User's Manual

iES20GF

Intelligent 20 Port Managed Gigabit Ethernet Switch

IEC61850 and IEEE1613 Compliant

iES20GF-v1/iES20GF-v2

https://is5com.com/products/

Version 1.92, Nov 2021

iS5 COMMUNICATIONS

SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS

COPYRIGHT NOTICE

TRADEMARKS

iS5Com is a registered trademark of iS5. All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

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

WARRANTY

iS5 warrants that all products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). iS5 will repair or replace products found to be defective within this warranty period including shipping costs. This warranty does not cover product modifications or repairs done by persons other than iS5-approved personnel, and this warranty does not apply to products that are misused, abused, improperly installed, or damaged by accident.

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. iS5 shall not be responsible for its use or infringements on third-parties because of the use of this publication. There may occasionally be unintentional errors on this publication. iS5 reserves the right to revise the contents of this publication without notice.

CONTACT INFORMATION

iS5 Communications Inc.
5895 Ambler Drive, Mississauga, Ontario, L4W 5B7
Tel: + 905-670-0004 // Fax: + 289-401-5206
Website: www.iS5Com.com

Technical Support
E-mail: support@iS5Com.com

Sales Contact
E-mail: sales@iS5Com.com

Table of Contents

Table of Figures

Table of Tables

FCC STATEMENT AND CAUTIONS

Federal Communications Commission Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment can generate, use, and radiate radio frequency energy. If not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will at his/her own expense, be required to correct the interference.

This is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Caution: LASER

This product contains a laser system and is classified as a CLASS 1 LASER PRODUCT. Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.

Caution: Service

This product contains no user-serviceable parts. Attempted service by unauthorized personnel shall render all warranties null and void.

Changes or modifications not expressly approved by iS5 Communications Inc. could invalidate specifications, test results, and agency approvals, and void the user's authority to operate the equipment.

Should this device require service, please contact support@iS5Com.com.

Caution: Physical Access

This product should be installed in a restricted access location. Access should only be gained by qualified service personnel or users who have been instructed on the reasons for the restrictions applied at the location, and any precautions that have been taken. Access must only be via the use of a tool or lock and key, or other means of security, and is controlled by the authority responsible for the location.

1. GETTING STARTED

1.1 About iES20GF

The iES20GF is an intelligent managed 20 port Gigabit Ethernet switch with up to 20 x 10/100/1000Base-T(X) RJ45, and up to 4 x 100/1000Base-X SFP, or 4 x 100Base-FX, or 4 x 1000Base-SX/LX ports.

The switch is IEC61850-3 and IEEE1613 compliant.

The iES20GF provides redundancy support through functions such as STP/RSTP/MSTP assuring protection of all mission critical network applications. iES20GF can be managed via the Web, iManage Software Suite, Telnet, and Console (CLI) / SSH v2.

The switch is made of IP-40 galvanized steel and has a wide operating temperature range from -40°C to +85°C, which is suitable for the harshest of environments without the use of fans.

1.2 References

[1] Cisco.com, *Configuring QoS* https://www.cisco.com/c/en/us/td/docs/switches/metro/me1200/gui/guide/b_ME1200_Web_GUI_book/b_ME1200_Web_GUI_book_chapter_011010.pdf Online, Accessed on Mar 26, 2019

[2] Network Working Group, RFC 3768, Virtual Router Redundancy Protocol (VRRP), https://tools.ietf.org/html/rfc3768#section-5.3.6 Online, Accessed on Mar 29, 2019

[3] Network Working Group, RFC 4668, RADIUS Authentication Client MIB for IPv6, https://tools.ietf.org/html/rfc4668 , Online, Accessed on Apr 3, 2019

[4] Network Working Group, RFC 4670, RADIUS Accounting Client MIB for IPv6, https://tools.ietf.org/html/rfc4670 , Online, Accessed on Apr 3, 2019

[5] Network Working Group, RFC 3164, The BSD syslog Protocol, https://tools.ietf.org/html/rfc3748 , Online, Accessed on Apr 3, 2019

[6] Oracle.com, STP Administration Guide, IST, CIST, AND CST, https://docs.oracle.com/cd/E19934-01/html/E21706/z40037c31414269.html#scrolltoc, Online, Accessed on Apr 3, 2019

[7] Stack Overflow, *Maximum size of ICMP IPv6 packet,* https://stackoverflow.com/questions/15434362/maximum-size-of-icmp-ipv6-packet

[8] Cisco.com, *Cisco APIC and QoS* https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/Cisco-APIC-and-QoS.html#id_34903 , Online, Accessed on Apr 17, 2019

[9] Cisco.com, Chapter: Configuring QoS, QoS Components, https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/16-6/configuration_guide/qos/b_166_qos_9400_cg/b_166_qos_9400_cg_chapter_01.html Online, Accessed on Apr 17, 2019

[10] Juniper Networks, TechLibrary, Junos OS, Spanning-Tree Protocols Feature Guide, Loop Protection for Spanning-Tree Protocols, https://www.juniper.net/documentation/en_US/junos/topics/topic-map/spanning-tree-loop-protection.html Online, Accessed on Apr 30, 2019

[11] Cisco.com, Configuring Traffic Storm Control, https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_storm.pdf Online, Accessed on May 1, 2019

[12] Cisco.com, AAA Overview, https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfaaa.pdf Online, Accessed on May 1, 2019

1.3 Acronyms

The following table shows all acronyms used in this document.

Acronym	Explanation
AAA	Authentication, authorization, and accounting (network security services)
ACE	Access Control Entry
ACL	Access Control List
AF	Assured Forwarding
ARP	Address Resolution Protocol

Acronym	Explanation
BPDU	Bridge Protocol Data Unit
CIST	Common and Internal Spanning Tree
CLI	Command Line Interface
DCHP	Dynamic Host Configuration Protocol
DDM	Digital Diagnostic Monitoring
DEI	Discard Eligibility (subfield in *an IEEE 802.1Q frame header*)
DNS	Domain Name Server
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DP	Drop Precedence
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
HLN	Hardware Address Length
HRD	hardware address space (i.e. ARP *hardware address* type (ar$*hrd*)))
HSR	High-availability Seamless Redundancy
HTTPS	Hyper Text Transfer Protocol Secure or HTTP over SSL
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol (IP)
IPMC(v4)	IP(v4) MultiCast
LAG	Link Aggregation Group
LACP	Link Aggregation Control Protocol
LLDP	Link Layer Discovery Protocol
LLDP- MED	LLDP - Media Endpoint Discovery
LLDPDU	LLDP Data Unit
MIB	Management Information Base

Acronym	Explanation
MRP	Media Redundancy Protocol
MSTI	Multiple Spanning Tree Instances
MSTP	Multiple Spanning Tree Protocol
NTP	Network Time Protocol
OID	Object Identifier
OUI	Organizationally Unique Identifier (In Linux)
PDU	Protocol Data Unit
PID	Process Identifier
P2P	Point-To-Point (link)
PSH	Push Function (a value for the ACE)
PWR	Power
QCE	QoS Control Entry
QCL	QoS Control List
QoS	Quality of Service
RARP	Reverse Address Resolution Protocol (Reverse ARP)
RIP	Routing Information Protocol
RMON	Remote Monitoring
RSTP	Rapid Spanning Tree Protocol
SIP	Source IP
SMAC	Source MAC Address
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSAP	Source Service Access Point
SSH	Secure Shel
TACACS	Terminal Access Controller Access Control System
TCN	Topology Change Notification

Acronym	Explanation
TCP	Transmission Control Protocol
THA	target Hardware Address
TLV	Type-Length-Value
TPID	Tag protocol identifier
TTL	Time to live
SSH	Secure Shell
UDP	User Datagram Protocol
URG	Urgent Pointer Field Significant (an ACE value)
USM	User-based Security Model
UTC	Coordinated Universal Time
VACM	View based Access Control Model
VCXO	Voltage Controlled Crystal Oscillator
VID	VLAN ID

