep in mind that this feature should only be used for ports connected to an end node device.
Auto Edge	Check to enable automatic edge detection on a bridge port. The bridge will then determine that a port is at the edge of the network if no BPDU's are received on the port.
Restricted – Role	Enabling this function will prevent the port from being selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. This port will be selected as an Alternate Port after the Root Port has been selected. The function can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
Restricted -TCN	Enabling this function will prevent the port from propagating received topology change notifications and topology changes to other ports. The function 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, the port will disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not affect this setting.
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.

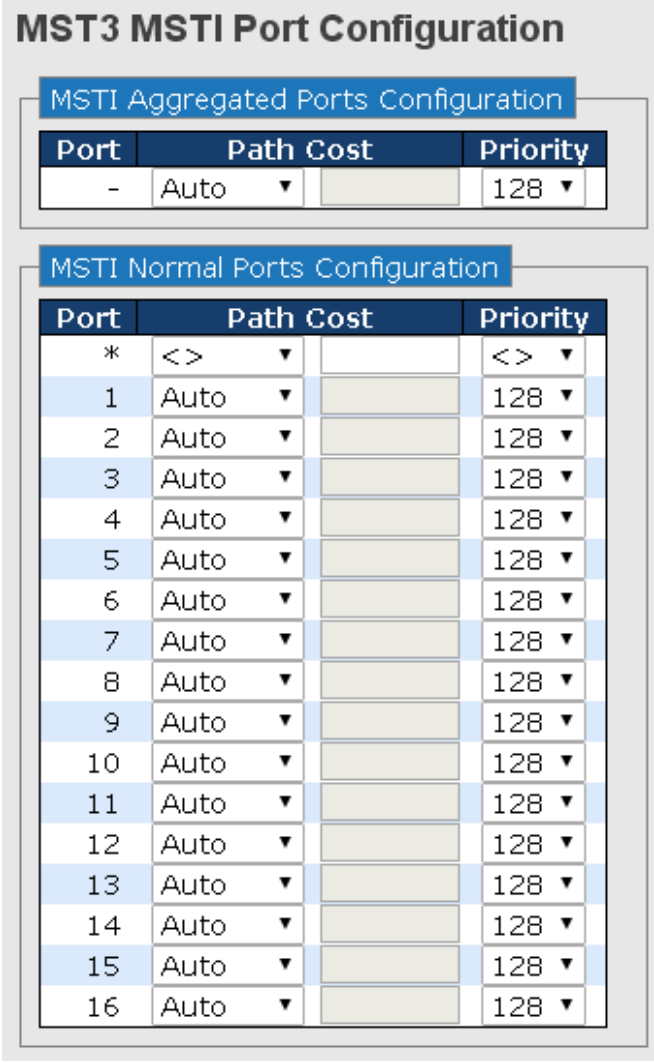
Save	Click to save the configurations.

4.1.4 MSTI Ports

This page allows you to configure STA attributes for interfaces in a specific MSTI, including path cost, and port priority. You may use a different priority or path cost for ports of the same media type to indicate the preferred path.



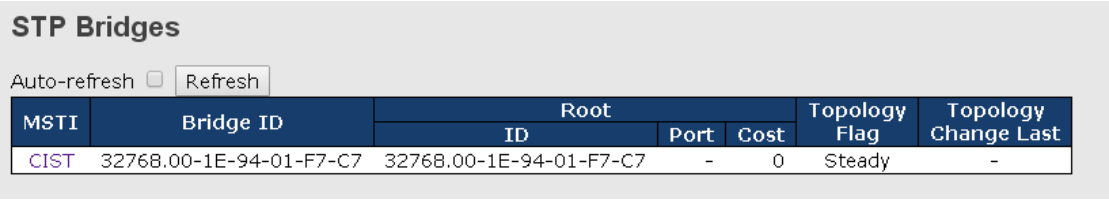
Choose a MSTI and click on **Get** will bring you to the following page.



Label	Description
Port	The port identifier
Path Cost	As this parameter is used by the STA to determine the best path between devices, lower values are suggested for ports attached to faster media, and higher values for ports with slower media. (Path cost takes precedence over port priority.) The value will control the path cost incurred by the port. Auto will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Specific will allow you to enter a user-defined value.
Priority	Specify the priority for a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (usually with the lowest value) will be used as an active link in the Spanning Tree. In this way, a port with higher priority is less likely to be blocked if the Spanning Tree Algorithm discovers network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

4.1.5 Bridge Status

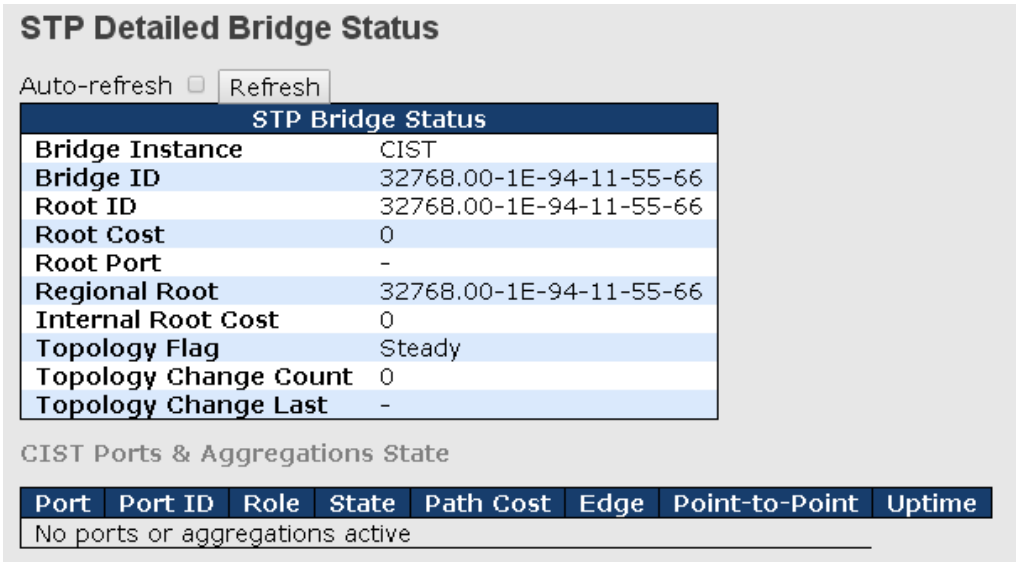
This page will show STA information on the global bridge such as the switch and individual ports.



Label	Description
MSTI	Indicates the bridge instance.
Bridge ID	A unique identifier for this bridge, consisting of the bridge priority, and MAC address (where the address is taken from the switch system).
Root	Root ID: A unique identifier of the device in the Spanning Tree that this switch has been accepted as the root device, consisting of the priority and MAC address. Root Port: the number of the port on this switch that is

	closest to the root. This switch communicates with the root device through this port. If no root port is designated, it means this switch has been accepted as the root device of the Spanning Tree network. Root Cost: the path cost from the root port on this switch to the root device. The cost for the root bridge zero. For all other bridges, it is the sum of the port path costs on the least cost path to the root bridge.
Technology Flag	The current state of the Topology Change Notification flag (TCN) for this bridge instance.
Technology Change Last	Time since the Spanning Tree was last reconfigured.

Click on CIST will bring out the following information window. Regional Root is the bridge ID of the designated regional root bridge, inside the MSTP region of this bridge. Internal Root Path is the path cost regional root path cost. The cost for the Regional Root Bridge is zero, and 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. Note that these parameters only apply to the CIST instance.

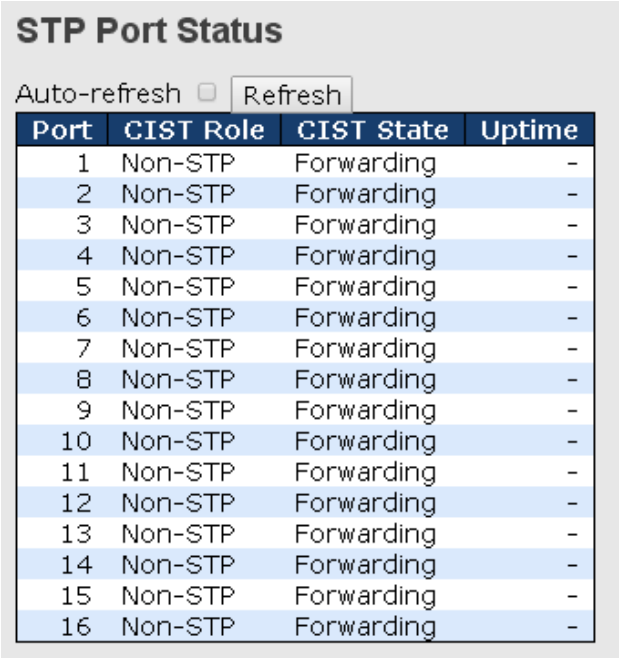


Label	Description
Port	The port identifier.
Port ID	The port identifier used by the RSTP protocol, consisting of the priority and the logical port index of the bridge port.
Role	The role of a port is assigned based on whether it is part of

	the active topology connecting the bridge to the root bridge (i.e., root port), connecting a LAN through the bridge to the root bridge (i.e., designated port); or is an alternate or backup port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed.
State	Displays the current state of this port in the Spanning Tree
Path Cost	The path cost of the port contributed to the paths towards the spanning tree root which include this port. It can be a value assigned by the **Auto** setting or any explicitly configured value.
Edge	The current RSTP 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 transitions directly to the Forwarding Port State, since there is no possibility of it participating in a loop.
Point-to-Point	Indicates a connection to exactly one other bridge. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transition RSTP states.
Uptime	The time since the bridge port was last initialized.

4.1.6 Port Status

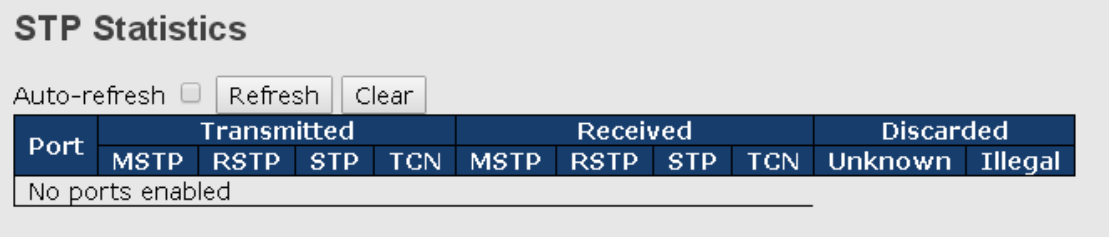
This page shows the STA functional status of participating ports.



Label	Description
Port	The port identifier.
CIST Role	The role of a port is assigned based on whether it is part of the active topology connecting the bridge to the root bridge (i.e., root port), connecting a LAN through the bridge to the root bridge (i.e., designated port); or is an alternate or backup port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed.
CIST State	Displays the current state of this port in the Spanning Tree. There are three states. **Blocking**: the port will receive STA configuration messages, but will not forward packets. **Learning**: The port transmits configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. The port address table will be cleared, and the port will learn addresses. **Forwarding**: The port will forward packets while learning addresses.
Uptime	The time since the bridge port was last initialized.

4.1.7 Port Statistics

This page shows statistics on spanning tree protocol packets crossing each port.

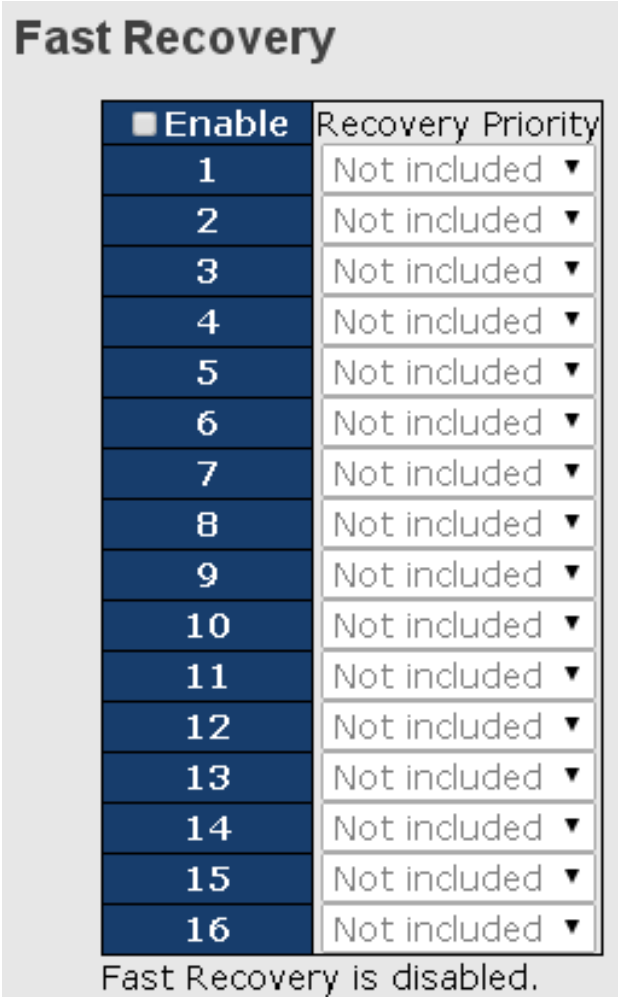


Label	Description
Port	The port identifier.
Transmitted/Received	MSTP: the number of MSTP Configuration BPDUs received/ transmitted on a port. RSTP: the number of RSTP Configuration BPDUs received/ transmitted on a port. RTP: the number of legacy STP Configuration BPDU's received/ transmitted on a port. TCN: the number of (legacy) Topology Change Notification

	BPDUs received/transmitted on a port.
Discarded	Unknown: the number of unknown Spanning Tree BPDUs received (and discarded) on a port. Illegal: the number of illegal Spanning Tree BPDUs received (and discarded) on a port.

4.2 Fast Recovery

Fast recovery mode can be set to connect multiple ports to one or more switches, thereby providing redundant links. Fast recovery mode supports 5 priorities. Only the first priority will be the active port, and the other ports with different priorities will be backup ports.



Label	Description
Enable	Activate fast recovery mode
Recovery Priority	Specify the recovery priority for each port.
Save	Click to save the configurations.

Management

The switch can be controlled via a built-in web server which supports Internet Explorer (Internet Explorer 5.0 or above versions) and other Web browsers such as Chrome. Therefore, you can manage and configure the switch easily and remotely. You can also upgrade firmware via a Web browser. The Web management function not only reduces network bandwidth consumption, but also enhances access speed and provides a user-friendly viewing screen.

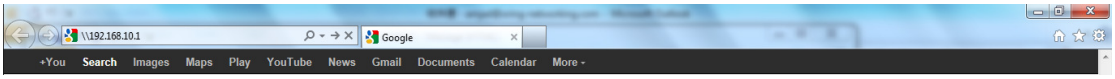
Note: By default, IE5.0 or later version do not allow Java applets to open sockets. You need to modify the browser setting separately in order to enable Java applets for network ports.

Management via Web Browser

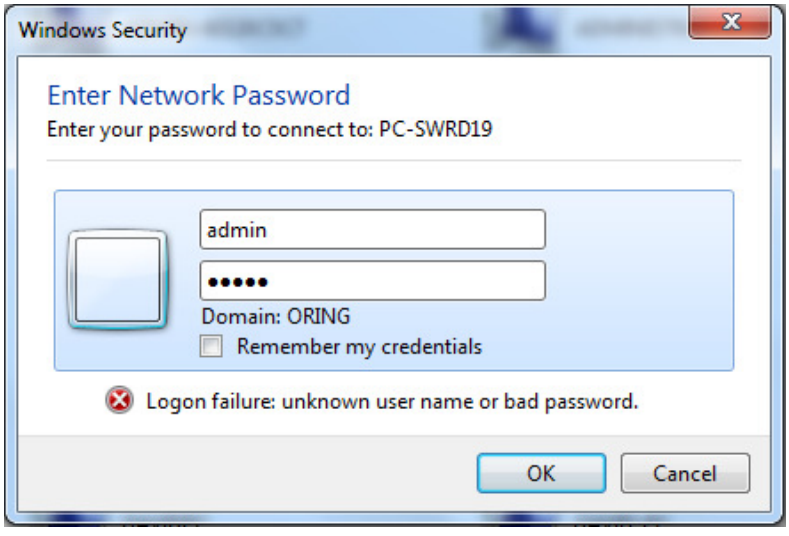
Follow the steps below to manage your switch via a Web browser

System Login

1. Launch an Internet Explorer.
2. Type http:// and the IP address of the switch. Press **Enter**.



3. A login screen appears.
4. Type in the username and password. The default username and password is **admin**.
5. Press **Enter** or click **OK**, the management page appears.



Note: you can use the following default values:

IP Address: **192.168.10.1**

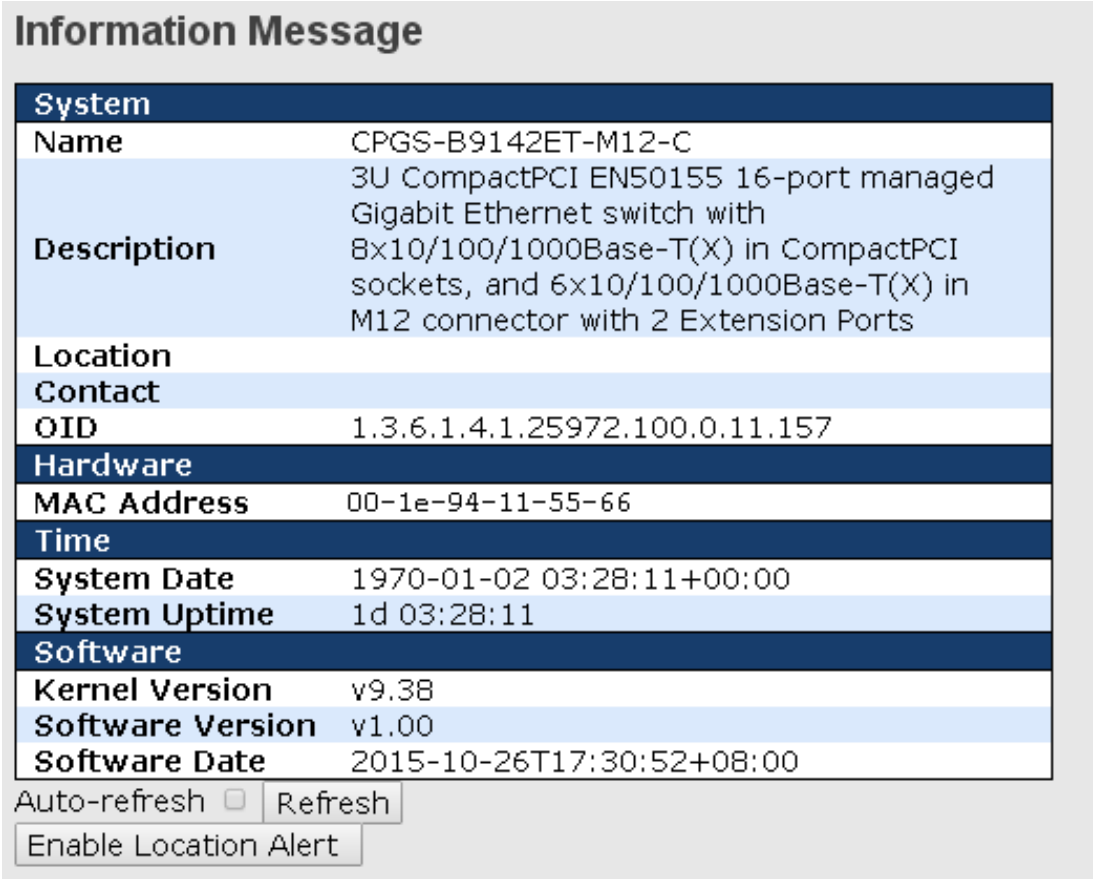
Subnet Mask: **255.255.255.0**

Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

After logging in, you will see the information of the switch as below.



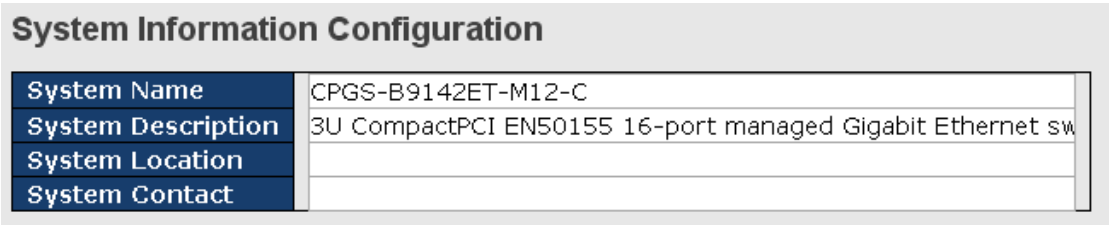
On the left hand side of the management interface shows links to various settings. Clicking on the links will bring you to individual configuration pages.

5.1 Basic Settings

The Basic Settings page allows you to configure the basic functions of the switch.

5.1.1 System Information

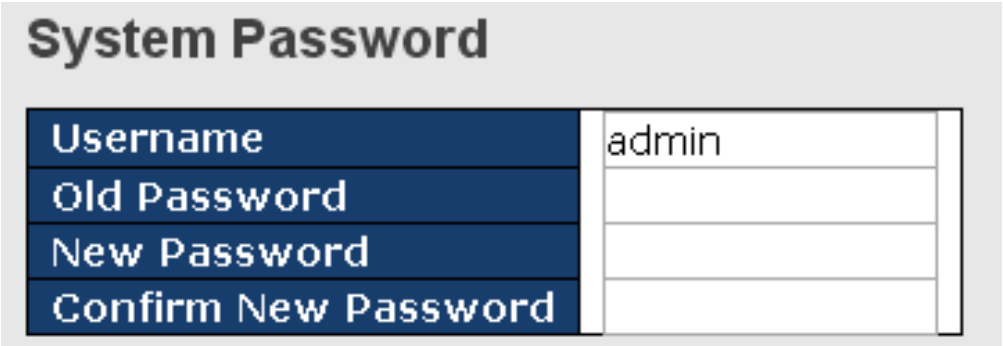
This page shows the general information of the switch.



Label	Description
System Name	An administratively assigned name for the managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string consisting of alphabets (A-Z, a-z), digits (0-9), and minus sign (-). Space is not allowed to be part of the 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 Description	Description of the device
System Location	The physical location of the node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and only ASCII characters from 32 to 126 are allowed.
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and only ASCII characters from 32 to 126 are allowed.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.2 Admin & Password

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

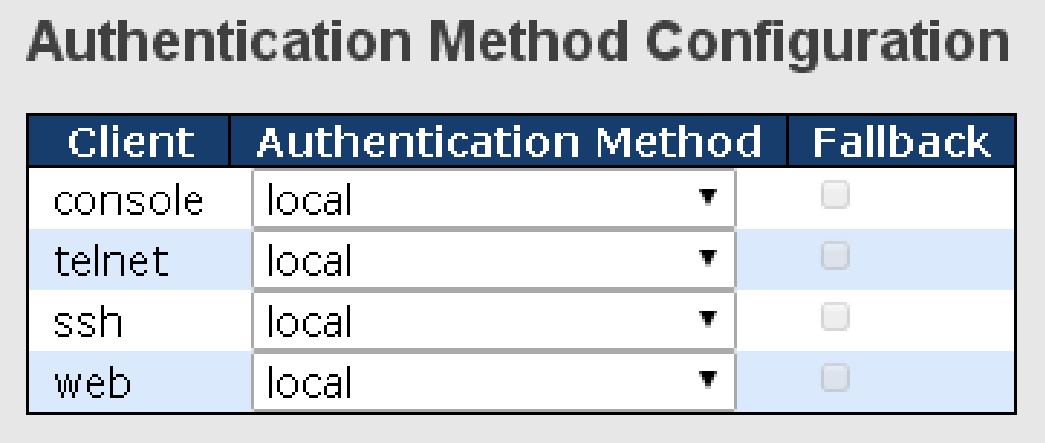


Label	Description
Username	Type the username you want to use to log in.
Old Password	The existing password. If this is incorrect, you cannot set the new password.
New Password	The new system password. The allowed string length is 0 to 31,

	and only ASCII characters from 32 to 126 are allowed.
Confirm password	Re-type the new password.

5.1.3 Authentication

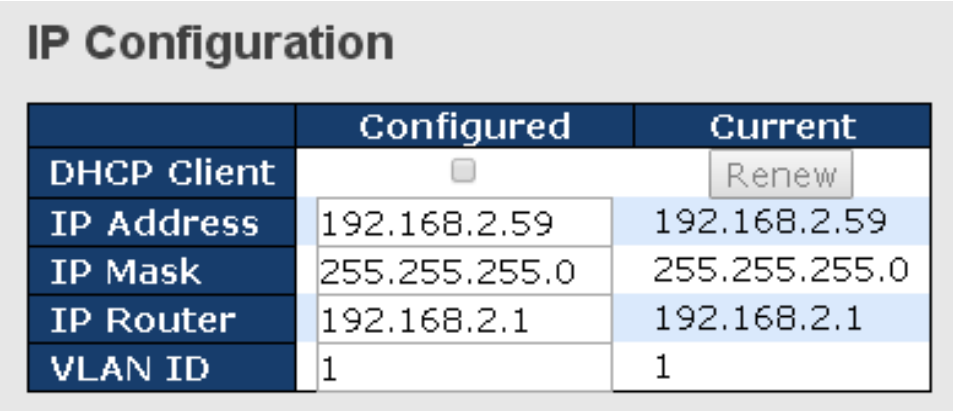
This page allows you to configure how a user is authenticated when he/she logs into the switch via one of the management interfaces.



Label	Description
Client	The management client for which the configuration below applies.
Authentication Method	Authentication Method can be set to one of the following values: **None**: authentication is disabled and login is not possible. **Local**: local user database on the switch is used for authentication. **Radius**: a remote RADIUS server is used for authentication.
Fallback	Check to enable fallback to local authentication. If none of the configured authentication servers are active, the local user database is used for authentication. This is only possible if authentication method is set to a value other than **none** or **local**.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.4 IP Settings

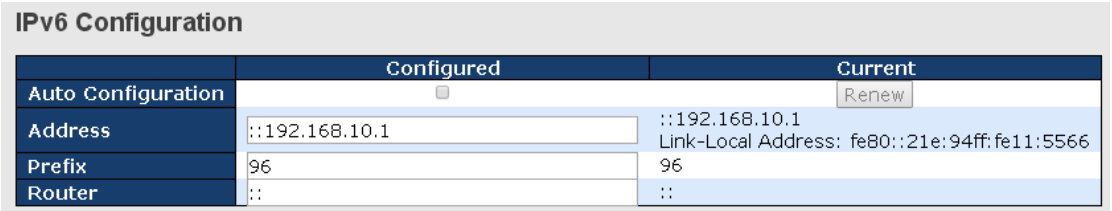
This page allows you to configure IP information for the switch. You can specify and configure the settings manually by disabling DHCP Client. After inputting the values, click **Renew** and the new values will be applied, which will be displayed under **Current**.



Label	Description
DHCP Client	Enable the DHCP client by checking this box. If DHCP fails or the configured IP address is zero, DHCP will retry. If DHCP retry fails, DHCP will stop trying and the configured IP settings will be used.
IP Address	Assigns an IP address to be used by the switch. If DHCP client function is enabled, you do not need to assign the IP address. The network DHCP server will assign an IP address to the switch and it will be displayed in this column. The default IP is **192.168.10.1**.
IP Mask	Assigns the subnet mask of the IP address. If DHCP client function is enabled, you do not need to assign the subnet mask.
IP Router	Assigns the network gateway for the switch. The default gateway is **192.168.10.254**.
VLAN ID	Provides the managed VLAN ID. The allowed range is 1 through 4095.

5.1.5 IPv6 Settings

IPv6 is the next-generation IP that uses a 128-bit address standard. It is developed to supplement, and eventually replace the IPv4 protocol. You can configure IPv6 information of the switch on the following page.

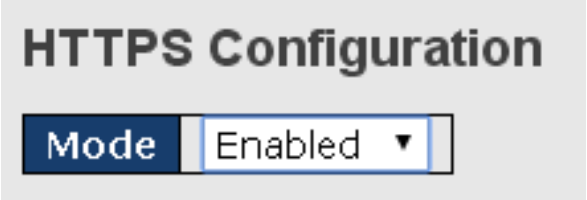


Label	Description
Auto Configuration	Check to enable IPv6 auto-configuration. If the system cannot

	obtain the stateless address in time, the configured IPv6 settings will be used. The router may delay responding to a router solicitation for a few seconds; therefore, the total time needed to complete auto-configuration may be much longer.
Address	Specify an IPv6 address for the switch. IPv6 address consists of 128 bits represented as eight groups of four hexadecimal digits with a colon separating each field (:). For example, in 'fe80::215:c5ff:fe03:4dc7', the symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
Prefix	Specify an IPv6 prefix for the switch. The allowed range is 1 to 128.
Router	Specify an IPv6 address for the switch. IPv6 address consists of 128 bits represented as eight groups of four hexadecimal digits with a colon separating each field (:). For example, in 'fe80::215:c5ff:fe03:4dc7', the symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

5.1.6 HTTPS

You can configure the HTTPS mode in the following page.



Label	Description
Mode	Indicates the selected HTTPS mode. When the current connection is HTTPS, disabling HTTPS will automatically redirect web browser to an HTTP connection. The modes include: **Enabled**: enable HTTPS. **Disabled**: disable HTTPS.
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously

	saved values.

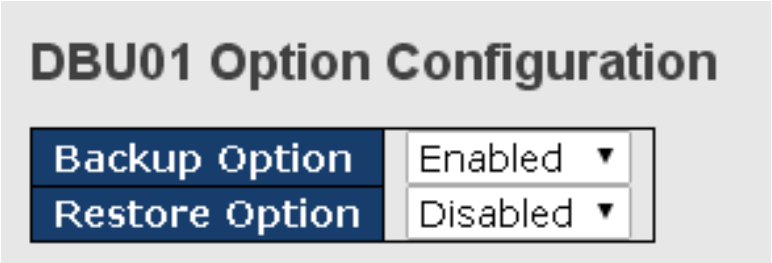
5.1.7 SSH

SSH (Secure Shell) is a cryptographic network protocol intended for secure data transmission and remote access by creating a secure channel between two networked PCs. You can configure the SSH mode in the following page.

Label	Description
Mode	Indicates the selected SSH mode. The modes include: **Enabled**: enable SSH. **Disabled**: disable SSH.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.8 DBU01 Configuration

DBU01 is an embedded configuration backup/restore function. It allows you to store and restore device configurations without using a PC.

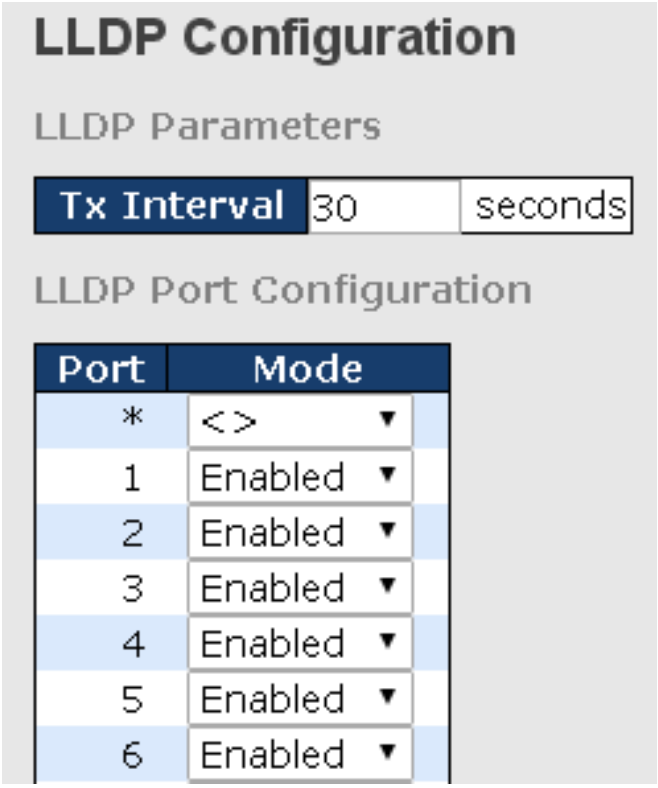


Label	Description
Backup Option	Enable or disable backup function. If enabled, existing configurations will be stored as a backup file.
Restore Option	Enable or disable backup function. If enabled, the system will apply saved configurations to the device.

5.1.9 LLDP

LLDP (Link Layer Discovery Protocol) provides a method for networked devices to receive

and/or transmit their information to other connected devices on the network that are also using the protocols, and to store the information that is learned about other devices. This page allows you to examine and configure current LLDP port settings.

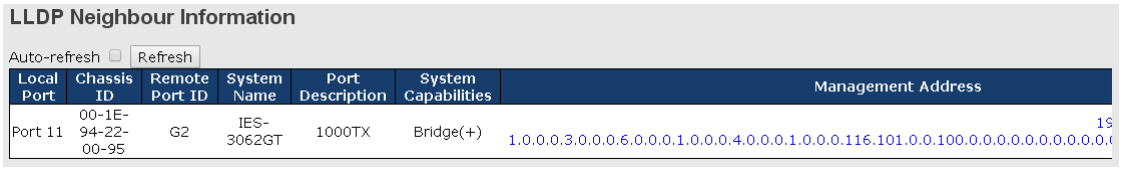


Label	Description
Port	The switch port number to which the following settings will be applied.
Mode	Indicates the selected LLDP mode. **Rx only**: the switch will not send out LLDP information, but LLDP information from its neighbors will be analyzed. **Tx only**: the switch will drop LLDP information received from its neighbors, but will send out LLDP information. **Disabled**: the switch will not send out LLDP information, and will drop LLDP information received from its neighbors. **Enabled**: the switch will send out LLDP information, and will analyze LLDP information received from its neighbors.

LLDP Neighbor Information

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

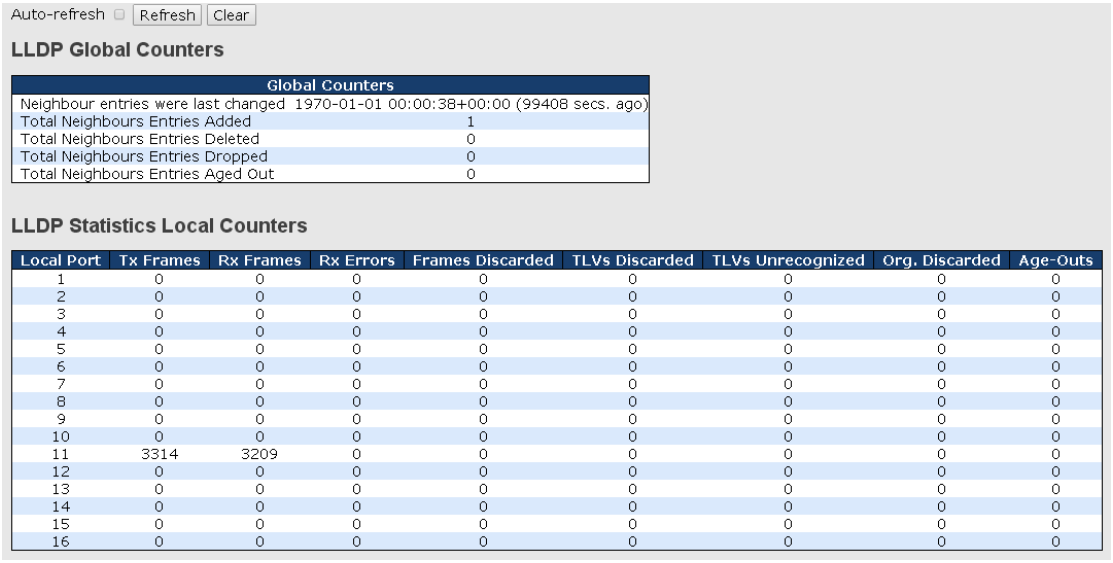
following information:



Label	Description
Local Port	The port that you use to transmits and receives LLDP frames.
Chassis ID	The identification number of the neighbor sending out the LLDP frames.
Remote Port ID	The identification of the neighbor port.
System Name	The name advertised by the neighbor.
Port Description	The description of the port advertised by the neighbor.
System Capabilities	Description of the neighbor's capabilities. The capabilities include: 1. **Other** 2. **Repeater** 3. **Bridge** 4. **WLAN Access Point** 5. **Router** 6. **Telephone** 7. **DOCSIS Cable Device** 8. **Station Only** 9. **Reserved** When a capability is enabled, a (+) will be displayed. If the capability is disabled, a (-) will be displayed.
Management Address	The neighbor's address which can be used to help network management. This may contain the neighbor's IP address.

LLDP Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters will apply settings to the whole switch stack, while local counters will apply settings to specified switches.



Global Counters

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

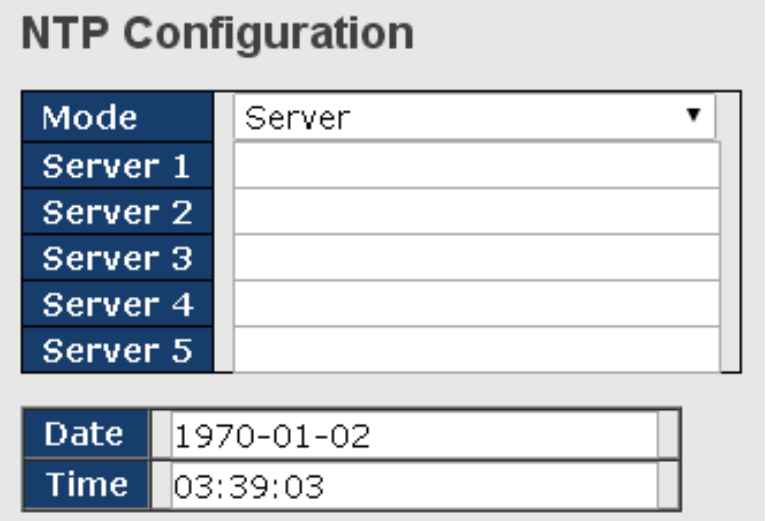
Local Counters

Label	Description
Local Port	The port that receives or transmits LLDP frames.
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.
Rx Errors	The number of received LLDP frames containing errors.
Frames Discarded	If a port receives an LLDP frame, and the switch's internal table is full, the LLDP frame will be counted and discarded. This situation is known as "too many neighbors" in the LLDP standard. LLDP frames require a new entry in the table if Chassis ID or Remote Port ID is not included in the table. Entries are removed from the

	table when a given port links down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (Type Length Value). If a TLV is malformed, it will be counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.
Org. Discarded	The number of organizationally TLVs received.
Age-Outs	Each LLDP frame contains information about how long the LLDP information is valid (age-out time). If no new LLDP frame is received during the age-out time, the LLDP information will be removed, and the value of the age-out counter will be incremented.
Refresh	Click to refresh the page immediately.
Clear	Click to clear the local counters. All counters (including global counters) are cleared upon reboot.
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals.

5.1.10 NTP

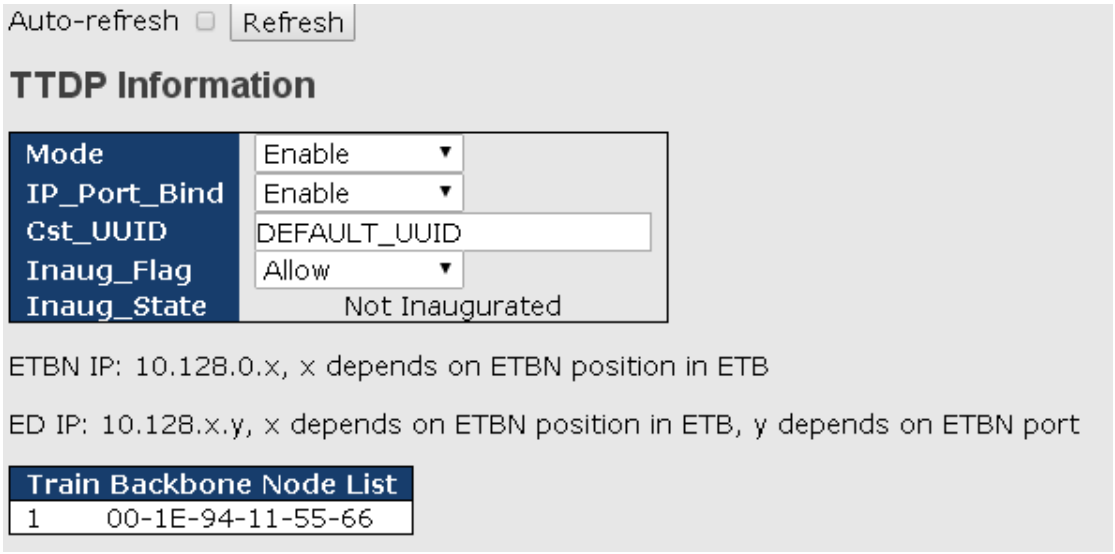
The function allows you to specify the Network Time Protocol (NTP) servers to query for the current time to maintain an accurate time on the switch, ensuring the system log record meaningful dates and times for event entries. With NTP, the switch can set its internal clock periodically according to an NTP time server. Otherwise, the switch will only record the time from the factory default set at the last boot-up. When the NTP client is enabled, the switch regularly sends a request for a time update to a configured time server. A maximum of five time servers are supported. The switch will attempt to poll each server in the configured sequence.



Label	Description
Mode	Select a mode from the drop-down list or disable either mode by selecting Disable. Disabling the NTP server or client mode will not remove the configurations.
Server 1-4	Sets the IP address for the time servers. Up to four servers are supported. The switch will update the time from the servers, starting from the first to the fifth in sequence if any of them fails. The polling interval is fixed at 15 minutes.
Date	Set up a local date.
Time	Set up a local time.

5.1.11 TTDP

TTDP, also known as Train Topology Discovery Protocol, is designed to provide a flexible network environment for railway applications, which must constantly adapt to changing train configurations. The protocol will identify the location of onboard network devices and reassign an IP address to them based on the new arrangement of the carriages. This will help train operators vastly improve their operational efficiency.