1.4 Software Features

- Web or CLI based Management (Console or Telnet / SSH v2)
- DHCP Server / Relay
- VLAN (802.1Q) for segregating and securing network traffic
- Supports SNMPv1/v2/v3
- Traffic Prioritization—Storm Control and Quality of Service (QoS) including DSCP-Based QoS Ingress Port Classification
- Multicast traffic—IGMP Snooping (IGMP v1/v2 / v3) and unregistered IPMCv4 Flooding
- Warnings (Syslog and SMTP) and Fault Alarm (power failure)
- Monitoring and Diagnostics—MAC Table and Port Statistics (ports monitoring including for SFP ports, system information, issuing PING packets for troubleshooting IP connectivity issues)
- SNTP for synchronizing of clocks over network
- Supports standard IEC 62439-2 MRP (Media Redundancy Protocol) functionality

1.5 Hardware Specifications

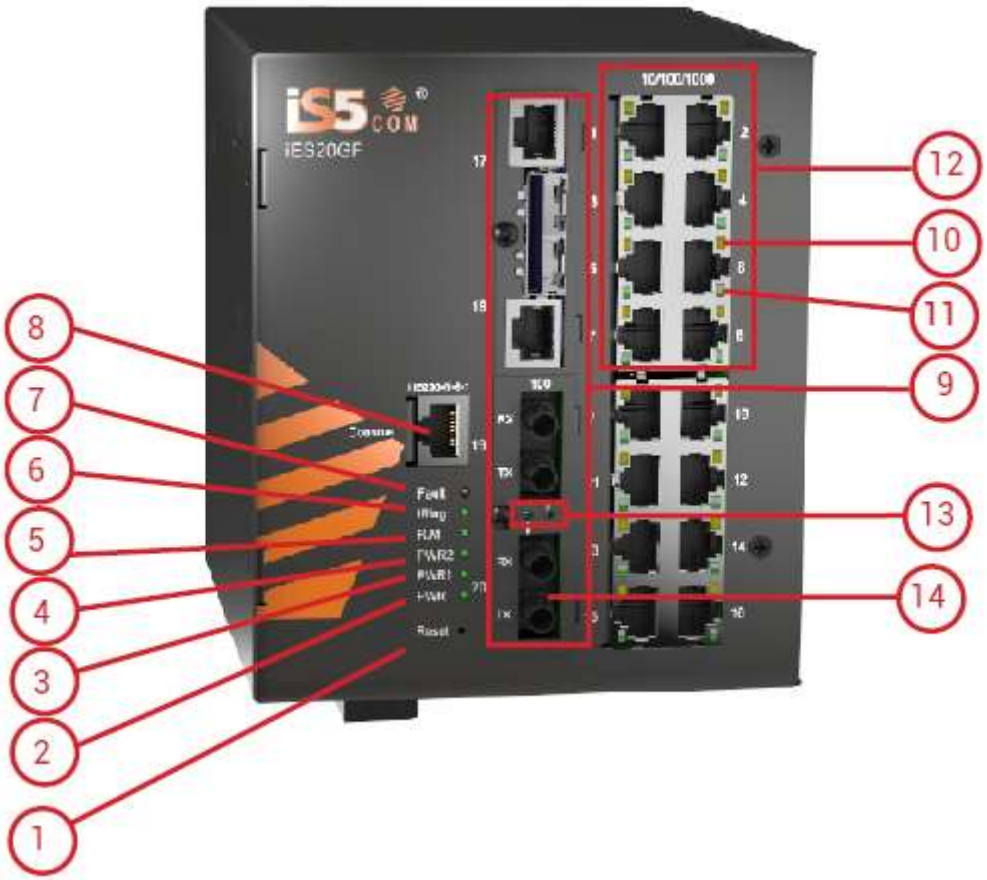
Description	Specification
10/100/1000 Base-T(X) RJ45 Ports Auto MDI/MDIX	Up to 20
Combo of 10/100/1000 Base-T(X) RJ45 and 100/1000Base-X SFP, or 10/100/1000 Base-T(X) RJ45, or 100/1000 Base-X SFP, or 100FX MM/SM SC/ST, or 1000SX MM SC/ST, 1000LX SM SC/ST ports	Up to 4
RS-232 Serial Console Port	RS-232 in RJ45 connector with console cable: 115200 bps, 8, N, 1
Warning / Monitoring System	Relay output for fault event alarming 2 alarm warning methods for system events supported: • SYSLOG with server / client structure; recording and viewing events in the System Event Log • SMTP for notification via email Event selection per port
Alarm	Relay output to carry capacity of 1 A at 24 VDC
Physical Characteristics	
Enclosure	IP-40 Galvanized Steel
Dimensions (W x D x H)	133.7 (W) x 157.5 (D) x 154.1 (H) mm (5.27 x 6.20 x 6.07 inches)
Weight (g)	~3000 g
Power	
Input Power	Redundant Power Supplies: Dual Input 10-48VDC, Dual Input 36-75VDC, or Dual Input 110-370VDC or 90-264VAC
Power Consumption (Typ.)	20 Watts
Overload Current Protection	Present
Reverse Polarity Protection	Internal

2. HARDWARE OVERVIEW

2.1 Front Panel

iS5 provides the following modules:

Description	Specification
10/100/1000 Base-T(X) RJ45 Ports	Up to 20
Combo of 10/100/1000 Base-T(X) RJ45 and 100/1000Base-X SFP, or 10/100/1000 Base-T(X) RJ45, or 100/1000 Base-X SFP, or 100FX MM/SM SC/ST, or 1000SX MM SC/ST, 1000LX SM SC/ST ports	Up to 4
RS-232 Serial Console Port	RS-232 with RJ45 connector with console cable: 115200 bps, 8, N, 1



1 Reset button. Push the button 3 seconds for reset; 5 seconds for factory default.
2 LED for PWR. When the PWR UP, the green led will be light on
3 LED for PWR1
4 LED for PWR2
5 LED for R.M (Ring master). When the LED light on, it means that the switch is the ring master of Ring. LED for Ring. When the led light on, it means the Ring is activated.
6 LED for Ring. When the led light on, it means the iRing is activated.
7 LED for Fault. When the light on, it means Power failure or Port down/fail.
8 Console port (RJ-45)
9 100/1000Base-X SC/ST/LC or 100/1000 Base-X SFPs

10 LED for Ethernet ports link status.
11 LED for Ethernet ports speed status
12 10/100/1000Base-T(X) ports
13 LED for SC/ST/LC or SFP ports link status
14 100/1000Base-X SC/ST/LC or 100/1000 Base-X SFP

2.2 Front Panel LED

LED	Color	Status	Description
PWR	Green	On	DC power module up
PW1	Green	On	DC power module 1 activated.
PW2	Green	On	DC Power module 2 activated.
R.M	Green	On	Ring Master.
Ring	Green	On	Ring enabled.
		Slowly blinking	Ring has only One link. (lack of one link to build the ring.)
		Fast blinking	Ring work normally.
Fault	Amber	On	Fault relay. Power failure or Port down/fail.
10/100/1000Base-T(X) Fast Ethernet ports			
LNK	Green	On	Port link up.
ACT	Green	Blinking	Data transmitted.
Full Duplex	Amber	On	Port works under full duplex.
SFP			
LNK	Green	On	Port link up.
ACT	Green	On	Data transmitted.

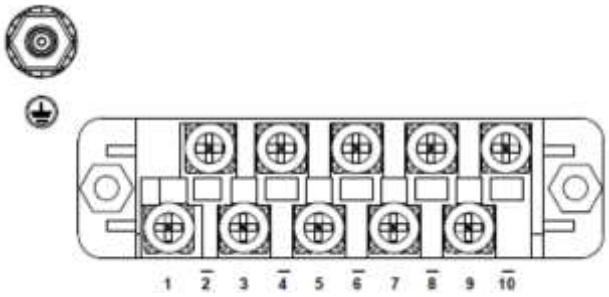
2.3 Bottom View of Panel

The Phillips Screw Terminal Block, located on the bottom of the unit, has Phillips screws with compression plates, allowing either bare wire connections or crimped terminal lugs. The use of #6 size ring lugs is recommended to ensure secure and reliable connections under severe shock or vibration. The terminal block comes with a safety cover which must be removed before connecting any wires. This cover must be re-attached after wiring to ensure personnel safety.