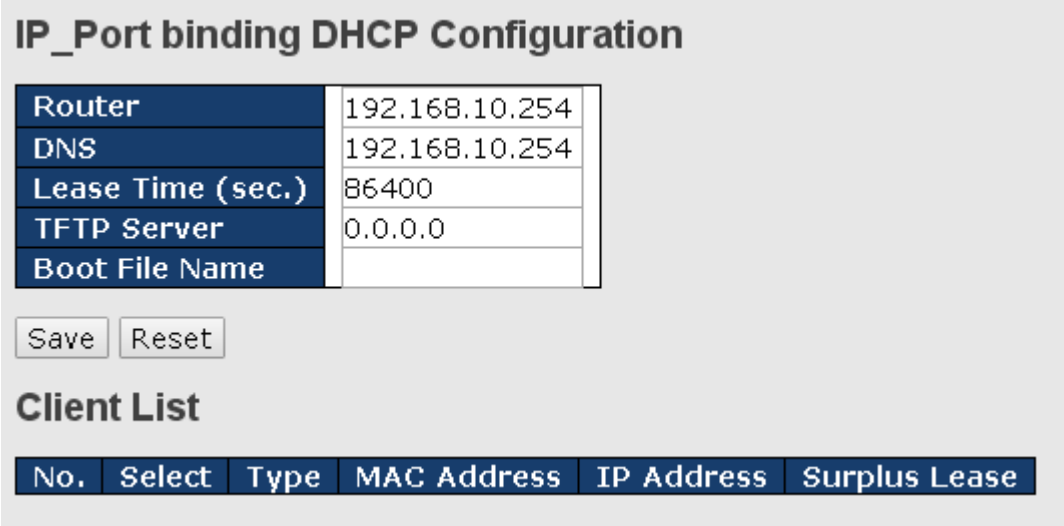


Label	Description
Mode	Enable or disable TTDP function.
IP Port Bind	When enabled, TTDP will take control of the original DHCP server, active DHCP server, stop forwarding DHCP packets, modify pool to assign custom TTDP IP to DHCP request, and POST to DHCP setting is forbidden.
Cst UUID	You can input any value such as TTDP_TOP, which will assign this

	ETBN to head of train. Only one train head is allowed in one ETB, and all ETBNs start inauguration when a head is set.
Inaug Flag	When the value is set to **Inhibit**, all ETBNs will not finish inauguration (set IP) even when ETB has become stable.
Inaug State	There are three kinds of states. **Not Inaugurated** indicates ETB is not stable or no train head is detected. **Ready for Inauguration** means ETB is stable and is ready to change IP. **Inaugurated** means ETB is stable and IP is changed.
ETBN IP	This function only appears in CUSTOM_IP mode. All ETBN will set their IP addresses according to the format of train head during Inauguration. You can set one segment of the IP address to “x” which will be replaced with switch order when the IP address is reconfigured. For example, default format is **10.128.0.x**.
ED IP	This function only appears in CUSTOM_IP mode. All ETBN will set their IP addresses according to the format of train head during Inauguration. You can set one segment of the IP address to “x” and one to “y” to one column of IP; “x” will be replaced with switch order, while “y” will be replaced with port number when the IP address is reconfigured. For example, default format is **10.128.x.y.**
IP Mask	This function only appears in CUSTOM_IP mode. All ETBNs will set and assign a mask according to the format of train head format during inauguration.
Train Backbone Node List	This column shows the full list of ETBNs with their order and MAC after inauguration.

Port IP Binding Setting

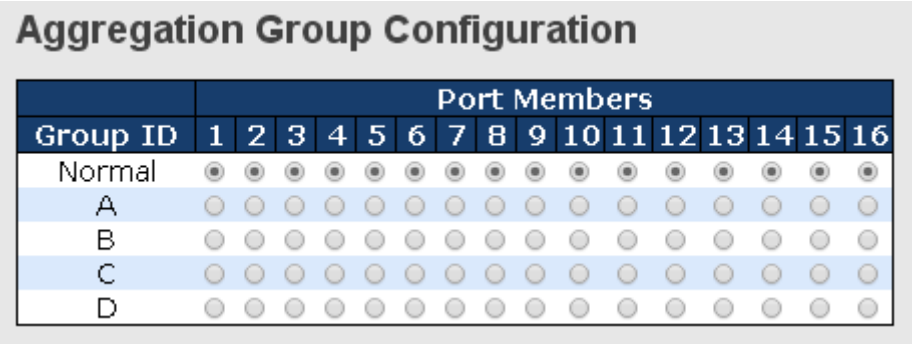
This page allows you to assign IP addresses for EDs. This function is similar to DHCP except that IP/mask is auto setting.



Label	Description
Router	The IP address of gateway.
DNS	The IP address of the domain name server.
Lease Time	Lease timer counted in seconds.
TFTP Server	The IP address of the TFTP sever (Option 66).
Boot File Name	The name of the Boot file (Option 67).
Client List	Table of the IP address assigned to the ED.

Aggregation

This page allows you to configure the aggregation for TTDP. This aggregation is only for TTDP, independent from switch.

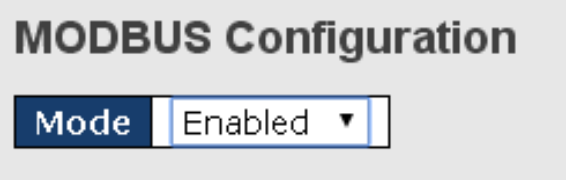


Label	Description
Group ID	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
Port Members	Each switch port is listed for each group ID. Select a radio button

	to include a port in an aggregation, or add it to Normal group to remove the port from the aggregation. By default, all ports belong to Normal group (no aggregation).

5.1.12 Modbus TCP

Modbus TCP uses TCP/IP and Ethernet to carry the data of the Modbus message structure between compatible devices. The protocol is commonly used in SCADA systems for communications between a human-machine interface (HMI) and programmable logic controllers. This page enables you to enable and disable Modbus TCP support of the switch.



Label	Description
Mode	Enable or Disalble Modbus TCP function

5.1.13 Backup/Restore Configurations

You can save/view or load switch configurations. The configuration file is in XML format.

5.1.14 Firmware Update

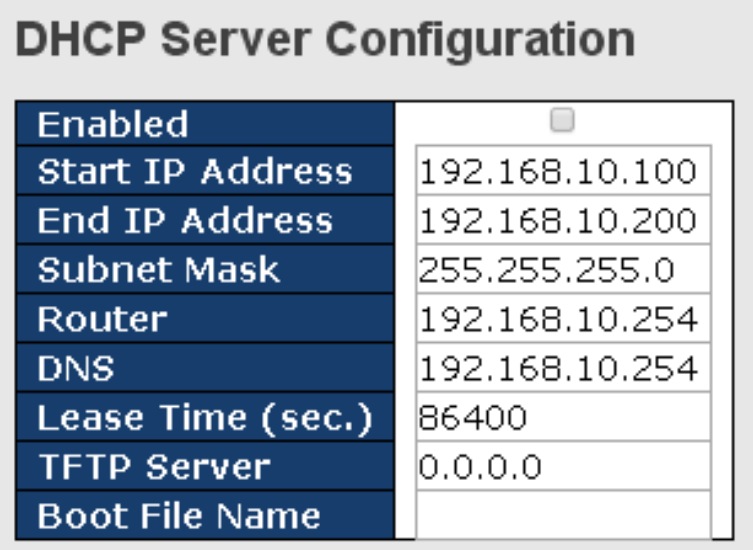
This page allows you to update the firmware of the switch.

5.2 DHCP Server/Relay

The switch provides DHCP server/relay functions. By enabling DHCP, the switch will become a DHCP server and dynamically assigns IP addresses and related IP information to network clients.

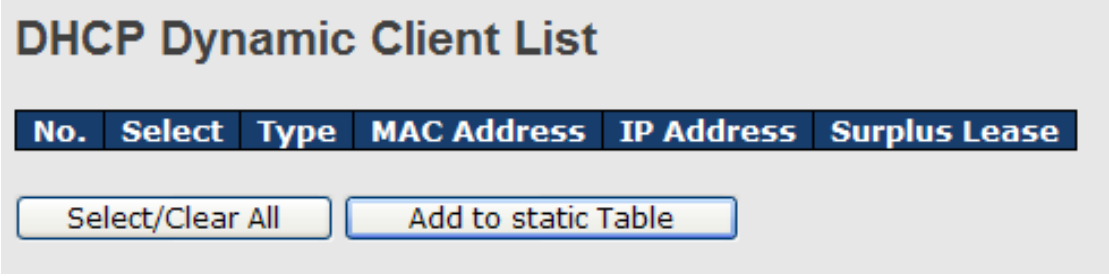
5.2.1 Settings

This page allows you to set up DHCP settings for the switch. You can check the **Enabled** checkbox to activate the function. Once the box is checked, you will be able to input information in each column.



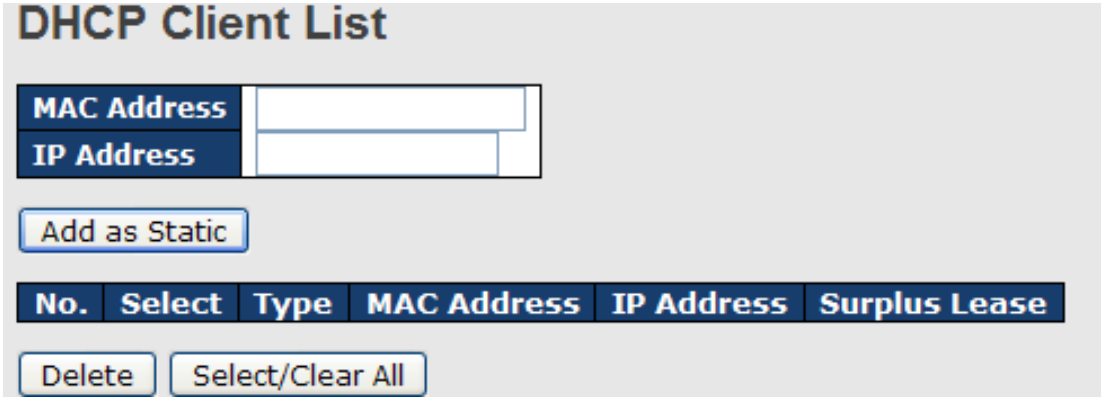
5.2.2 Dynamic Client List

When DHCP server functions are activated, the switch will collect DHCP client information and display in the following table.



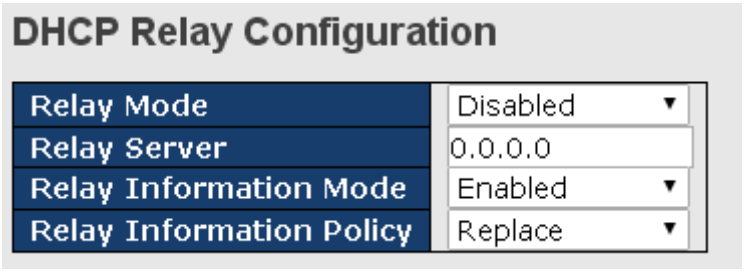
5.2.3 Client List

You can assign a specific IP address within the dynamic IP range to a specific port. When a device is connected to the port and requests for dynamic IP assigning, the switch will assign the IP address that has previously been assigned to the connected device.



5.2.4 DHCP Relay

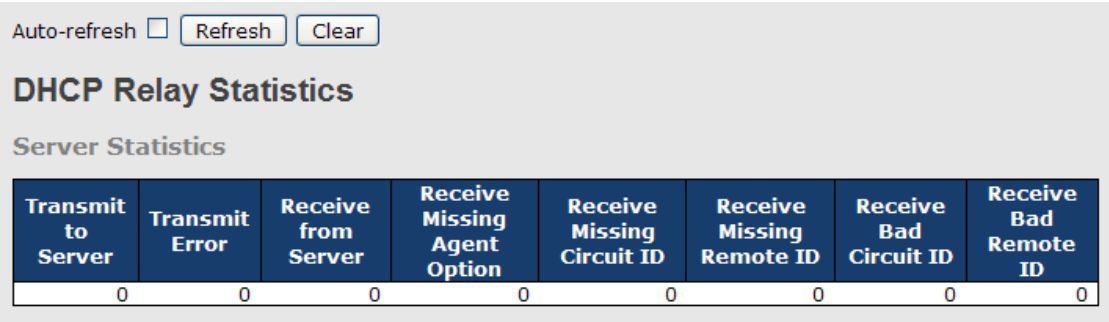
DHCP relay is used to forward and transfer DHCP messages between the clients and the server when they are not in the same subnet domain. You can configure the function in this page.



Label	Description
Relay Mode	Enable or disable DHCP relay function. **Enabled**: activate DHCP relay. When DHCP relay is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain to prevent the DHCP broadcast message from flooding for security considerations. **Disabled**: disable DHCP relay.
Relay Server	Enter the IP address of the DHCP relay server. A DHCP relay agent is used to forward and transfer DHCP messages between the clients and the server when they are not in the same subnet domain.
Relay Information Mode	Enable or disable DHCP relay information mode. **Enabled**: activate DHCP relay information. When DHCP relay information is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to a DHCP

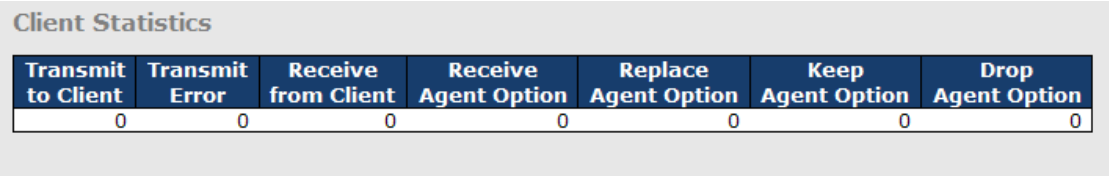
	server and removes it from a DHCP message when transferring to a DHCP client. The format of DHCP option 82 circuit ID is "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, and the fifth and sixth characters are the module ID. In stand-alone devices, the module ID always equals to 0; in stacked devices, it means switch ID. The last two characters are the port number. For example, "00030108" means the DHCP message received form VLAN ID 3, switch ID 1, and port No. 8. The option 82 remote ID value equals to the switch MAC address. **Disabled**: disable DHCP relay information.
Relay Information Policy	Indicates the policies to be enforced when receiving DHCP relay information. When DHCP relay information mode is enabled, if the agent receives a DHCP message that already contains relay agent information, it will enforce the policy. The Replace option is invalid when relay information mode is disabled. **Replace**: replace the original relay information when a DHCP message containing the information is received. **Keep**: keep the original relay information when a DHCP message containing the information is received. **Drop**: drop the package when a DHCP message containing the information is received.

The relay statistics shows the information of relayed packets of the switch.



Label	Description
Transmit to Sever	The number of packets relayed from the client to the server.
Transmit Error	The number of packets with errors when being sent to clients.
Receive from Server	The number of packets received from the server.

Receive Missing Agent Option	The number of packets received without agent information.
Receive Missing Circuit ID	The number of packets received with Circuit ID.
Receive Missing Remote ID	The number of packets received with the Remote ID option missing.
Receive Bad Circuit ID	The number of packets whose Circuit ID do not match the known circuit ID.
Receive Bad Remote ID	The number of packets whose Remote ID do not match the known Remote ID.



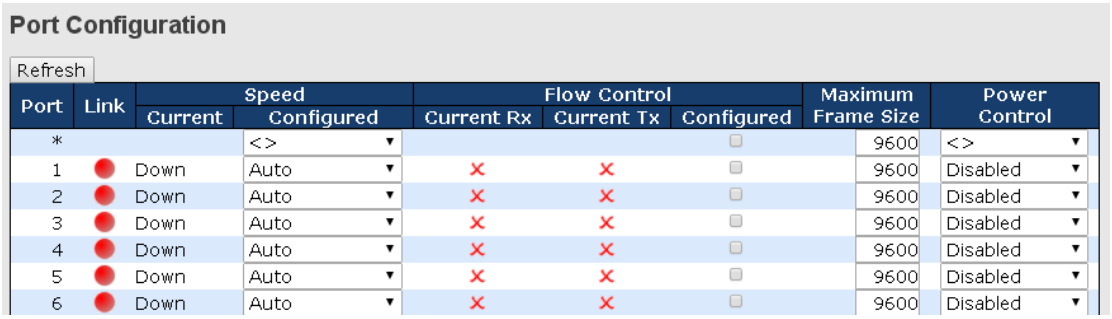
Label	Description
Transmit to Client	The number of packets relayed from the server to the client.
Transmit Error	The number of packets with errors when being sent to servers.
Receive from Client	The number of packets received from the server.
Receive Agent Option	The number of received packets containing relay agent information.
Replace Agent Option	The number of packets replaced when received messages contain relay agent information.
Keep Agent Option	The number of packets whose relay agent information is retained.
Drop Agent Option	The number of packets dropped when received messages contain relay agent information.

5.3 Port Setting

Port Setting allows you to manage individual ports of the switch, including traffic, power, and trunks.

5.3.1 Port Control

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

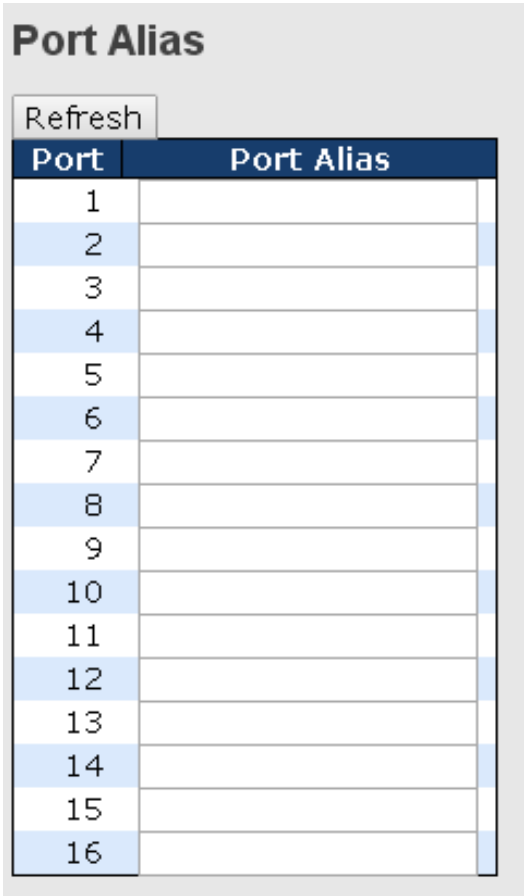


Label	Description
Port	The switch port number to which the following settings will be applied.
Link	The current link state is shown by different colors. Green indicates the link is connected and red means the link is disconnected.
Current Link Speed	Indicates the current speed of the port.
Configured Link Speed	You can choose the speed for a given port from the drop-down list. **Auto:** selects the highest speed supported by the link partner. **Disabled:** disables switch port configuration. **<>:** configures all ports.
Flow Control	When **Auto** is selected for the speed, the flow control will be negotiated to the capacity advertised by the link partner. When a fixed speed is selected, the speed setting will be used. **Current Rx** indicates whether pause frames on the port are obeyed, and **Current Tx** indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last auto-negotiation. You can check the **Configured** column to use flow control. This setting is related to the setting of **Configured Link Speed**.
Maximum Frame Size	You can enter the maximum frame size allowed for the switch port in this column, including FCS. The allowed range is 1518 bytes to 9600 bytes.
Power Control	Shows the current power consumption of each port in percentage. The **Configured** column allows you to change power saving parameters for each port. **Disabled**: all power savings functions are disabled. **ActiPHY**: this function saves power when no link is present. By enabling it, Ethernet ports that are not connected to a link will stay in a low-power mode and transmitters will not continuously send

	signals where there is no receiver connected. **PerfectReach**: this function reduces active power for cable lengths shorter than the IEEE defined maximum of 100 meters. It will determine the optimal power levels to drive Ethernet signals based on automatic cable length detection without sacrificing signal integrity and link reliability. **Enabled**: enable both power saving methods.

5.3.2 Port Alias

You can assign a port alias name for each port to enable easy identification of the devices connected to the port.

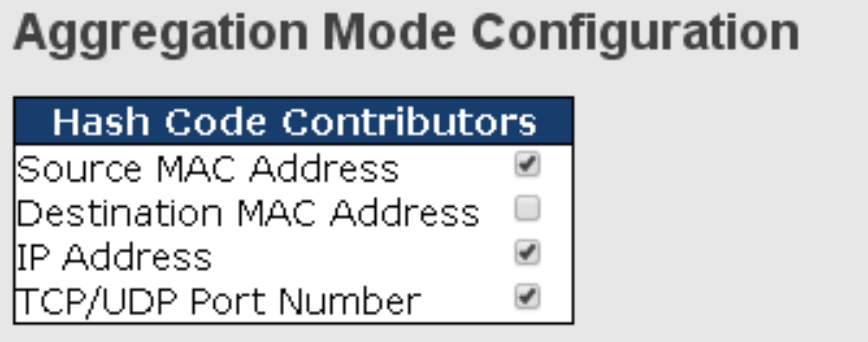


5.3.3 Port Trunk

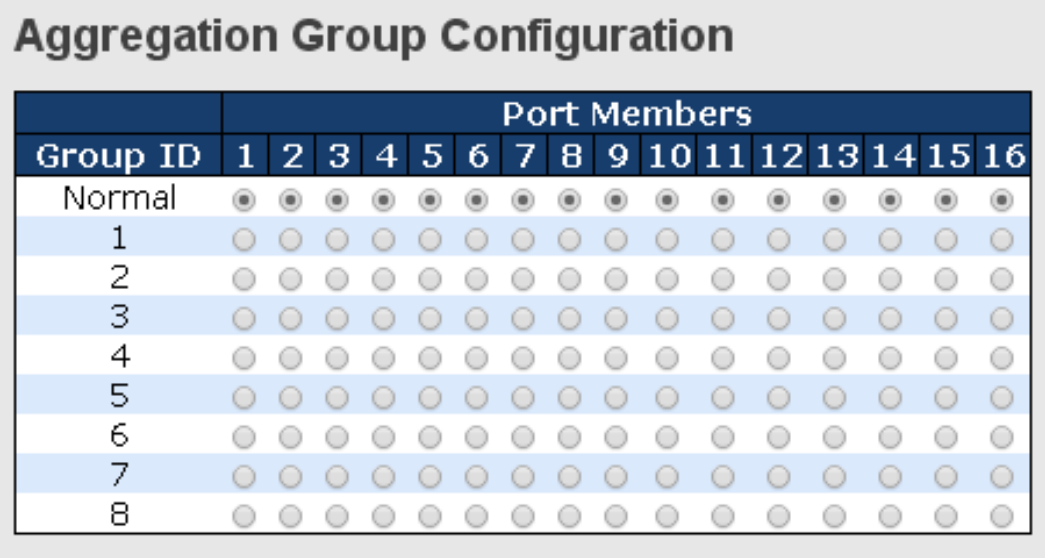
Aggregation Mode/Group

A port trunk is a group of ports that have been grouped together to function as one logical path. This method provides an economical way for you to increase the bandwidth between the switch and another networking device. In addition, it is useful when a single physical link between the devices is insufficient to handle the traffic load. This page allows you to configure

the aggregation hash mode and the aggregation group.



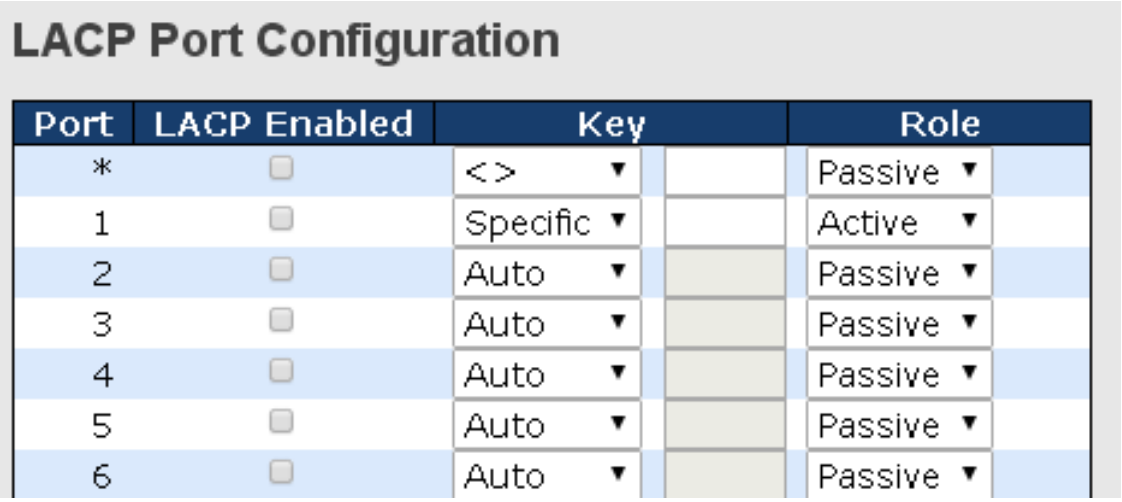
Label	Description
Source MAC Address	Check the box if you want to use source MAC address to calculate the destination port for the frame. Otherwise, leave it blank. By default, **Source MAC Address** is enabled (checked).
Destination MAC Address	Check the box if you want to use destination MAC address to calculate the destination port for the frame. Otherwise, leave it blank. By default, **Destination MAC Address** is disabled (unchecked).
IP Address	Check the box if you want to use IP address to calculate the destination port for the frame. Otherwise, leave it blank. By default, **IP Address** is enabled (checked).
TCP/UDP Port Number	Check the box if you want to use TCP/IP port number to calculate the destination port for the frame. Otherwise, leave it blank. By default, **TCP/UDP Port Number** is enabled (checked).



Label	Description
Group ID	Indicates the ID of each aggregation group. **Normal** means no aggregation. Only one group ID is valid per port.
Port Members	Lists each switch port for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and the ports must be in the same speed in each group.

LACP Ports

LACP (Link Aggregation Control Protocol) trunks are similar to static port trunks, but they are more flexible because LACP is compliant with the IEEE 802.3ad standard. Hence, it is interoperable with equipment from other vendors that also comply with the standard. This page allows you to enable LACP functions to group ports together to form single virtual links and change associated settings, thereby increasing the bandwidth between the switch and other LACP-compatible devices.

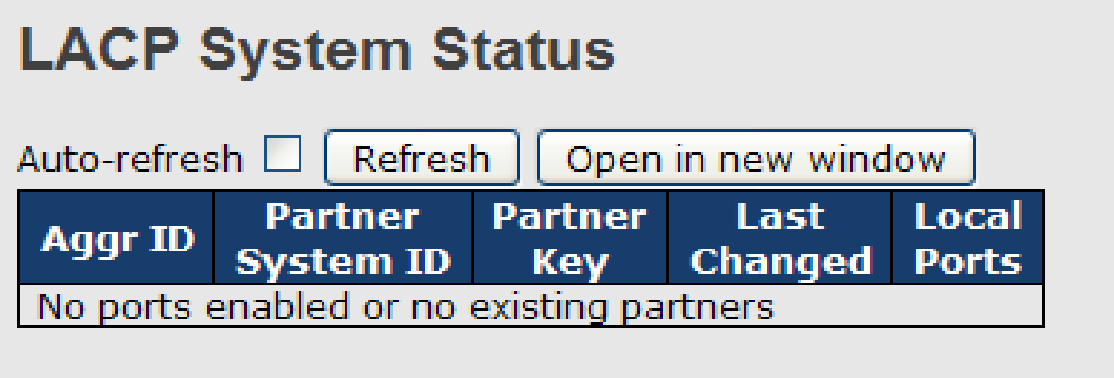


Label	Description
Port	Indicates the port No. for LACP settings.
LACP Enabled	Check to enable the LACP function for that port.
Key	The **Key** value varies with the port, ranging from 1 to 65535. **Auto** will set the key according to the physical link speed (10Mb = 1, 100Mb = 2, 1Gb = 3). **Specific** allows you to enter a user-defined value. Ports with the same key value can join in

	the same aggregation group, while ports with different keys cannot.
Role	You can select configure a LACP mode for a port. **Active** means the port will send LACP regardless of whether its counterpart uses passive LACP or not and **Passive** means the port will not send LACP packets unless its counterpart uses active LACP, that is when the port is spoken to.

LACP System Status

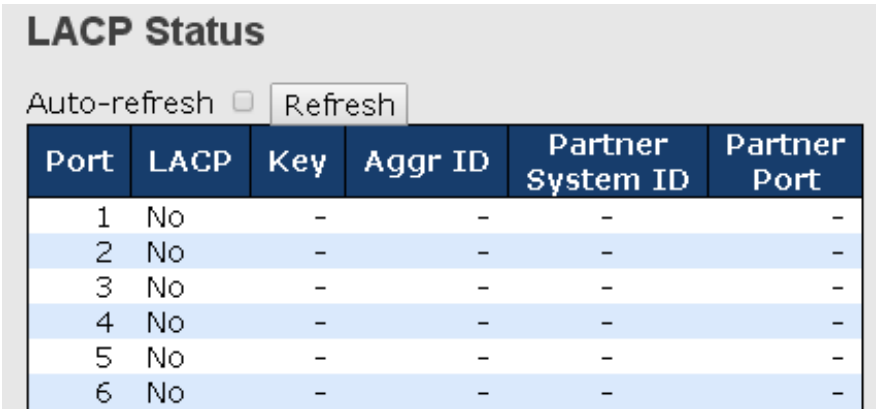
This page provides a status overview for all LACP instances.



Label	Description
Aggr ID	The aggregation ID is associated with the aggregation instance. For LLAG, the ID is shown as '**isid:aggr-id**' and for GLAGs as '**aggr-id**'.
Partner System ID	System ID (MAC address) of the aggregation partner.
Partner Key	The key assigned by the partner to the aggregation ID.
Last Changed	The time since this aggregation was changed.
Local Ports	Indicates which ports belong to the aggregation of the switch/stack. The format is: "**Switch ID:Port**".
Refresh	Click to refresh the page immediately.
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals.

LACP Port Status

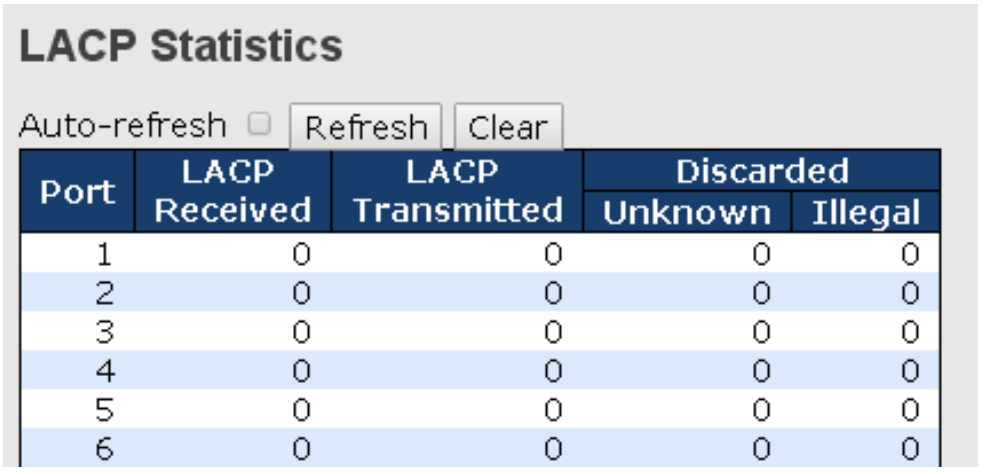
This page provides an overview of the LACP status for all ports.



Label	Description
Port	Switch port number.
LACP	**Yes** means LACP is enabled and the port link is up. **No** means LACP is not enabled or the port link is down. **Backup** means the port cannot join in the aggregation group unless other ports are removed. The LACP status is disabled.
Key	The key assigned to the port. Only ports with the same key can be aggregated.
Aggr ID	The aggregation ID assigned to the aggregation group.
Partner System ID	The partner's system ID (MAC address).
Partner Port	The partner's port number associated with the port.
Refresh	Click to refresh the page immediately.
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals.

LACP Port Statistics

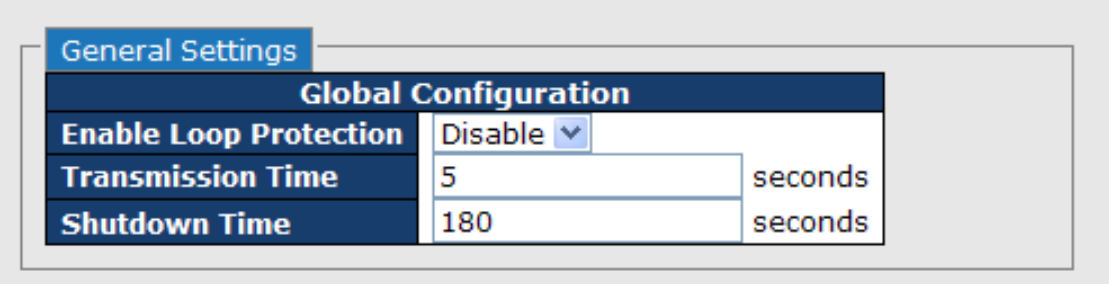
This page provides an overview of the LACP statistics for all ports.



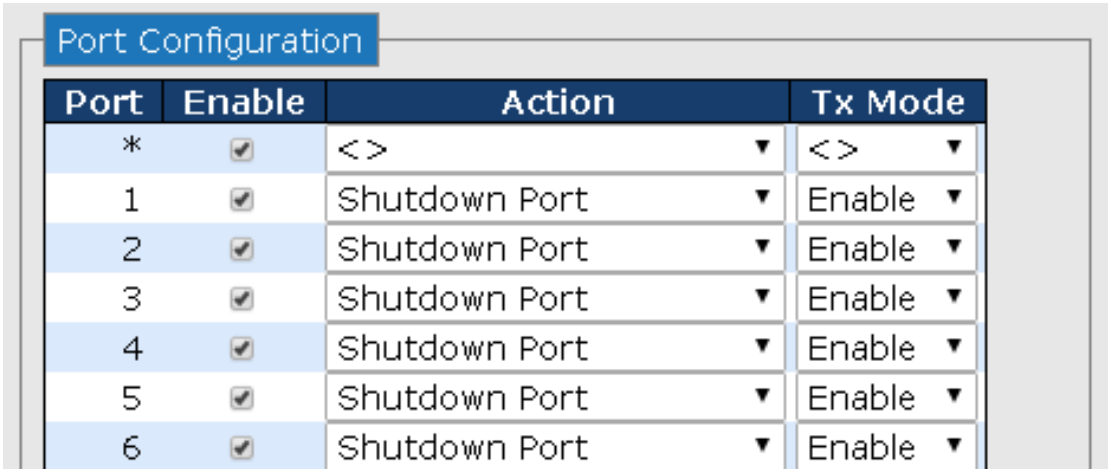
Label	Description
Port	Switch port number.
LACP Transmitted	The number of LACP frames sent from each port.
LACP Received	The number of LACP frames received at each port.
Discarded	The number of unknown or illegal LACP frames discarded at each port.
Refresh	Click to refresh the page immediately.
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals.
Clear	Click to clear the counters for all ports.

5.3.4 Loop Protection

This page helps you detect general loopback conditions caused by hardware problems or faulty protocol settings. This function will send a control frame on the participating ports, and the switch monitors inbound traffic to see if the frame is looped back. When receiving loop packets, the port will be disabled automatically, preventing the loop attack from affecting other network devices.

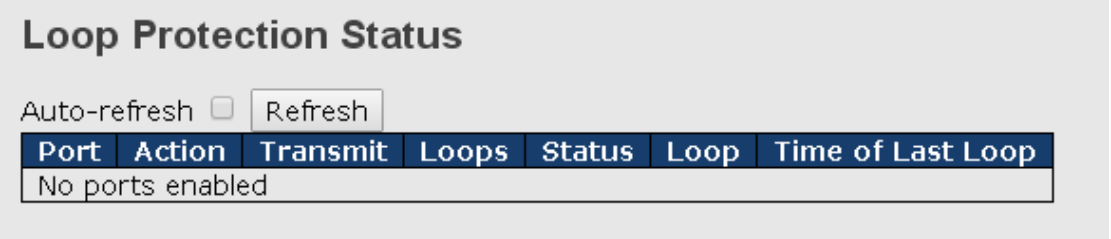


Label	Description
Enable Loop Protection	Activate loop protection functions (as a whole).
Transmission Time	The interval between each loop protection PDU sent on each port. The valid value is 1 to 10 seconds.
Shutdown Time	The period (in seconds) for which a port will be kept disabled when a loop is detected (shutting down the port). The valid value is 0 to 604800 seconds (7 days). A value of zero will keep a port disabled permanently (until the device is restarted).



Label	Description
Port	Switch port number.
Enable	Activate loop protection functions (as a whole or individually).
Action	Select the action to take when a loop is detected. Valid values include **Shutdown Port**, **Shutdown Port**, and **Log or Log Only**.
Tx Mode	When enabled, the port will actively generate loop protection PDUs. When disabled, the port will only passively look for looped PDUs.

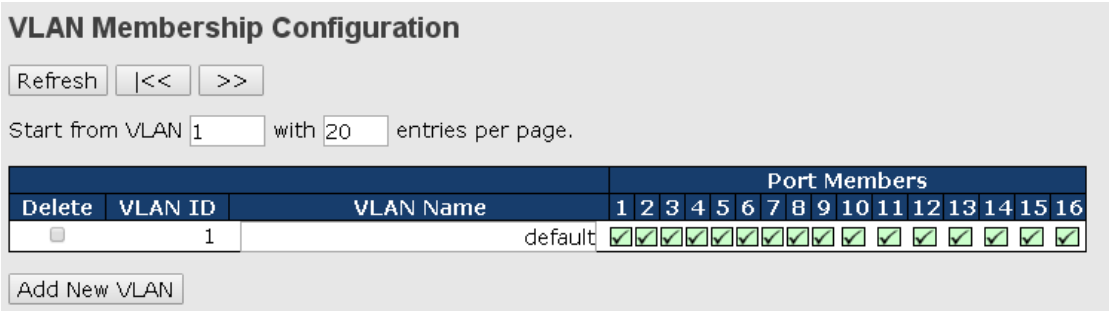
This page shows the status of loop protection.



5.4 VLAN

5.4.1 VLAN Membership

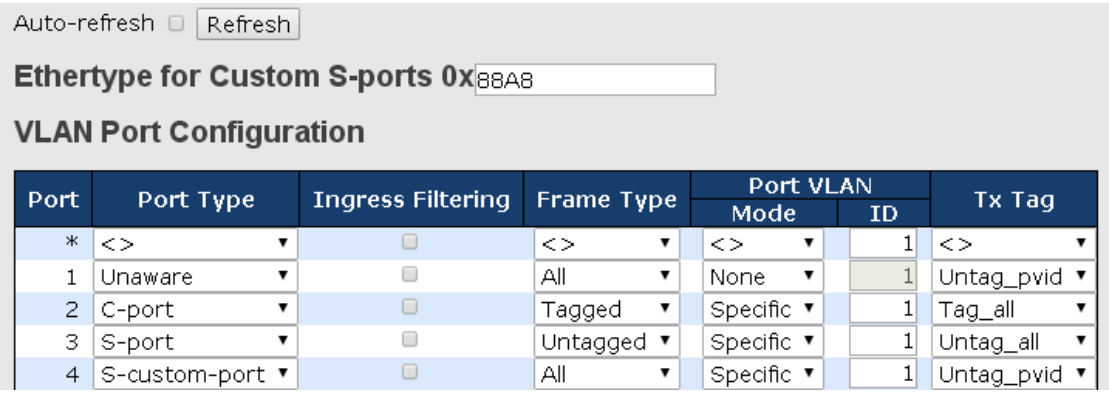
A VLAN (Virtual LAN) is a logical LAN based on a physical LAN with links that does not consist of a physical (wired or wireless) connection between two computing devices but is implemented using methods of network virtualization. A VLAN can be created by partitioning a physical LAN into multiple logical LANs using a VLAN ID. You can assign switch ports to a VLAN and add new VLANs in this page.



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
VLAN Name	The name for the VLAN.
Port Members	Check the box to specify the port to be a member of the entry.
Add New VLAN	Click to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Valid values for a VLAN ID are 1 through 4095. After clicking **Save**, the new VLAN will be enabled on the selected switch stack but contains no port members. A VLAN without any port members on any stack will be deleted when you click Save. Click **Delete** to undo the addition of new VLANs.

5.4.2 Port Configurations

This page allows you to set up VLAN ports individually.



Label	Description
Ethertype for customer S-Ports	This field specifies the Ether type used for custom S-ports. This is a global setting for all custom S-ports.