The iES10G series supports dual redundant power supplies (PWR1 and PWR2). There are 3 options:

- LV: Dual Input 10-48VDC
- MV: Dual Input 36-75VDC
- HV: Single Input 110-370VDC or 90-264VAC

There are also connections for the Failsafe Relay. The Failsafe Relay is rated 1A @ 24VDC. Connections to the Terminal block are listed in the table below.



Terminal Number	Description	Connection
1	PWR1 (L) – Live	Connect to the (Live) of DC power supply 1 or (Live) terminal of an AC power source.
2	PWR1 (G) – Ground	DC Power supply 1 ground connection or AC power round connection.
3	PWR1 (N) – Neutral	Connect to the Neutral of the DC power supply 1 or (Neutral) terminal of an AC power source.
4	G – Chassis Ground	Connected to the ground bus for DC inputs or Safety Ground terminal for AC Units. Chassis Ground connects to both power supply surge grounds via a removable jumper.
5	PWR2 (L) – Live	Connect to the (Live) terminal of Power supply 2 or backup DC power source.
6	PWR2 (G) – Ground	Power supply 2 or backup DC power source ground connection.
7	PWR2 (N) – Neutral	Connect to the (Neutral) terminal of Power supply 2 the second or backup DC power source.
8	RLY NO	Failsafe Relay, (Normally Open) contact.
9	RLY CM	Failsafe Relay (Common) contact.
10	RLY NC	Failsafe Relay (Normally Closed) contact.

Chassis Ground Connection

The iES20GF chassis ground connection, located next to the terminal block, uses a #6-32 Screw. We recommend terminating the ground connection using a #6 ring lug, and a torque setting of 15 in.lbs (1.7Nm).

- *100-240VAC rated equipment: A 250VAC appropriately rated circuit breaker must be installed.*
- *Equipment must be installed according to the applicable country wiring codes.*
- *When equipped with a HI voltage power supply and DC backup,*

- *120-370VDC rated equipment: A 370VDC appropriately rated circuit breaker must be installed.*
- *A circuit breaker is not required for DC power supply voltages of 10-48VDC.*
- *For Dual DC power supplies, separate circuit breakers must be installed and separately identified.*
- *Equipment must be installed according to the applicable country wiring*

2.4 Rear Panel

The components on the rear of the iES20GF are shown below:

1. Screw holes (4) for wall mount kit.
2. DIN-Rail mount

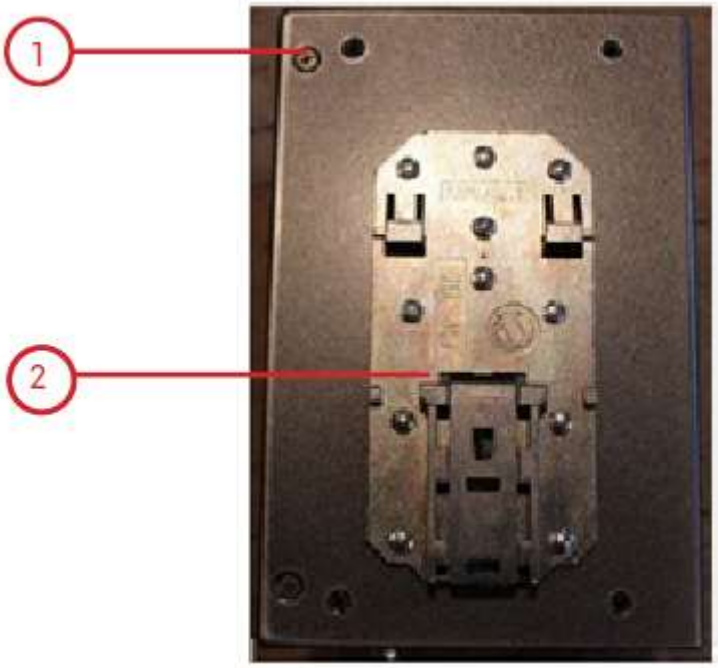


Figure 1 – Rear Panel

2.5 Side Panel

The components on the side of the iES10G are shown below:

1. Screw holes (4) for wall mount kit.

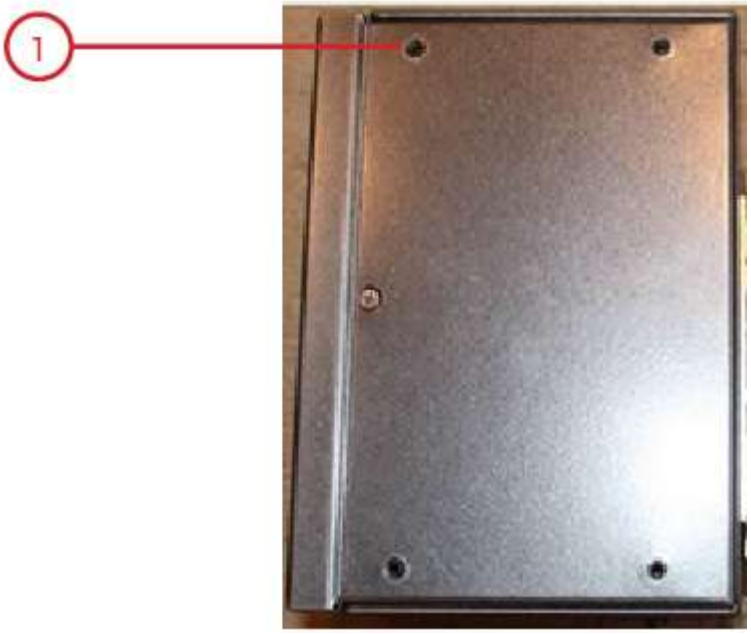


Figure 2 – Side Panel

3. HARDWARE INSTALLATION

3.1 Installing the Switch on DIN-Rail

Every switch has a DIN-Rail bracket on the rear panel. The DIN-Rail bracket helps secure the switch on to the DIN-Rail.

3.1.1 Mounting on DIN-Rail

Step 1: Slant the switch and hook the top 2 catches of the metal bracket onto the top of the DIN-Rail.

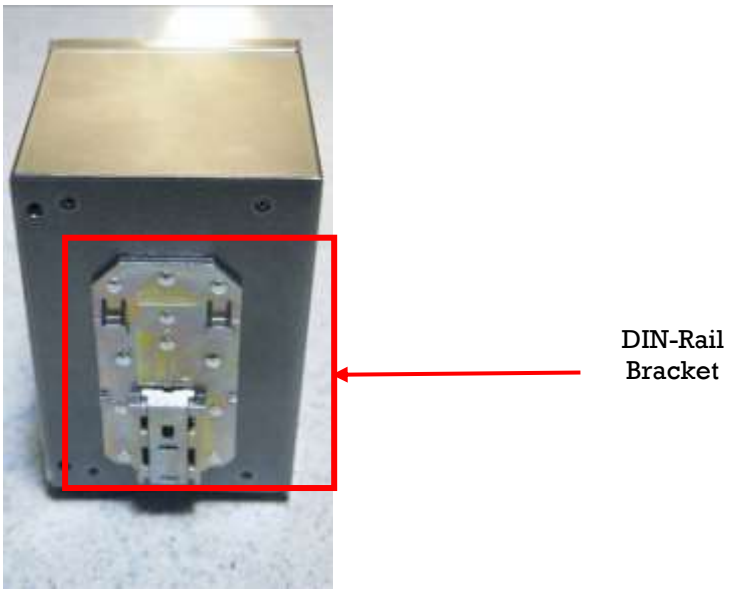


Figure 3 - DIN-Rail Bracket

Step 2: Push the bottom of the switch toward the DIN-Rail until the bracket snaps in place.

Figure 4 - Switch Mounted on DIN-Rail

3.2 Wall Mount Installation

The switch can also be panel or wall mounted. The following steps show how to mount the switch on a panel or wall.

3.2.1 Mounting iES20GF on a Wall or Panel

Option 1: Side of switch

Fix mounting brackets to the side of switch using the 4 screws included in the package.

Figure 5 - Brackets Mounted on Side of Switch

Option 2: back of switch:

Fix mounting brackets to back of switch using 4 screws included in the package.

Figure 6 - Brackets Mounted on back of Switch

Note: To avoid damage to the unit, only use the screws provided to mount the panel mount.

3.3 Connection

3.3.1 Ethernet Cables

The iES20GF switches have standard Ethernet ports. According to the link type, the switches use CAT 3, 4, 5, and 5e UTP cables to connect to any other network device (e.g. PCs, servers, switches, routers, or hubs). For cable types and specifications, refer to the following table.

Table 1 – Port Numbering

Cable	Type	Max. Length	Connector
10BASE-T	Cat. 3, 4, 5 100-ohm	UTP 100 m (328ft)	RJ-45
100BASE-TX	Cat. 5 100-ohm UTP	UTP 100 m (328ft)	RJ-45
1000BASE-T	Cat. 5/Cat. 5e 100-ohm UTP	UTP 100 m (328ft)	RJ-45

3.3.2 Pin Assignments

With 10/100/1000BASE-T(X) cables, pins 1 and 2 are used for transmitting data, and pins 3 and 6 are used for receiving data. All pin assignments are as follows:

Table 2 – 10/100 Base-T(X) Line Pin Assignments

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

Table 3 – 1000 Base-T Line Pin Assignments

Pin Number	Assignment
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-

The iES20GF supports Auto MDI/MDI- X operation. Use a cable to connect the switch to a PC.

Table 4 – 10/100 Base-T(X) MDI/MDI- X Pin Assignments

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

Table 5 – 1000 Base-T MDI/MDI- X Pin Assignments

Pin Number	MDI port	MDI-X port
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

Note: "+" and "-" signs represent the polarity of the wires that make up each wire pair.

3.3.3 SFP

The switches come with fiber optical ports that can connect to other devices using SFP modules. The fiber optical ports are multimode or singlemode with LC connectors. Remember that the TX port of Switch A should be connected to the RX port of Switch B.

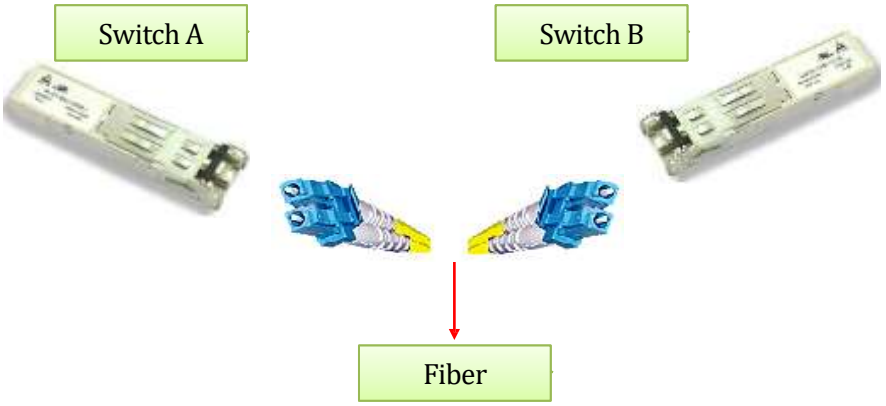


Figure 7 – SFPs

3.4 Console Cable

The switches can be managed via the console port (a RS-232 Serial interface) by a RS-232 cable supplied with the switch. Connect the port to a PC using the RS-232 cable with an RJ-45 connector to a DB-9 female connector. The DB-9 female connector of the RS-232 cable should be connected to the PC, while the other end of the cable (with the RJ-45 connector) should be connected to the console port of the switch (Standard Cisco Serial Cable supplied with iRBX6GF).

Table 6 – Signals and Pinouts from Console Port RJ-45 to DB-9 Serial Port Adapter

Console Port		**PC COM Port**	
RJ-45		**DB-9**	
Pins	**Signals**	**Pins**	**Signals**
1	NC[1]	—	—
2	NC[1]	—	—
3	TXD[2]	2	RXD[3]
4	GND[4]	5	GND[4]
5	GND[4]	5	GND[4]
6	RXD[3]	3	TXD[2]
7	NC[1]	—	—
8	NC[1]	—	—

1. NC indicates not connected.
2. TXD indicates transmit data
3. RXD indicates receive data
4. GND indicates ground

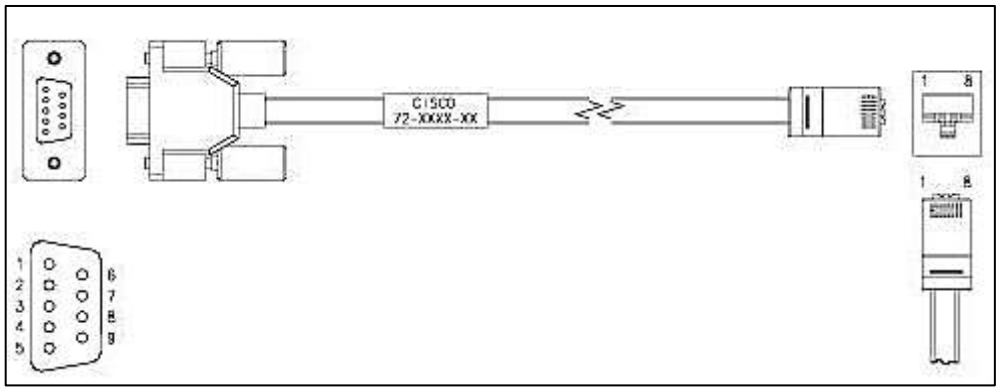


Figure 8 – Console Cable Connection

4. REDUNDANCY OVERVIEW

Using redundancy for minimizing system downtime is one of the most important concerns for industrial networking devices. The existing redundancy technologies widely used in commercial applications are STP, RSTP, and MSTP.

4.1 STP/RSTP/MSTP

4.1.1 STP/RSTP

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 when two or more paths run to the same destination, broadcast packets could get in to an infinite loop and cause 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.

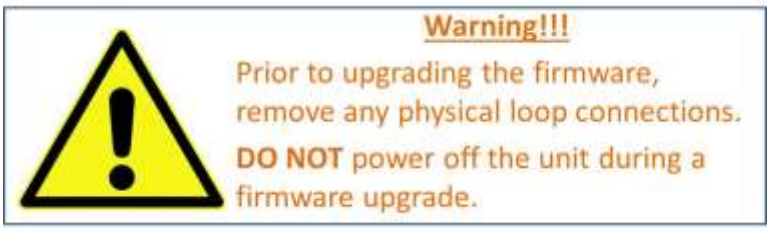
4.1.2 MSTP

MSTP was developed to improve recovery times since STP and RSTP takes seconds, which is not acceptable in some industrial applications. MSTP supports multiple spanning trees within a network by grouping and mapping multiple VLAN's into different spanning-tree instances, known as Multiple Spanning Tree Instances (MSTI)'s, forming individual MST regions. Each switch is assigned an MST region. Each MST region consists of one or more MSTP switches with the same VLAN's, at least one MST instance, and the same MST region name. This allows the switches to use different paths in the network to effectively balance loads.

4.2 Fast Recovery

Fast recovery mode can be set to connect multiple ports to one or more switches. iES20GF with fast recovery modes will provide redundant links. Only the first priority will be the active port, the other ports with different priorities will be backup ports.

5. Web Management



This section introduces configuration of the switch by a web browser.

An embedded HTML web site resides in the flash memory of the CPU board. It contains advanced management features that allow the user to manage the iRBX6GF switch from anywhere on the network via a standard web browser such as Microsoft Internet Explorer.

The Web Management function supports Internet Explorer 5.0 or later. It is based on Java Applets with an aim at reducing network bandwidth consumption and enhances access speed in a viewing screen.

Note: By default, IE 5.0 or later versions do not allow Java Applets to open sockets. The browser settings need to be explicitly modified to enable Java Applets to be used on network ports.

The default values are as below:

- **IP Address:** *192.168.10.1*
- **Subnet Mask:** *255.255.255.0*
- **Default Gateway:** *192.168.10.254*
- **User Name:** *admin*
- **Password:** *admin*

To login, perform the following:

1. Launch Internet Explorer.
2. Type http:// and the switch's IP address (default is 192.168.10.1), and then press **Enter**.