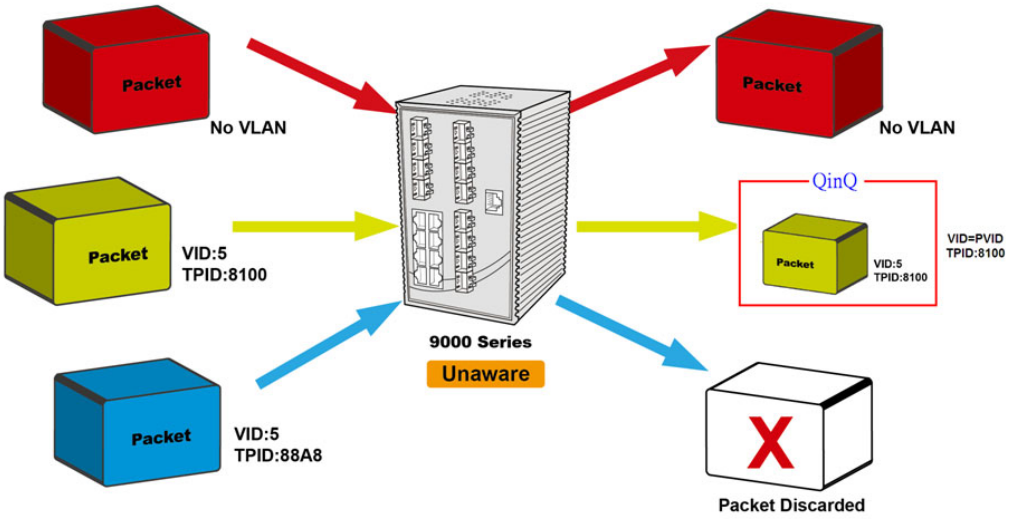
Port	The switch port number to which the following settings will be applied.
Port type	Port can be one of the following types: **Unaware**, **Customer** (**C-port**), **Service** (**S-port**), **Custom Service** (**S-custom-port**). If port type is **Unaware**, all frames are classified to the port VLAN ID and tags are not removed. For description of each type of ports, please refer to the following table.
Ingress Filtering	You can enable ingress filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame will be discarded. By default, ingress filtering is disabled (no check mark).
Frame Type	Determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on the port will be discarded. By default, the field is set to All.
Port VLAN Mode	The allowed values are **None** or **Specific**. This parameter affects VLAN ingress and egress processing. If **None** is selected, a VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN-aware switches. Tx tag should be set to Untag_pvid when this mode is used. If **Specific** (the default value) is selected, a port VLAN ID can be configured (see below). Untagged frames received on the port are classified to the port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the port VLAN ID, a VLAN tag with the classified VLAN ID will be inserted in the frame.
Port VLAN ID	Configures the VLAN identifier for the port. The allowed range of the values is 1 through 4095. The default value is 1. Note: The port must be a member of the same VLAN as the port VLAN ID.
Tx Tag	Determines egress tagging of a port. **Untag_pvid**: all VLANs except the configured PVID will be tagged. **Tag_all**: all VLANs are tagged. **Untag_all**: all VLANs are untagged.

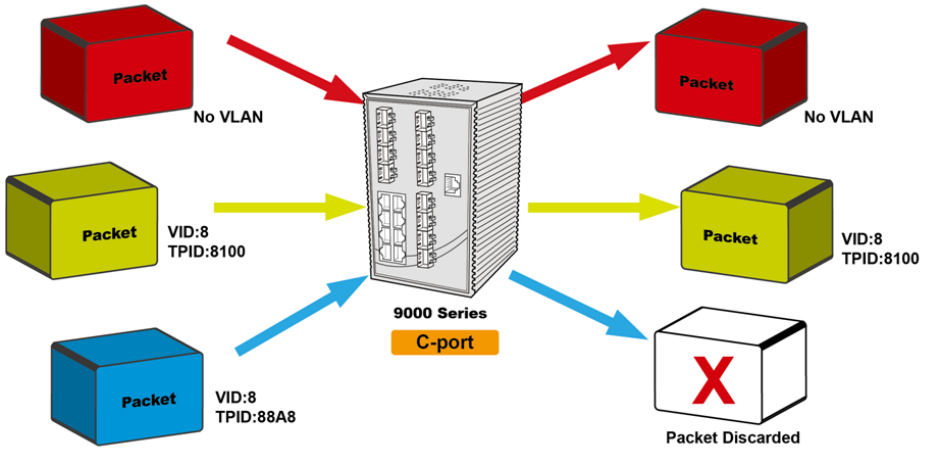
Introduction of Port Types

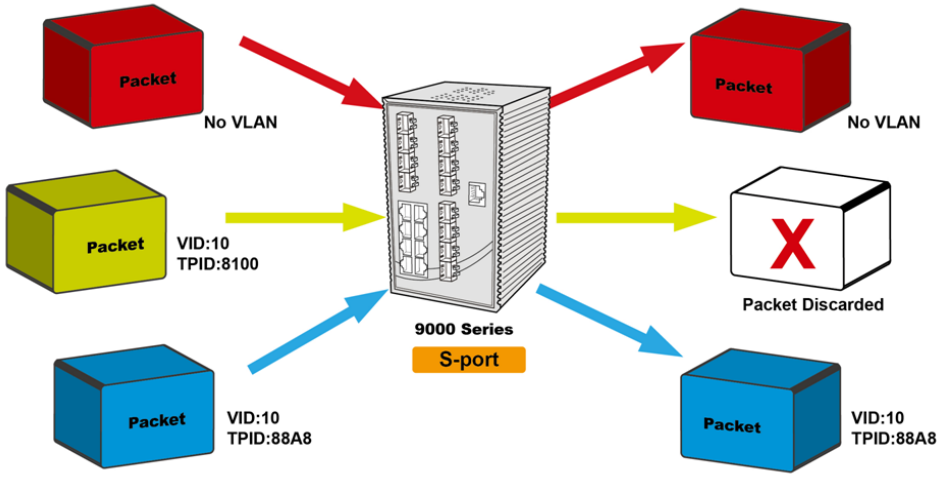
Below is a detailed description of each port type, including Unaware, C-port, S-port, and S-custom-port.

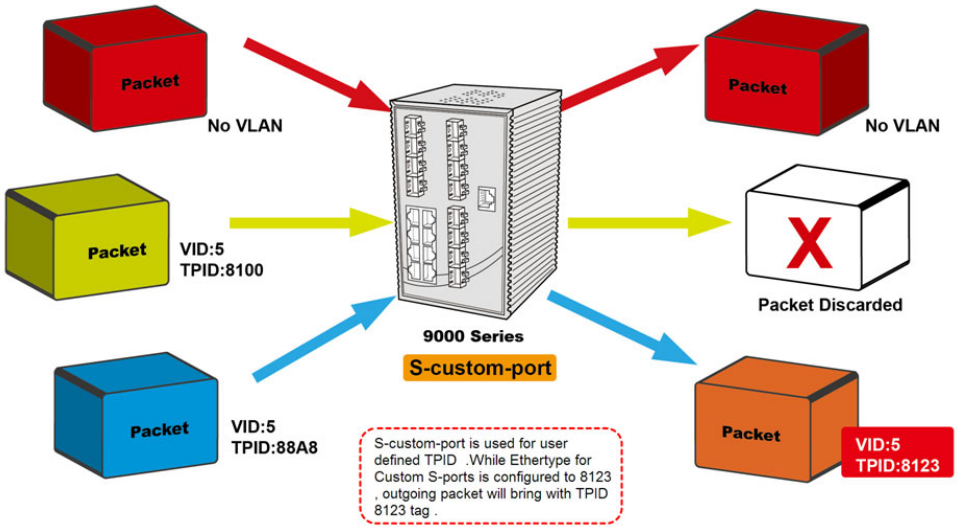
	Ingress action	Egress action
Unaware **The function of Unaware can be used for 802.1QinQ (double tag).**	When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded. When the port receives tagged frames: 1. If the tagged frame contains a TPID of 0x8100, it will become a double-tag frame and will be forwarded. 2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of a frame transmitted by Unaware port will be set to 0x8100. The final status of the frame after egressing will also be affected by the Egress Rule.
C-port	When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded. When the port receives tagged frames: 1. If the tagged frame contains a TPID of 0x8100, it will be forwarded. 2. If the TPID of tagged frame is not 0x8100 (ex. 0x88A8), it will be discarded.	The TPID of a frame transmitted by C-port will be set to 0x8100.
S-port	When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded. When the port receives tagged frames: 1. If the tagged frame contains a TPID of 0x8100, it will be forwarded. 2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8100), it will be discarded.	The TPID of a frame transmitted by S-port will be set to 0x88A8.
S-custom-port	When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded. When the port receives tagged frames: 1. If the tagged frame contains a TPID of 0x8100, it will be forwarded. 2. If the TPID of tagged frame is not 0x88A8 (ex. 0x8100), it will be discarded.	The TPID of a frame transmitted by S-custom-port will be set to a self-customized value, which can be set by the user via **Ethertype for Custom S-ports.**

Below are the illustrations of different port types:



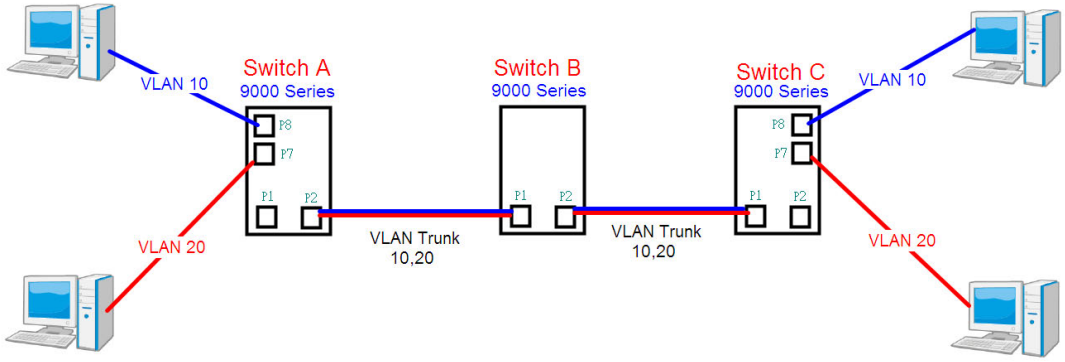






Examples of VLAN Settings

VLAN Access Mode:

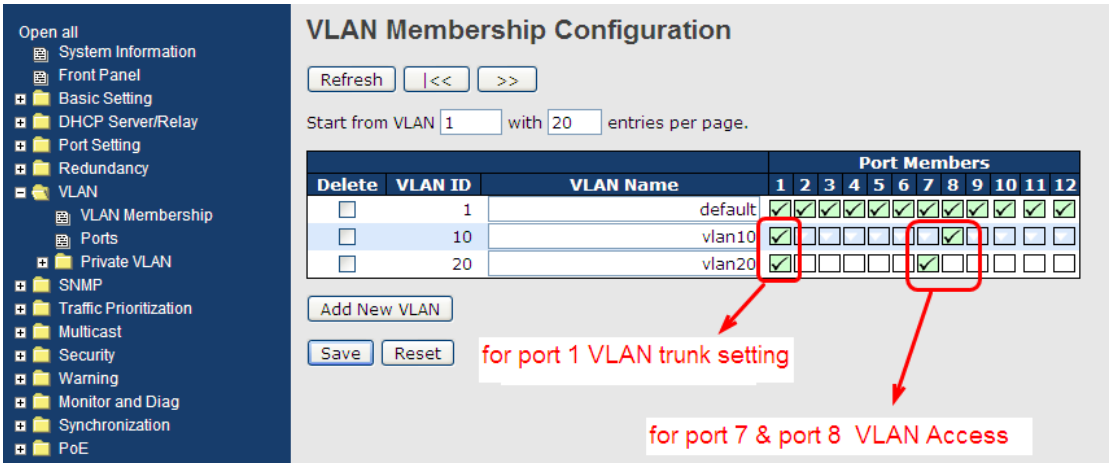


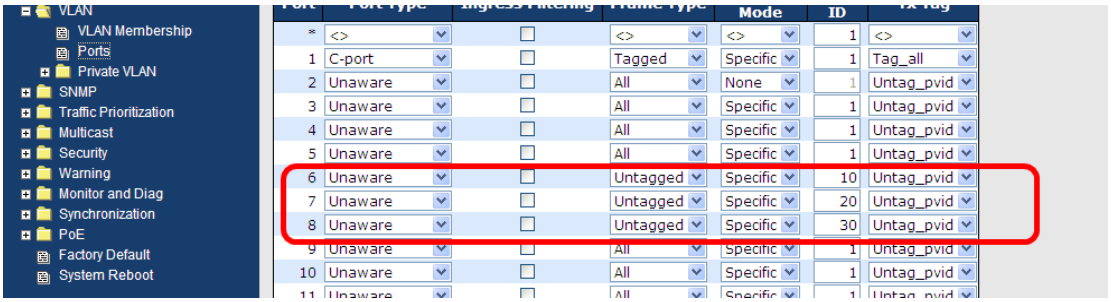
Switch A,

Port 7 is VLAN Access mode = Untagged 20

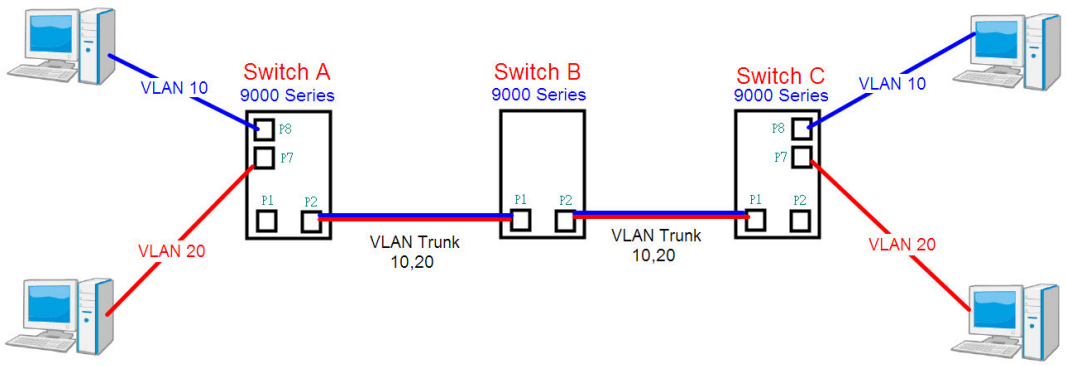
Port 8 is VLAN Access mode = Untagged 10

Below are the switch settings.





VLAN 1Q Trunk Mode:

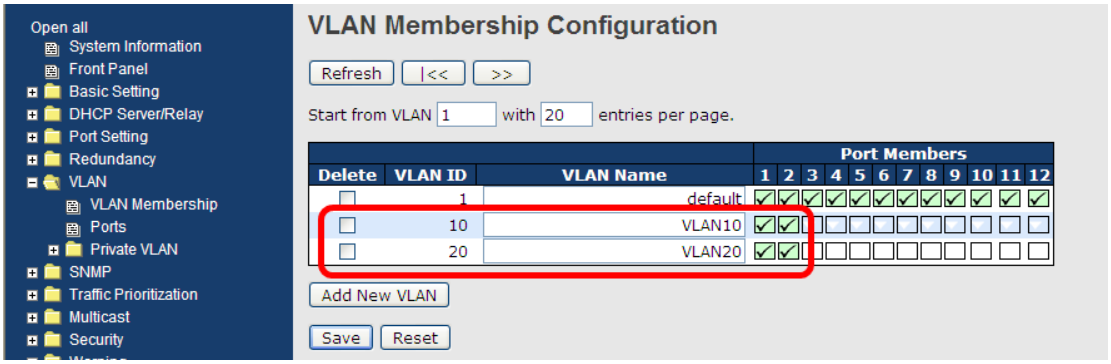


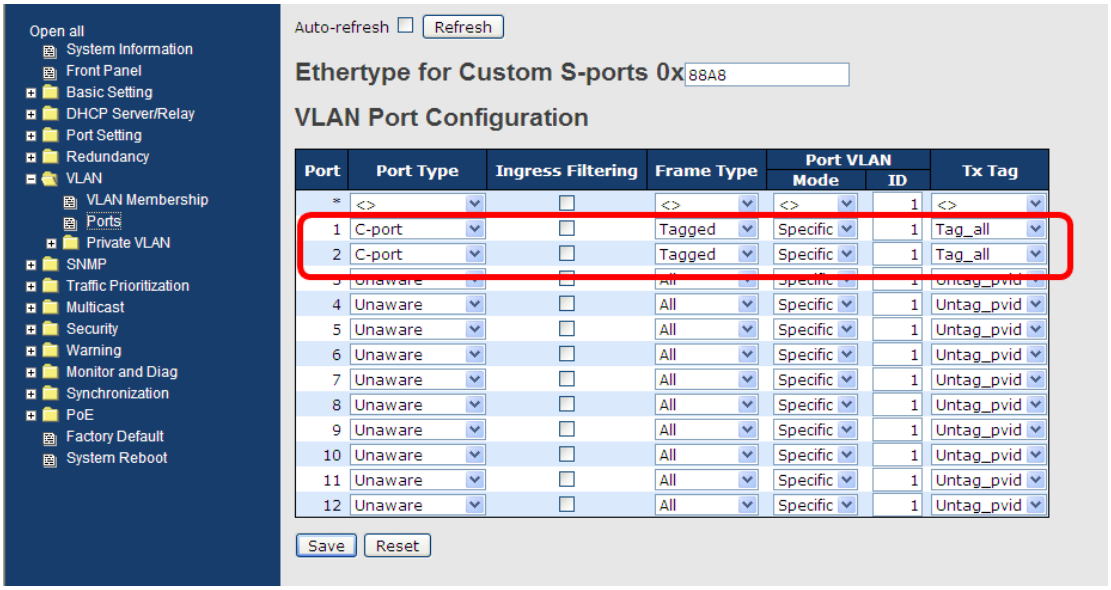
Switch B,

Port 1 = VLAN 1Qtrunk mode = tagged 10, 20

Port 2 = VLAN 1Qtrunk mode = tagged 10, 20

Below are the switch settings.



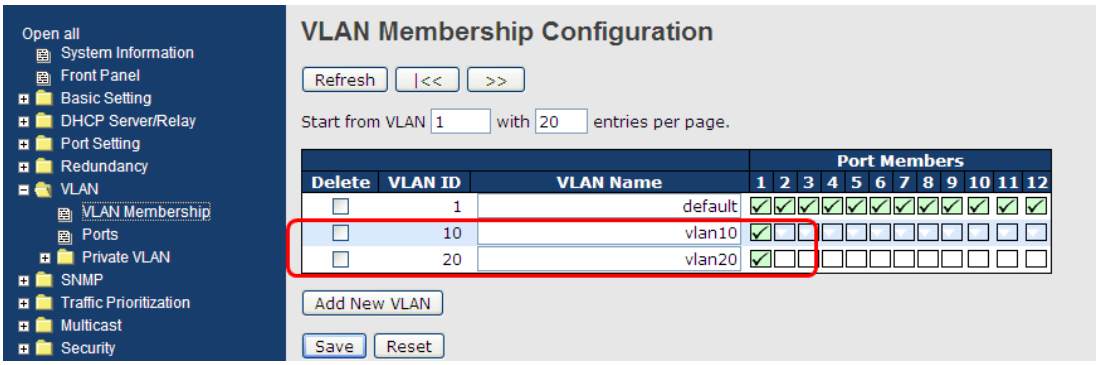


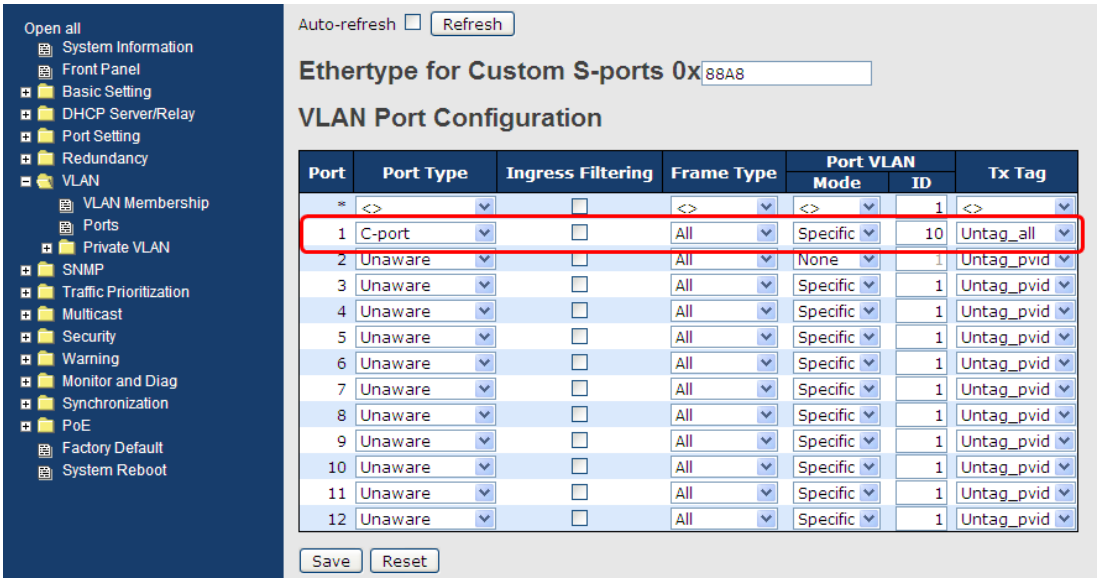
VLAN Hybrid Mode:

Port 1 VLAN Hybrid mode = untagged 10

Tagged 10, 20

Below are the switch settings.

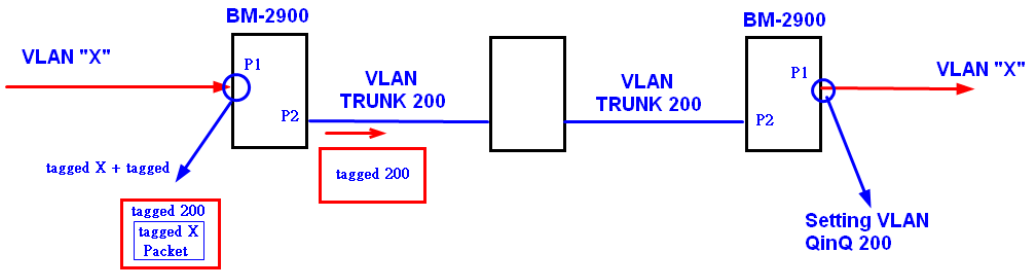




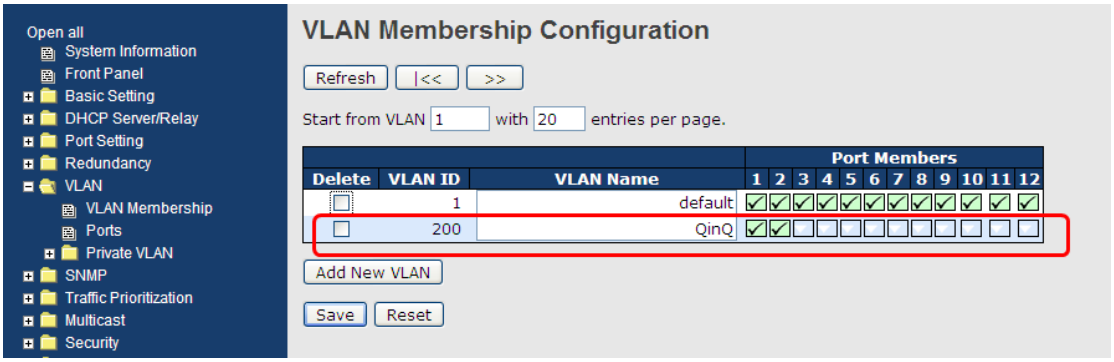
VLAN QinQ Mode:

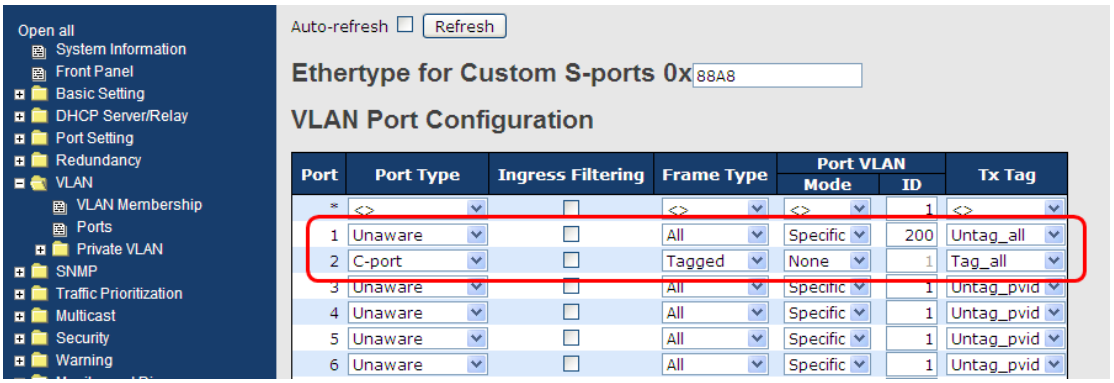
VLAN QinQ mode is usually adopted when there are unknown VLANs, as shown in the figure below.

VLAN “X” = Unknown VLAN



9000 Series Port 1 VLAN Settings:

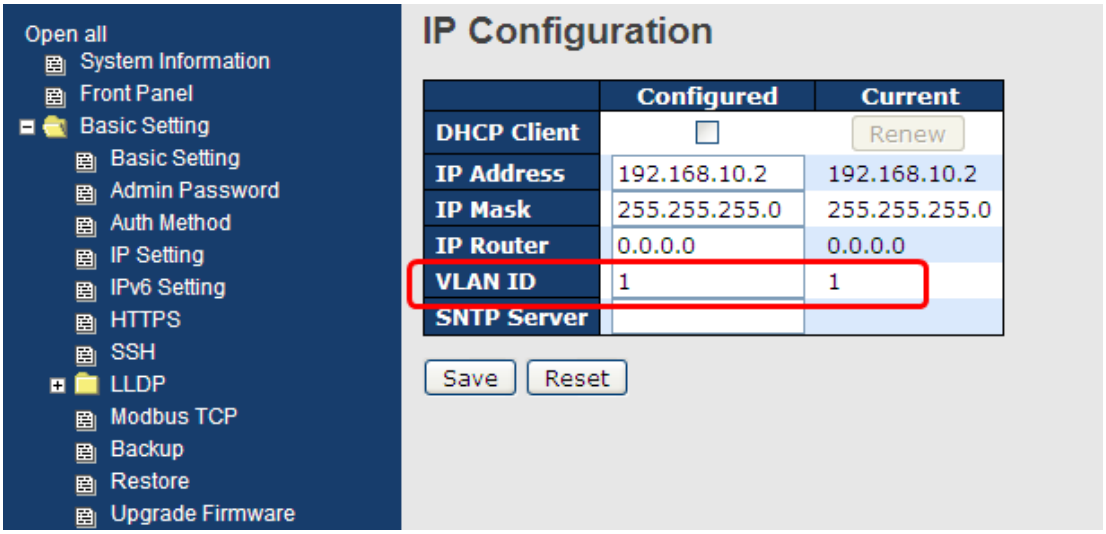




VLAN ID Settings

When setting the management VLAN, only the same VLAN ID port can be used to control the switch.

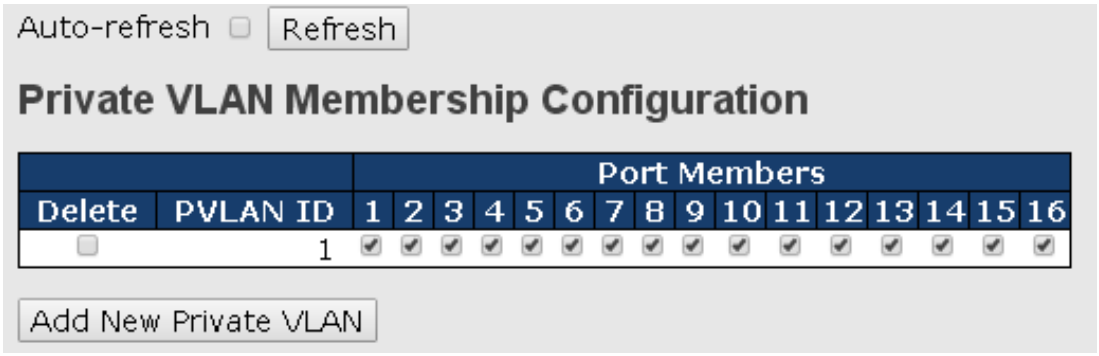
9000ies VLAN Settings:



5.4.3 Private VLAN

A private VLAN contains switch ports that can only communicate with a given "uplink". The restricted ports are called private ports. Each private VLAN typically contains many private ports and a single uplink. The switch forwards all frames received on a private port out the uplink port, regardless of VLAN ID or destination MAC address. A port must be a member of both a VLAN and a private VLAN to be able to forward packets. This page allows you to configure private VLAN memberships for the switch. By default, all ports are VLAN unaware and members of VLAN 1 and private VLAN 1.

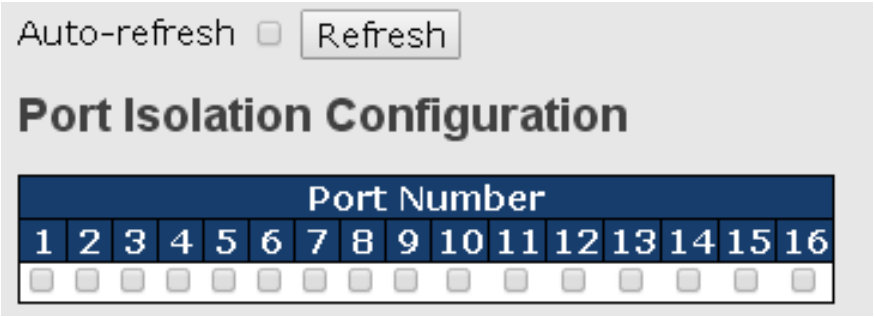
Private LAN Membership



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

A private VLAN is defined as a pairing of a primary VLAN with a secondary VLAN. A promiscuous port is a port that can communicate with all other private VLAN port types via the primary VLAN and any associated secondary VLANs, whereas isolated ports can communicate only with a promiscuous port.

Port Isolation

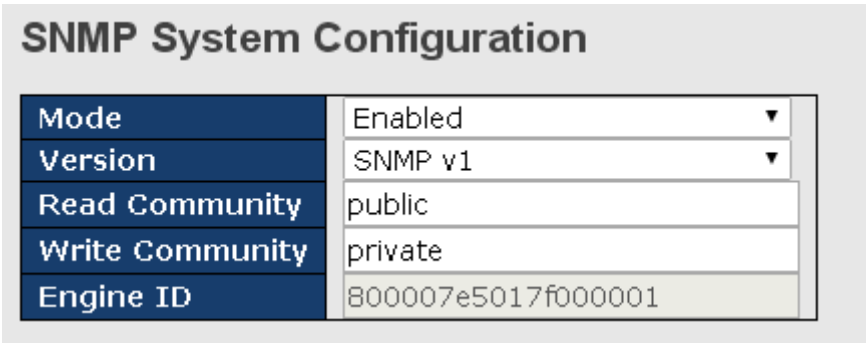


Label	Description
Port Members	When checked, port isolation is enabled for that port. When unchecked, port isolation is disabled for that port. By default, port isolation is disabled for all ports.

5.5 SNMP

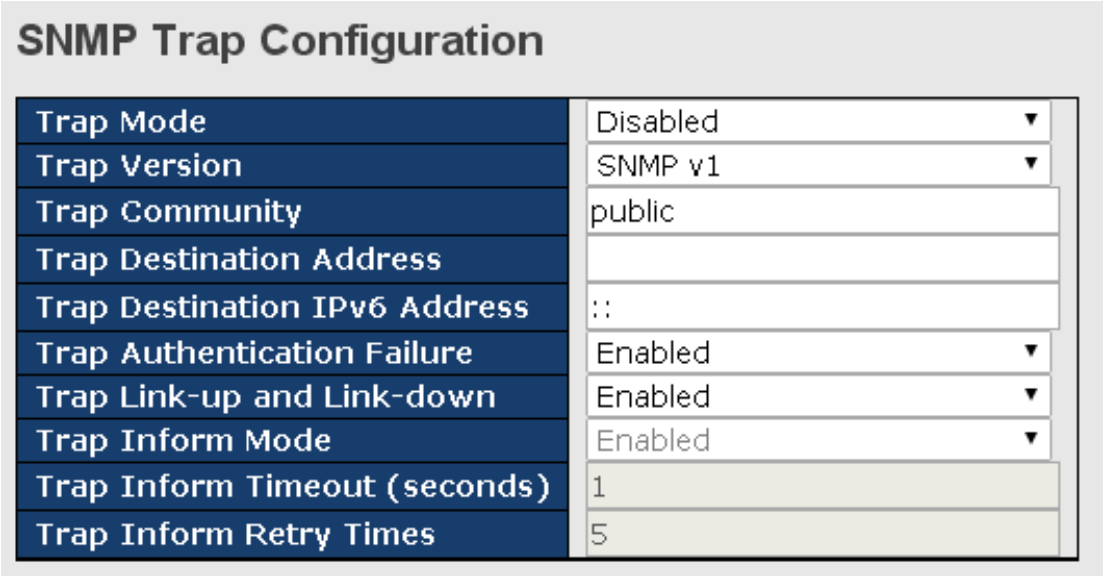
SNMP (Simple Network Management Protocol) is a protocol for managing devices on IP networks. It is mainly used network management systems to monitor the operational status of networked devices. In an event-triggered situation, traps and notifications will be sent to administrators.

5.5.1 SNMP System/Trap Configurations



Label	Description
Mode	Indicates existing SNMP mode. Possible modes include: **Enabled**: enable SNMP mode. **Disabled**: disable SNMP mode.
Version	Indicates the supported SNMP version. Possible versions include: **SNMP v1**: supports SNMP version 1. **SNMP v2c**: supports SNMP version 2c.

	SNMP v3: supports SNMP version 3.
Read Community	The community string is like a password for SNMP-enabled devices. There are two types of community strings: read and read-write. The read community string only allows you to read the value. It is usually set as public.
Write Community	The community string is like a password for SNMP-enabled devices. There are two types of community strings: read and read-write. The read-write community string allows you to read and write a value. It is usually set as private. If the community string and the type of action you are querying is not specified correctly, the query will fail.
Engine ID	An engine ID is a unique string used to identify an SNMP agent in a device. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.



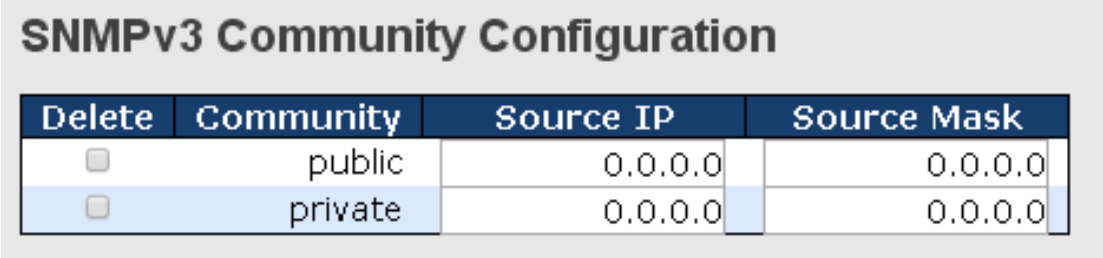
Label	Description
Trap Mode	Indicates existing SNMP trap mode. Possible modes include: **Enabled**: enable SNMP trap mode **Disabled**: disable SNMP trap mode
Trap Version	Indicates the supported SNMP trap version. Possible versions include: **SNMP v1**: supports SNMP trap version 1 **SNMP v2c**: supports SNMP trap version 2c

	SNMP v3: supports SNMP trap version 3
Trap Community	Trap community string allows you to receive traps (asynchronous notifications) from the agent. This string acts as the password for network elements. The read-only string, which is public, lets you read data values, but doesn't let you modify the data. For example, you can read the number of packets that have been transferred through the ports on your router, but you cannot reset the counters. The read-write community which is private allows you to read and modify data values; therefore, you can read the counters, reset their values, and even reset the interfaces or do other things that change the router's configuration. It's important to change these defaults before your device goes live on the network.
Trap Destination Address	Enter an IP address of the SNMP manager that will receive traps. The value between 0.0.0.0 and 255.255.255.255 is the IP address assigned by the computer to handle unsolicited data generated by SNMP trap events.
Trap Destination IPv6 Address	Enter the IPv6 address of the SNMP manager to receive notification messages. IPv6 address consists of 128 bits represented as eight groups of four hexadecimal digits with a colon separating each field (:). For example, in 'fe80::215:c5ff:fe03:4dc7', the symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also uses a following legally IPv4 address. For example, '::192.1.2.34'.
Trap Authentication Failure	When enabled, a notification message will be sent to specified IP trap managers whenever authentication of an SNMP request fails. When disabled, no messages will be sent when this happens.
Trap Link-up and Link-down	When enabled, a notification message will be sent to specified IP trap managers when a port link is established or broken. When disabled, no messages will be sent when this happens.
Trap Inform Mode	An option only available for version 2c and 3 hosts, this function will send notifications as inform messages. Unlike trap messages which do not send a response to the switch upon receipt, inform messages include a request for acknowledgement of receipt and are thus more reliable. While informs are ideal to ensure that critical information is received by the host, they consume more system resources because they must be kept in memory until a response is received.

	Informs also add to network traffic. Hence, take these effects into consideration when you decide whether to issue notifications as traps or informs.
Trap Inform Timeout (seconds)	This is the time, in second, to wait for an acknowledgment before resending an inform message. The range of the value is between 0 and 2147 seconds and the default is 1 second.
Trap Inform Retry Times	The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. The range of the value is 0 to 255 and the default is 5.
Trap Probe Security Engine ID	An option only available for SNMPv3. When enabled, the engine ID of the SNMP trap probe will be used in trap and inform messages.
Trap Security Engine ID	An option only available for SNMPv3 which indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When “Trap Probe Security Engine ID” is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. Only 10-64 hex digits are allowed, excluding a string of all 0’s or all F’s.
Trap Security Name	An option only available for SNMPv3 which indicates the SNMP trap security name. SNMPv3 traps and informs use USM for authentication and privacy. A unique security name is needed when SNMPv3 traps or informs are enabled.

5.5.2 SNMP Community Configurations

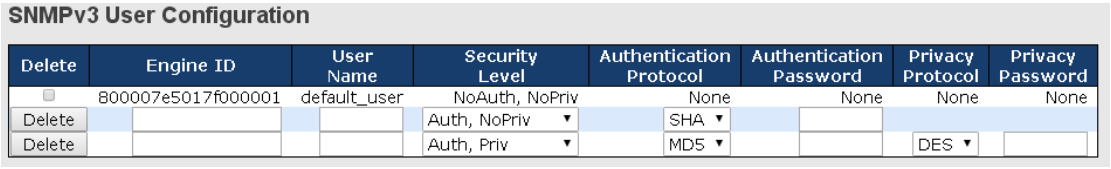
You can define access to the SNMP data on your devices by creating one or more SNMP communities. An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. This page allows you to configure SNMPv3 community table. The entry index key is **Community**.



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Community	Indicates the SNMP community string.
Source IP	Indicates the source IP address for all SNMP traps leaving a router.
Source Mask	Indicates the SNMP source address mask.

5.5.3 SNMP User Configurations

Each SNMP user has a specified username, a group to which the user belongs, authentication password, authentication protocol, privacy protocol, and privacy password. When you create a user, you must associate it with an SNMP group. The user then inherits the security model of the group. This page allows you to configure the SNMPv3 user table. The entry index keys are **Engine ID** and **User Name**.



Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	This is the engine ID for the SNMP agent on the remote device where the user resides. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. The engine ID is used with a hashing function to generate keys for authentication and encryption of SNMP v3 messages. If you do not specify an engine ID, one is generated when you enable the standalone SNMP agent.
User Name	A string identifying the name of user connecting to the SNMP agent. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
Security Level	Indicates the security model assigned to the user, including: **NoAuth, NoPriv**: no authentication and encryption is used in SNMP communications. **Auth, NoPriv**: Authentication is used but data is not encrypted. **Auth, Priv**: both authentication and encryption is used.
Authentication Protocol	Indicates the authentication protocol for user authentication, including: **None**: no authentication protocol.

	MD5: an optional flag to indicate that this user is using MD5 authentication protocol. **SHA**: an optional flag to indicate that this user is using SHA authentication protocol. The value of security level cannot be modified if the entry already exists, which means the value must be set correctly at the time of entry creation.
Authentication Password	A string identifying the authentication pass phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. Only ASCII characters from 33 to 126 are allowed.
Privacy Protocol	Indicates the privacy protocol used for data privacy, including: **None**: no privacy protocol. **DES**: an optional flag to indicate that this user is using DES authentication protocol.
Privacy Password	A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and only ASCII characters from 33 to 126 are allowed.

5.5.4 SNMP Group Configurations

An SNMP group is an access control policy for you to add users. Each SNMP group is configured with a security model, and is associated with an SNMP view. A user within an SNMP group should match the security model of the SNMP group. These parameters specify what type of authentication and privacy a user within an SNMP group uses. Each SNMP group name and security model pair must be unique. This page allows you to configure the SNMPv3 group table. The entry index keys are **Security Model** and **Security Name**.

SNMPv3 Group Configuration

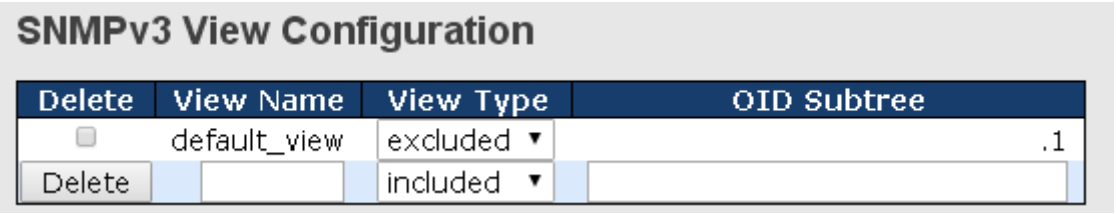
Delete	Security Model	Security Name	Group Name
☐	v1	public	default_ro_group
☐	v1	private	default_rw_group
☐	v2c	public	default_ro_group
☐	v2c	private	default_rw_group
☐	usm	default_user	default_rw_group

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Security Model	Indicates the security model that this entry should belong to. Possible

	security models include: **v1**: Reserved for SNMPv1. **v2c**: Reserved for SNMPv2c. **usm**: User-based security model (USM).
Security Name	The name of user connecting to the SNMP agent. The name varies with the selected security model. For SNMP v1 and v2c, the name is configured on the SNMPv3 Communities Configuration menu. For USM (or SNMPv3), the names is based on those configured in the SNMPv3 Users Configuration menu. You need to delete the current entry to modify an entry for USM.
Group Name	The name of the SNMP group. The string length is limited between 1 and 32 characters and only ASCII characters from 33 to 126 are allowed.

5.5.5 SNMP View Configurations

The SNMP v3 View table specifies the MIB object access requirements for each View Name. You can specify specific areas of the MIB that can be accessed or denied based on the entries or create and delete entries in the View table in this page. The entry index keys are **View Name** and **OID Subtree**.