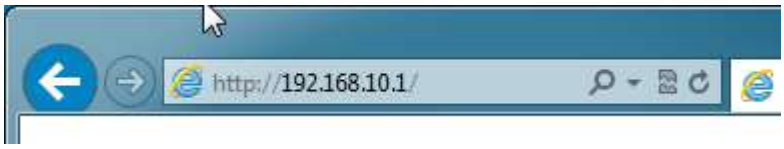


Figure 9 – Switch's IP Address Screen

3. The **Welcome to ….** screen appears. Click GET STARTED
4. The login screen appears (see Figure 10 – Login Screen).

Figure 10 – Login Screen

5. Enter the username and password. The default username and password are "admin".

6. Click **OK**. The main interface of the Web Management appears (see Figure 11).

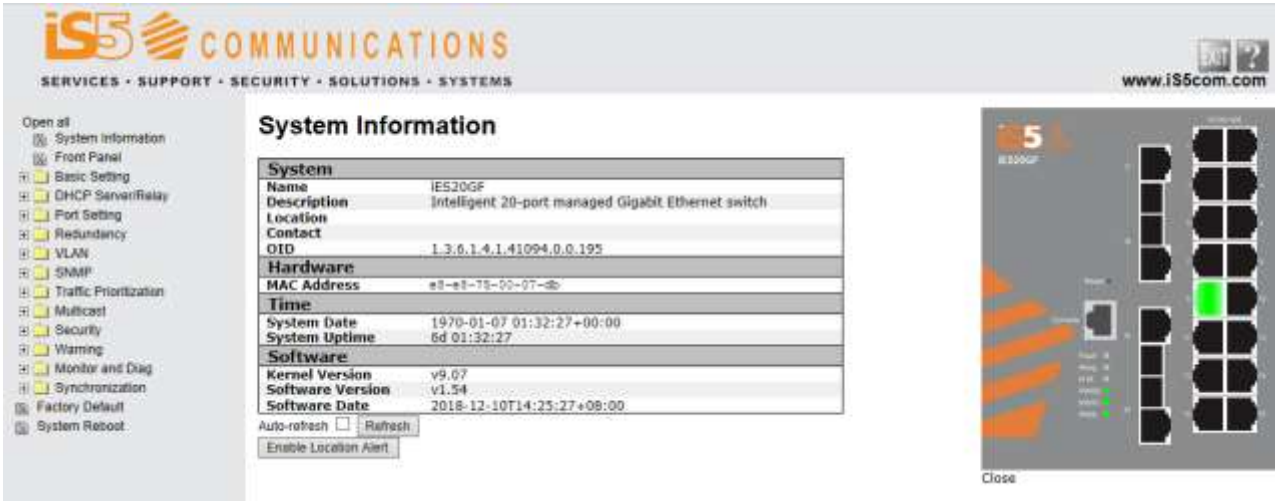


Figure 11 – Main Interface or System Information tab

Note: Session timeout is 10 minutes.

On the left hand side, links to various settings are shown. Use them to access the different features of the switch.

5.1 Basic Setting

5.1.1 Basic Setting (System Information Configuration)

This page allows the programming of the system information of the switch.

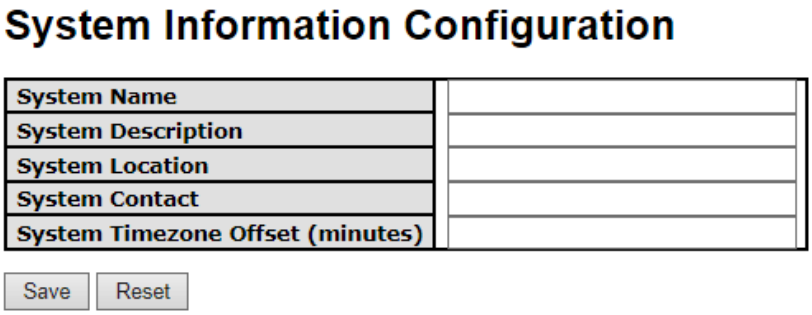


Figure 12 – System Information Configuration

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.
System Time zone offset (minutes)	Provides the time-zone offset from UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.2 Banner

This page allows the user to configure the System Login Banner Title and System Banner Message. The Banner appears when you are trying to access the device through WebUI or CLI.

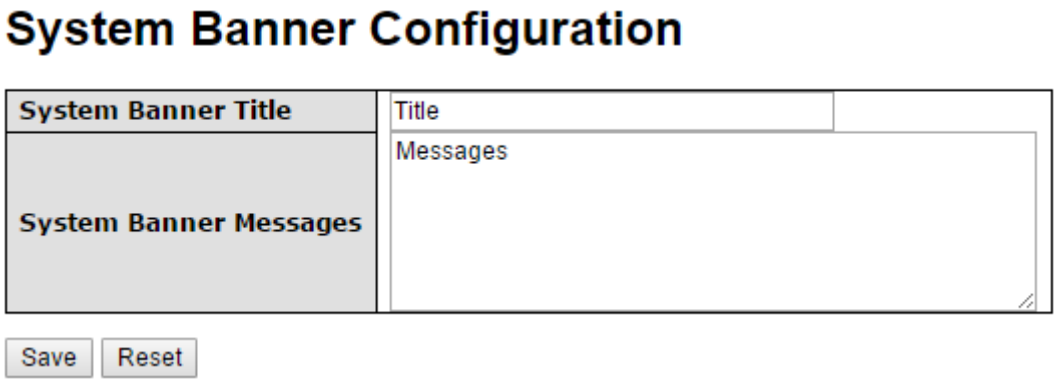


Figure 13 – System Banner Configuration

Label	Description
System Banner Title	The title of the Login Banner. Note: restricted to 0 – 64 characters
System Banner Message	The content of the Login Banner Message. Note: restricted to 0 – 512 characters
Save	Click to save changes.
Reset	Click to reset changes.

5.1.3 Admin Password

This page allows the user to configure the system admin password required to access the web interface or log in to the CLI.

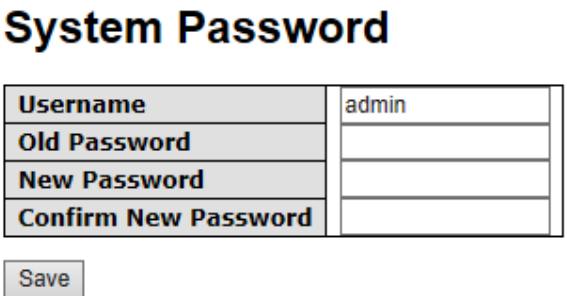


Figure 14 - System Password

Label	Description
Username	It shows the username entered.
Old Password	The existing password. If it is incorrect, a new password can't be set.
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 New Password	Re-type the new password.
Save	Click to save changes.

5.1.4 Guest Password

This page allows the user to configure the system guest password required to access the web interface or the CLI.

Figure 15 – Guest Password Configuration

Label	Description
Guest name	The guest name should be used. Default guest name is *guest.*
Old Password	The existing password. If this is incorrect, you cannot set the new password. Default guest password is *guest*
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 New Password	Re-type the new password.
Save	Click to save changes.

5.1.5 Authentication Method

Configure how a user is authenticated when he/she logs into the switch via one of the management interfaces.

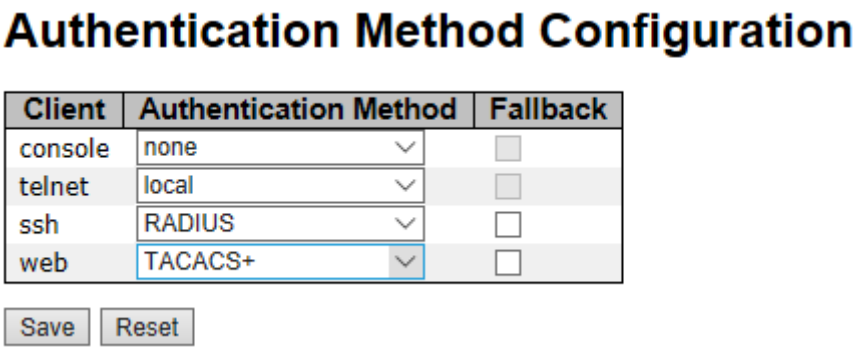


Figure 16 - Authentication Method Configuration

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 **(Remote Authentication Dial-In User Service)** server is used for authentication. **TACACS+**: Terminal Access Controller Access Control System (TACACS) can be used for authentication.
Fallback	Enable fallback to local authentication by checking this box. If none of the configured authentication servers is alive, the local user database is used for authentication. This is available only if the 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

5.1.6 Auto Logout

The Auto logout time for WebUI and CLI access can be defined by an user.

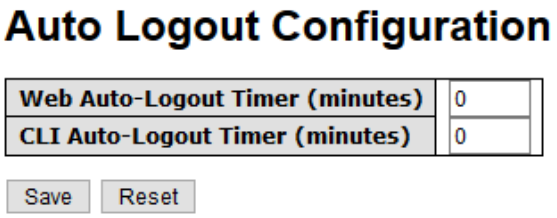


Figure 17 - Auto Logout Configuration

Label	Description
Web Auto-Logout Timer (minutes)	Define the auto logout time for WebUI access Note: value 0-9999 min ; Default: 0 which means 10 min.
CLI Auto-Logout Timer (minutes)	Define the auto logout time for CLI access Note: value 0-9999 min ; Default: 0 which means 10 min.

5.1.7 IP Setting

You can configure IP information of the switch in this page.

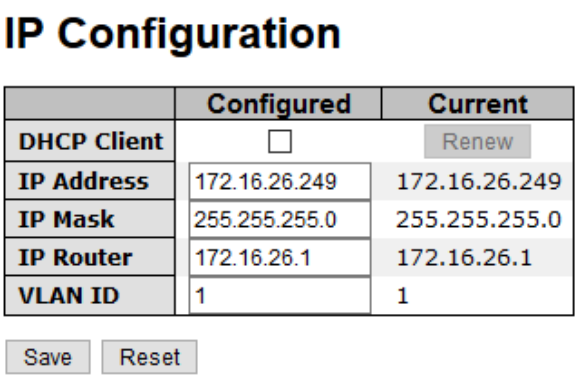


Figure 18 - IP Configuration

Configure the switch-managed IP information on this page.

The **Configured** column is used to view or change the IP configuration.
The **Current** column is used to show the active IP configuration.

Label	Description
DHCP Client	Enable the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP server does not respond around 35 seconds and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
IP Address	Assigns the IP address of the network in use. If DHCP client function is enabled, there is no need to assign the IP address. The network DHCP server will assign the IP address to the switch and it will be displayed in this column. The default IP is 192.168.10.1.
IP Mask	Provide the IP mask of this switch dotted decimal notation.
IP Router	Provide the IP address of the router in dotted decimal notation.
VLAN ID	Provide the managed VLAN ID. The allowed range is `1` to `4095`.
Renew	Click to renew DHCP. This button is only available if DHCP is enabled.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.8 IPv6 Setting

Configure the switch-managed IPv6 information on this page.

The **Configured** column is used to view or change the IP configuration.
The **Current** column is used to show the active IP configuration.

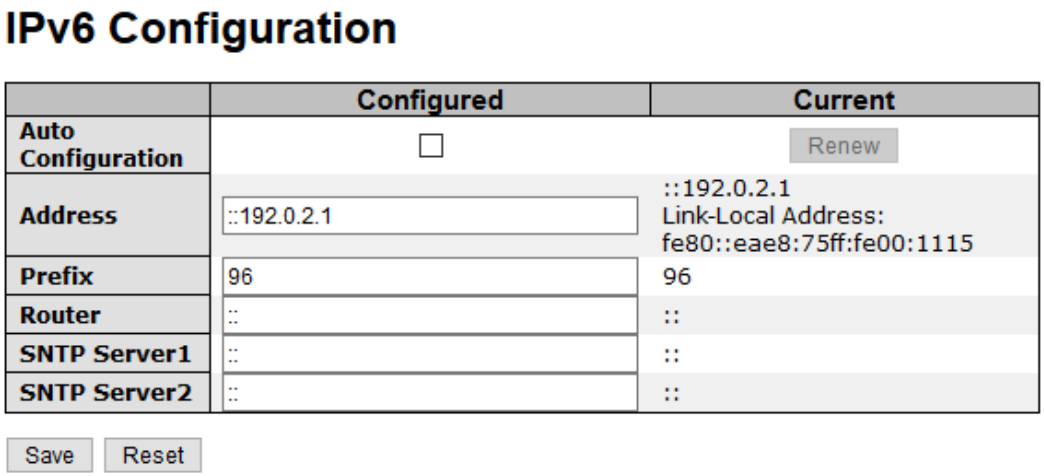


Figure 19 – IPv6 Configuration

Label	Description
Auto Configuration	Enable IPv6 auto-configuration by checking this box. If 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, the total time needed to complete auto-configuration can be significantly longer.

Label	Description
Address	Provide the IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
Prefix	Provide the IPv6 Prefix of this switch. The allowed range is 1 to 128.
Router	Provide the IPv6 gateway address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. . For example, '::192.1.2.34'..
SNTP Server	Provide the IPv6 SNTP Server address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. . For example, '::192.1.2.34'.
Renew	Click to renew IPv6 AUTOCONF. This button is only available if IPv6 AUTOCONF is enabled.
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values

5.1.9 SNTP Configuration (only for SNTP Version)

Configure SNTP on this page.

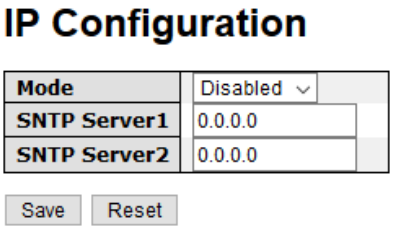


Figure 20 - SNTP Configuration

Label	Description
Mode	Indicates the selected Simple Network Time Protocol (SNTP) mode. The modes include: **Enabled**: Enable SNTP client mode operation. **Disabled**: Disable SNTP client mode operation.
Server Address	Provide the IPv4 address of a SNTP server.
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values

5.1.10 NTP Configuration (only for NTP Version)

Configure NTP on this page.

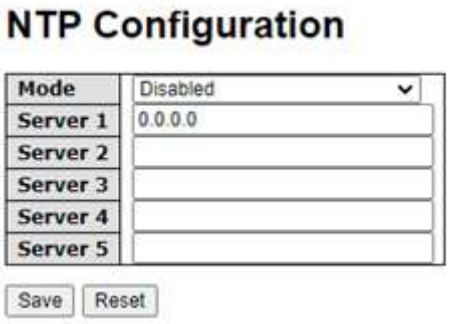


Figure 21 - NTP Configuration

Label	Description
Mode	Indicates the selected Network Time Protocol (NTP) mode. The modes include: **Enabled**: Enable NTP client mode operation. **Disabled**: Disable NTP client mode operation.
Server Address	Provide the IPv4 address of a NTP server. There 2 cells so a dual NTP server or active / active model is supported.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.11 Daylight Saving Time

This page allows the user to configure the Time Zone.