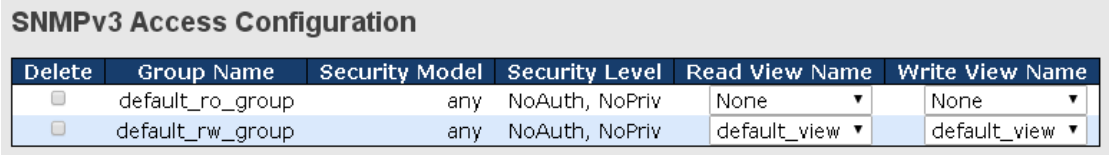


Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The string length is limited between 1 and 32 characters and only ASCII characters from 33 to 126 are allowed.
View Type	Indicates the view type that this entry should belong to. Possible view types include: **Included**: a branch within the MIB tree is included in the SNMP view. **Excluded**: a branch within the MIB tree is excluded from the SNMP view. In this case, another entry whose view type is **Included** should exist, and its OID subtree should overstep the **Excluded** entry.
OID Subtree	Object identifiers of branches within the MIB tree. Note that the first

	character must be a period (.). Wild cards can be used to mask a specific portion of the OID string using an asterisk.

5.5.6 SNMP Access Configurations

This page allows you to configure SNMPv3 access table. The entry index keys are **Group Name**, **Security Model**, and **Security Level**.



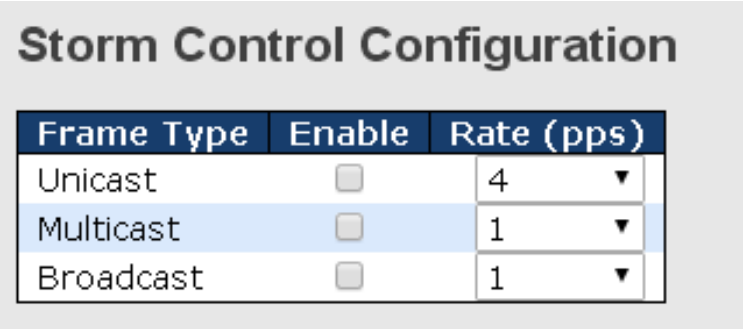
Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Group Name	The name of the SNMP group. The string length is limited between 1 and 32 characters and only ASCII characters from 33 to 126 are allowed.
Security Model	Indicates the security model that this entry should belong to. Possible security models include: **any**: Accepted any security model (v1|v2c|usm). **v1**: Reserved for SNMPv1. **v2c**: Reserved for SNMPv2c. **usm**: User-based Security Model (USM).
Security Level	Indicates the security model that this entry should belong to. Possible security models include: **NoAuth, NoPriv**: no authentication and encryption used in SNMP communications. **Auth, NoPriv**: Authentication is used but data is not encrypted. **Auth, Priv**: both authentication and encryption is used.
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values. The string length is limited between 1 and 32 characters and only ASCII characters from 33 to 126 are allowed.
Write View Name	The name of the MIB view defining the MIB objects for which this request may potentially SET new values. The string length is limited between 1 and 32 characters and only ASCII characters from 33 to 126 are allowed.

5.6 Traffic Prioritization

5.6.1 Storm Control

A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configuration, or users issuing a denial-of-service attack can cause a storm. Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port. In this page, you can specify the rate at which packets are received for unicast, multicast, and broadcast traffic. The unit of the rate can be either pps (packets per second) or kpps (kilopackets per second).

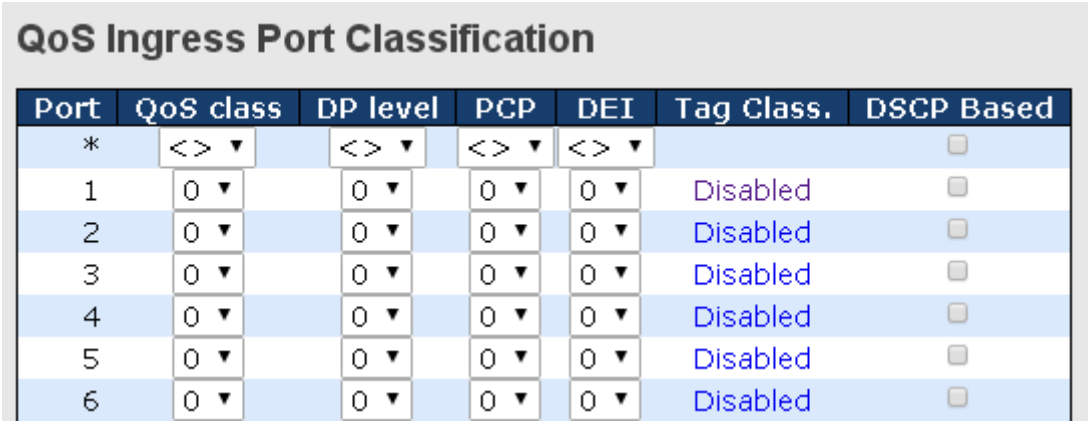
Note: frames sent to the CPU of the switch are always limited to approximately 4 kpps. For example, broadcasts in the management VLAN are limited to this rate. The management VLAN is configured on the IP setup page.



Label	Description
Frame Type	Frame types supported by the Storm Control function, including **Unicast**, **Multicast**, and **Broadcast**.
Status	Enables or disables the given frame type
Rate	The threshold above which packets are dropped. The rate is packet per second (pps). You can specify a value of 2n packets per second (pps) or by select one of the options in Kpps (value marked with the suffix “K”).

5.6.2 Port Classification

QoS (Quality of Service) is a method to achieve efficient bandwidth utilization between devices by prioritizing frames according to individual requirements and transmit the frames based on their importance. Frames in higher priority queues receive a bigger slice of bandwidth than those in a lower priority queue.

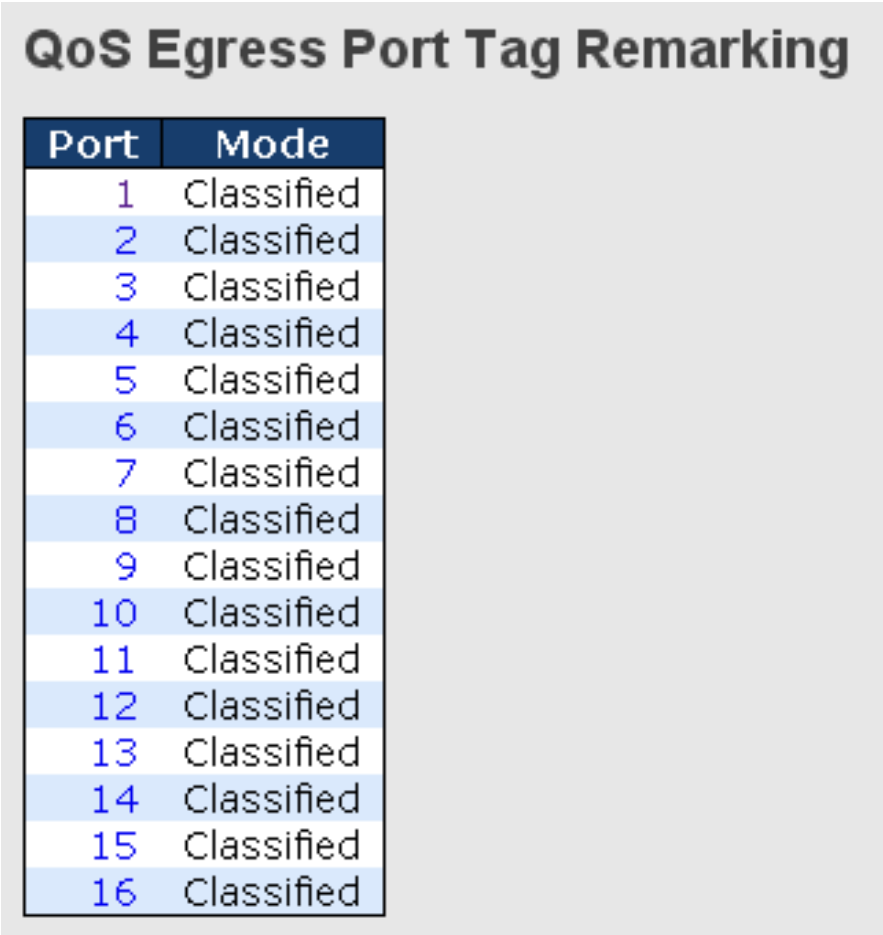


Label	Description
Port	The port number for which the configuration below applies
QoS Class	Controls the default QoS class All frames are classified to a QoS class. There is a one to one mapping between QoS class, queue, and priority. A QoS class of 0 (zero) has the lowest priority. If the port is VLAN aware and the frame is tagged, then the frame is classified to a QoS class that is based on the PCP value in the tag as shown below. Otherwise the frame is classified to the default QoS class. PCP value: 0 1 2 3 4 5 6 7 QoS class: 1 0 2 3 4 5 6 7 If the port is VLAN aware, the frame is tagged, and Tag Class is enabled, then the frame is classified to a QoS class that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default QoS class. The classified QoS class can be overruled by a QCL entry. Note: if the default QoS class has been dynamically changed, then the actual default QoS class is shown in parentheses after the configured default QoS class.
DP level	Controls the default Drop Precedence Level All frames are classified to a DP level. If the port is VLAN aware and the frame is tagged, then the frame is classified to a DP level that is equal to the DEI value in the tag. Otherwise the frame is classified to the default DP level. If the port is VLAN aware, the frame is tagged, and Tag Class is

	enabled, then the frame is classified to a DP level that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DP level. The classified DP level can be overruled by a QCL entry.
PCP	Controls the default PCP value All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.
DEI	Controls the default DEI value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.
Tag Class	Shows the classification mode for tagged frames on this port **Disabled**: Use default QoS class and DP level for tagged frames. **Enabled**: Use mapped versions of PCP and DEI for tagged frames. Click on the mode to configure the mode and/or mapping. Note: this setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN-unaware ports are always classified to the default QoS class and DP level.
DSCP Based	Click to enable DSCP-based QoS ingress port classification

5.6.3 Port Tag Remarking

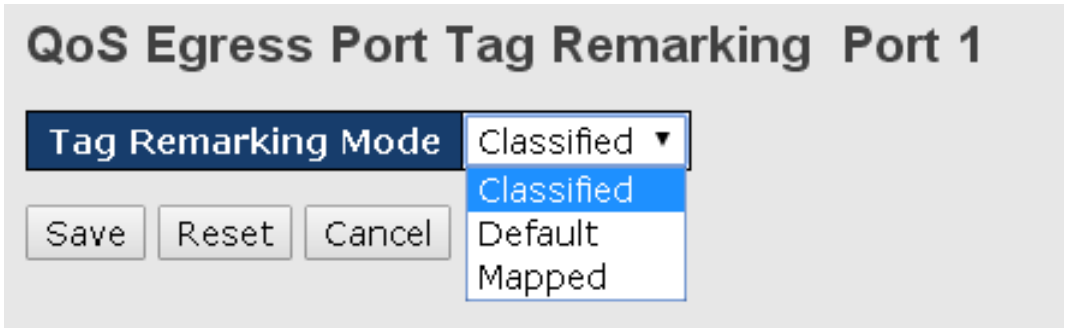
You can set QoS egress queues on a port such as classifying data and marking it according to its priority and the policies. Packets will then travel across the switch's internal paths carrying their assigned QoS tag markers. At the egress port, these markers are read and used to determine which queue each data packet is forwarded to. When the traffic does not conform to the conditions set in a policer command, you can remark the traffic.

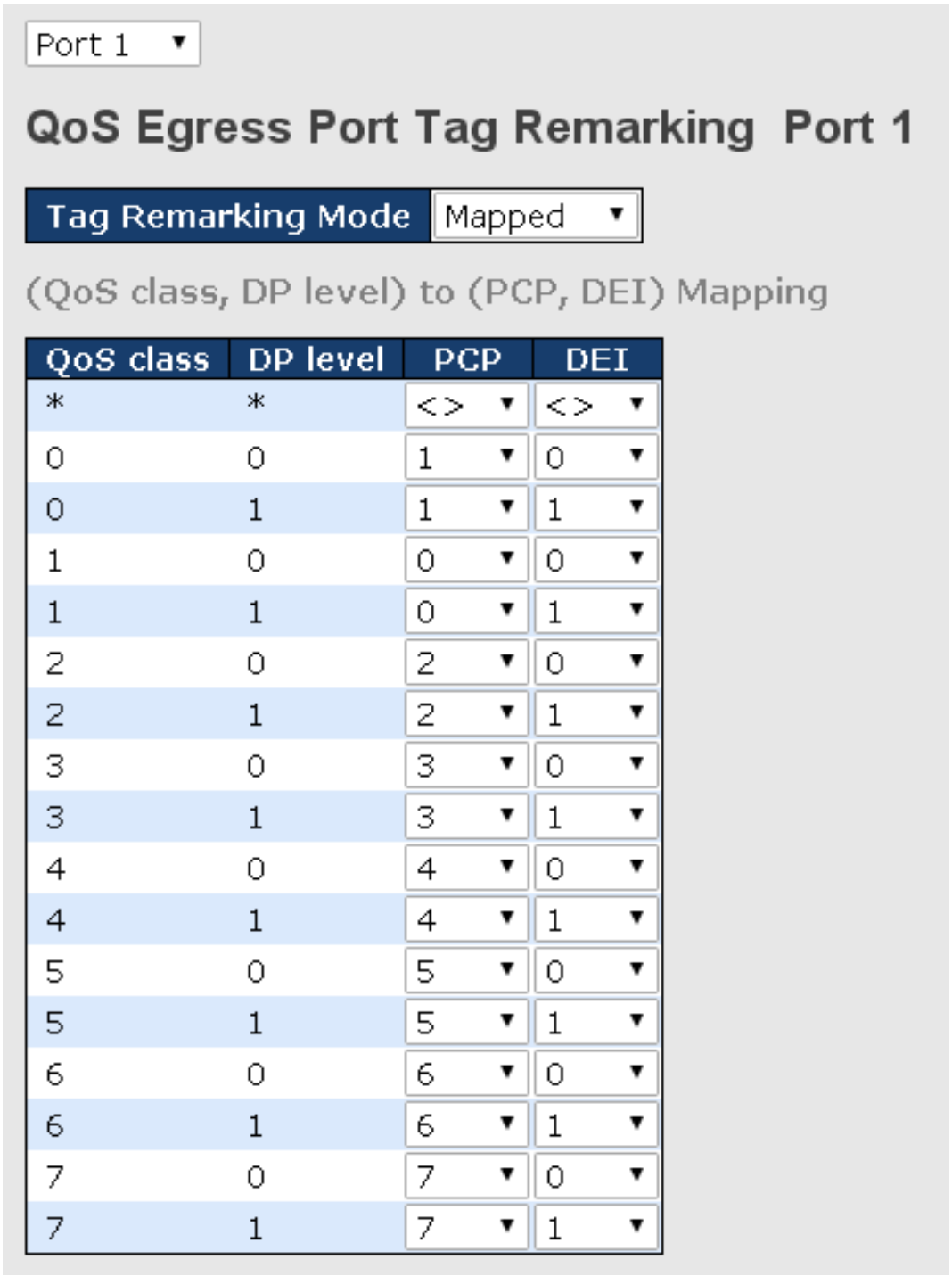


Label	Description
Port	The switch port number to which the following settings will be applied. Click on the port number to configure tag remarking
Mode	Shows the tag remarking mode for this port **Classified**: use classified PCP/DEI values **Default**: use default PCP/DEI values **Mapped**: use mapped versions of QoS class and DP level

Click on an entry in the Port field will take you to the configuration page of the remarking mode where you can set up classified PCP/DEI values, default PCP/DEI values, or mapped versions of QoS class and drop priority.

You can choose three tag remarking modes including **Classified**, **Default**, and **Mapped**. **Classified** will use classified PCP (Priority Code Point or User Priority) and DEI (Drop Eligible Indicator) values. **Default** will use default PCP/DEI values. **Mapped** will use mapped versions of QoS class and drop precedence level.



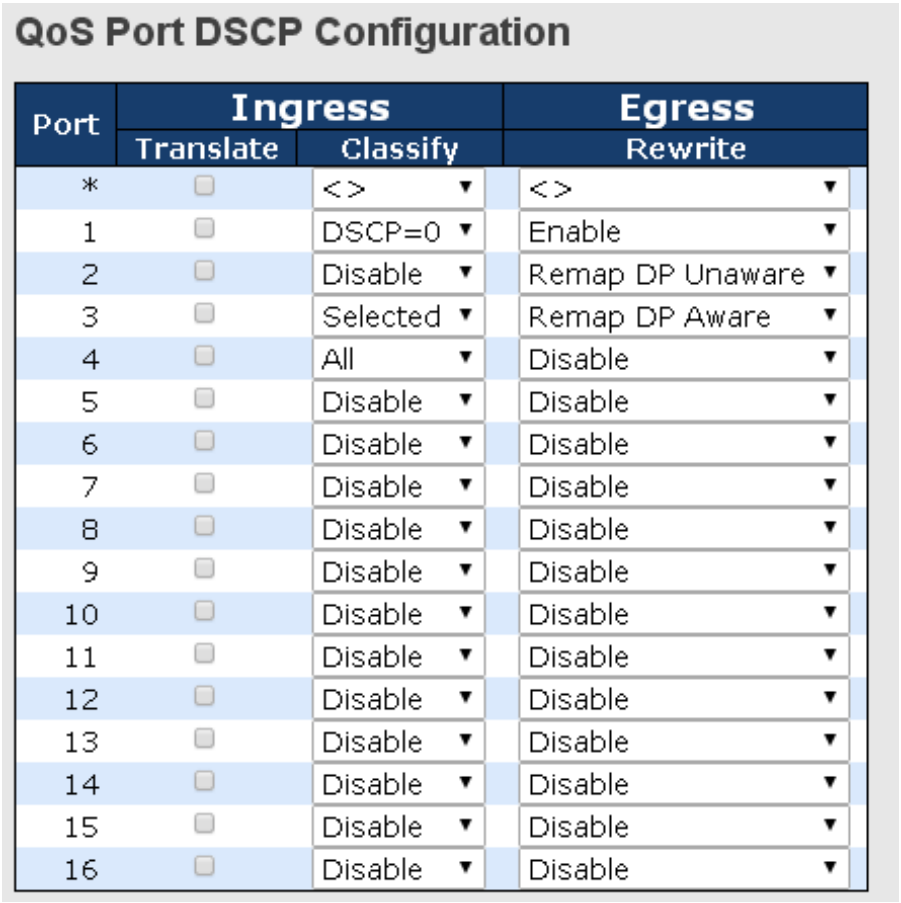


QoS class	DP level	PCP	DEI
*	*	<>	<>
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	1
2	0	2	0
2	1	2	1
3	0	3	0
3	1	3	1
4	0	4	0
4	1	4	1
5	0	5	0
5	1	5	1
6	0	6	0
6	1	6	1
7	0	7	0
7	1	7	1

Label	Description
QoS class/DP level	Shows the mapping options for QoS class values and DP levels (drop precedence).
PCP	Priority Code Point: maps to the frame priority level. Values in order of priority are: 1 (background), 0 (best effort), 2 (excellent effort), 3 (critical application), ..., 7 (network control). These values can be used to prioritize different classes of traffic.
DEI	Drop Eligible Indicator: indicates frames eligible to be dropped in the presence of congestion.

5.6.4 Port DSCP

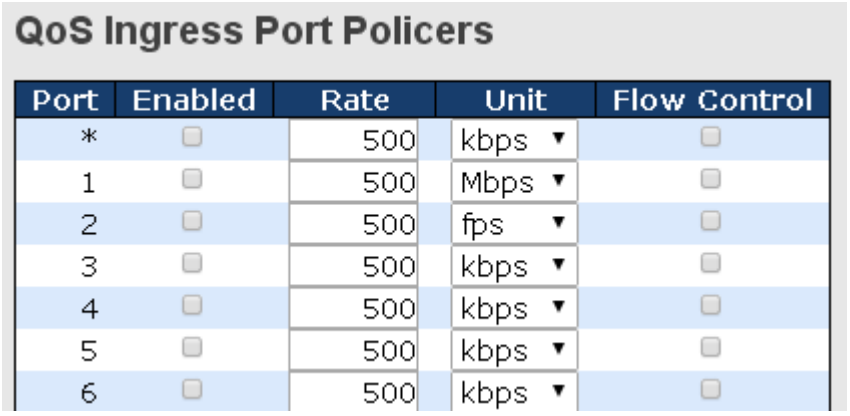
DSCP (Differentiated Services Code Point) is a measure of QoS. It can classify data packets by using the 6-bit DS field in the IP header so you can manage each traffic class differently and efficiently, thereby achieving optimized use of network bandwidth. DSCP-enabled routers on the network will read the DSCP value of the data packet and put the packet into different queues before transmission, such as high priority and most efficient transmission. With such QoS functions, you can ensure low-latency for critical traffic. This page allows you to configure DSCP settings for each port.



Label	Description
Port	Shows the list of ports for which you can configure DSCP Ingress and Egress settings.
Ingress	In **Ingress** settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: **Translate:** check to enable the function **Classify:** includes four values **Disable**: no Ingress DSCP classification **DSCP=0**: classify if incoming (or translated if enabled) DSCP is 0. **Selected**: classify only selected DSCP whose classification is enabled as specified in **DSCP Translation** window for the specific DSCP. **All**: classify all DSCP
Egress	Port egress rewriting can be one of the following options: **Disable**: no Egress rewrite **Enable**: rewrite enabled without remapping **Remap DP Unaware**: DSCP from the analyzer is remapped and the frame is remarked with a remapped DSCP value. The remapped DSCP value is always taken from the '**DSCP Translation->Egress Remap DP0**' table. **Remap DP Aware**: DSCP from the analyzer is remapped and the frame is remarked with a remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the '**DSCP Translation->Egress Remap DP0**' table or from the '**DSCP Translation->Egress Remap DP1**' table.

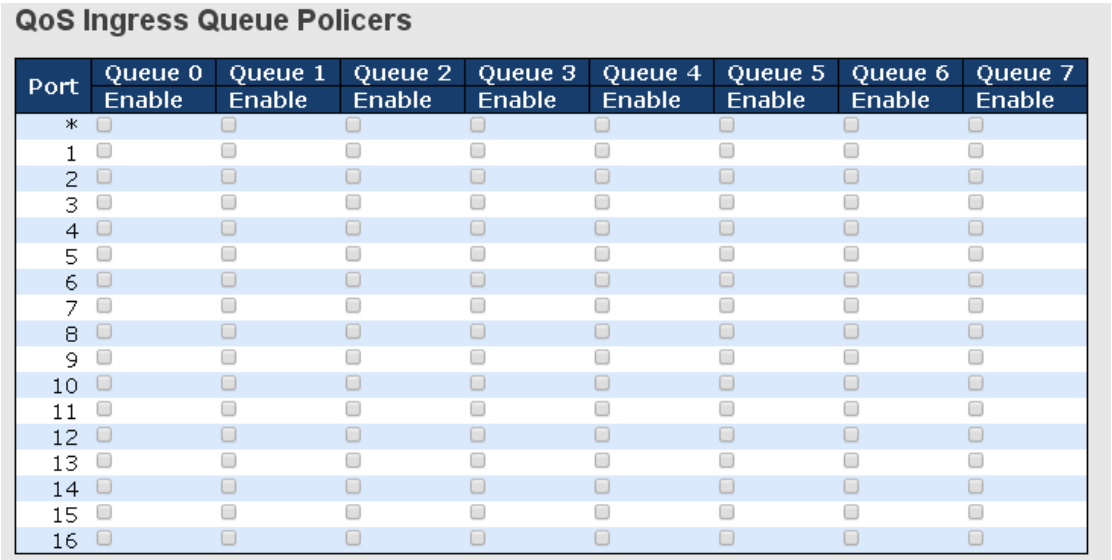
5.6.5 Policing

Policing is a traffic regulation mechanism for limiting the rate of traffic streams, thereby controlling the maximum rate of traffic sent or received on an interface. When the traffic rate exceeds the configured maximum rate, policing drops or remarks the excess traffic. This page allows you to configure Policer for all switch ports.



Label	Description
Port	The port number for which the configuration below applies
Enable	Check to enable the policer for individual switch ports
Rate	Configures the rate of each policer. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps** or **fps**, and is restricted to 1 to 3300 when the **Unit** is **Mbps** or **kfps**.
Unit	Configures the unit of measurement for each policer rate as **kbps**, **Mbps**, **fps**, or **kfps**. The default value is **kbps**.
Flow Control	If **Flow Control** is enabled and the port is in **Flow Control** mode, then pause frames are sent instead of being discarded.

5.6.6 Queue Policing



Label	Description
Port	The port number for which the configuration below applies.

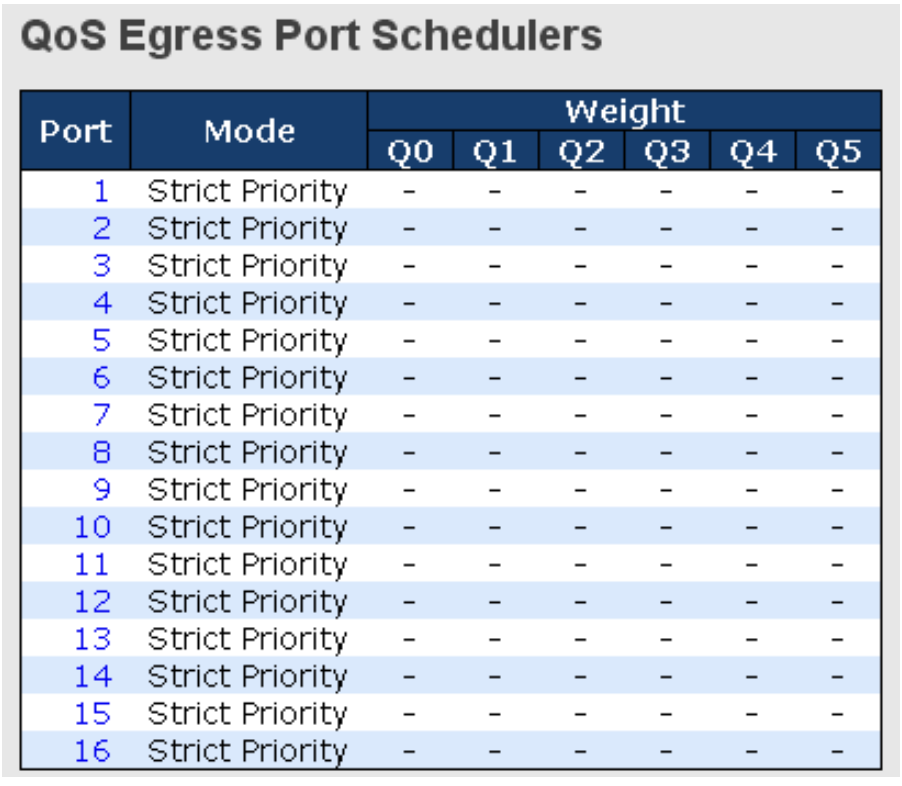
Queue Enable	Check to enable queue policer for individual switch ports
Rate	Configures the rate of each queue policer. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps**, and is restricted to 1 to 3300 when the **Unit** is **Mbps**. This field is only shown if at least one of the queue policers is enabled.
Unit	Configures the unit of measurement for each queue policer rate as kbps or Mbps. The default value is **kbps**. This field is only shown if at least one of the queue policers is enabled.

5.6.7 Port Scheduler

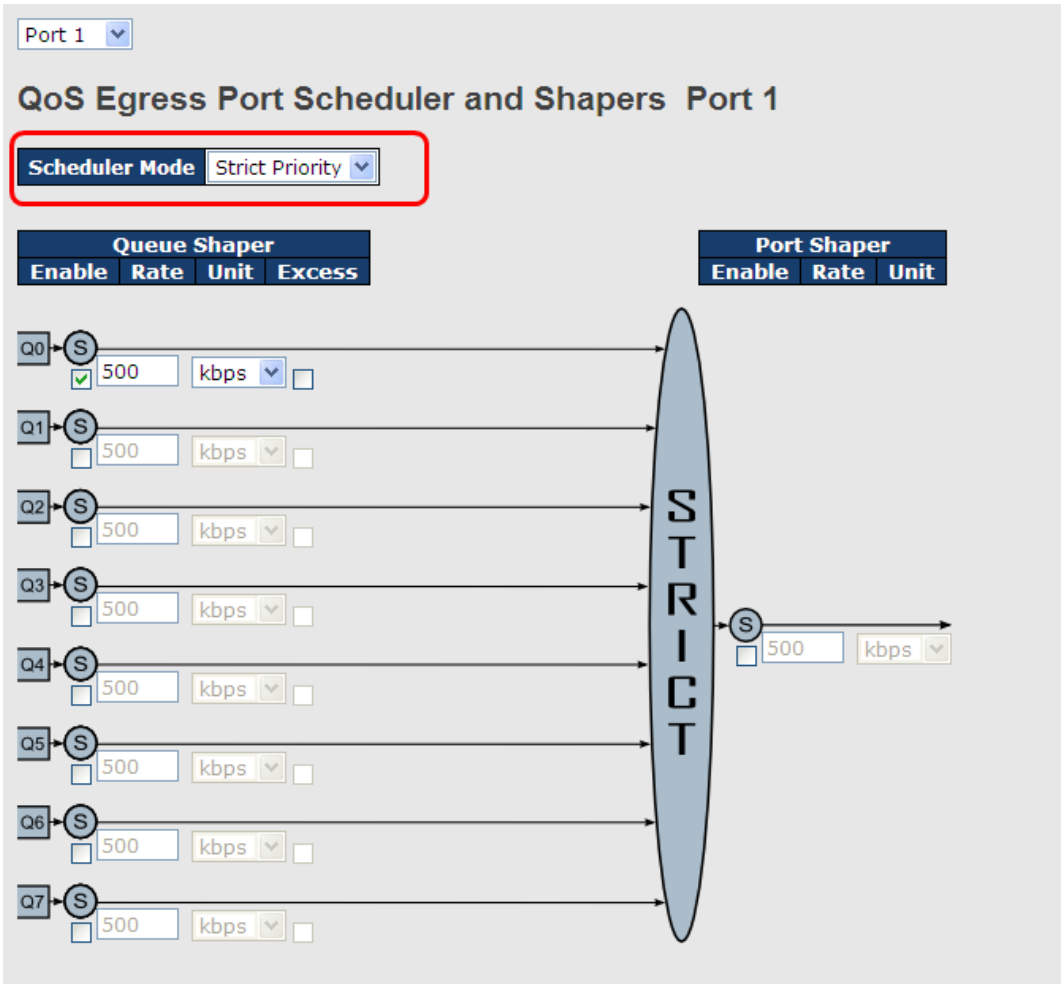
Port scheduling can solve performance degradation during network congestions. The schedulers allow switches to maintain separate queues for packets from each source and prevent specific traffic to use up all bandwidth. This page allows you to configure Scheduler and Shapers for individual ports.

Strict Priority

Strict Priority uses queues based only priority. When traffic arrives at the device, traffic on the highest priority queue will be transmitted first, followed by traffic on lower priorities. If there is always some content in the highest priority queue, then the other packets in the rest of queues will not be sent until the highest priority queue is empty. The SP algorithm is preferred when the received packets contain high priority data, such as voice and video.



Click on the port number will lead to the following page.

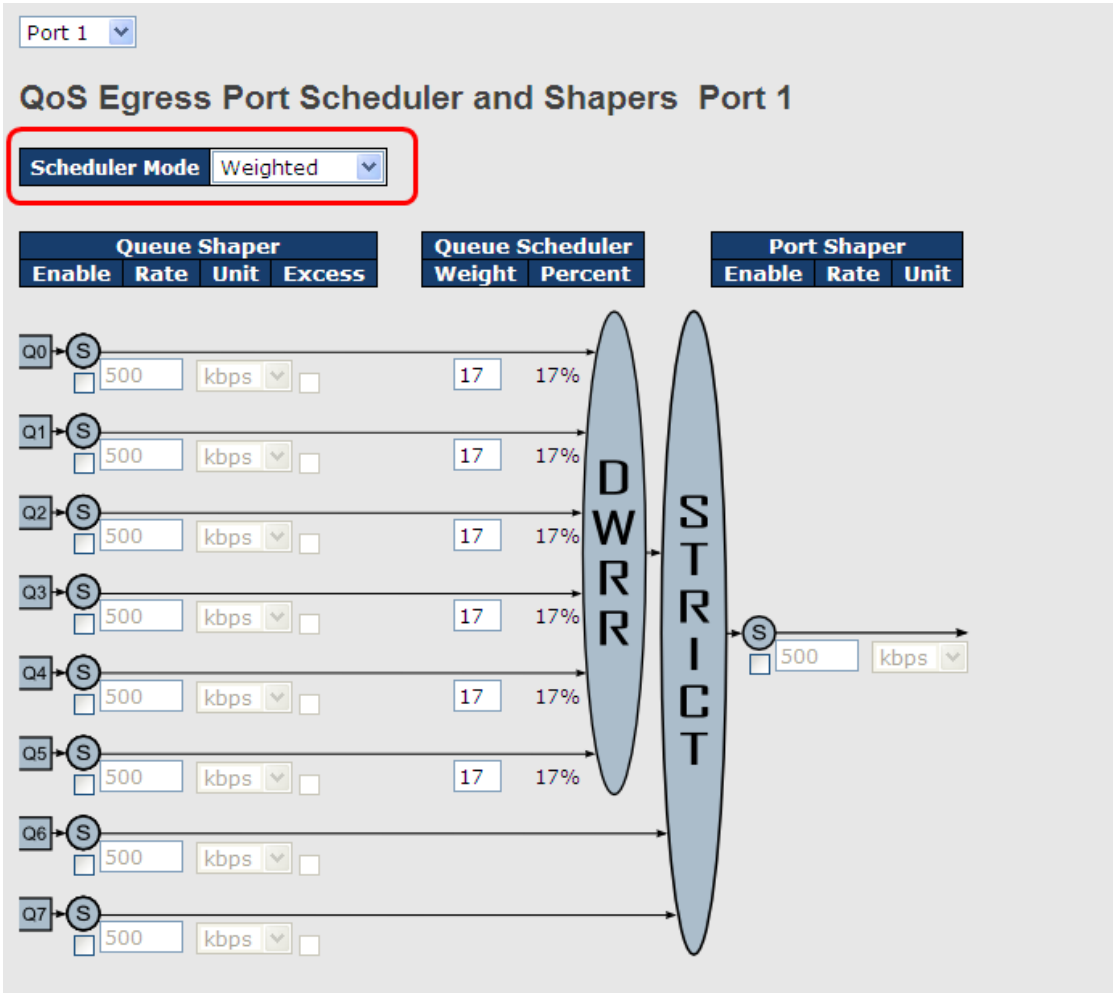


Label	Description
Scheduler Mode	Two scheduling modes are available: **Strict Priority** or **Weighted**.
Queue Shaper Enable	Check to enable queue shaper for individual switch ports.
Queue Shaper Rate	Configures the rate of each queue shaper. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps**", and it is restricted to 1 to 3300 when the **Unit** is **Mbps**.
Queues Shaper Unit	Configures the rate for each queue shaper. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps**, and it is restricted to 1 to 3300 when the **Unit** is **Mbps**.
Queue Shaper Excess	Allows the queue to use excess bandwidth.
Port Shaper Enable	Check to enable port shaper for individual switch ports.
Port Shaper Rate	Configures the rate of each port shaper. The default value is **500** This value is restricted to 100 to 1000000 when the **Unit** is **kbps**,

	and it is restricted to 1 to 3300 when the **Unit** is **Mbps**.
Port Shaper Unit	Configures the unit of measurement for each port shaper rate as **kbps** or **Mbps**. The default value is **kbps**.

Weighted

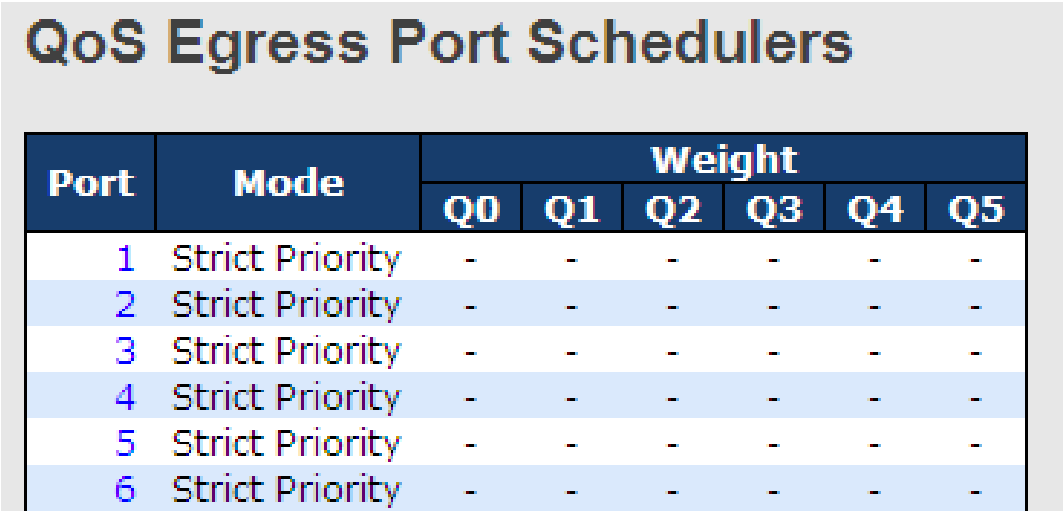
Weighted scheduling will deliver traffic on a rotating basis. It can guarantee each queue's minimum bandwidth based on their bandwidth weight when there is traffic congestion. Only when a port has more traffic than it can handle will this mode be activated. A queue is given an amount of bandwidth regardless of the incoming traffic on that port. Queue with larger weights will have more guaranteed bandwidth than others with smaller weights.



Label	Description
Scheduler Mode	Two scheduling modes are available: **Strict Priority** or **Weighted.**
Queue Shaper Enable	Check to enable queue shaper for individual switch ports.
Queue Shaper Rate	Configures the rate of each queue shaper. The default value is

	500. This value is restricted to 100 to 1000000 when the **Unit** is **kbps**, and it is restricted to 1 to 3300 when the **Unit** is **Mbps**.
Queues Shaper Unit	Configures the rate of each queue shaper. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit**" is **kbps**, and it is restricted to 1 to 3300 when the **Unit** is **Mbps**.
Queue Shaper Excess	Allows the queue to use excess bandwidth
Queue Scheduler Weight	Configures the weight of each queue. The default value is **17**. This value is restricted to 1 to 100. This parameter is only shown if **Scheduler Mode** is set to **Weighted**.
Queue Scheduler Percent	Shows the weight of the queue in percentage. This parameter is only shown if **Scheduler Mode** is set to **Weighted**.
Port Shaper Enable	Check to enable port shaper for individual switch ports
Port Shaper Rate	Configures the rate of each port shaper. The default value is **500**. This value is restricted to 100 to 1000000 when the **Unit** is **kbps**, and it is restricted to 1 to 3300 when the **Unit** is **Mbps**.
Port Shaper Unit	Configures the unit of measurement for each port shaper rate as **kbps** or **Mbps**. The default value is **kbps**.

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

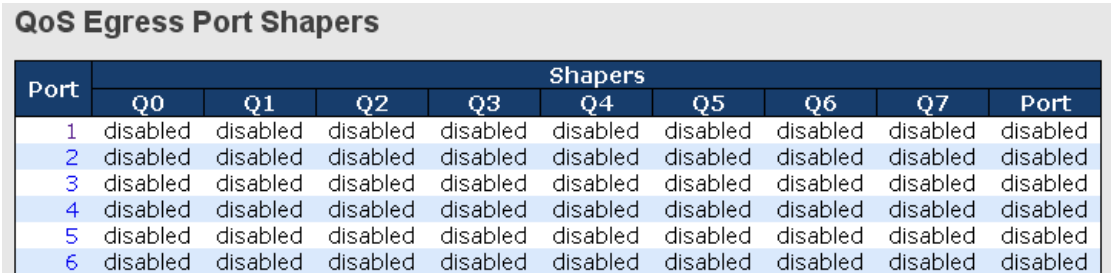


Label	Description
Port	The switch port number to which the following settings will be applied. Click on the port number to configure the schedulers

Mode	Shows the scheduling mode for this port
Qn	Shows the weight for this queue and port

5.6.8 Port Shaping

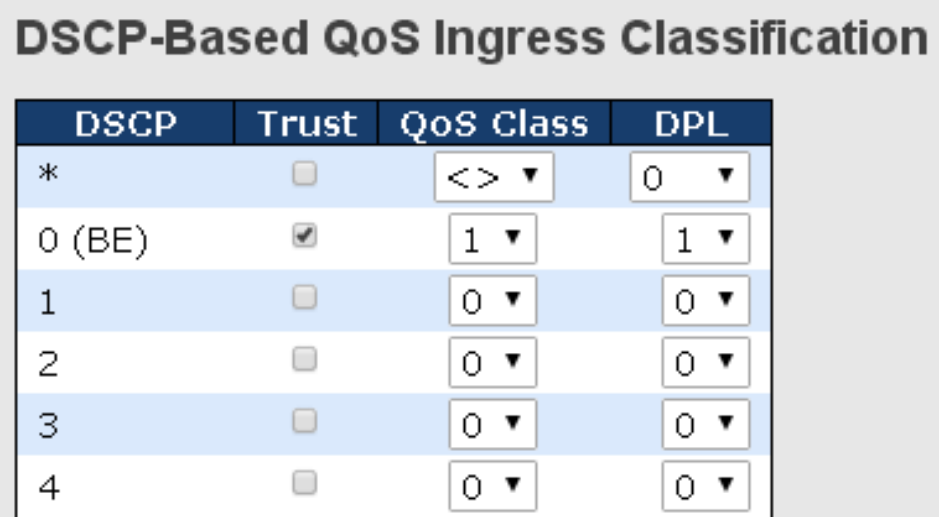
Port shaping enables you to limit traffic on a port, thereby controlling the amount of traffic passing through the port. With port shaping, you can shape the aggregate traffic through an interface to a rate that is less than the line rate for that interface. When configuring port shaping on an interface, you specify a value indicating the maximum amount of traffic allowable for the interface. This value must be less than the maximum bandwidth for that interface.