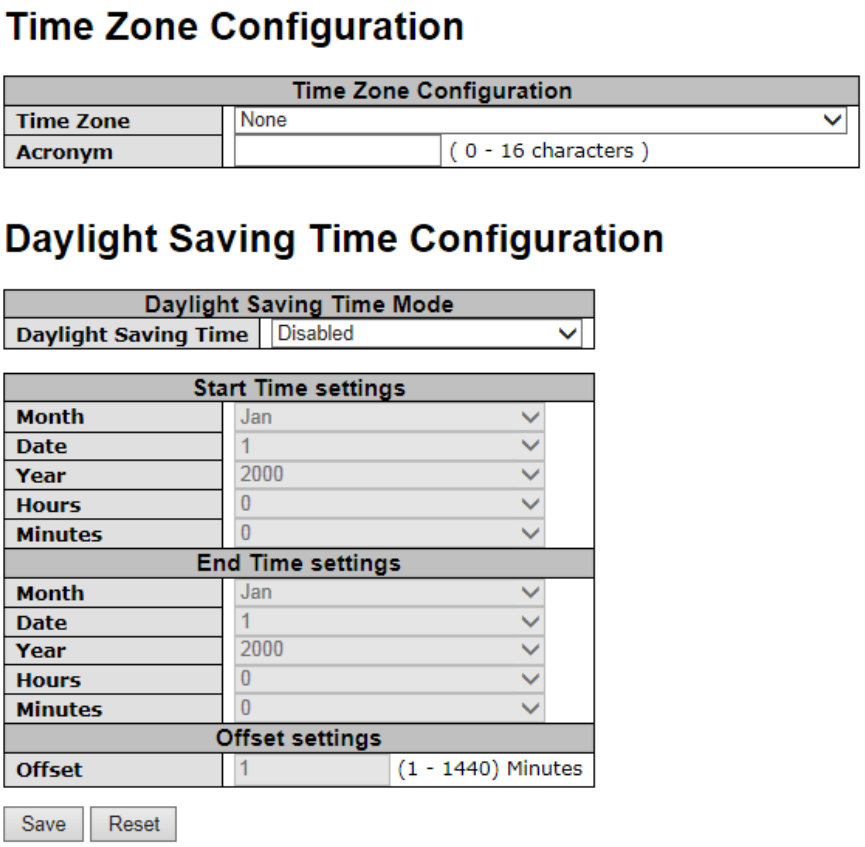


Figure 22 - Time Zone Configuration

Label	Description
Time Zone Configuration	Lists various time zones worldwide. Select appropriate **Time Zone** from the drop down and click **Save** to set.
Time Zone Acronym	The user can set the acronym of the time zone. This is a user configurable acronym to identify the time zone. Range : Up to 16 alpha-numeric characters and can contain '-', '_' or '.'
Daylight Savings Time Mode	This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Options include: **Disable:** to disable the Daylight Saving Time configuration. (Default) **Recurring:** The Daylight Saving Time duration configuration will be repeated every year. **Non-Recurring:** The Daylight Saving Time duration configuration will be for used once.
Recurring Configurations	
Start Time Settings	• **Week** - Select the starting week number. (Recurring) • **Day** - Select the starting day. (Recurring) • **Month** - Select the starting month. • **Date** - Select the starting date. (Non-Recurring) • **Year** - Select the starting year. (Non-Recurring) • **Hours** - Select the starting hour. • **Minutes** - Select the starting minute.

Label	Description
End Time Settings	• **Week** - Select the ending week number. (Recurring) • **Day** - Select the ending day. (Recurring) • **Month** - Select the ending month. • **Date** - Select the ending date. (Non-Recurring) • **Year** - Select the ending year. (Non-Recurring) • **Hours** - Select the ending hour.
Offset Settings	Enter the number of minutes to be added during Daylight Saving Time. Range: 1 to 1440
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values

5.1.12 Switch Time Configuration

Configure date and time on this page.

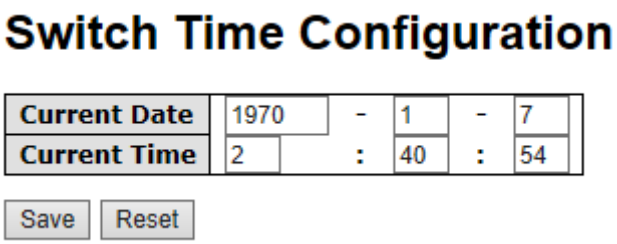


Figure 23 – Switch Time Configuration

Mode	Description
Current Date	Modify **Current Date** in the following order: Year – Month - Day
Current Time	Modify **Current Time** in the following order: Hour : Minutes : Seconds
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previous saved values

5.1.13 HTTPS

HTTPS (HTTP over SSL or HTTP Secure) is the use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sublayer under regular HTTP application layering. HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the web server.

Configure HTTPS settings in the following page.

Figure 24 - HTTPS Configuration

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

5.1.14 SSH

Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line login and remote command execution, but any network service can be secured with SSH.

Configure SSH settings in the following page.

Figure 25 - SSH Configuration

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.

5.1.15 Telnet

This page allows the user to enable or disable Telnet settings.

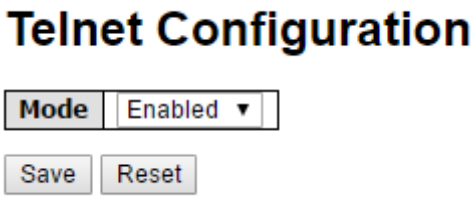


Figure 26 - Telnet Configuration

Label	Description
Mode	Indicates the selected Telnet mode. The modes include: **Enabled**: enable telnet. **Disabled**: disable Telnet.

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

5.1.16 LLDP

5.1.16.1 LLDP Configurations

Link Layer Discovery Protocol (LLDP) is a vendor independent link layer or neighbor discovery protocol used by network devices for advertising their identity and capabilities to neighbors on a LAN segment. Enable LLDP globally to standardize network topology across all devices if you have a multi-vendor network.

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

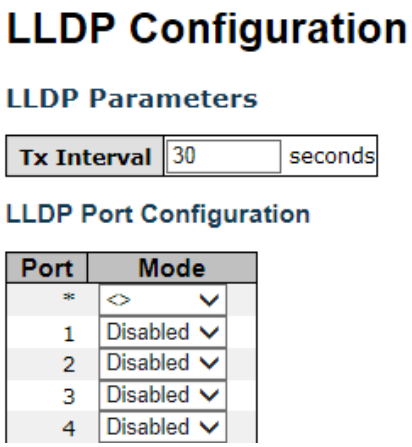


Figure 27 - LLDP Configuration

Label	Description
LLDP Parameters	
Tx Interval	The switch periodically transmits LLDP frames to its neighbours for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds.
LLDP Port Configuration	
Port	The switch port number of the logical LLDP port.
Mode	Select LLDP mode. By default, LLDP is Enabled. **Disabled** The switch will not send out LLDP information, and will drop LLDP information received from neighbours. **Enabled** The switch will send out LLDP information, and will analyze LLDP information received from neighbours.

5.1.16.2 LLDP Neighbour Information

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

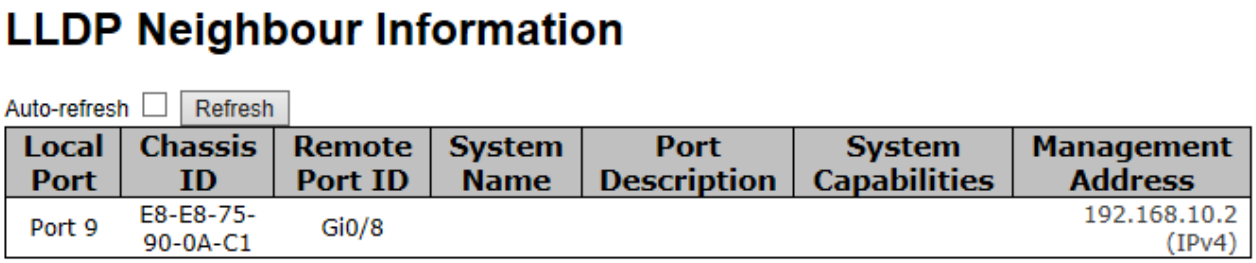


Figure 28 - LLDP Neighbor Information

Label	Description
Local Port	The port on which the LLDP frame was received.
Chassis ID	The **Chassis ID** is the identification of the neighbour's LLDP frames.
Remote Port ID	The **Remote Port ID** is the identification of the neighbour 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	**Management Address** is the neighbour unit's address that is used for higher layer entities to assist discovery by the network management. For instance, this could hold the neighbour's IP address.
Refresh	Click to refresh the page immediately
Auto-refresh	Check to enable an automatic refresh. Automatic refresh occurs every 3 seconds.

5.1.16.3 Port Statistics

This page provides an overview of all LLDP traffic.

Two types of counters are shown. **Global Counters** are counters that refer to the whole switch, while **Local Counters** refer to per port counters for the currently selected switch.

Auto-refresh ☐ Refresh Clear

LLDP Global Counters

Global Counters	
Neighbour entries were last changed	1970-01-06 23:39:01+00:00 (11707 secs. ago)
Total Neighbours Entries Added	5
Total Neighbours Entries Deleted	4
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0
9	518	516	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0
11	143	140	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	275	149	0	0	0	0	156	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0

Figure 29 - LLDP Global Counters

5.1.16.3.1 Global Counters

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

5.1.16.3.2 Local Counters

Label	Description
Local Port	The port on which LLDP frames are received or transmitted.
Tx Frames	The number of LLDP frames transmitted on the port
Rx Frames	The number of LLDP frames received on the port

Label	Description
Rx Errors	The number of received LLDP frames containing errors
Frames Discarded	If a LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given port's link is down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLV (Type Length Value). If a TLV is malformed, it will be counted and discarded.
TLVs	The number of well-formed TLVs but with an unknown type value
Org. Discarded	The number of received organizationally TLVs
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 this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

5.1.17 Modbus TCP

This page shows Modbus TCP support of the switch. (For more information regarding Modbus, refer to http://www.modbus.org/).