Label	Description
Port	The switch port number to which the following settings will be applied. Click on the port number to configure the shapers
Mode	Shows **disabled** or actual queue shaper rate - e.g. "800 Mbps"
Q0~Q7	Shows **disabled** or actual port shaper rate - e.g. "800 Mbps"

5.6.9 DSCP-based QoS

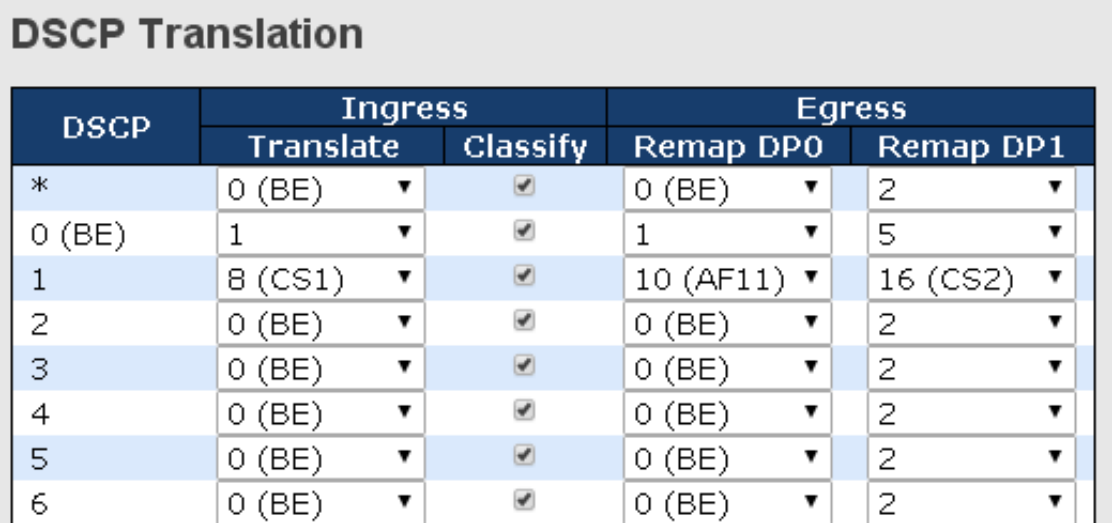
This page allows you to configure DSCP-based QoS ingress classification settings for all ports.



Label	Description
DSCP	DSP value in ingress package. The maximum value is 64
Trust	Check to trust a specific DSCP value. Only frames with trusted DSCP values are mapped to a specific QoS class and drop precedence level. Frames with untrusted DSCP values are treated as a non-IP frame.
QoS Class	QoS class value can be any number from 0-7.
DPL	Drop Precedence Level (0-1)

5.6.10 DSCP Translation

This page allows you to configure basic QoS DSCP translation settings for all switches. DSCP translation can apply to **Ingress** or **Egress**.

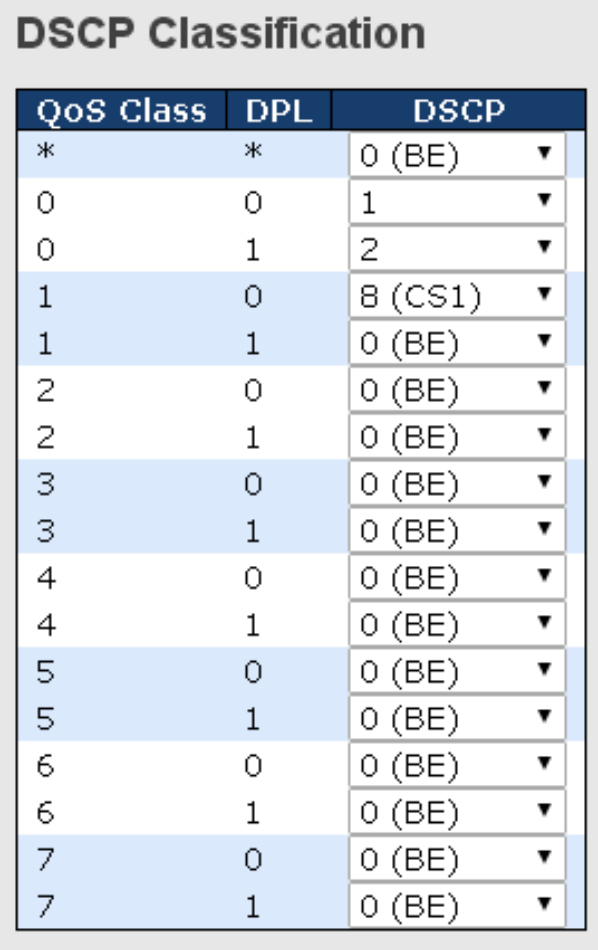


Label	Description
DSCP	Maximum number of supported DSCP values is 64 and valid DSCP value ranges from 0 to 63.
Ingress	Ingress DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two parameters for this: 1. **Translate:** Enables ingress translation of DSCP values based on the specified classification method. DSCP can be translated to any of (0-63) DSCP values. 2. **Classify:** Enable classification at ingress side according to the definition in the QoS Port DSCP Configuration table.
Egress	Configurable engress parameters include;

	Remap DP0: Re-maps DP0 field to selected DSCP value. DP0 means a drop precedence with a low priority. You can select the DSCP value from a selected menu to which you want to remap. DSCP value ranges from 0 to 63. **Remap DP1**: Re-maps DP1 field to selected DSCP value. DP1 means a drop precedence with a high priority. You can select the DSCP value from a selected menu to which you want to remap. DSCP value ranges from 0 to 63.

5.6.11 DSCP Classification

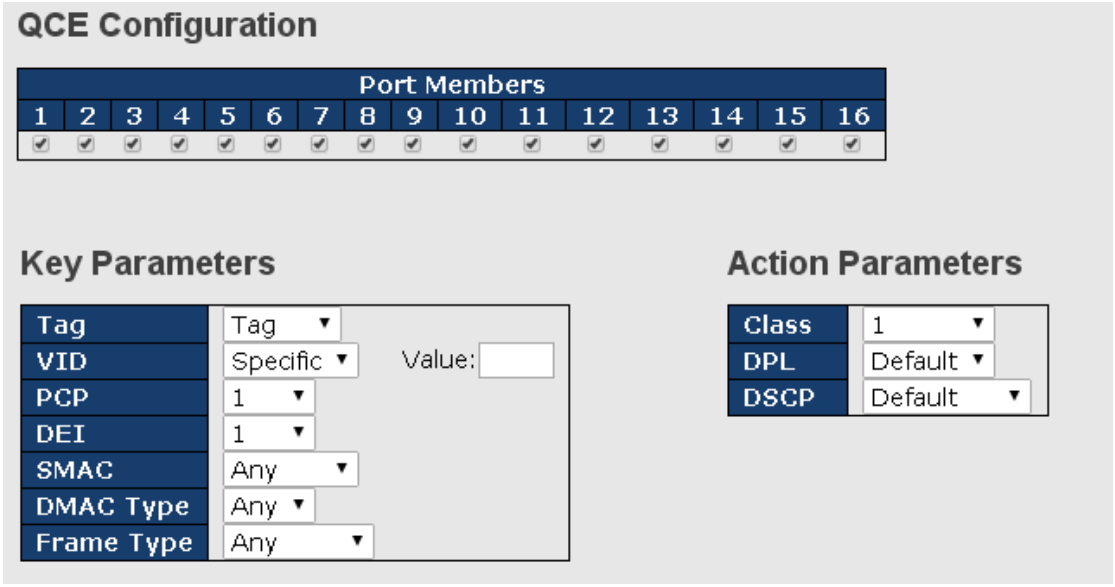
This page allows you to configure the mapping of QoS class and drop precedence level to DSCP value.



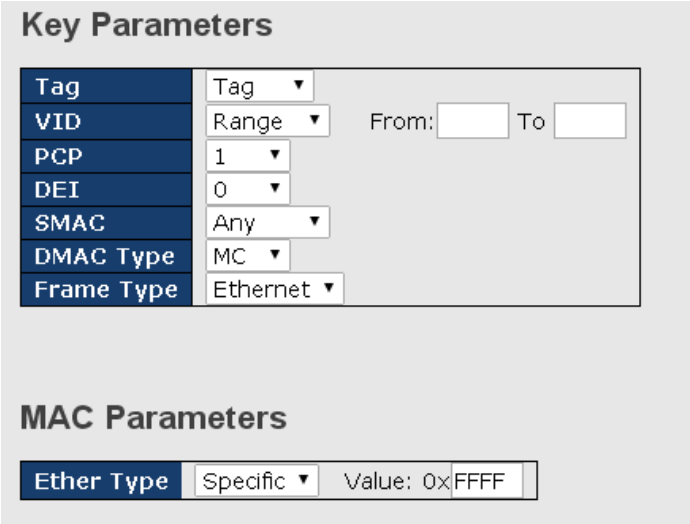
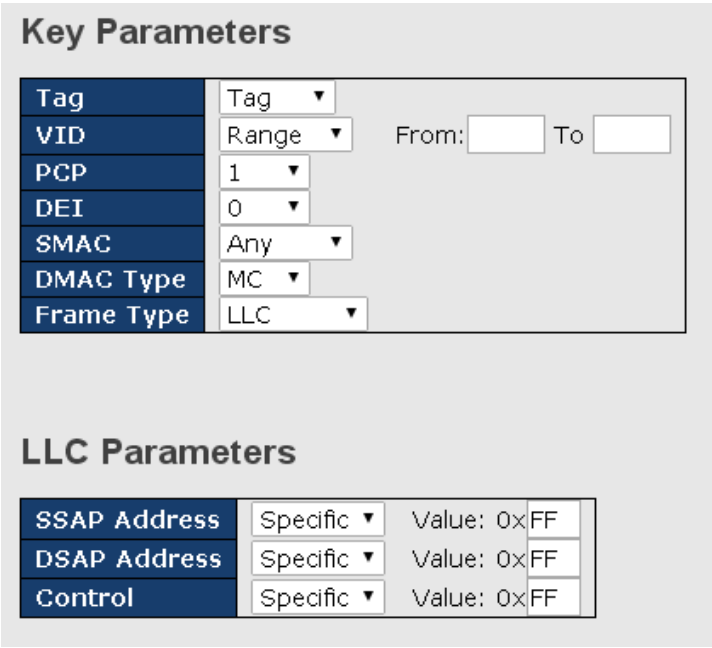
Label	Description
QoS Class	Actual QoS class
DPL	Actual Drop Precedence Level
DSCP	Select the classified DSCP value (0-63)

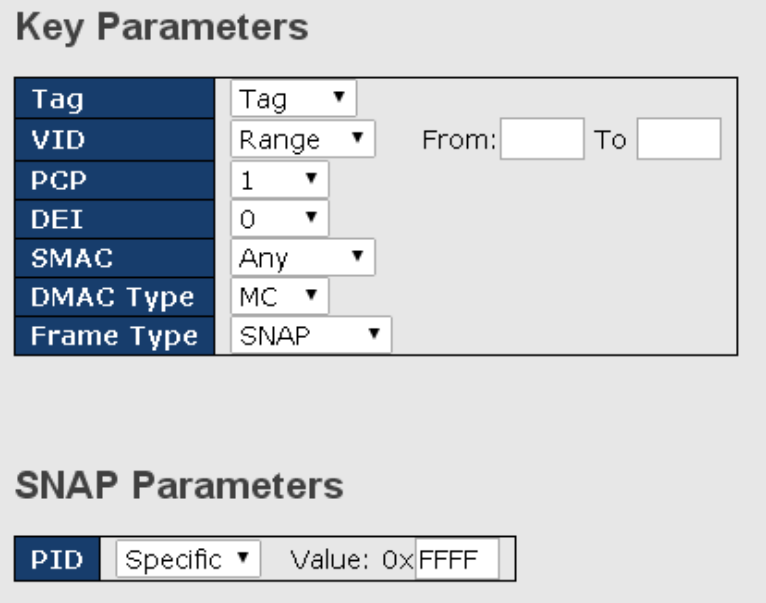
5.6.12 QoS Control List

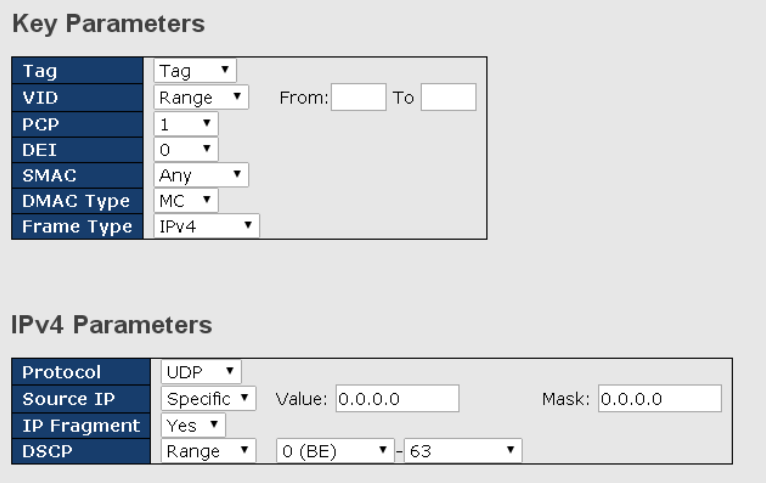
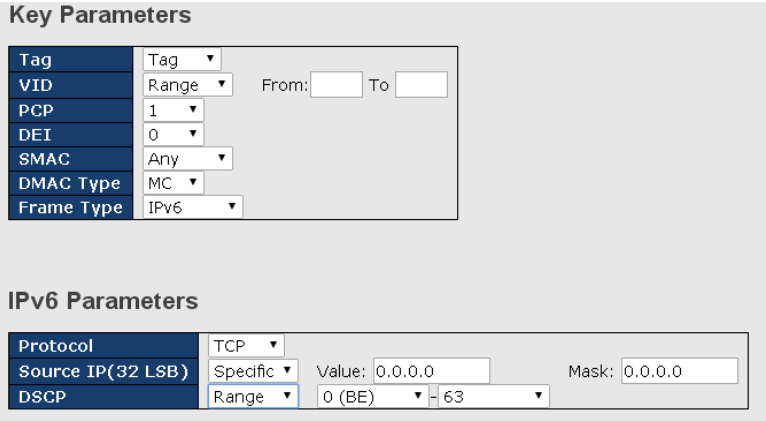
This page shows all the QCE (Quality Control Entries) for a given QCL. You can edit or add new QoS control entries in this page. A QCE consists of several parameters. These parameters vary with the frame type you select.



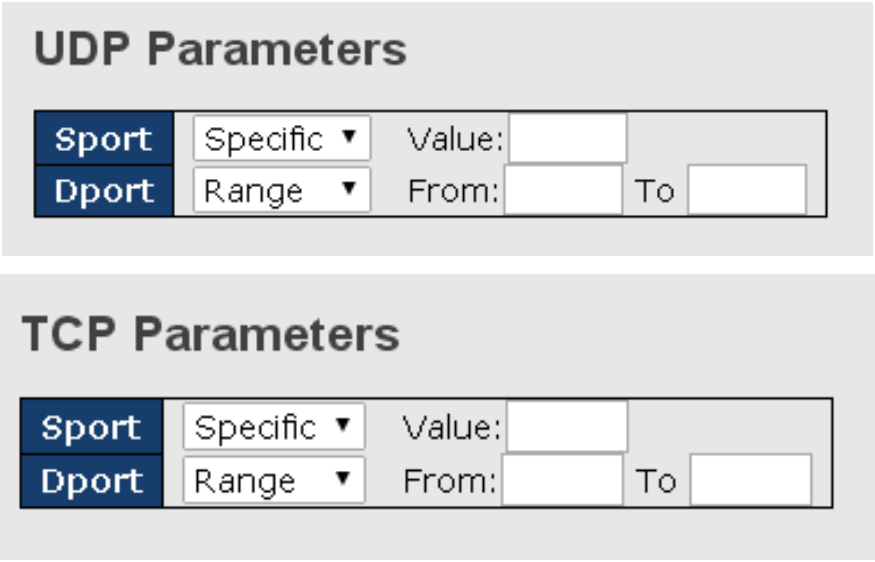
Label	Description
Port Members	Check to include the port in the QCL entry. By default, all ports are included.
Key Parameters	Key configurations include: **Tag**: VLAN tag type, can be any value, untag or tag. **VID**: VLAN ID, can be any value, a specific value between 1 and 4095, or a range. **PCP**: Priority Code Point, can be specific numbers (0, 1, 2, 3, 4, 5, 6, 7), a range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or **Any** **DEI**: Drop Eligible Indicator, can be any of values between 0 and 1 or **Any** **SMAC**: Source MAC Address, can be 24MS bits (OUI) or **Any** **DMAC Type**: the type of destination MAC address, including **unicast** (**UC**), **multicast** (**MC**), **broadcast** (**BC**) or **Any**. **Frame Type:** require ACLs to provide frame filtering based on frame type. Available options include **Any**, **Ethernet**, **LLC**, **SNAP**, **IPv4**, and **IPv6**. Note: all frame types are explained below.
Any	Allow all types of frames

Ethernet	This option can only be used to filter Ethernet II formatted packets. You can choose Ethernet type as Any or Specific which allows you to specify a value ranging from 0x600 to 0xFFFF. The default value is **Any**. 
LLC	**SSAP Address**: valid SSAP (Source Service Access Point) values can range from 0x00 to 0xFF or **Any**. The default value is **Any**. **DSAP Address**: valid DSAP (Destination Service Access Point) values can range from 0x00 to 0xFF or **Any**. The default value is **Any**. **Control**: valid values can range from 0x00 to 0xFF or **Any**. The default value is **Any**. 

SNAP	SNAP (SubNetwork Access Protocol) can be distinguished by an OUI and a Protocol ID. If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP. If the OUI is that of a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if value of the OUI field is 00-00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI is other than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff. **PID**: Specify a value from 0x00 to 0xFFFF or any. The default value is **Any**. 
IPv4	**Protocol**: Specifies the IP protocol to filter for this rule including Any, UDP, TCP, and Other **Source IP**: you need to enter both the address and mask format for a specific source IP address. The address and mask must be in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When the mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero. **IP Fragment**: indicates whether or not fragmented packets are accepted. Fragmentation can ensure data pass through a network device whose maximum transfer unit is smaller than the

	original packet's size. 
IPv6	**Protocol**: (Specifies the IP protocol to filter for this rule including Any, UDP, TCP, and Other **Source IP**: For a specific IPv6 source address, you need to enter the least significant 32 bits (a.b.c.d) using the same type of mask as that used for an IPv4 address. **DSCP**: specify a Diffserv Code Point value which can be a specific value, a range, or any. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43. 
Action Parameters	Class QoS class: (0-7) or **Default** Valid Drop Precedence Level value can be (0-1) or **Default**. Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or **Default**. Default means that the default classified value is not modified by this QCE.

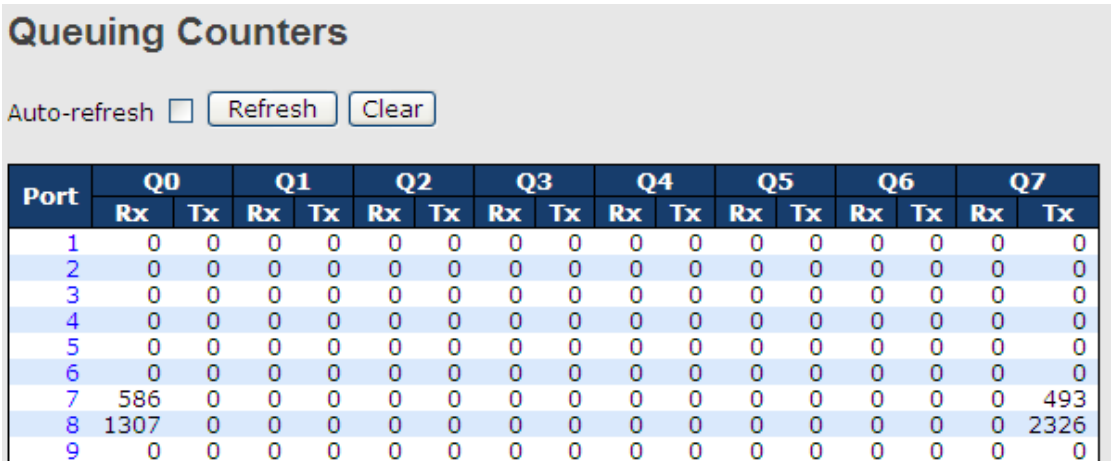
UDP/TCP Parameters



Label	Description
Sport	Source TCP/UDP port.
Dport	Destination TCP/UDP port.

5.6.13 QoS Statistics

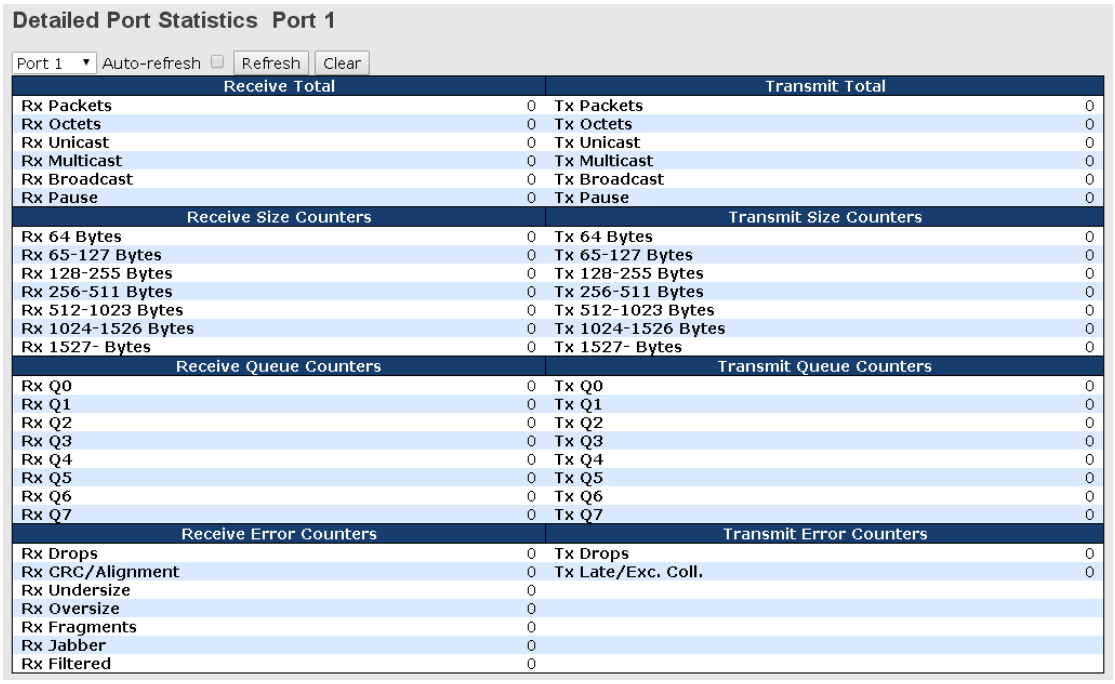
This page shows information on the number of packets sent and received at each queue.



Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	586	0	0	0	0	0	0	0	0	0	0	0	0	0	0	493
8	1307	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2326
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

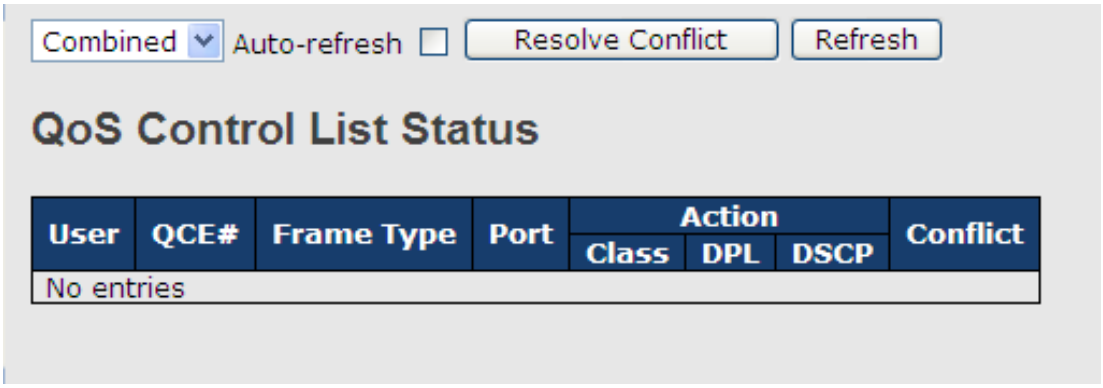
Label	Description
Port	The switch port number to which the following settings will be applied.
Qn	There are 8 QoS queues per port. Q0 is the lowest priority.
Rx / Tx	The number of received and transmitted packets per queue.

Click on the port number will take you to the following page where you can see the traffic information of each port.



5.6.14 QCL Status

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



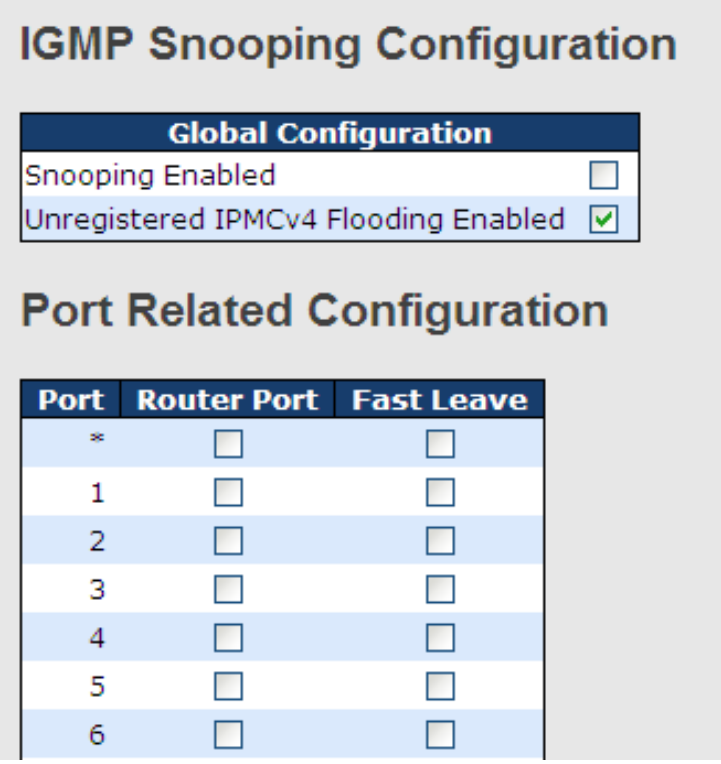
Label	Description
User	Indicates the QCL user.
QCE#	Indicates the index of QCE.
Frame Type	Indicates the type of frame to look for incoming frames. Possible frame types are: **Any**: the QCE will match all frame type.

	Ethernet: Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. **LLC**: Only (LLC) frames are allowed. **SNAP**: Only (SNAP) frames are allowed. **IPv4**: the QCE will match only IPV4 frames. **IPv6**: the QCE will match only IPV6 frames.
Port	Indicates the list of ports configured with the QCE.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: **Class**, **DPL**, and **DSCP**. **Class**: Classified QoS; if a frame matches the QCE, it will be put in the queue. **DPL**: Drop Precedence Level; if a frame matches the QCE, then DP level will set to a value displayed under DPL column. **DSCP**: if a frame matches the QCE, then DSCP will be classified with the value displayed under DSCP column.
Conflict	Displays the conflict status of QCL entries. As hardware resources are shared by multiple applications, 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 hardware resources required to add the QCL entry by pressing Resolve Conflict button.

5.7 Multicast

5.7.1 IGMP Snooping

IGMP (Internet Group Management Protocol) snooping monitors the IGMP traffic between hosts and multicast routers. The switch uses what IGMP snooping learns to forward multicast traffic only to interfaces that are connected to interested receivers. This conserves bandwidth by allowing the switch to send multicast traffic to only those interfaces that are connected to hosts that want to receive the traffic, instead of flooding the traffic to all interfaces in the VLAN. This page allows you to set up IGMP snooping configurations.



Label	Description
Snooping Enabled	Check to enable global IGMP snooping.
Unregistered IPMCv4Flooding enabled	Check to enable unregistered IPMC traffic flooding.
Router Port	Specifies 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	Check to enable fast leave on the port

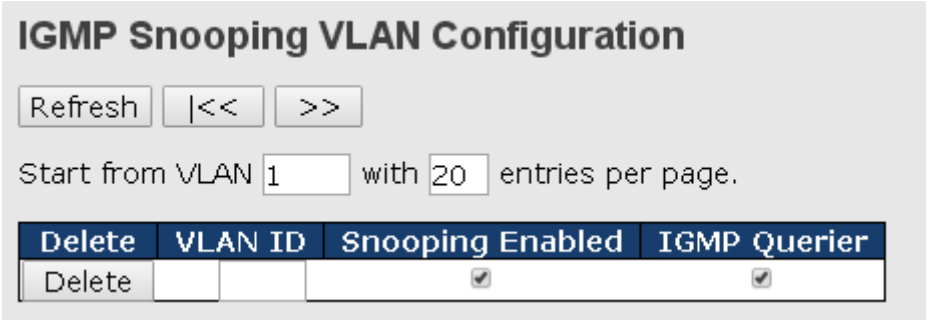
5.7.2 VLAN Configurations of IGMP Snooping

If a VLAN is not IGMP snooping-enabled, it floods multicast data and control packets to the entire VLAN in hardware. When snooping is enabled, IGMP packets are trapped to the CPU. Data packets are mirrored to the CPU in addition to being VLAN flooded. The CPU then installs hardware resources, so that subsequent data packets can be switched to desired ports in hardware without going to the CPU.

Each page shows up to 99 entries from the VLAN table, depending on the value in the Entries Per Page field. By default, the 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.

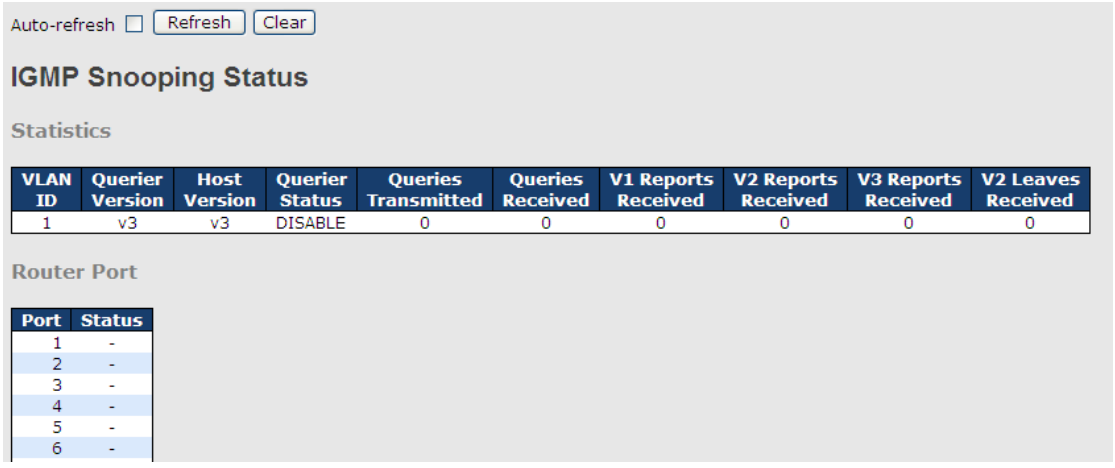
The **VLAN** field allows the user to select the starting point in the VLAN Table. Clicking **Refresh** will update the displayed table starting from that or the next closest VLAN Table match.
The **>>** button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached, the text **No more entries** is shown in the displayed table. Use the **|<<** button to start over.



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

5.7.3 IGMP Snooping Status

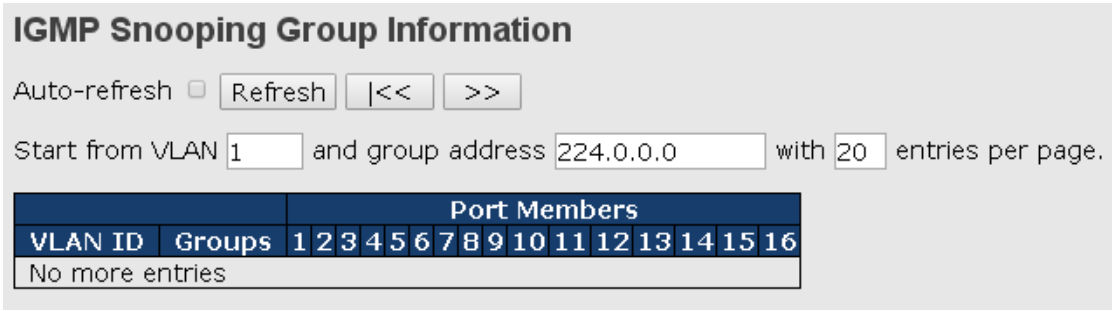
This page provides IGMP snooping status.



Label	Description
VLAN ID	The VLAN ID of the entry
Querier Version	Active Querier version
Host Version	Active Host version
Querier Status	Shows the Querier status as **ACTIVE** or **IDLE**
Querier Receive	The number of transmitted Querier
V1 Reports Receive	The number of received V1 reports
V2 Reports Receive	The number of received V2 reports
V3 Reports Receive	The number of received V3 reports
V2 Leave Receive	The number of received V2 leave packets
Refresh	Click to refresh the page immediately
Clear	Clear all statistics counters
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals
Port	Switch port number
Status	Indicates whether a specific port is a router port or not

5.7.4 Groups Information of IGMP Snooping

Information about entries in the **IGMP Group Table** is shown in this page. The **IGMP Group Table** is sorted first by VLAN ID, and then by group.

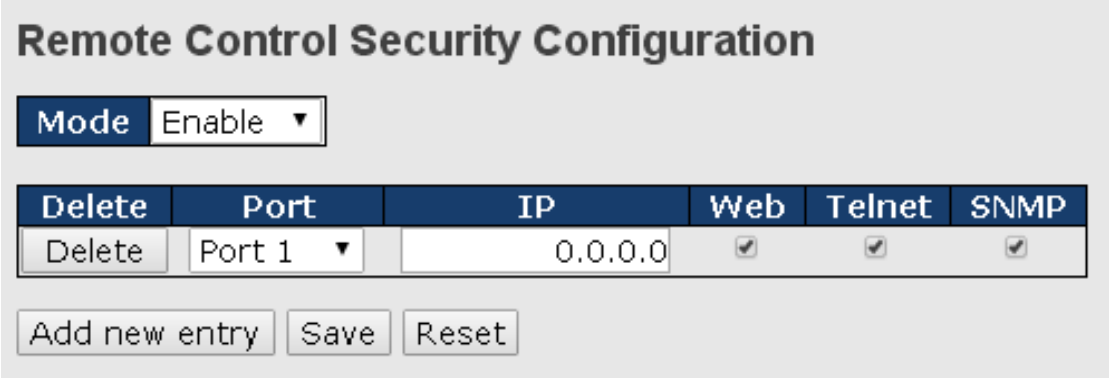


Label	Description
VLAN ID	The VLAN ID of the group
Groups	The group address of the group displayed
Port Members	Ports under this group

5.8 Security

5.8.1 Remote Control Security

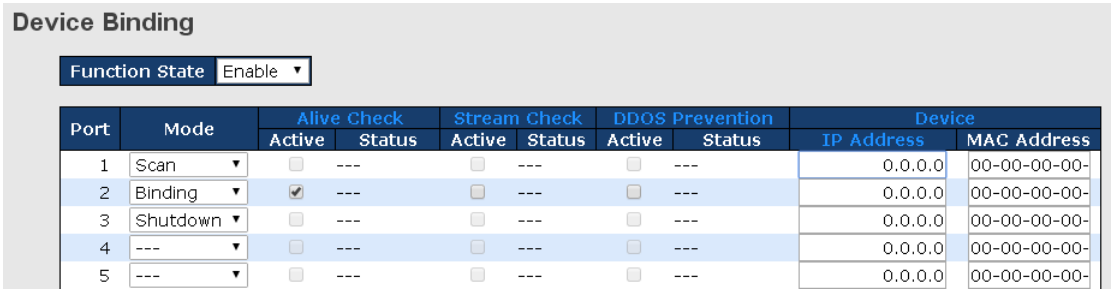
This page allows you to limit remote access to the management interface. When enabled, requests of the client which is not in the allowed list will be rejected.



Label	Description
Port	Port number of the remote client
IP Address	IP address of the remote client. **0.0.0.0** means "any IP".
Web	Check to enable management via a Web interface
Telnet	Check to enable management via a Telnet interface
SNMP	Check to enable management via a SNMP interface
Delete	Check to delete entries

5.8.2 Device Binding

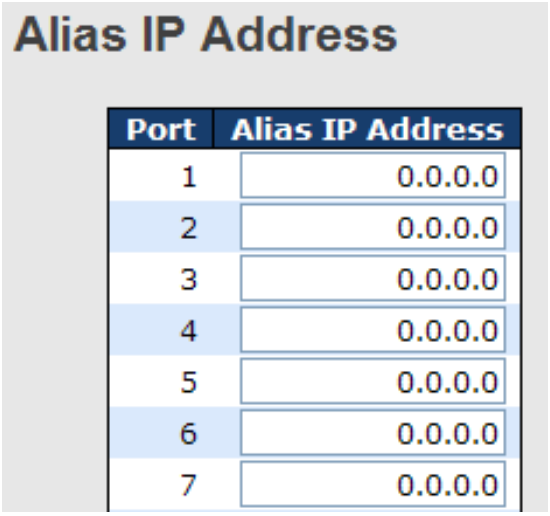
Device binding is ORing's proprietary technology which binds the IP/MAC address of a device with a specified Ethernet port. If the IP/MAC address of the device connected to the Ethernet port does not conform to the binding requirements, the device will be locked for security concerns. Device binding also provides security functions via alive checking, streaming check, and DoS/DDoS prevention.



Label	Description
Mode	Indicates the device binding operation for each port. Possible modes are: **---**: disable **Scan**: scans IP/MAC automatically, but no binding function **Binding**: enables binding. Under this mode, any IP/MAC that does not match the entry will not be allowed to access the network. **Shutdown**: shuts down the port (No Link)
Alive Check Active	Check to enable alive check. When enabled, the switch will ping the device continually.
Alive Check Status	Indicates alive check status. Possible statuses are: **---**: disable **Got Reply**: receive ping reply from device, meaning the device is still alive **Lost Reply**: not receiving ping reply from device, meaning the device might have been dead.
Stream Check Active	Check to enable stream check. When enabled, the switch will detect the stream change (getting low) from the device.
Stream Check Status	Indicates stream check status. Possible statuses are: **---**: disable **Normal**: the stream is normal. **Low**: the stream is getting low.
DDoS Prevention Acton	Check to enable DDOS prevention. When enabled, the switch will monitor the device against DDOS attacks.
DDoS Prevention Status	Indicates DDOS prevention status. Possible statuses are: **---**: disable **Analyzing**: analyzes packet throughput for initialization **Running**: analysis completes and ready for next move **Attacked**: DDOS attacks occur
Device IP Address	Specifies IP address of the device
Device MAC Address	Specifies MAC address of the device

Alias IP Address

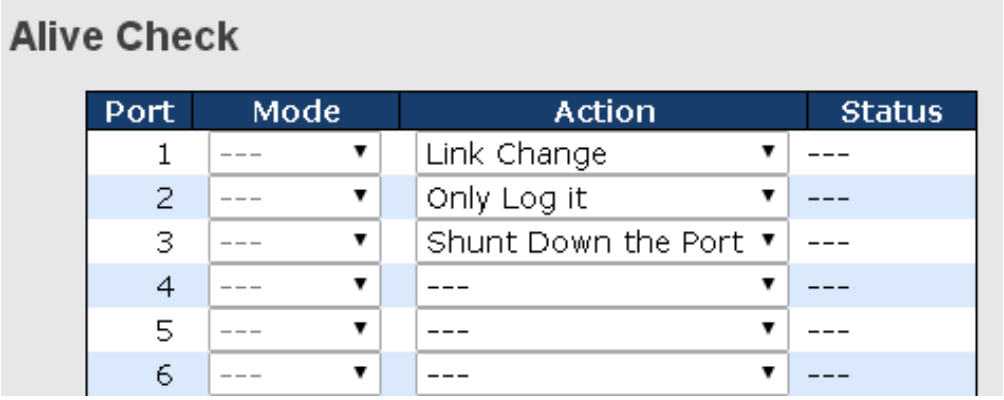
This page provides alias IP address configuration. Some devices might have more than one IP addresses. You could specify other IP addresses here.



Label	Description
Alias IP Address	Specifies alias IP address. Keep **0.0.0.0** if the device does not have an alias IP address.

Alive Check

Alive Checking monitors the real-time status of the device connected to the port. Alive-checking packets will be sent to the device to probe if the device is running. If the switch receives no response from the device, actions will be taken according to your configurations.



Label	Description
Link Change	Disables or enables the port.
Only log it	Simply sends logs to the log server.
Shunt Down the Port	Disables the port.
Reboot Device	Disables or enables PoE power.

DDoS Prevention

The switch can monitor ingress packets, and perform actions when DDOS attack occurred on this port. When network traffic from a specific device increases significantly in a short period of time, the switch will lock the IP address of that device to protect the network from attacks. You can configure DDoS prevention on this page to achieve maximum protection.

DDOS Prevention

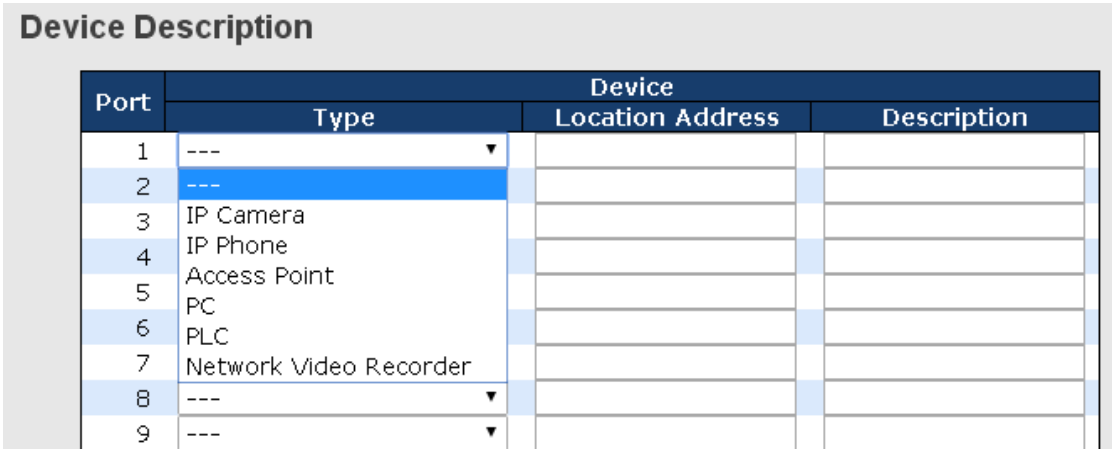
Port	Mode	Sensibility	Packet Type	Socket Number		Filter	Action	Status
				Low	High			
1	---	Normal	RX Total	80	80	Destination	Blocking 1 minute	---
2	---	Normal	RX Unicast	80	80	Destination	Blocking 10 minute	---
3	---	High	RX Multicast	80	80	Destination	Blocking	---
4	---	Normal	RX Broadcast	80	80	Destination	Shunt Down the Port	---
5	---	Normal	TCP	80	80	Destination	Only Log it	---
6	---	Normal	UDP	80	80	Source	---	---
7	---	Normal	TCP	80	80	Destination	---	---
8	---	Normal	TCP	80	80	Destination	---	---
9	---	Normal	TCP	80	80	Destination	---	---
10	---	Normal	TCP	80	80	Destination	---	---
11	---	Normal	TCP	80	80	Destination	---	---
12	---	Normal	TCP	80	80	Destination	---	---
13	---	Normal	TCP	80	80	Destination	---	---
14	---	Normal	TCP	80	80	Destination	---	---
15	---	Normal	TCP	80	80	Destination	---	---
16	---	Normal	TCP	80	80	Destination	---	---

Label	Description
Mode	Enables or disables DDOS prevention of the port
Sensibility	Indicates the level of DDOS detection. Possible levels are: **Low**: low sensibility **Normal**: normal sensibility **Medium**: medium sensibility **High**: high sensibility
Packet Type	Indicates the types of DDoS attack packets to be monitored. Possible types are: **RX Total**: all ingress packets **RX Unicast**: unicast ingress packets **RX Multicast**: multicast ingress packets **RX Broadcast**: broadcast ingress packets **TCP**: TCP ingress packets **UDP**: UDP ingress packets
Socket Number	If packet type is UDP (or TCP), please specify the socket number here. The socket number can be a range, from low to high. If the socket number is only one, please fill the same number in the low and high fields.
Filter	If packet type is UDP (or TCP), please choose the socket direction (**Destination**/**Source**).

Action	Indicates the action to take when DDOS attacks occur. Possible actions are: **---**: no action **Blocking 1 minute**: blocks the forwarding for 1 minute and log the event **Blocking 10 minute**: blocks the forwarding for 10 minutes and log the event **Blocking**: blocks and logs the event **Shunt Down the Port**: shuts down the port (No Link) and logs the event **Only Log it**: simply logs the event **Reboot Device**: if PoE is supported, the device can be rebooted. The event will be logged.
Status	Indicates the DDOS prevention status. Possible statuses are: **---**: disables DDOS prevention **Analyzing**: analyzes packet throughput for initialization **Running**: analysis completes and ready for next move **Attacked**: DDOS attacks occur

Device Description

This page allows you to configure device description settings.

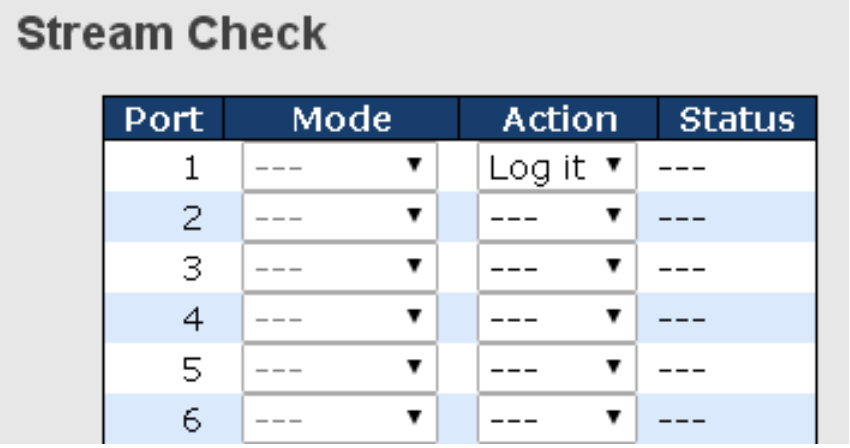


Label	Description
Device Type	Indicates device types. Possible types are: **---**: no specification **IP Camera** **IP Phone**

	Access Point **PC** **PLC** **Network Video Recorder**
Location Address	Indicates location information of the device. The information can be used for Google Mapping.
Description	Device descriptions

Stream Check

Stream check monitors the consistency of real-time network traffic from the device bound with the port. When the traffic changes sharply all of a sudden, an alert will be issued. This page allows you to configure stream check settings.

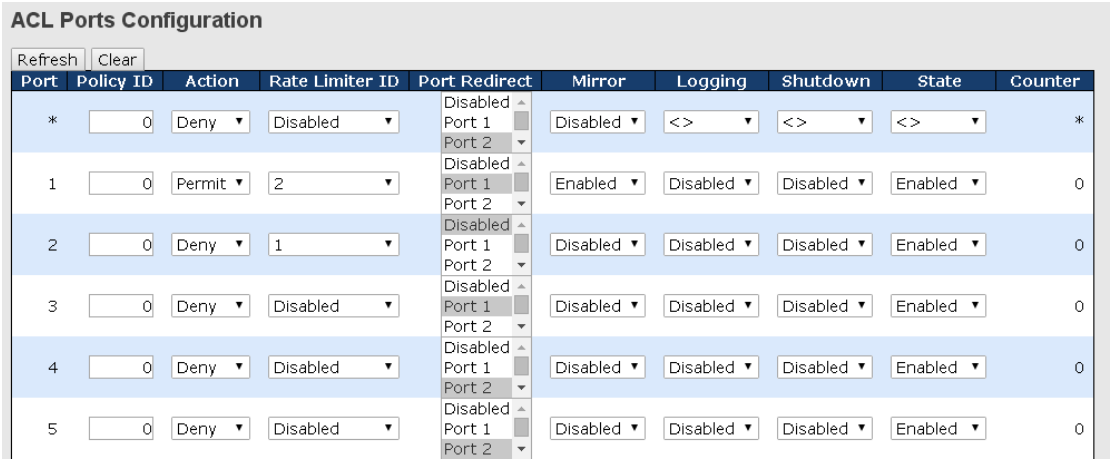


Label	Description
Mode	Enables or disables stream monitoring of the port
Action	Indicates the action to take when the stream gets low. Possible actions are: **---**: no action **Log it**: simply logs the event

5.8.3 ACL

An ACL (Access Control List) is a list of permissions attached to an object. An ACL specifies which users or system processes are authorized to access the objects and what operations are allowed on given objects.

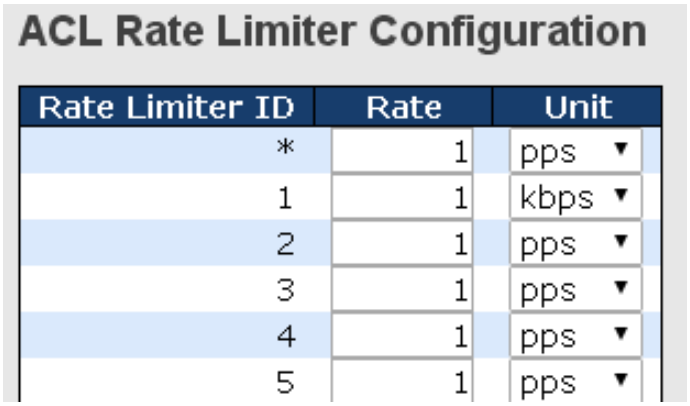
Port Configuration



Label	Description
Port	The switch port number to which the following settings will be applied
Policy ID	Select to apply a policy to the port. The allowed values are 1 to 8. The default value is **1**.
Action	Select to **Permit** to permit or **Deny** to deny forwarding. The default value is **Permit**.
Rate Limiter ID	Select a rate limiter for the port. The allowed values are Disabled or numbers from 1 to 15. The default value is Disabled.
Port Redirect	Indicates the port redirect operation implemented by the ACE. Frames matching the ACE are redirected to the listed port.
Mirror	Select which port frames are copied to. The allowed values are **Disabled** or a specific port number. The default value is **Disabled**.
Logging	Specifies the logging operation of the port. The allowed values are: **Enabled**: frames received on the port are stored in the system log **Disabled**: frames received on the port are not logged The default value is **Disabled**. Please note that system log memory capacity and logging rate is limited.
Shutdown	Specifies the shutdown operation of this port. The allowed values are: **Enabled**: if a frame is received on the port, the port will be disabled. **Disabled**: port shut down is disabled. The default value is **Disabled**.
Counter	Counts the number of frames that match this ACE.

Rate Limiters

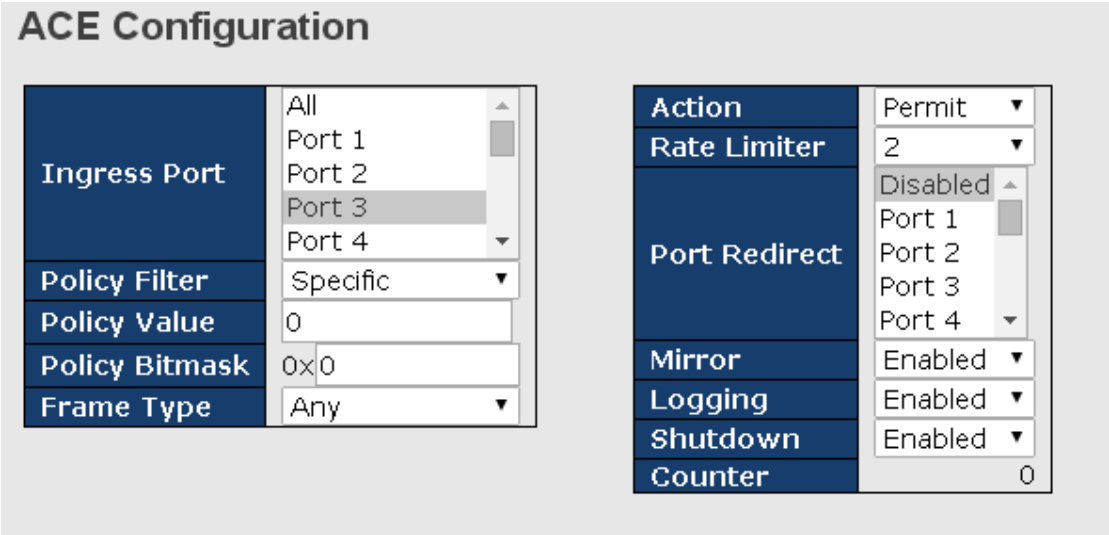
This page allows you to define the rate limits applied to a port.



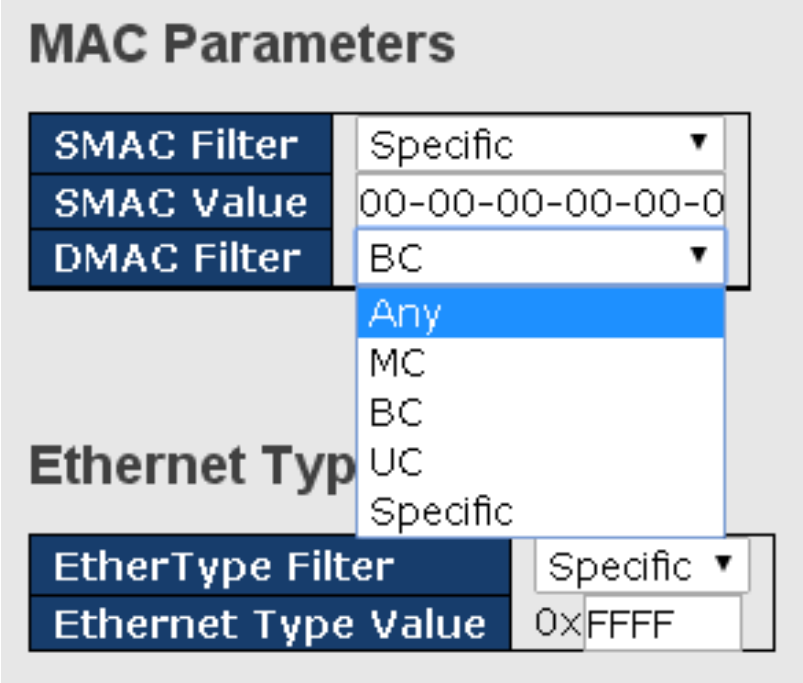
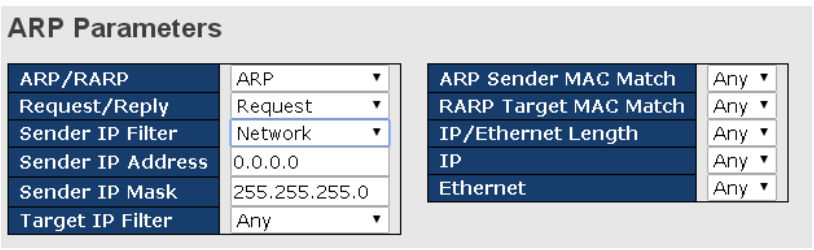
Label	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate	The rate unit is packet per second (pps), which can be configured as 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. The 1 kpps is actually 1002.1 pps.

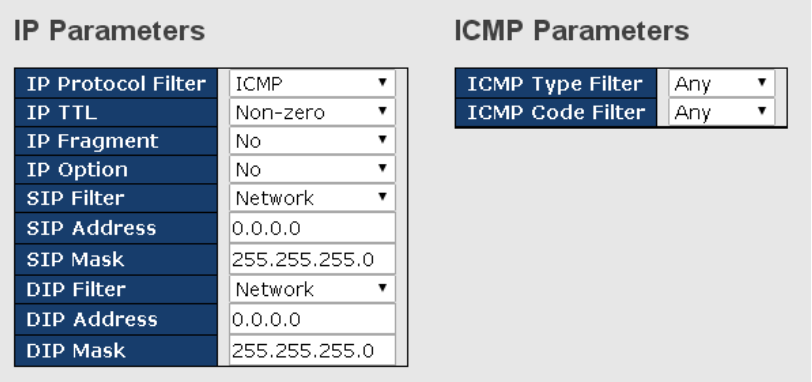
Access Control List

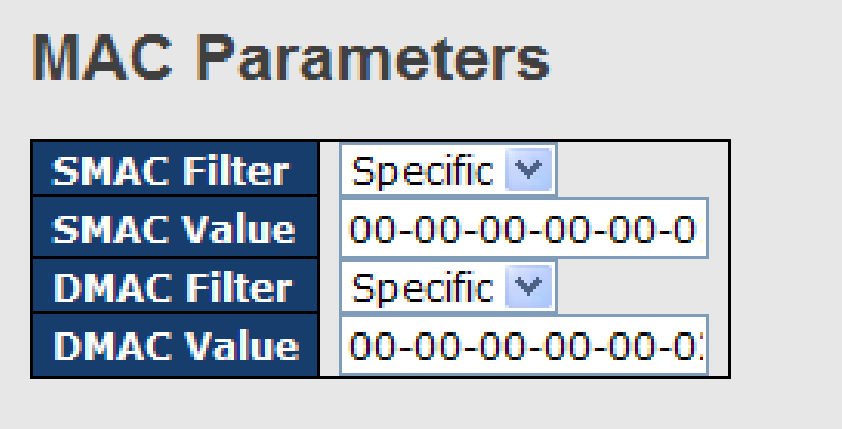
An ACE (Access Control Entry) is an element in an access control list (ACL). An ACL can have zero or more ACEs. Each ACE controls or monitors access to an object based on user-defined configurations. Each ACE consists of several parameters which vary with the frame type you have selected.



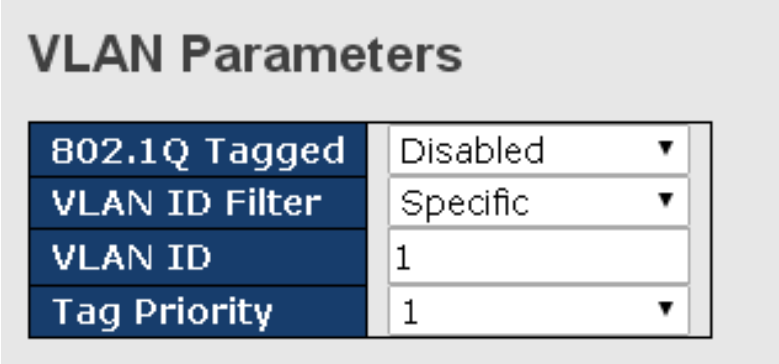
Label	Description
Ingress Port	Indicates the ingress port to which the ACE will apply. **Any**: the ACE applies to any port

	Port n: the ACE applies to this port number, where n is the number of the switch port. **Policy n**: the ACE applies to this policy number, where n can range from 1 to 8.
Policy Filter	Indicates the policy number filter for this ACE. Choose any will not specify any policy filter. Choose Specific will allow you to filter a specific policy with this ACE. You can enter a policy value and bitmask then.
Frame Type	Indicates the frame type of the ACE. These frame types are mutually exclusive. **Any**: any frame can match the ACE. **Ethernet Type**: only Ethernet type frames can match the ACE. The IEEE 802.3 descripts the value of length/types should be greater than or equal to 1536 decimal (equal to 0600 hexadecimal).  **ARP**: only ARP frames can match the ACE. Notice the ARP frames will not match the ACE with Ethernet type. 

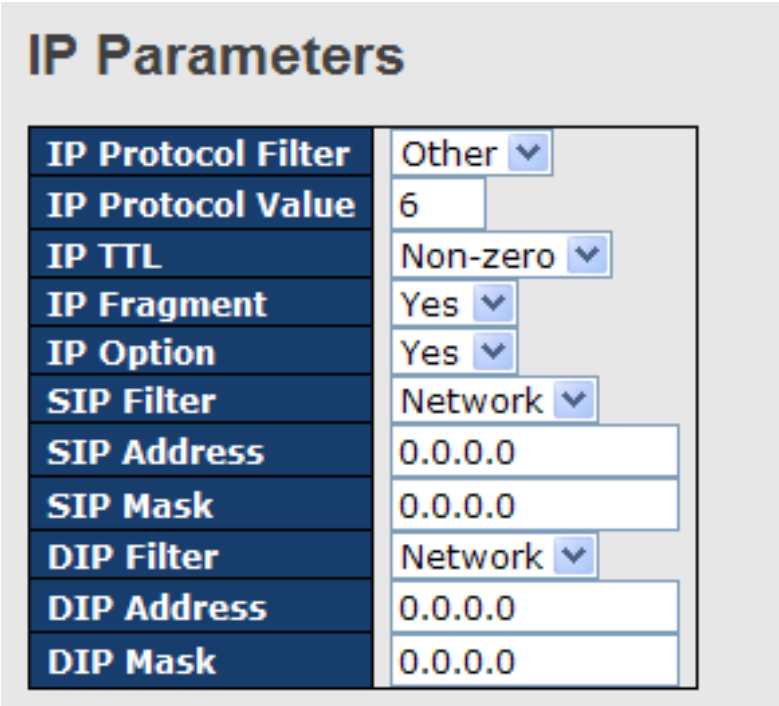
	IPv4: only IPv4 frames can match the ACE. Notice the IPv4 frames will not match the ACE with Ethernet type. 
Action	Specifies the action to take when a frame matches the ACE. Permit: takes action when the frame matches the ACE. Deny: drops the frame matching the ACE.
Rate Limiter	Specifies the rate limiter in number of base units. The allowed range is 1 to 15. **Disabled** means the rate limiter operation is disabled.
Port Redirect	Indicates the port redirect operation implemented by the ACE. Frames matching the ACE are redirected to the listed port.
Port Copy	Frames matching the ACE are copied to the port number specified here. The allowed range is the same as the switch port number range. Disabled means the port copy operation is disabled.
Logging	Specifies the logging operation of the ACE. The allowed values are: **Enabled**: frames matching the ACE are stored in the system log. **Disabled**: frames matching the ACE are not logged. Please note that system log memory capacity and logging rate is limited.
Shutdown	Specifies the shutdown operation of the ACE. The allowed values are: **Enabled**: if a frame matches the ACE, the ingress port will be disabled. **Disabled**: port shutdown is disabled for the ACE.
Counter	Indicates the number of times the ACE matched by a frame.



Label	Description
SMAC Filter	Specifies the type of source MAC address This parameter is only available when the frame type is Ethernet Type or ARP. **Any**: no SMAC filter is specified (SMAC filter status is "**don't-care**"). **Specific**: if you want to filter a specific source MAC address with the ACE, choose this value. A field for entering an SMAC value appears.
SMAC Value	When **Specific** is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". Frames matching the ACE will use this SMAC value.
DMAC Filter	Specifies the destination MAC filter for this ACE. **Any**: no DMAC filter is specified (DMAC filter status is "**don't-care**"). **MC**: frame must be multicast. **BC**: frame must be broadcast. **UC**: frame must be unicast. **Specific**: If you want to filter a specific destination MAC address with the 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". Frames matching the ACE will use this DMAC value.

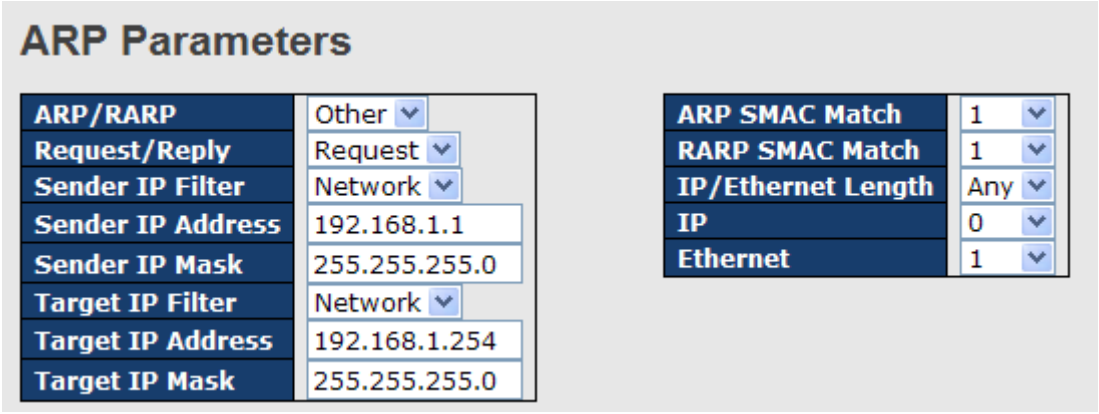


Label	Description
VLAN ID Filter	Specifies the VLAN ID filter for the ACE **Any**: no VLAN ID filter is specified (VLAN ID filter status is "**don't-care**"). **Specific**: if you want to filter a specific VLAN ID with the ACE, choose this value. A field for entering a VLAN ID number appears.
VLAN ID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



Label	Description
IP Protocol Filter	Specifies the IP protocol filter for the ACE **Any**: no IP protocol filter is specified ("**don't-care**"). **Specific**: if you want to filter a specific IP protocol filter with the ACE, choose this value. A field for entering an IP protocol filter appears. ICMP: selects ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. For more details of these fields, please refer to the help file. **UDP**: selects UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. For more details of these fields, please refer to the help file. **TCP**: selects TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. For more details of these fields, please refer to the help file.
IP Protocol Value	**Specific** allows you to enter a specific value. The allowed range is 0 to 255. Frames matching the ACE will use this IP protocol value.
IP TTL	Specifies the time-to-live settings for the ACE **Zero**: IPv4 frames with a time-to-live value greater than zero must not be able to match this entry. **Non-zero**: IPv4 frames with a time-to-live field greater than zero must be able to match this entry. **Any**: any value is allowed ("**don't-care**").
IP Fragment	Specifies the fragment offset settings for the ACE. This includes settings of More Fragments (MF) bit and Fragment Offset (FRAG OFFSET) for an IPv4 frame. **No**: IPv4 frames whose MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry. **Yes**: IPv4 frames whose MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry. **Any**: any value is allowed ("**don't-care**").
IP Option	Specifies the options flag settings for the ACE. **No**: IPv4 frames whose options flag is set must not be able to match this entry. **Yes**: IPv4 frames whose options flag is set must be able to match this entry. **Any**: any value is allowed ("**don't-care**").
SIP Filter	Specifies the source IP filter for this ACE.

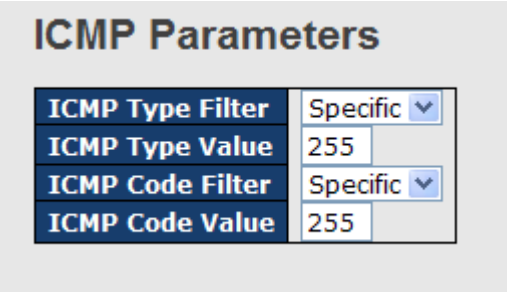
	Any: no source IP filter is specified (Source IP filter is "**don't-care**"). **Host**: source IP filter is set to **Host**. Specify the source IP address in the **SIP Address** field that appears. **Network**: source IP filter is set to **Network**. Specify the source IP address and source IP mask in the **SIP Address** and **SIP Mask** fields that appear.
SIP Address	When **Host** or **Network** is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.
SIP Mask	When **Network** is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
DIP Filter	Specifies the destination IP filter for the ACE **Any**: no destination IP filter is specified (destination IP filter is "**don't-care**"). **Host**: destination IP filter is set to **Host**. Specify the destination IP address in the **DIP Address** field that appears. **Network**: destination IP filter is set to **Network**. Specify the destination IP address and destination IP mask in the **DIP Address** and **DIP Mask** fields that appear.
DIP Address	When **Host** or **Network** is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.
DIP Mask	When **Network** is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.



Label	Description
ARP/RARP	Specifies the available ARP/RARP opcode (OP) flag for the ACE **Any**: no ARP/RARP OP flag is specified (OP is "**don't-care**"). **ARP**: frame must have ARP/RARP opcode set to ARP

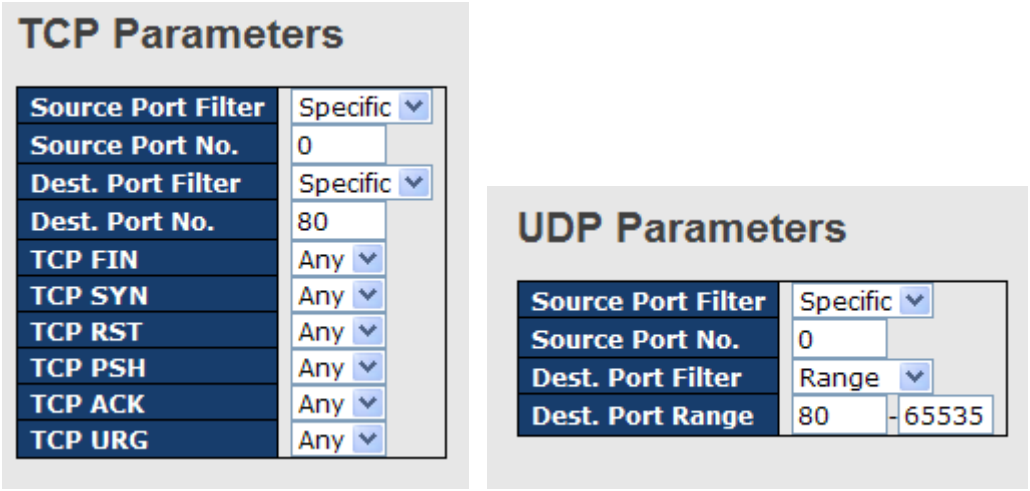
	RARP: frame must have ARP/RARP opcode set to RARP. **Other**: frame has unknown ARP/RARP Opcode flag.
Request/Reply	Specifies the available ARP/RARP opcode (OP) flag for the ACE **Any**: no ARP/RARP OP flag is specified (OP is "**don't-care**"). **Request**: frame must have ARP Request or RARP Request OP flag set. **Reply**: frame must have ARP Reply or RARP Reply OP flag.
Sender IP Filter	Specifies the sender IP filter for the ACE **Any**: no sender IP filter is specified (sender IP filter is "**don't-care**"). **Host**: sender IP filter is set to **Host**. Specify the sender IP address in the **SIP Address** field that appears. **Network**: sender IP filter is set to **Network**. Specify the sender IP address and sender IP mask in the **SIP Address** and **SIP Mask** fields that appear.
Sender IP Address	When Host or Network is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.
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	Specifies the target IP filter for the specific ACE **Any**: no target IP filter is specified (target IP filter is "**don't-care**"). **Host**: target IP filter is set to **Host**. Specify the target IP address in the **Target IP Address** field that appears. **Network**: target IP filter is set to **Network**. Specify the target IP address and target IP mask in the **Target IP Address** and **Target IP Mask** fields that appear.
Target IP Address	When **Host** or **Network** is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.
Target IP Mask	When **Network** is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.
ARP SMAC Match	Specifies whether frames will meet the action according to their sender hardware address field (SHA) settings. **0**: ARP frames where SHA is not equal to the SMAC address **1**: ARP frames where SHA is equal to the SMAC address **Any**: any value is allowed ("**don't-care**").
RARP SMAC Match	Specifies whether frames will meet the action according to their target hardware address field (THA) settings. **0**: RARP frames where THA is not equal to the SMAC address

	1: RARP frames where THA is equal to the SMAC address **Any**: any value is allowed ("**don't-care**")
IP/Ethernet Length	Specifies whether frames will meet the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings. **0**: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must not match this entry. **1**: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04) must match this entry. **Any**: any value is allowed ("**don't-care**").
IP	Specifies whether frames will meet the action according to their ARP/RARP hardware address space (HRD) settings. **0**: ARP/RARP frames where the HLD is equal to Ethernet (1) must not match this entry. **1**: ARP/RARP frames where the HLD is equal to Ethernet (1) must match this entry. **Any**: any value is allowed ("**don't-care**").
Ethernet	Specifies whether frames will meet the action according to their ARP/RARP protocol address space (PRO) settings. **0**: ARP/RARP frames where the PRO is equal to IP (0x800) must not match this entry. **1**: ARP/RARP frames where the PRO is equal to IP (0x800) must match this entry. **Any**: any value is allowed ("**don't-care**").



Label	Description
ICMP Type Filter	Specifies the ICMP filter for the ACE. **Any**: no ICMP filter is specified (ICMP filter status is "**don't-care**"). **Specific**: if you want to filter a specific ICMP filter with the 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 matching the ACE will use this ICMP value.
ICMP Code Filter	Specifies the ICMP code filter for the ACE. **Any**: no ICMP code filter is specified (ICMP code filter status is "**don't-care**"). **Specific**: if you want to filter a specific ICMP code filter with the 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 matching the ACE will use this ICMP code value.



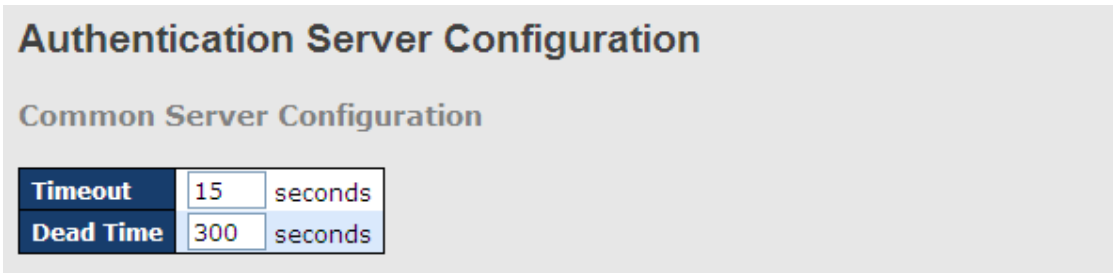
Label	Description
TCP/UDP Source Filter	Specifies the TCP/UDP source filter for the ACE **Any**: no TCP/UDP source filter is specified (TCP/UDP source filter status is "**don't-care**"). **Specific**: if you want to filter a specific TCP/UDP source filter with the ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears. **Range**: if you want to filter a specific TCP/UDP source range filter with the ACE, you can enter a specific TCP/UDP source range. 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 matching the ACE will use 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 matching the ACE will use this TCP/UDP source value.
TCP/UDP Destination Filter	Specifies the TCP/UDP destination filter for the ACE. **Any**: no TCP/UDP destination filter is specified (TCP/UDP destination filter status is "**don't-care**"). **Specific**: if you want to filter a specific TCP/UDP destination filter with the ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears. **Range**: if you want to filter a specific range TCP/UDP destination filter with the ACE, you can enter a specific TCP/UDP destination range. 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 matching the ACE will use 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 matching the ACE will use this TCP/UDP destination value.
TCP FIN	Specifies the TCP FIN ("no more data from sender") value for the ACE. **0**: TCP frames where the FIN field is set must not be able to match this entry. **1**: TCP frames where the FIN field is set must be able to match this entry. **Any**: any value is allowed ("**don't-care**").
TCP SYN	Specifies the TCP SYN ("synchronize sequence numbers") value for the ACE **0**: TCP frames where the SYN field is set must not be able to match this entry. **1**: TCP frames where the SYN field is set must be able to match this

	entry. **Any**: any value is allowed ("**don't-care**").
TCP PSH	Specifies the TCP PSH ("push function") value for the ACE **0**: TCP frames where the PSH field is set must not be able to match this entry. **1**: TCP frames where the PSH field is set must be able to match this entry. **Any**: any value is allowed ("**don't-care**").
TCP ACK	Specifies the TCP ACK ("acknowledgment field significant") value for the ACE **0**: TCP frames where the ACK field is set must not be able to match this entry. **1**: TCP frames where the ACK field is set must be able to match this entry. **Any**: any value is allowed ("**don't-care**").
TCP URG	Specifies the TCP URG ("urgent pointer field significant") value for the ACE **0**: TCP frames where the URG field is set must not be able to match this entry. **1**: TCP frames where the URG field is set must be able to match this entry. **Any**: any value is allowed ("**don't-care**").

5.8.4 Authentication, Authorization, and Accounting

An AAA server is an application that provides authentication, authorization, and accounting services for attempted access to a network. An AAA server can reside in a dedicated computer, an Ethernet switch, an access point or a network access server. The current standard by which devices or applications communicate with an AAA server is RADIUS (Remote Authentication Dial-In User Service). RADIUS is a protocol used between the switch and the authentication server. This page allows you to configure common settings for an authentication server.

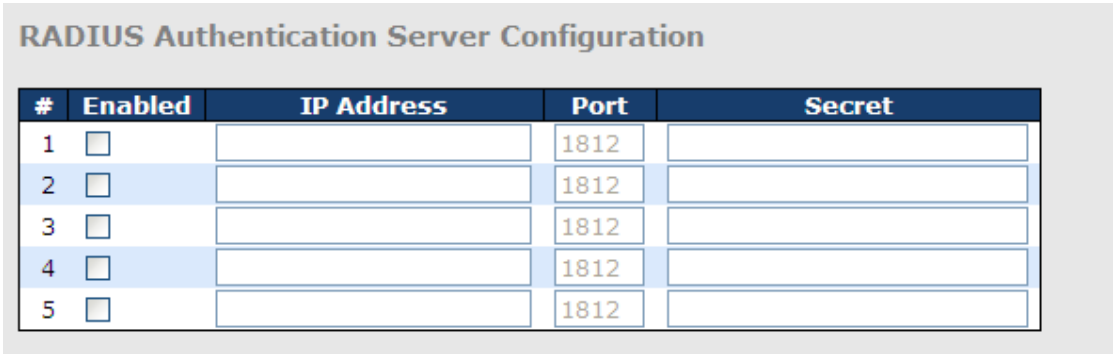


Label	Description
Timeout	The timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this time frame, we will consider it to be dead and continue with the next enabled server (if any). RADIUS servers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

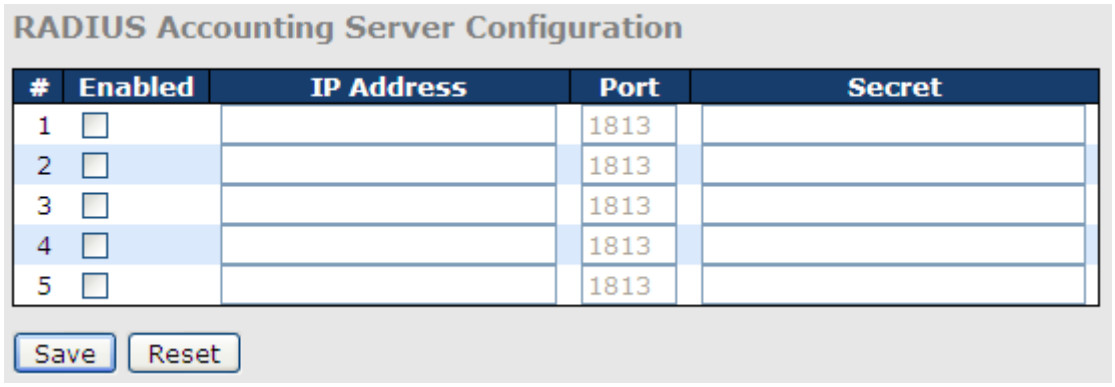
RADIUS Authentication and Accounting Server

When a user requests network connection, a RADIUS client which receives the request will perform an initial access negotiation with the user to obtain identity/password information. The client then passes the information to a RADIUS server as part of an authentication/authorization request.

The RADIUS server matches data from the authentication/authorization request with information in a trusted database. If a match is found and the user's credentials are correct, the RADIUS server sends an accept message to the client to grant access. If a match is not found or a problem is found with the user's credentials, the server returns a reject message to deny access. The NAD then establishes or terminates the user's connection. The NAD may then forward accounting information to the RADIUS server to document the transaction; the RADIUS server may store or forward this information as needed to support billing for the services provided.

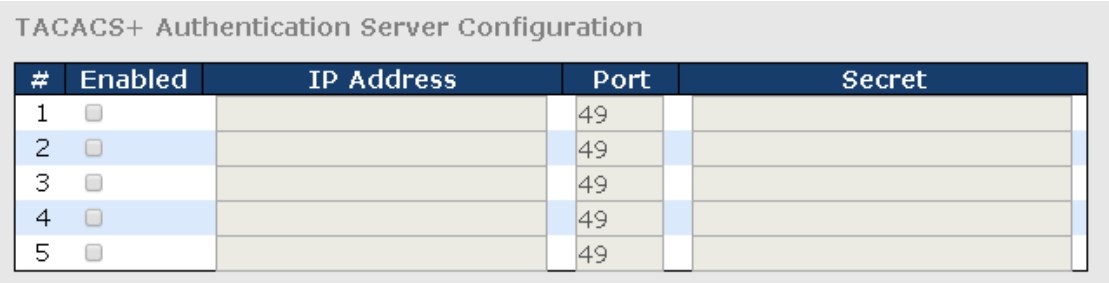


Label	Description
#	The RADIUS authentication server number for which the configuration below applies.
Enabled	Check to enable the RADIUS authentication server.
IP Address	The IP address or hostname of the RADIUS authentication server. IP address is expressed in dotted decimal notation.
Port	The UDP port to use on the RADIUS authentication server. If the port is set to **0** (zero), the default port (1812) is used on the RADIUS authentication server.
Secret	The secret is a text string used by RADIUS to encrypt the client and server authenticator field during exchanges between the router and a RADIUS authentication server. The router encrypts PPP PAP passwords using this text string. The secret - up to 29 characters long - shared between the RADIUS authentication server and the switch stack.



Label	Description
#	The RADIUS accounting server number for which the configuration below applies.

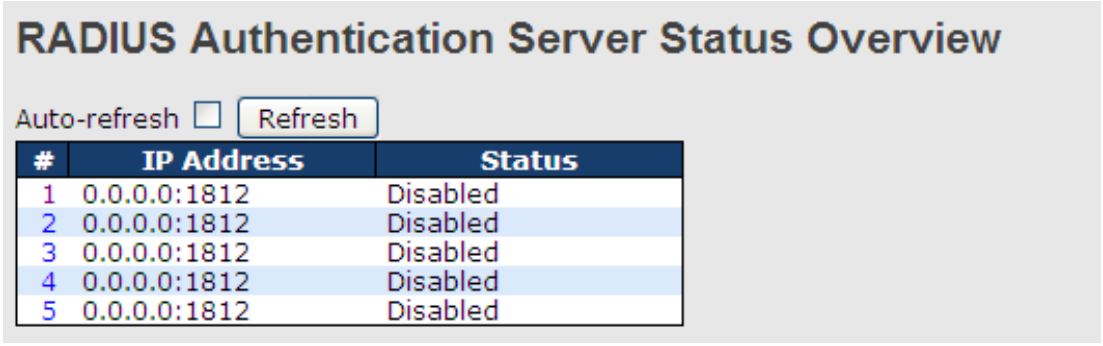
Enabled	Check to enable the RADIUS accounting server
IP Address	The IP address or hostname of the RADIUS accounting server. IP address is expressed in dotted decimal notation.
Port	The UDP port to use on the RADIUS accounting server. If the port is set to **0** (zero), the default port (1813) is used on the RADIUS accounting server.
Secret	The secret is a text string used by RADIUS to encrypt the client and server authenticator field during exchanges between the router and a RADIUS accounting server. The router encrypts PPP PAP passwords using this text string. The secret - up to 29 characters long - shared between the RADIUS accounting server and the switch stack.



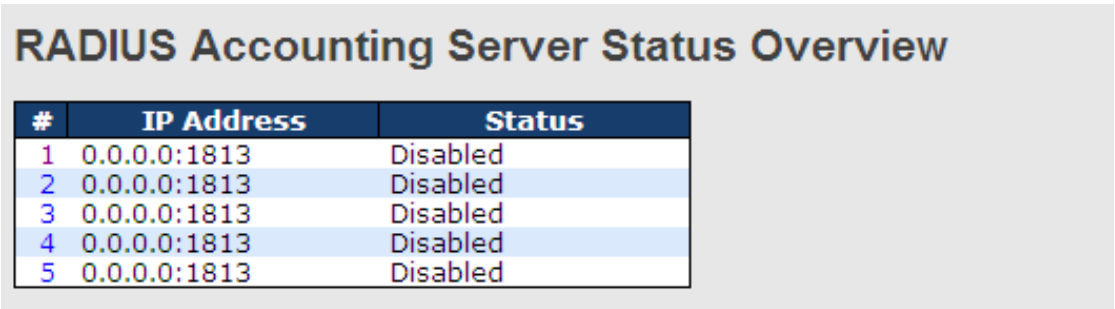
Label	Description
#	The RADIUS accounting server number for which the configuration below applies.
Enabled	Check to enable the RADIUS accounting server
IP Address	The IP address or hostname of the RADIUS accounting server. IP address is expressed in dotted decimal notation.
Port	The UDP port to use on the RADIUS accounting server. If the port is set to **0** (zero), the default port (1813) is used on the RADIUS accounting server.
Secret	The secret is a text string used by RADIUS to encrypt the client and server authenticator field during exchanges between the router and a TACACS+ server. The router encrypts PPP PAP passwords using this text string. The secret - up to 29 characters long - shared between the TACACS+ server and the switch stack.

RADIUS Authentication and Accounting Server Status

This page provides information about the status of the RADIUS server configurable on the authentication configuration page.

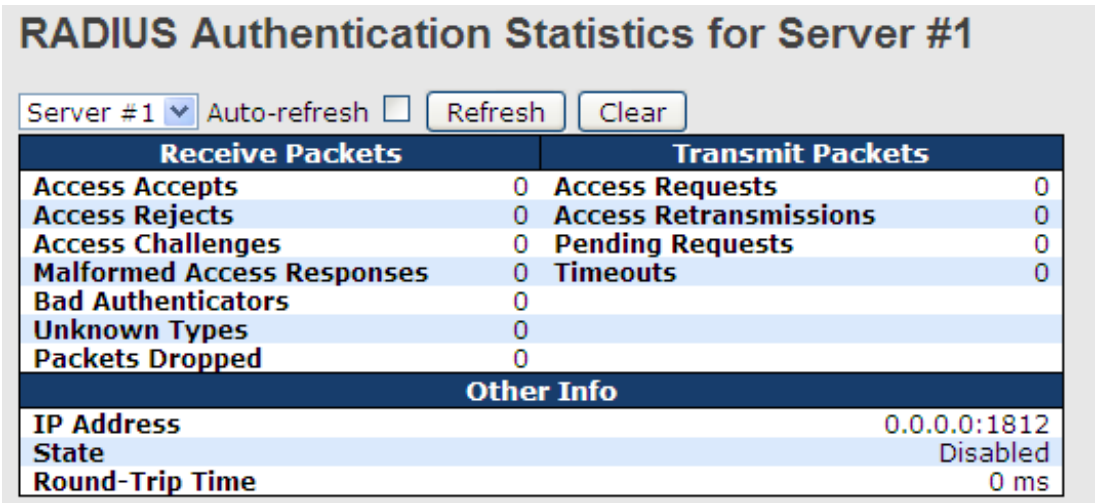


Label	Description
#	The RADIUS server number. Click to navigate to detailed statistics of the server
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of the server
Status	The current status of the server. This field has one of the following values: **Disabled**: the server is disabled. **Not Ready**: the server is enabled, but IP communication is not yet up and running. **Ready**: the server is enabled, IP communications are built, and the RADIUS module is ready to accept access attempts. **Dead** (X seconds left): access attempts are made to this server, but it does not reply within the configured timeout. The server has temporarily been disabled, but will be re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.



Label	Description
#	The RADIUS server number. Click to navigate to detailed statistics of the server
IP Address	The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of the server
Status	The current status of the server. This field has one of the following values: Disabled: the server is disabled. **Not Ready**: the server is enabled, but IP communication is not yet up and running. **Ready**: the server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. **Dead (X seconds left)**: accounting attempts are made to this server, but it does not reply within the configured timeout. The server has temporarily been disabled, but will be re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

When you click on the port number in RADIUS Overview page, you will see this pages showing the access statistics of the authentication and accounting servers. Use the server drop-down list to switch between the backend servers to show related details.



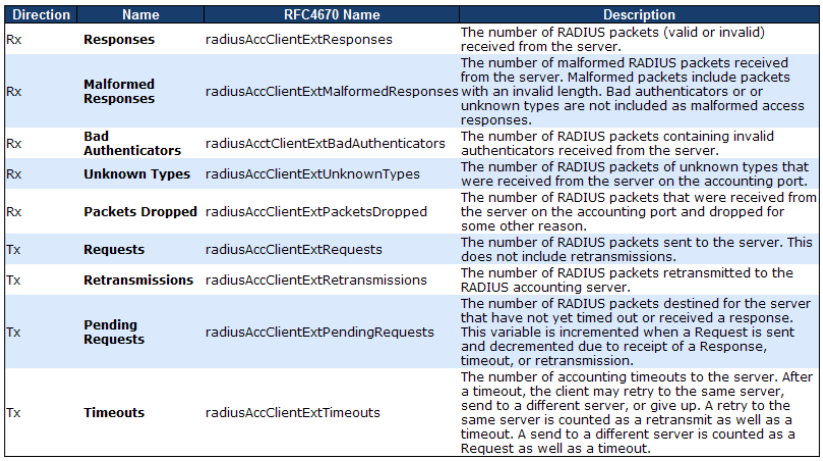
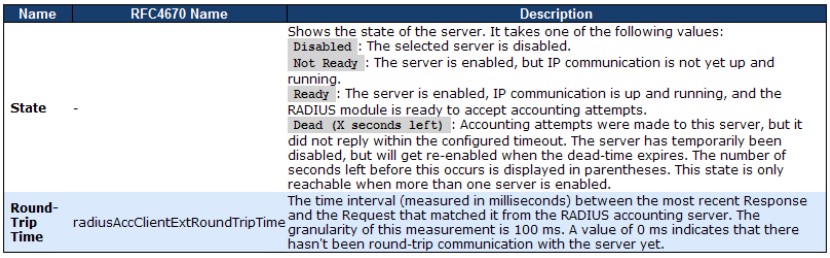
Label	Description
Packet Counters	RADIUS authentication server packet counters. There are seven ‘receive’ and four ‘transmit’ counters.

	<table><tr><th>Direction</th><th>Name</th><th>RFC4668 Name</th><th>Description</th></tr><tr><td>Rx</td><td>Access Accepts</td><td>radiusAuthClientExtAccessAccepts</td><td>The number of RADIUS Access-Accept packets (valid or invalid) received from the server.</td></tr><tr><td>Rx</td><td>Access Rejects</td><td>radiusAuthClientExtAccessRejects</td><td>The number of RADIUS Access-Reject packets (valid or invalid) received from the server.</td></tr><tr><td>Rx</td><td>Access Challenges</td><td>radiusAuthClientExtAccessChallenges</td><td>The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.</td></tr><tr><td>Rx</td><td>Malformed Access Responses</td><td>radiusAuthClientExtMalformedAccessResponses</td><td>The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.</td></tr><tr><td>Rx</td><td>Bad Authenticators</td><td>radiusAuthClientExtBadAuthenticators</td><td>The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.</td></tr><tr><td>Rx</td><td>Unknown Types</td><td>radiusAuthClientExtUnknownTypes</td><td>The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.</td></tr><tr><td>Rx</td><td>Packets Dropped</td><td>radiusAuthClientExtPacketsDropped</td><td>The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.</td></tr><tr><td>Tx</td><td>Access Requests</td><td>radiusAuthClientExtAccessRequests</td><td>The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.</td></tr><tr><td>Tx</td><td>Access Retransmissions</td><td>radiusAuthClientExtAccessRetransmissions</td><td>The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.</td></tr><tr><td>Tx</td><td>Pending Requests</td><td>radiusAuthClientExtPendingRequests</td><td>The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.</td></tr><tr><td>Tx</td><td>Timeouts</td><td>radiusAuthClientExtTimeouts</td><td>The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.</td></tr></table>
Other Info	This section contains information about the state of the server and the latest round-trip time. <table><tr><th>Name</th><th>RFC4668 Name</th><th>Description</th></tr><tr><td>State</td><td>-</td><td>Shows the state of the server. It takes one of the following values: <code>Disabled</code> : The selected server is disabled. <code>Not Ready</code> : The server is enabled, but IP communication is not yet up and running. <code>Ready</code> : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. <code>Dead (X seconds left)</code> : Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.</td></tr><tr><td>Round-Trip Time</td><td>radiusAuthClientExtRoundTripTime</td><td>The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.</td></tr></table>

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address			0.0.0.0:1813
State			Disabled
Round-Trip Time			0 ms

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

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

Direction	Name	RFC4670 Name	Description
Rx	**Responses**	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	**Malformed Responses**	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or or unknown types are not included as malformed access responses.
Rx	**Bad Authenticators**	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
Rx	**Unknown Types**	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
Rx	**Packets Dropped**	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
Tx	**Requests**	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
Tx	**Retransmissions**	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
Tx	**Pending Requests**	radiusAccClientExtPendingRequests	The number of RADIUS packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, timeout, or retransmission.
Tx	**Timeouts**	radiusAccClientExtTimeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

Name	RFC4670 Name	Description
State	-	Shows the state of the server. It takes one of the following values: `Disabled` : The selected server is disabled. `Not Ready` : The server is enabled, but IP communication is not yet up and running. `Ready` : The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. `Dead (X seconds left)` : Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

5.8.5 NAS (802.1x)

A NAS (Network Access Server) is an access gateway between an external communications network and an internal network. For example, when the user dials into the ISP, he/she will be given access to the Internet after being authorized by the access server. The authentication between the client and the server include IEEE 802.1X- and MAC-based.

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 backend servers (RADIUS) determine whether the user is allowed access to the network.

MAC-based authentication allows for authentication of more than one user on the same port, and does not require the users to have special 802.1X software installed on their system. The switch uses the users' MAC addresses to authenticate against the backend server. As intruders can create counterfeit MAC addresses, MAC-based authentication is less secure than 802.1X authentication.

Overview of 802.1X (Port-Based) Authentication

In an 802.1X network environment, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the

man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames which encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible as it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) does not 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 the result to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Note: in an environment where two backend servers are enabled, the server timeout is configured to X seconds (using the authentication configuration page), and the first server in the list is currently down (but not considered dead), if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, it will never be authenticated because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. Since the server has not failed (because the X seconds have not expired), the same server will be contacted when the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

Overview of MAC-Based Authentication

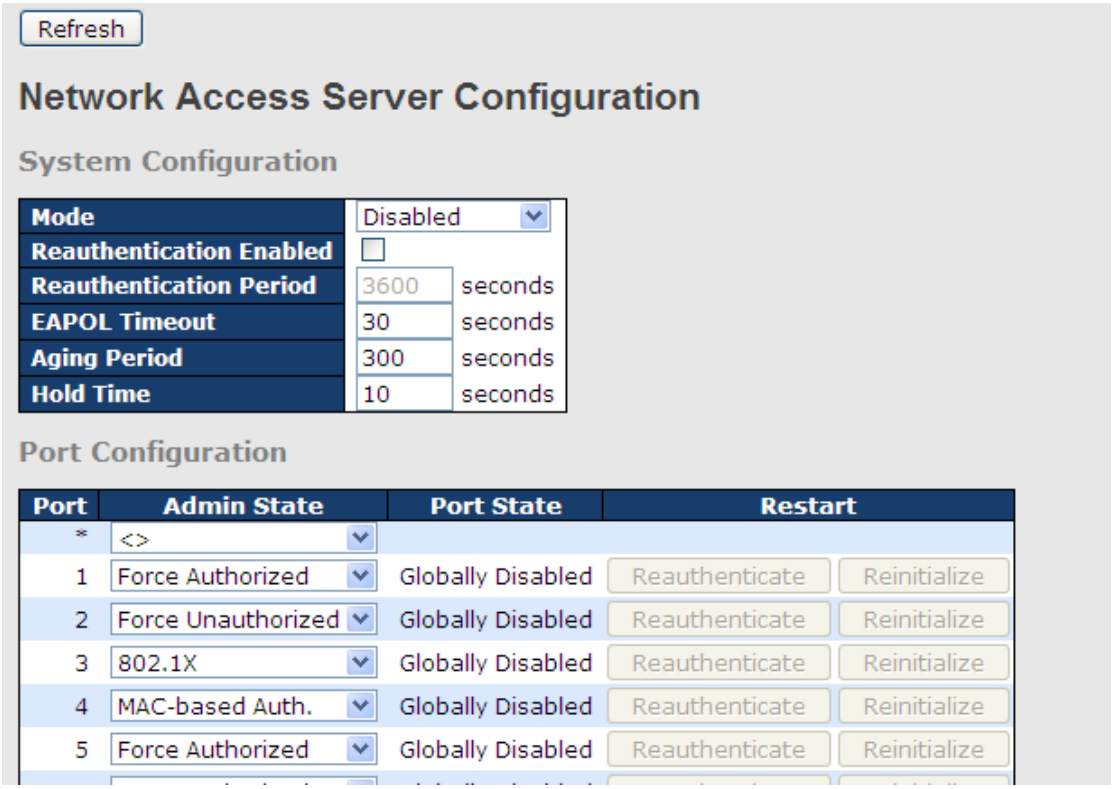
Unlike 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by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

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using static entries into the MAC Table. Only then will frames from the client be forwarded on the switch.

There are no EAPOL frames involved in this authentication, and therefore, MAC-based authentication has nothing to do with the 802.1X standard.

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

802.1X and MAC-Based authentication configurations consist of two sections: system- and port-wide.



Label	Description
Mode	Indicates if 802.1X and MAC-based authentication is globally enabled or disabled on the switch. If globally disabled, all ports are allowed to forward frames.
Reauthentication Enabled	If checked, clients are reauthenticated after the interval specified by the reauthentication period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port. 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 does not imply that a client is still present on a port (see Age Period below).
Reauthentication Period	Determines the period, in seconds, after which a connected client must be re-authenticated. This is only active if the **Reauthentication Enabled** checkbox is checked. Valid range of the value is 1 to 3600 seconds.
EAPOL Timeout	Determines the time for retransmission of Request Identity EAPOL frames. Valid range of the value is 1 to 65535 seconds. This has no effect for MAC-based ports.
Age Period	This setting applies to the following modes, i.e. modes using the **Port Security** functionality to secure MAC addresses: **MAC-Based Auth**.: When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. For ports in **MAC-based Auth.** mode, reauthentication does not cause direct communications between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.
Hold Time	This setting applies to the following modes, i.e. modes using the **Port Security** functionality to secure MAC addresses: **MAC-Based Auth**.: If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "**Configuration→Security→AAA**" page) - the client is put on hold in 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.
Port	The port number for which the configuration below applies
Admin State	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available: **Force Authorized** In this mode, the switch will send one EAPOL Success frame when the port link is up, and any client on the port will be allowed network access without authentication. **Force Unauthorized** In this mode, the switch will send one EAPOL Failure frame when the port link is up, and any client on the port will be disallowed network access. **Port-based 802.1X** In an 802.1X network environment, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames which encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server is RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible as it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) does not 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 the result to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant. Note: in an environment where two backend servers are enabled,

	the server timeout is configured to X seconds (using the authentication configuration page), and the first server in the list is currently down (but not considered dead), if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, it will never be authenticated because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. Since the server has not failed (because the X seconds have not expired), the same server will be contacted when 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. **a. Single 802.1X** In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they are not authenticated individually. To overcome this security breach, use the Single 802.1X variant. Single 802.1X is not yet an IEEE standard, but features many of the same characteristics as port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communications between the supplicant and the switch. If more than one supplicant are connected to a port, the one that comes first when the port's link is connected will be the first one considered. If that supplicant does not provide valid credentials within a certain amount of time, the chance will be given to another supplicant. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated. **b. Multi 802.1X** In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for

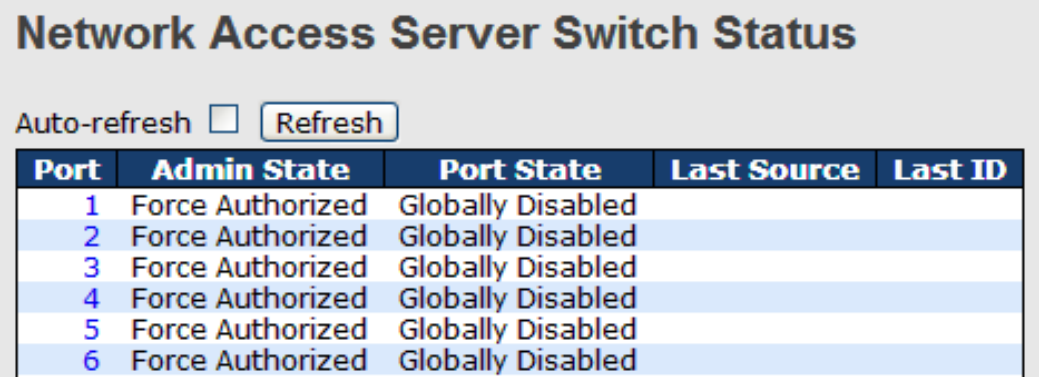
	instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they are not authenticated individually. To overcome this security breach, use the Multi 802.1X variant. Multi 802.1X is not yet an IEEE standard, but features many of the same characteristics as port-based 802.1X. In Multi 802.1X, one or more supplicants can be authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module. In Multi 802.1X it is not possible to use the multicast BPDU MAC address as the destination MAC address for EAPOL frames sent from the switch to the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality. **MAC-based Auth.** Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string in 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 advantage of MAC-based authentication over 802.1X-based authentication is that the clients do not 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	The current state of the port. It can undertake one of the following values: **Globally Disabled**: NAS is globally disabled. **Link Down**: NAS is globally enabled, but there is no link on the port. **Authorized**: the port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. **Unauthorized:** the port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. **X Auth/Y Unauth**: the port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.
Restart	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect. **Reauthenticate**: schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication).

	For MAC-based authentication, reauthentication will be attempted immediately. The button only has effect on successfully authenticated clients on the port and will not cause the clients to be temporarily unauthorized. **Reinitialize**: forces a reinitialization of the clients on the port and hence a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.

NAS Switch Status

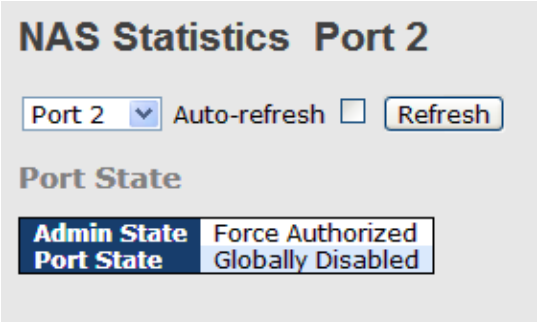
This page shows the information on current NAS port statuses.



Label	Description
Port	The switch port number. Click to navigate to detailed 802.1X statistics of each port.
Admin State	The port's current administrative state. Refer to **NAS Admin State** for more details regarding each value.
Port State	The current state of the port. Refer to **NAS Port State** for more details regarding each value.
Last Source	The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.
Last ID	The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

This page provides detailed IEEE 802.1X statistics for a specific switch port using port-based

authentication. For MAC-based ports, only the statistics of selected backend server statistics will be shown. Use the drop-down list to select which port details to be displayed.

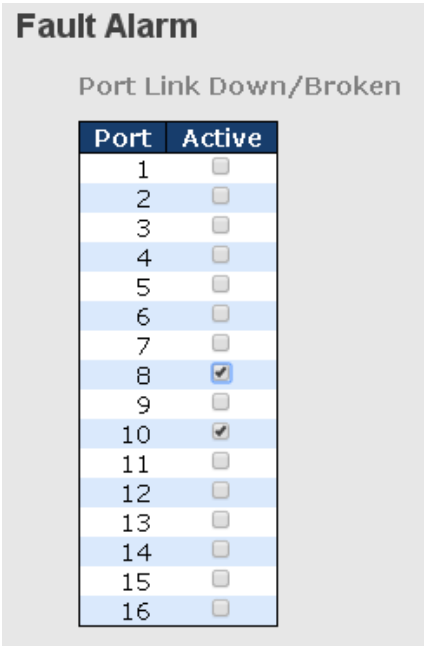


Label	Description
Admin State	The port's current administrative state. Refer to **NAS Admin State** for more details regarding each value.
Port State	The current state of the port. Refer to **NAS Port State** for more details regarding each value.

5.9 Warning

5.9.1 Fault Alarm

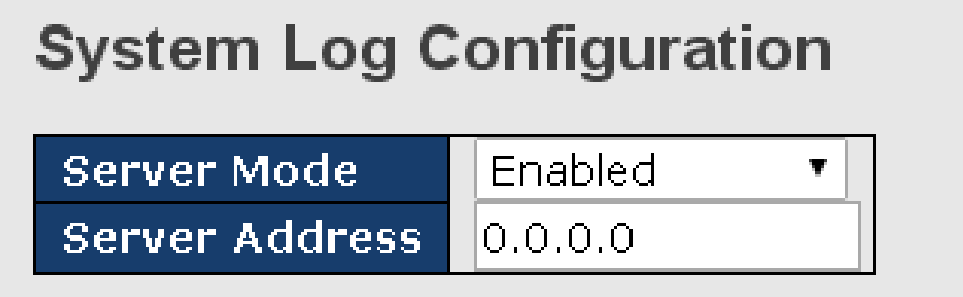
When any selected fault event happens, the Fault LED on the switch panel will light up and the electric relay will signal at the same time. The following pages allow you to set up alert conditions based on your needs for individual switch ports, including actions to be taken during disconnection and power failure.



5.9.2 System Warning

SYSLOG Setting

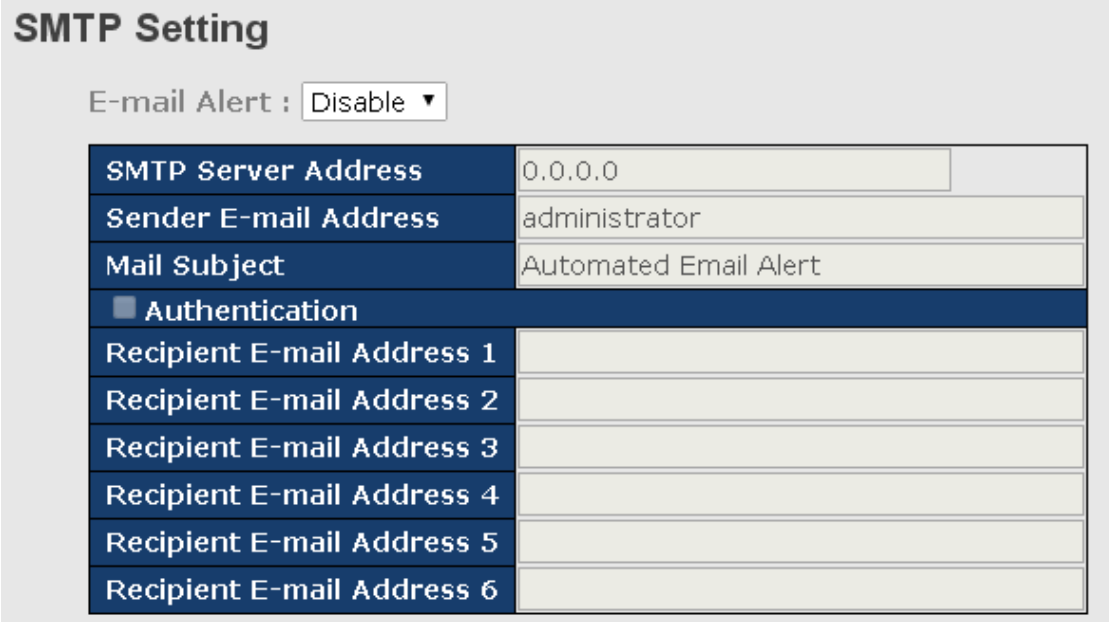
SYSLOG is a protocol that allows a device to send event notification messages across IP networks to event message collectors. It permits separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. As Syslog messages are UDP-based, the sender and receiver will not be aware of it if the packet is lost due to network disconnection and no UDP packet will be resent.



Label	Description
Server Mode	Indicates existing server mode. When the mode operation is enabled, the syslog message will be sent to syslog server. The syslog protocol is based on UDP communications and received on UDP port 514 and the syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always be sent even if the syslog server does not exist. Possible modes are: **Enabled**: enable server mode **Disabled**: disable server mode
SYSLOG Server IP Address	Indicates the IPv4 host address of syslog server. If the switch provides DNS functions, it also can be a host name.

SMTP Setting

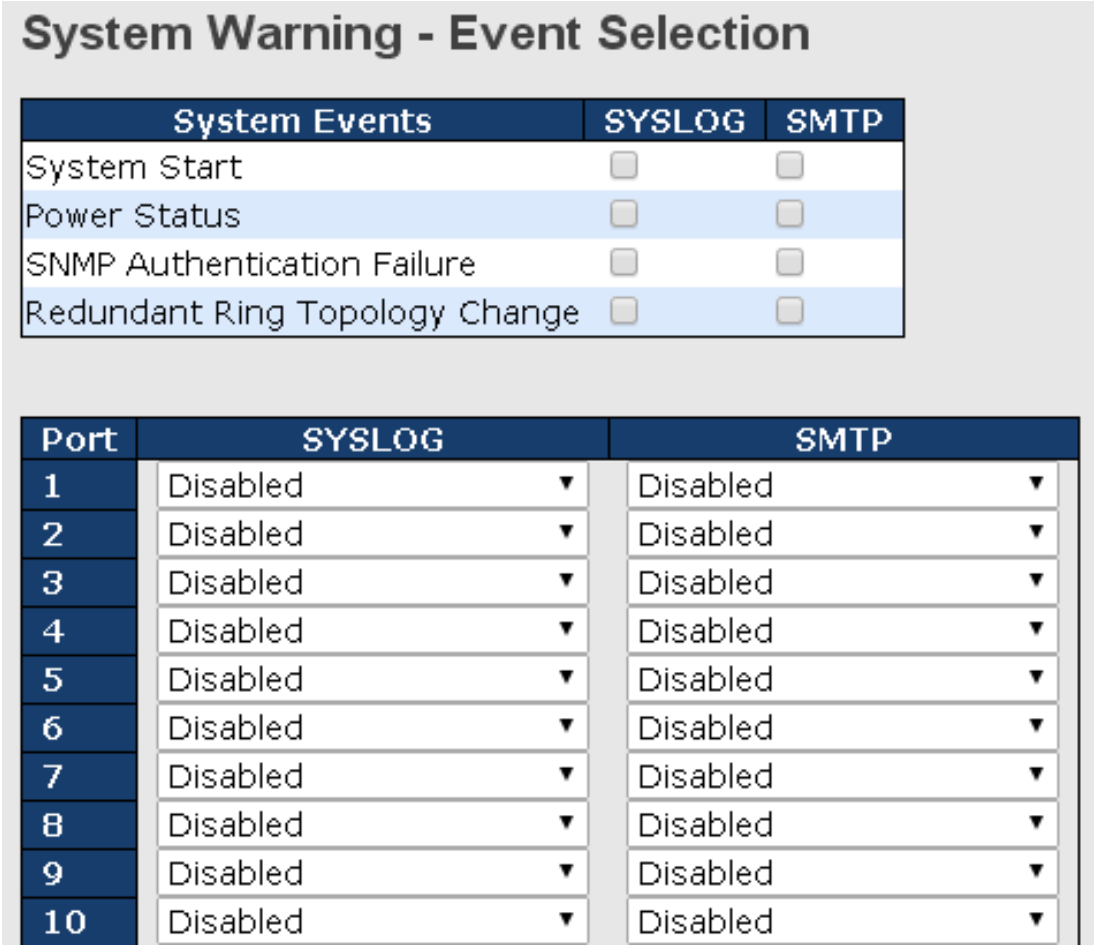
SMTP (Simple Mail Transfer Protocol) is a protocol for transmitting e-mails across the Internet. By setting up SMTP alert, the device will send a notification e-mail when a user-defined event occurs.



Label	Description
E-mail Alarm	Enables or disables transmission of system warnings by e-mail
Sender E-mail Address	SMTP server IP address
Mail Subject	Subject of the mail
Authentication	■ **Username:** the authentication username ■ **Password:** the authentication password ■ **Confirm Password:** re-enter password
Recipient E-mail Address	The recipient's e-mail address. A mail allows for 6 recipients.
Apply	Click to activate the configurations
Help	Shows help file

Event Selection

The device supports both SYSLOG and SMTP alerts. Check the corresponding box to enable the system event warning method you want. Please note that the checkboxes will gray out if SYSLOG or SMTP is disabled.

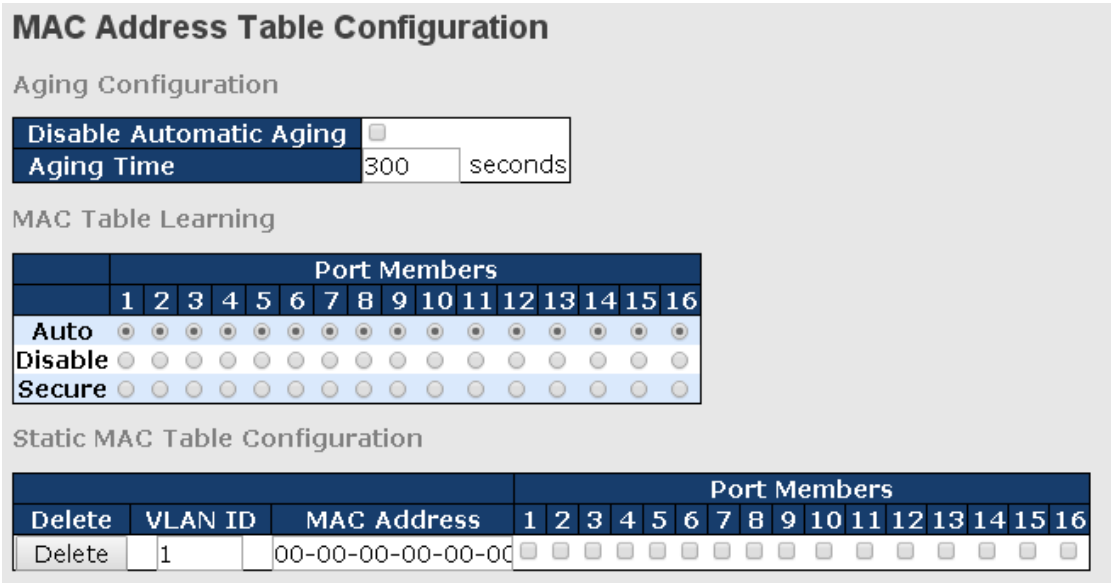


Label	Description
System Cold Start	Sends out alerts when the system is restarted
Power Status	Sends out alerts when power is up or down
SNMP Authentication Failure	Sends out alert when SNMP authentication fails
O-Ring Topology Change	Sends out alerts when O-Ring topology changes
Port Event SYSLOG / SMTP event	■ **Disable** ■ **Link Up** ■ **Link Down** ■ **Link Up & Link Down**
Apply	Click to activate the configurations
Help	Shows help file

5.10 Monitor and Diag

5.10.1 MAC Table

A MAC address tablet is a table in a network switch that maps MAC addresses to ports. The switch uses the table to determine which port the incoming packet should be forwarded to. Entries in a MAC address table fall into two types: dynamic and static entries. Entries in a static MAC table are added or removed manually and cannot age out by themselves. Entries in a dynamic MAC tablet will age out after a configured aging time. Such entries can be added by learning or manual configuration.

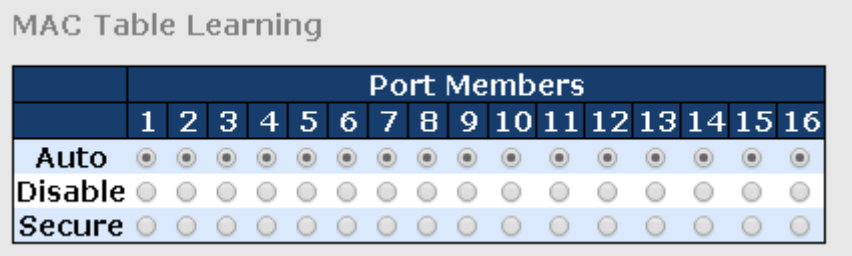


Aging Configuration

Aging enables the switch to track only active MAC addresses on the network and flush out MAC addresses that are no longer used, thereby keeping the table current. By default, aged entries are removed after 300 seconds. You can configure aging time by entering a value in the **Age Time** box in seconds. The allowed range is 10 to 1000000 seconds. You can also disable the automatic aging of dynamic entries by checking **Disable Automatic Aging**.

MAC Table Learning

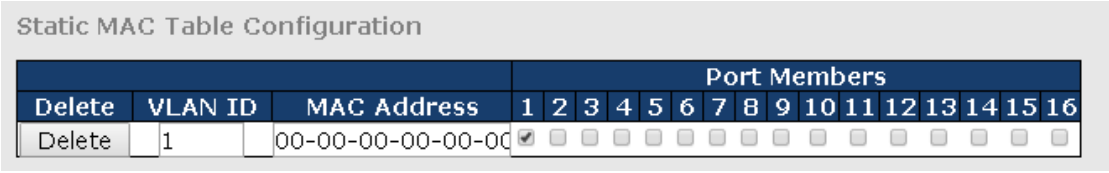
The switch can add the address and port on which the packet was received to the MAC table if the address does not exist in the table by examining the source address of each packet received on a port. This is called learning. It allows the MAC table to expand dynamically. If the learning mode for a given port is grayed out, it means another module is in control of the mode, and thus the user cannot change the configurations. An example of such a module is MAC-Based authentication under 802.1X.



Label	Description
Auto	Learning is done automatically as soon as a frame with unknown SMAC is received.
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped. Note: make sure the link used for managing the switch is added to the static Mac table before changing to secure learning mode, otherwise the management link will be lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

Static MAC Table Configurations

This tablet shows the static entries in the MAC table which can contain up to 64 entries. Using static MAC address entries can reduce broadcast packets remarkably and are suitable for networks where network devices seldom change. You can manage the entries in this page. The MAC table is sorted first by VLAN ID and then by MAC address.



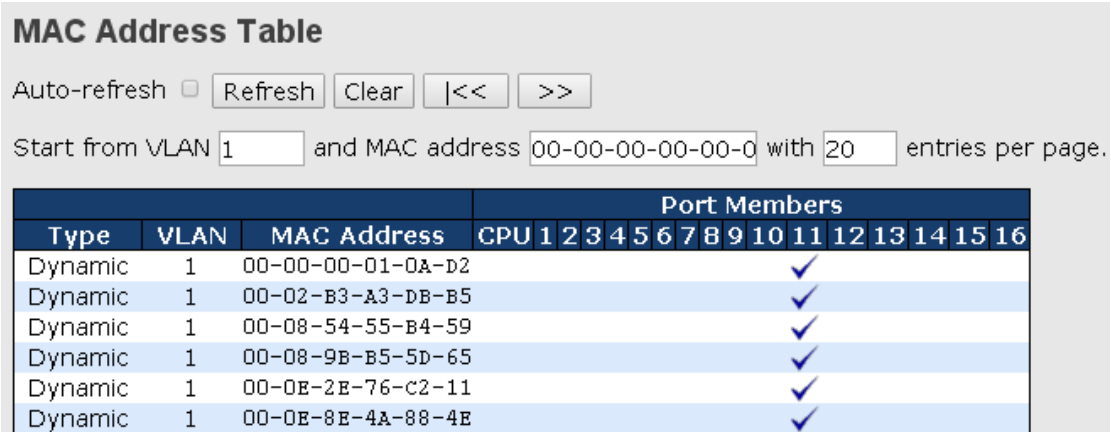
Label	Description
Delete	Check to delete an entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry
MAC Address	The MAC address for the entry
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck to modify the entry.
Adding New Static Entry	Click to add a new entry to the static MAC table. You can specify the VLAN ID, MAC address, and port members for the new entry. Click **Save** to save the changes.

MAC Table Status

Each page shows up to 999 entries from the MAC table, with a default value of 20, selected by 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.

Each page shows up to 999 entries from the MAC table, with a default value of 20, selected by 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** fields allow the user to select the starting point in the MAC table. Clicking **Refresh** will update the displayed table starting from that or the closest next MAC table match. In addition, the two input fields will – upon clicking **Refresh** - assume the value of the first displayed entry, allows for continuous refresh with the same start address. The **>>** button will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When it reaches the end, the text "**no more entries**" is shown in the displayed table. Use the **|<<** button to start over.

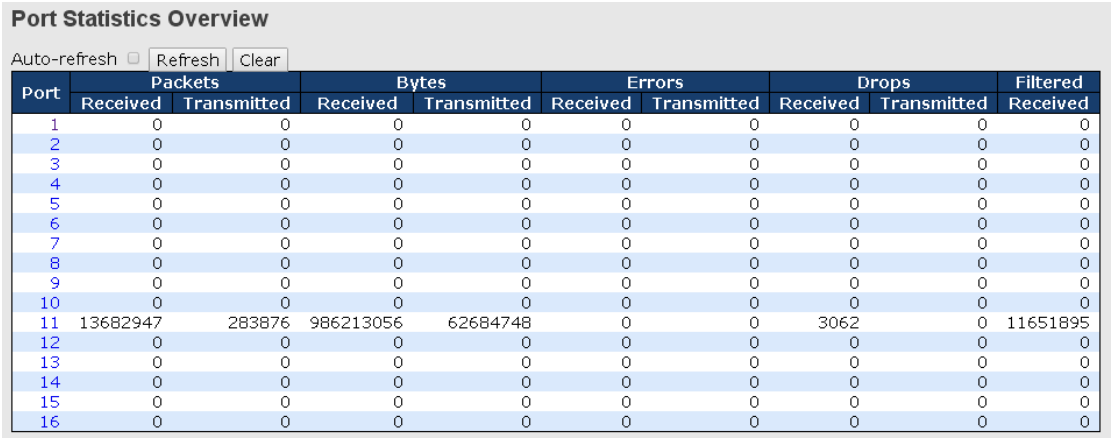


Label	Description
Type	Indicates whether the entry is a static or dynamic entry.
MAC address	The MAC address of the entry.
VLAN	The VLAN ID of the entry.
Port Members	The ports that are members of the entry.

5.10.2 Port Statistics

Traffic Overview

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



Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	13682947	283876	986213056	62684748	0	0	3062	0	11651895
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0

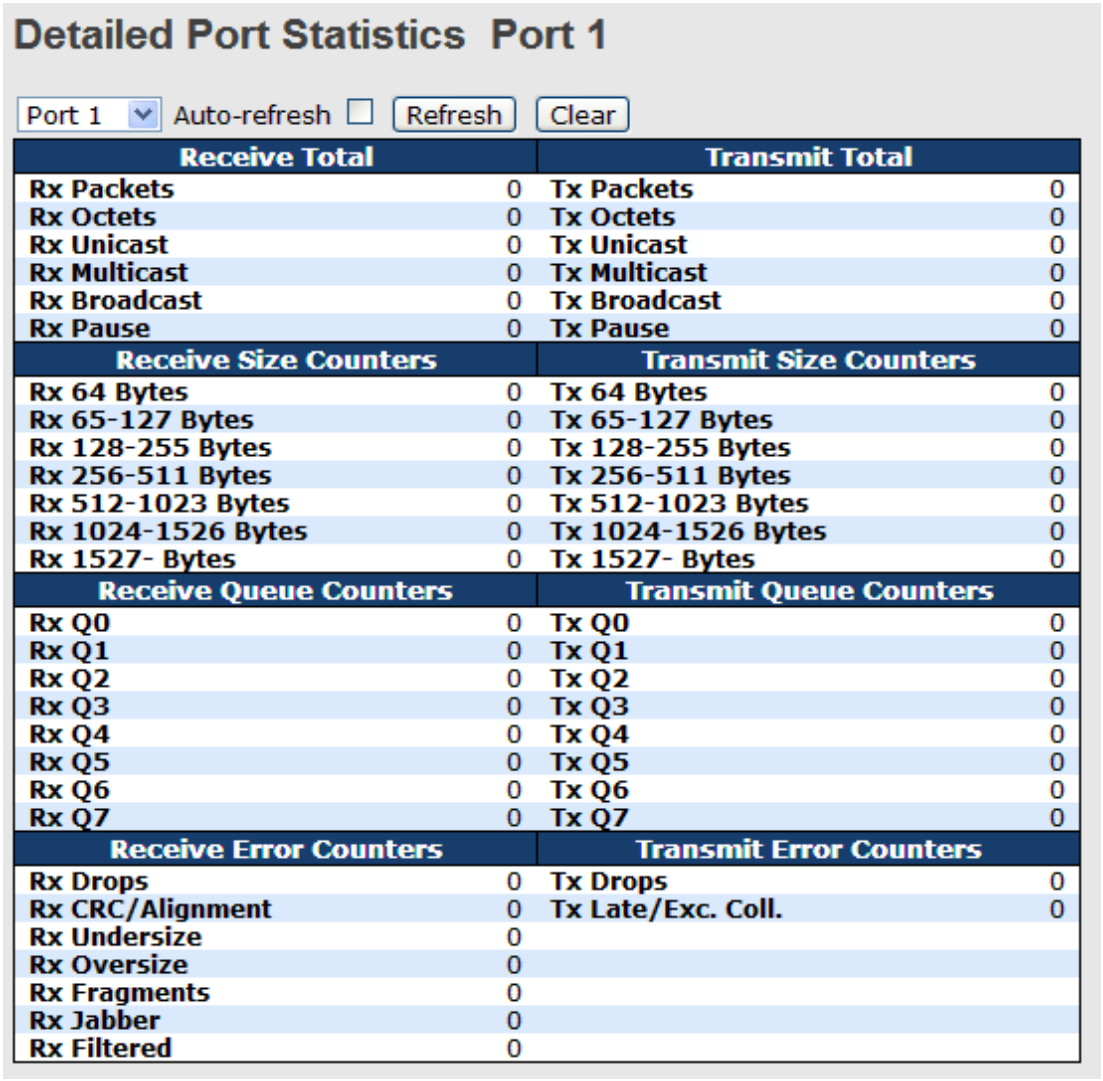
Label	Description
Port	The switch port number to which the following settings will be applied.
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions per port.
Drops	The number of frames discarded due to ingress or egress congestion.
Filtered	The number of received frames filtered by the forwarding process.
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals.
Refresh	Updates the counter entries, starting from the current entry ID.
Clear	Flushes all counters entries.

Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port drop-down list to decide the details of which switch port to be displayed.

The displayed counters include the total number for receive and transmit, the size for receive and transmit, and the errors for receive and transmit.

Detailed Statistics – Total Receive & Transmit



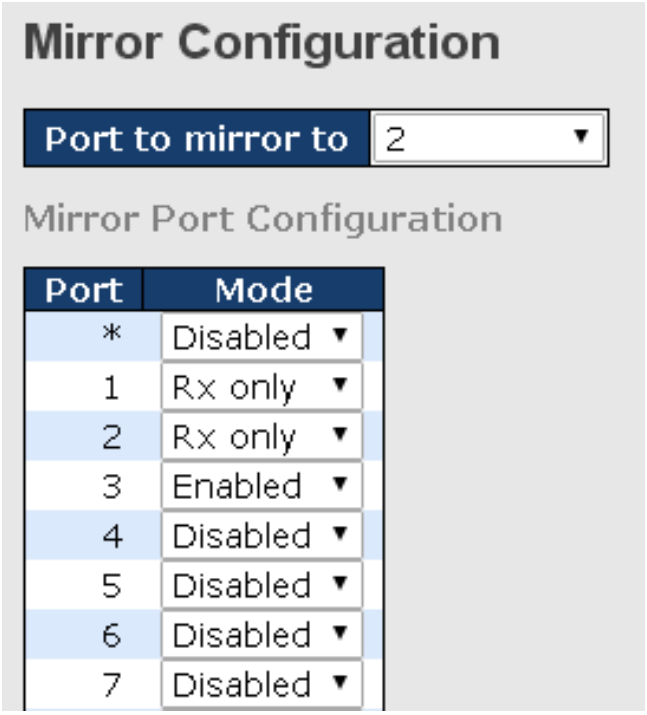
Label	Description
Rx and Tx Packets	The number of received and transmitted (good and bad) packets
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes, including FCS, except framing bits
Rx and Tx Unicast	The number of received and transmitted (good and bad) unicast packets
Rx 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	The number of MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation
Rx Drops	The number of frames dropped due to insufficient receive buffer 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 a valid CRC
Rx Oversize	The number of long[2] frames received with a valid CRC
Rx Fragments	The number of short[1] frames received with an invalid CRC
Rx Jabber	The number of long[2] frames received with an invalid CRC
Rx Filtered	The number of received frames filtered by the forwarding process
Tx Drops	The number of frames dropped due to output buffer congestion
Tx Late / Exc.Coll.	The number of frames dropped due to excessive or late collisions

1. Short frames are frames smaller than 64 bytes.
2. Long frames are frames longer than the maximum frame length configured for this port.

5.10.3 Port Mirroring

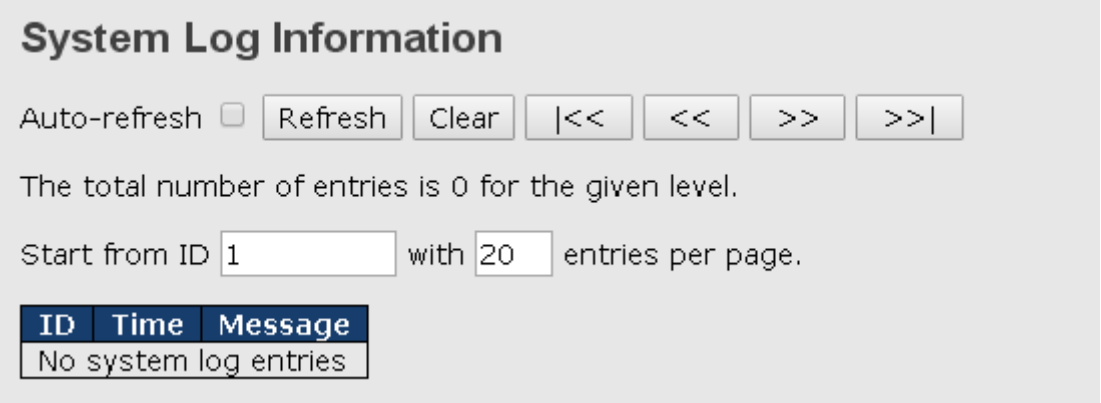
Port mirroring function will copy the traffic of one port to another port on the same switch to allow the network analyzer attached to the mirror port to monitor and analyze packets. The function is useful for troubleshooting. To solve network problems, selected traffic can be copied or mirrored to a mirror port where a frame analyzer can be attached to analyze the frame flow. The traffic to be copied to the mirror port can be all frames received on a given port (also known as ingress or source mirroring) or all frames transmitted on a given port (also known as egress or destination mirroring). The port to which the monitored traffic is copied is called mirror port.



Label	Description
Port	The switch port number to which the following settings will be applied.
Mode	Drop-down list for selecting a mirror mode. **Rx only**: only frames received on this port are mirrored to the mirror port. Frames transmitted are not mirrored. **Tx only**: only frames transmitted from this port are mirrored to the mirror port. Frames received are not mirrored. **Disabled**: neither transmitted nor recived frames are mirrored. **Enabled**: both received and transmitted frames are mirrored to the mirror port. Note: for a given port, a frame is only transmitted once. Therefore, you cannot mirror Tx frames to the mirror port. In this case, mode for the selected mirror port is limited to **Disabled** or **Rx nly**.

5.10.4 System Log Information

This page provides switch system log information.

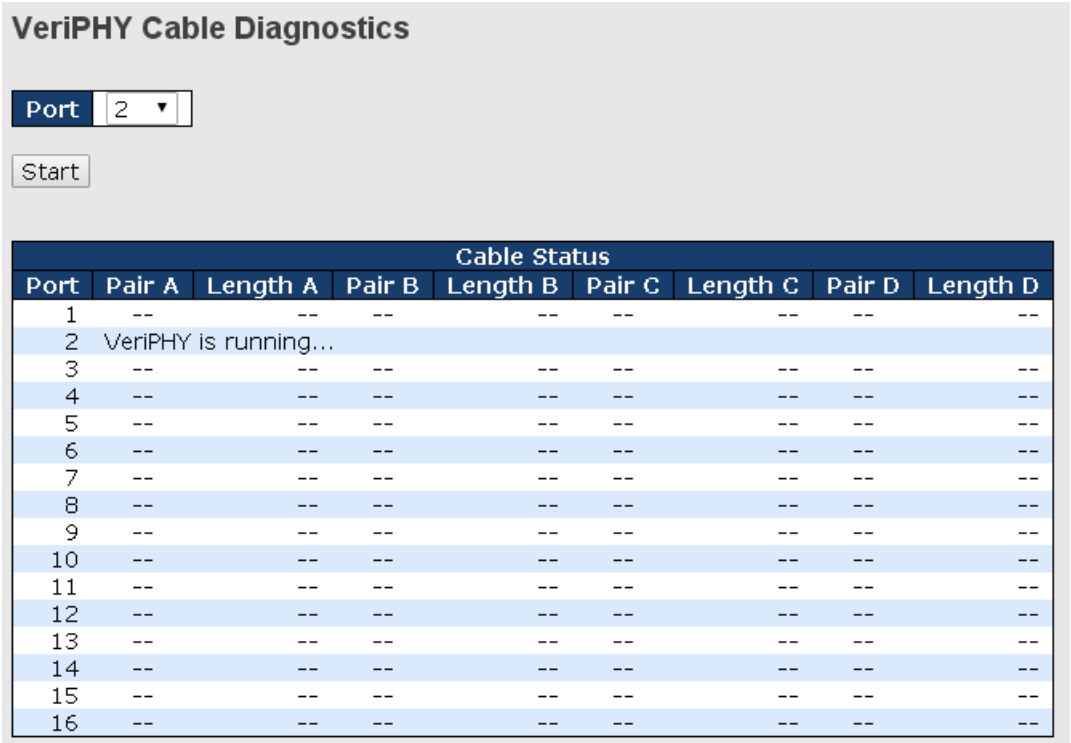


Label	Description
ID	The ID (>= 1) of the system log entry
Time	The time of the system log entry
Message	The MAC address of the switch
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Updates system log entries, starting from the current entry ID
Clear	Flushes all system log entries
|<<	Updates system log entries, starting from the first available entry ID
<<	Updates system log entries, ending at the last entry currently displayed

>>	Updates system log entries, starting from the last entry currently displayed.
>>|	Updates system log entries, ending at the last available entry ID.

5.10.5 Cable Diagnostics

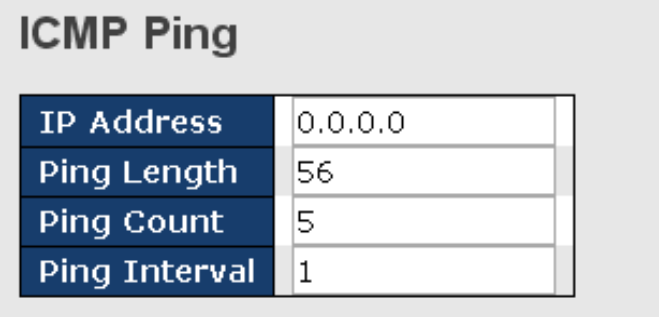
You can perform cable diagnostics for all ports or selected ports to diagnose any cable faults (short, open etc.) and feedback a distance to the fault. Simply select the port from the drop-down list and click Start to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that VeriPHY diagnostics is only accurate for cables 7 - 140 meters long. 10 and 100 Mbps ports will be disconnected while running VeriPHY diagnostics. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is completed.



Label	Description
Port	The port for which VeriPHY Cable Diagnostics is requested
Cable Status	Port: port number Pair: the status of the cable pair Length: the length (in meters) of the cable pair

5.10.6 Ping

This command sends ICMP echo request packets to another node on the network. Using the ping command, you can see if another site on the network can be reached.



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

PING6 server ::10.10.132.20

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

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

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

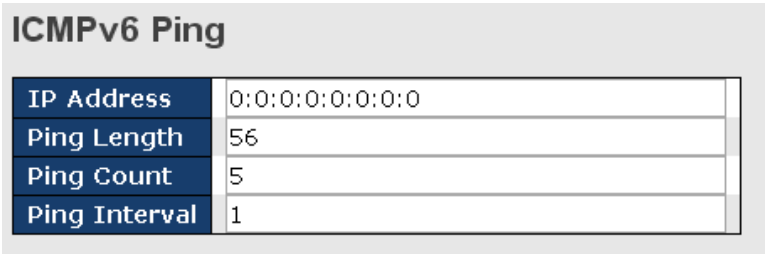
64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms

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

Sent 5 packets, received 5 OK, 0 bad

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

Label	Description
IP Address	The destination IP Address
Ping Length	The payload size of the ICMP packet. Values range from 8 to 1400 bytes.
Ping Count	The number of ICMP packets to be sent.
Ping Interval	The interval at which ICMP packets will be sent.



PING6 server ::192.168.10.1

sendto

sendto

sendto

sendto

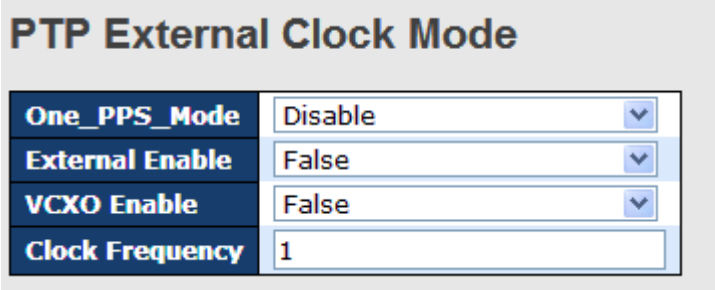
sendto

Sent 5 packets, received 0 OK, 0 bad

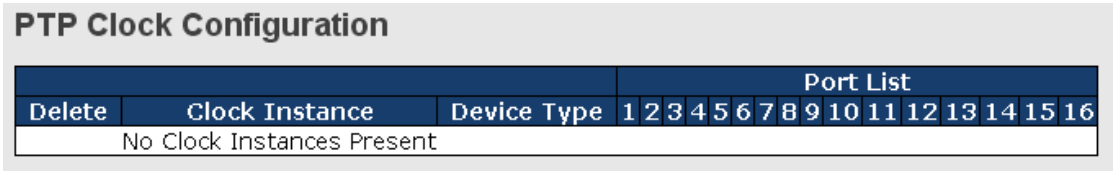
5.11 Synchronization

5.11.1 PTP

PTP External Clock Mode is a protocol for synchronizing clocks throughout a computer network. On a local area network, it achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems.



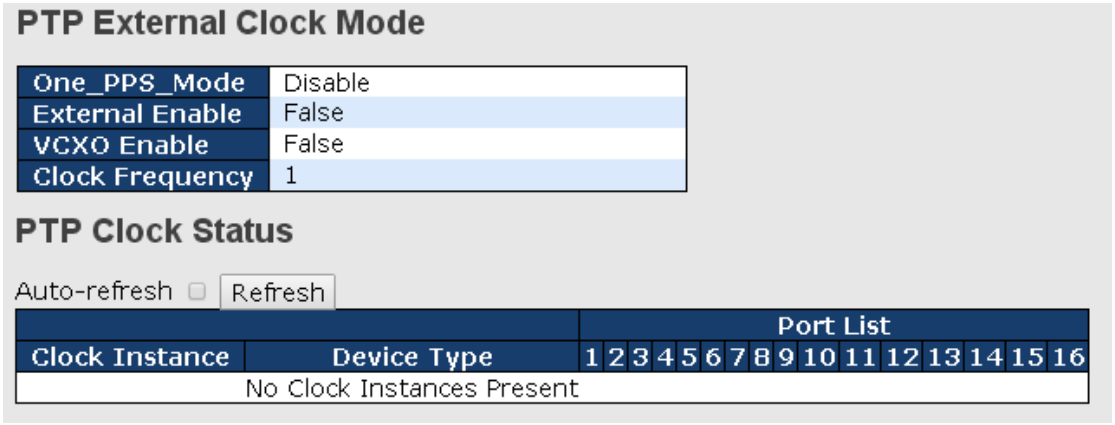
Label	Description
One_PPS_Mode	The box allows you to select One_pps_mode configurations. The following values are possible: **Output**: enable the 1 pps clock output. **Input**: enable the 1 pps clock input. **Disable**: disable the 1 pps clock in/out-put.
External Enable	The box allows you to configure external clock output. The following values are possible: **True**: enable external clock output. **False**: disable external clock output.
VCXO_Enable	The box allows you to configure the external VCXO rate adjustment. The following values are possible: **True**: enable external VCXO rate adjustment. **False**: disable external VCXO rate adjustment.
Clock Frequency	The box allows you to set clock frequency. The range of values is 1 - 25000000 (1 - 25MHz).



Label	Description
Delete	Check this box and click **Save** to delete the clock instance
Clock Instance	Indicates the instance of a particular clock instance [0..3] Click on the clock instance number to edit the clock details
Device Type	Indicates the type of the clock instance. There are five device types. **Ord-Bound**: ordinary/boundary clock **P2p Transp**: peer-to-peer transparent clock **E2e Transp**: end-to-end transparent clock **Master Only**: master only **Slave Only**: slave only
Port List	Set check mark for each port configured for this Clock Instance.
2 Step Flag	Static member defined by the system; **true** if two-step Sync events and Pdelay_Resp events are used
Clock Identity	Shows a unique clock identifier
One Way	If **true**, one-way measurements are used. This parameter applies only to a slave. In one-way mode no delay measurements are performed, i.e. this is applicable only if frequency synchronization is needed. The master always responds to delay requests.
Protocol	Transport protocol used by the PTP protocol engine Ethernet PTP over Ethernet multicast ip4multi PTP over IPv4 multicast ip4uni PTP over IPv4 unicast Note: IPv4 unicast protocol only works in Master Only and Slave Only clocks For more information, please refer to **Device Type**. In a unicast Slave Only clock, you also need to configure which master clocks to request Announce and Sync messages from. For more information, please refer to Unicast Slave Configuration
VLAN Tag Enable	Enables VLAN tagging for PTP frames Note: Packets are only tagged if the port is configured for vlan tagging. i.e:

	Port Type != Unaware and PortVLAN mode == None, and the port is member of the VLAN.
VID	VLAN identifiers used for tagging the PTP frames
PCP	Priority code point values used for PTP frames

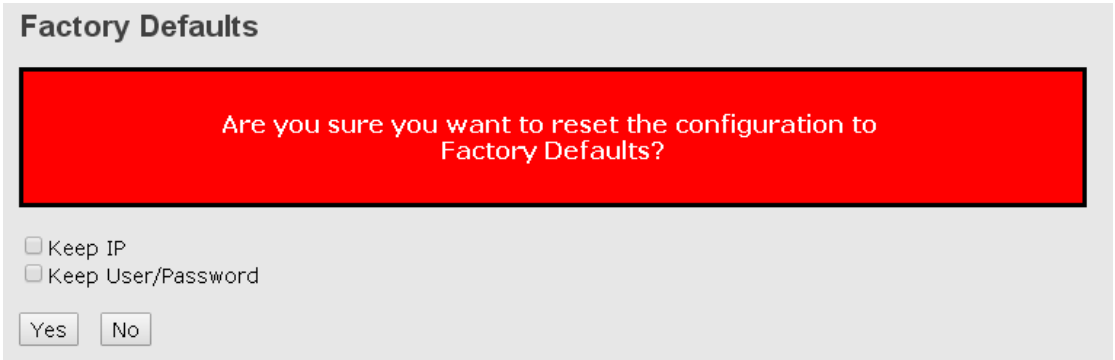
You can click on Status link to read the details of your configuration.



5.12 Troubleshooting

5.12.1 Factory Defaults

This function is to force the switch back to the original factory settings. To reset the switch, select **Reset to Factory Defaults** from the drop-down list and click **Yes**. Only the IP configuration is retained.

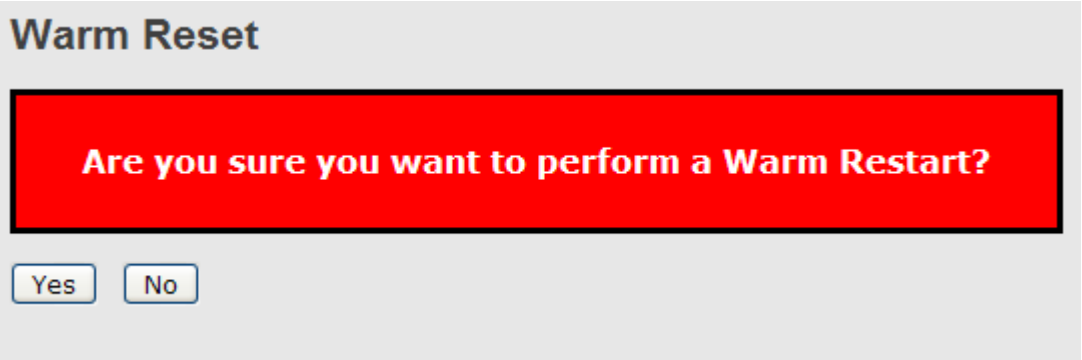


Label	Description
Yes	Click to reset the configuration to factory defaults
No	Click to return to the Port State page without resetting

5.12.2 System Reboot

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

have powered on the devices.



Label	Description
Yes	Click to reboot device
No	Click to return to the **Port State** page without rebooting

Command Line Management

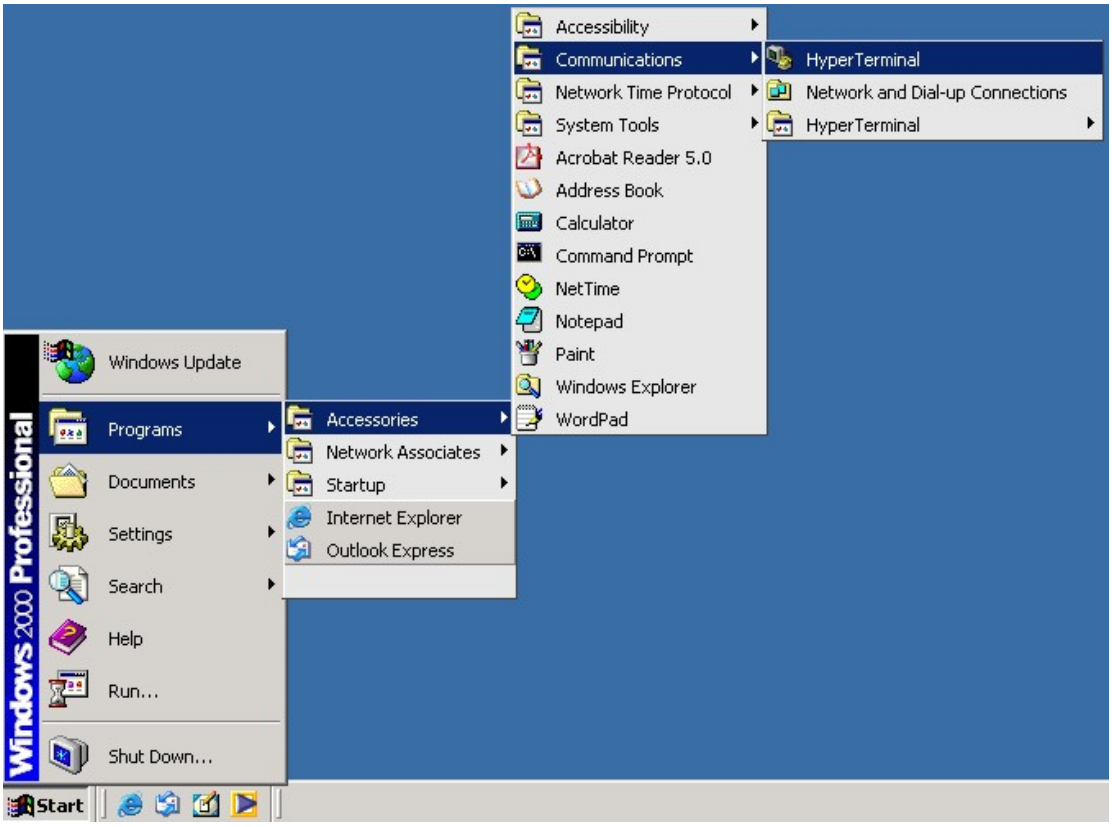
Besides Web-based management, the switch also supports CLI management. You can use console or telnet to manage the switch by CLI.

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

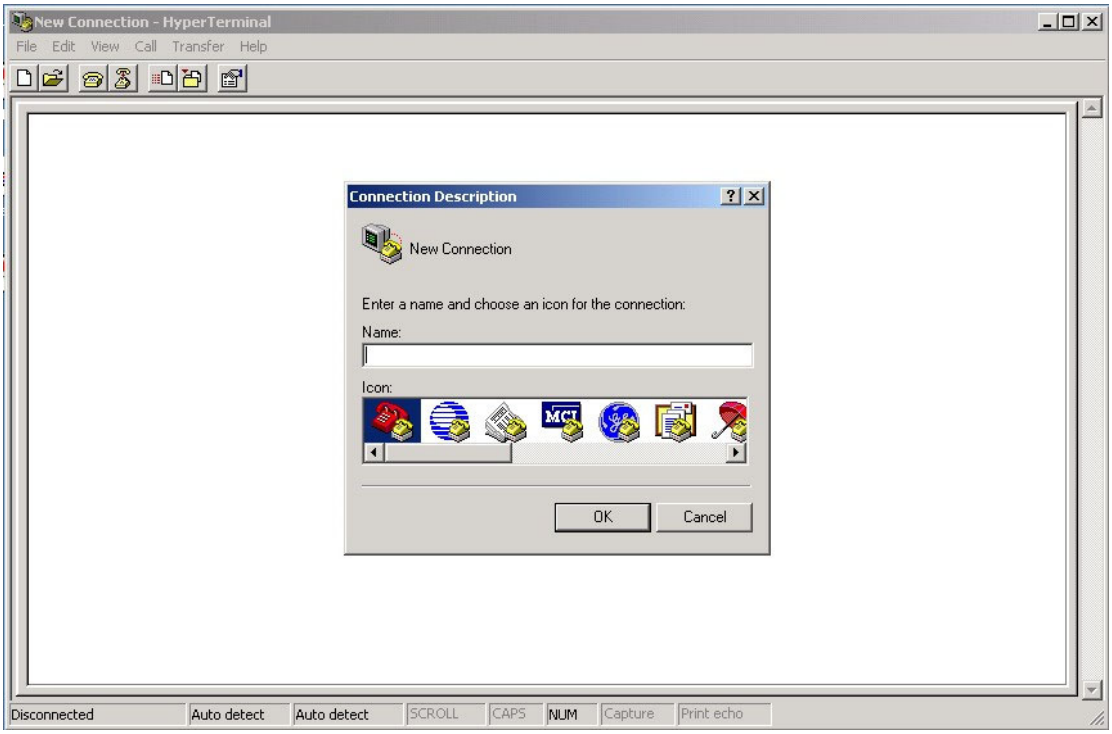
Before configuring RS-232 serial console, connect the RS-232 port of the switch to your PC Com port using a RJ45 to DB9-F cable.

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

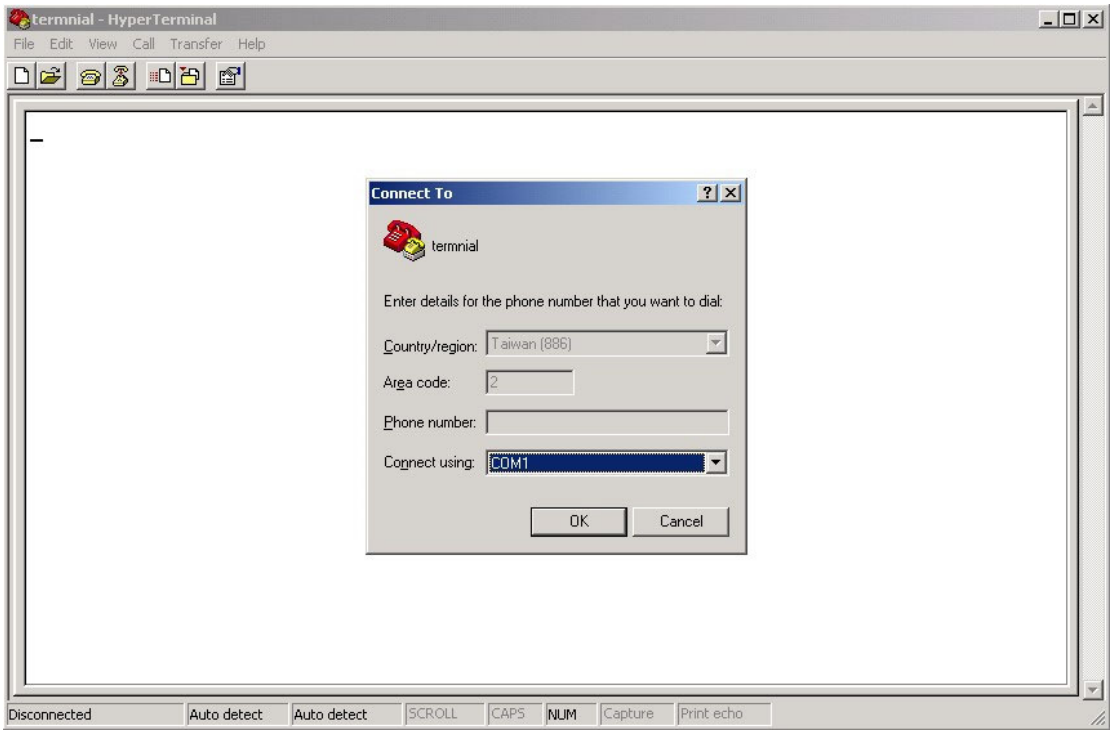
Step 1: On Windows desktop, click on **Start** -> **Programs** -> **Accessories** -> **Communications** -> **Hyper Terminal**



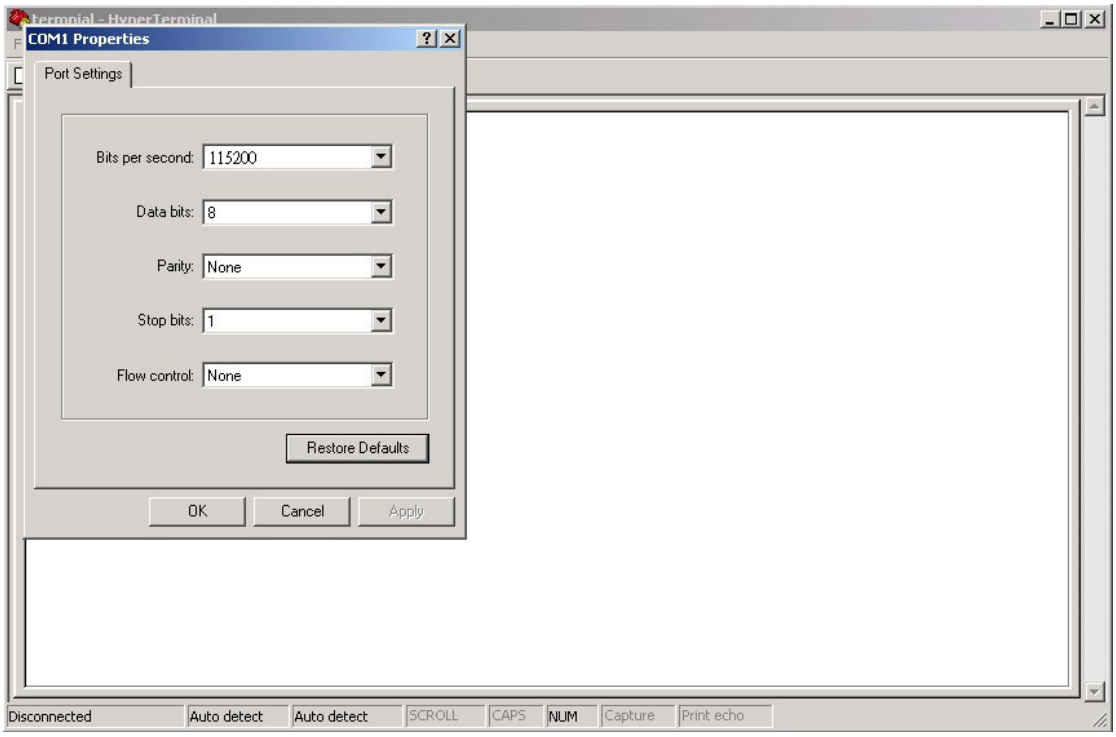
Step 2. Input a name for the new connection.



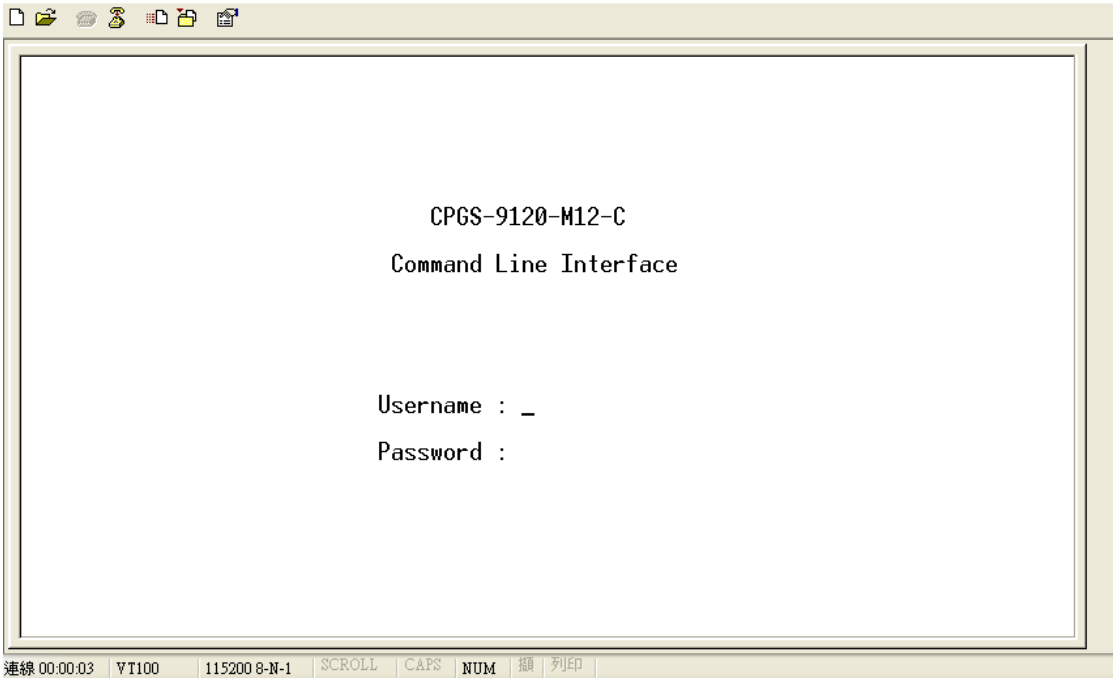
Step 3. Select a COM port in the drop-down list.



Step 4. A pop-up window that indicates COM port properties appears, including bits per second, data bits, parity, stop bits, and flow control.



Step 5. The console login screen will appear. Use the keyboard to enter the Username and Password (same as the password for Web browsers), then press **Enter**.



CLI Management by Telnet

You can can use **TELNET**to configure the switch. The default values are:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

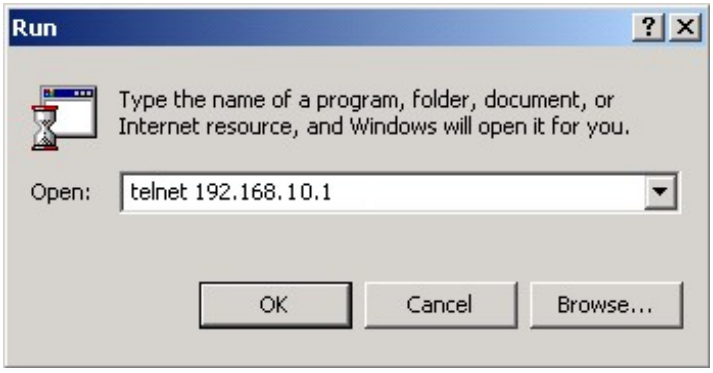
Default Gateway: **192.168.10.254**

User Name: **admin**

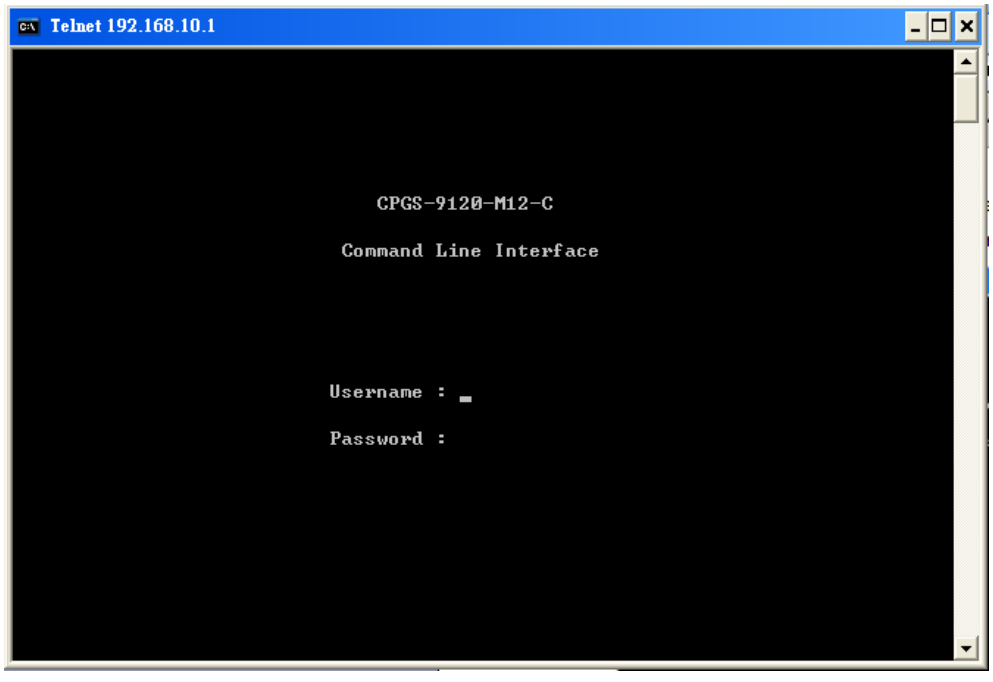
Password: **admin**

Follow the steps below to access console via Telnet.

Step 1. Telnet to the IP address of the switch from the **Run** window by inputingcommands (or from the MS-DOS prompt) as below.



Step 2. The Login screen will appear. Use the keyboard to enter the Username and Password (same as the password for Web browser), and then press **Enter.**



Commander Groups

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

System

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

Syslog

Syslog>	ServerConfiguration [<ip_addr>]

IP

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

Auth

Auth>	Configuration
	Timeout [<timeout>]
	Deadtime [<dead_time>]
	RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
	ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
	Client [console|telnet|ssh|web] [none|local|radius] [enable|disable]

	Statistics [<server_index>]

Port

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

Aggr

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

LACP

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

STP

STP>	Configuration
	Version [<stp_version>] Non-certified release, v
	Txhold [<holdcount>]lt 15:15:15, Dec 6 2007

	MaxAge [<max_age>]
	FwdDelay [<delay>]
	bpduFilter [enable|disable]
	bpduGuard [enable|disable]
	recovery [<timeout>]
	CName [<config-name>] [<integer>]
	Status [<msti>] [<port_list>]
	Msti Priority [<msti>] [<priority>]
	Msti Map [<msti>] [clear]
	Msti Add <msti> <vid>
	Port Configuration [<port_list>]
	Port Mode [<port_list>] [enable|disable]
	Port Edge [<port_list>] [enable|disable]
	Port AutoEdge [<port_list>] [enable|disable]
	Port P2P [<port_list>] [enable|disable|auto]
	Port RestrictedRole [<port_list>] [enable|disable]
	Port RestrictedTcn [<port_list>] [enable|disable]
	Port bpduGuard [<port_list>] [enable|disable]
	Port Statistics [<port_list>]
	Port Mcheck [<port_list>]
	Msti Port Configuration [<msti>] [<port_list>]
	Msti Port Cost [<msti>] [<port_list>] [<path_cost>]
	Msti Port Priority [<msti>] [<port_list>] [<priority>]

Dot1x

Dot1x>	Configuration [<port_list>]
	Mode [enable|disable]
	State [<port_list>] [macbased|auto|authorized|unauthorized]
	Authenticate [<port_list>] [now]
	Reauthentication [enable|disable]
	Period [<reauth_period>]
	Timeout [<eapol_timeout>]
	Statistics [<port_list>] [clear|eapol|radius]
	Clients [<port_list>] [all|<client_cnt>]

	Agetime [<age_time>]
	Holdtime [<hold_time>]

IGMP

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

LLDP

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

MAC

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

	Flush

VLAN

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

PVLAN

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

QOS

QoS>	Configuration [<port_list>]
	Classes [<class>]
	Default [<port_list>] [<class>]
	Tagprio [<port_list>] [<tag_prio>]
	QCL Port [<port_list>] [<qcl_id>]
	QCL Add [<qcl_id>] [<qce_id>] [<qce_id_next>] (etype <etype>) | (vid <vid>) | (port <udp_tcp_port>) | (dscp <dscp>) | (tos <tos_list>) | (tag_prio <tag_prio_list>) <class>
	QCL Delete <qcl_id> <qce_id>
	QCL Lookup [<qcl_id>] [<qce_id>]
	Mode [<port_list>] [strict|weighted]
	Weight [<port_list>] [<class>] [<weight>]

	Rate Limiter [<port_list>] [enable|disable] [<bit_rate>]
	Shaper [<port_list>] [enable|disable] [<bit_rate>]
	Storm Unicast [enable|disable] [<packet_rate>]
	Storm Multicast [enable|disable] [<packet_rate>]
	Storm Broadcast [enable|disable] [<packet_rate>]

ACL

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

Mirror

Mirror>	Configuration [<port_list>]
	Port [<port>|disable]

	Mode [<port_list>] [enable|disable|rx|tx]

Config

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

SNMP

SNMP>	Trap Inform Retry Times [<retries>]
	Trap Probe Security Engine ID [enable|disable]
	Trap Security Engine ID [<engineid>]
	Trap Security Name [<security_name>]
	Engine ID [<engineid>]
	Community Add <community> [<ip_addr>] [<ip_mask>]
	Community Delete <index>
	Community Lookup [<index>]
	User Add <engineid> <user_name> [MD5|SHA] [<auth_password>] [DES] [<priv_password>]
	User Delete <index>
	User Changekey <engineid> <user_name> <auth_password> [<priv_password>]
	User Lookup [<index>]
	Group Add <security_model> <security_name> <group_name>
	Group Delete <index>
	Group Lookup [<index>]
	View Add <view_name> [included|excluded] <oid_subtree>
	View Delete <index>
	View Lookup [<index>]
	Access Add <group_name> <security_model> <security_level> [<read_view_name>] [<write_view_name>] Access Delete <index>
	Access Lookup [<index>]

Firmware

Firmware>	Load <ip_addr_string> <file_name>

fault

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

SFLOW

SFLOW>	mode [enable|disable]
	version [v2|v5]
	rate [<integer>]
	interval [<integer>]
	coladdr [<ip_addr>]
	colport [<integer>]
	show

Technical Specifications