Figure 30 - MODBUS Configuration

Label	Description
Mode	Disable or enable Modbus function.
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values.

Note: For Modbus commands, see .AppendixA

5.1.18 Backup

This page allows the user to save/view switch configurations.

The configuration file is in XML format with a hierarchy of tags:

Header tags: `<?xml version="1.0"?>` and `<configuration>`. These tags are mandatory and must be present at the beginning of the file.

Section tags: `<platform>`, `<global>` and `<switch>`. The platform section must be the first section tag

and this section must include the correct platform ID and version. The global section is optional and includes configuration which is not related to specific switch ports. The switch section is optional and includes configuration which is related to specific switch ports.

Module tags: `<ip>`, `<mac>`, `<port>` etc. These tags identify a module controlling specific parts of the configuration.

Group tags: `<port_table>`, `<vlan_table>` etc. These tags identify a group of parameters, typically a table.

Parameter tags: `<mode>`, `<entry>` etc. These tags identify parameters for the specific section, module and group. The `<entry>` tag is used for table entries.

Configuration parameters are represented as attribute values. When saving the configuration from the switch, the entire configuration including syntax descriptions is included in the file. The file may then be modified using an editor and loaded to a switch.

The example below shows a small configuration file only including configuration of the MAC address age time and the learning mode per port. When loading this file, only the included parameters will be changed. This means that the age time will be set to 200 and the learn mode will be set to automatic.

```
<?xml version="1.0"?>
<configuration>
  <platform>
    <pid val="3"></pid>
    <version val="1"></version>
  </platform>
  <global>
    <mac>
      <age val="200"></age>>
    </mac>
  </global>
  <switch sid="1">
    <mac>
      <entry port="1-24" learn_mode="auto"></entry>
    </mac>
  </switch>
</configuration>
```

Save Configuration—click to save the configuration file.

Figure 31 – Configuration Save

5.1.19 Restore

This page allows the user to load a previously saved configuration to the switch.

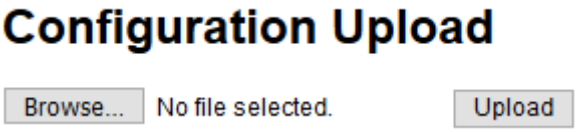


Figure 32 – Configuration Upload

5.1.20 Firmware Update

This page allows the user to update the firmware of the switch. Select the file to be load then press upload. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

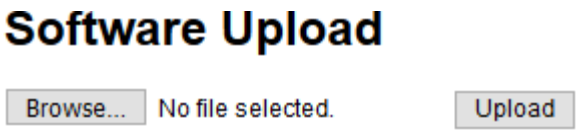


Figure 33 – Software Upload

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

5.2 DHCP Server/Relay

The switch provides dynamic host configuration protocol (DHCP) server functions. By enabling DHCP, the switch will become a DHCP server. A DHCP server automatically assigns an IP address, subnet mask, domain name server (DNS) address and other pertinent configuration parameters to DHCP client. A DHCP client is the endpoint that receives configuration information from a DHCP server.

5.2.1 Setting

Enable DHCP in this page.

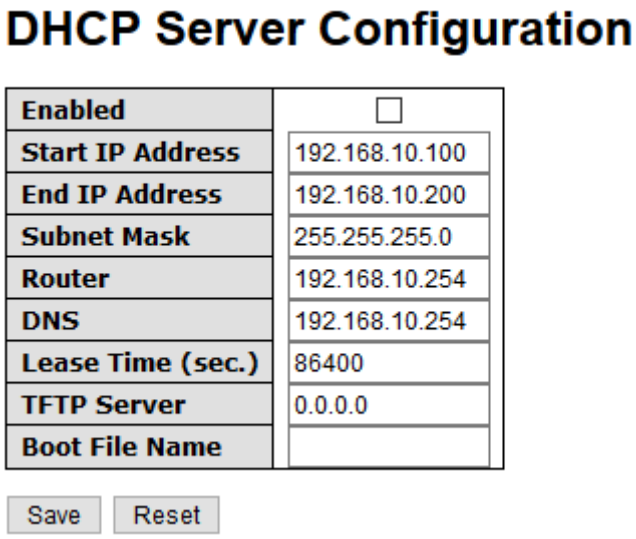


Figure 34 – DHCP Server Configuration

Label	Description
Enabled	Enable/Disable DHCP server.
Start IP Address	The first IP address of IP pool.
End IP Address	The Last IP address of IP pool.
Subnet Mask	The subnet mask.
Router	The IP address of the 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 Boot File (Option 67).
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.2 DHCP Dynamic Client List

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

Figure 35 – DHCP Dynamic Client List

Label	Description
Type	The type of client (Dynamic or Static).
MAC Address	The MAC Address of client.
IP Address	The IP address of client.
Surplus Lease	The surplus Lease time.
Select/Clear All	Select or Clear all check boxes.
Add to Static Table	Add dynamic entry to static table.

5.2.3 DHCP Static Client List

DHCP server can automatically assign an IP address to DHCP client.

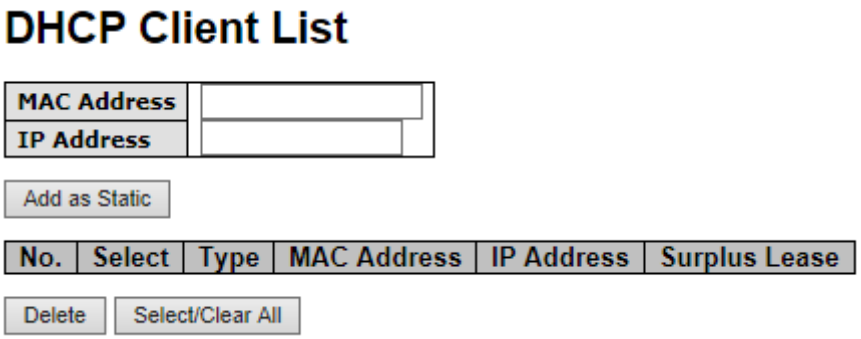


Figure 36 – DHCP Static Client List

Label	Description
MAC Address	The MAC Address of client.
IP Address	The IP address of client
Surplus Lease	The surplus Lease time. The length of time for which a DHCP client holds the IP address information. When a lease expires, the client must renew it
Add as Static	Add dynamic entry to static table.
Type	The type of client (Dynamic or Static).
Delete	Delete selected entry.
Select/Clear All	Select or Clear all check boxes.

5.2.4 DHCP Relay Agent

Configure DHCP Relay on this page..

5.2.4.1 Relay

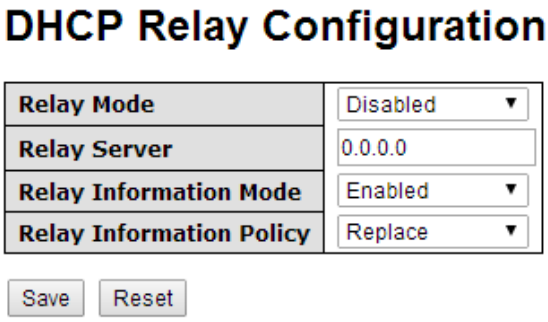


Figure 37 – DHCP Relay Configuration

Label	Description
Relay Mode	Indicates the existing DHCP relay mode. The modes include: **Enabled**: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations. **Disabled**: Disable DHCP relay mode operation
Relay Server	Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and transfer DHCP messages between the client and the server when they are not in the same subnet domain.
Relay Information Mode	Indicates the existing DHCP relay information mode. The format of DHCP option 82 circuit ID format is "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, 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. The mode include: **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. It only works when the DHCP relay mode is enabled. **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. The policy includes: **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.
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values.

5.2.4.2 Relay Statistics

This page provides statistics for DHCP relay.

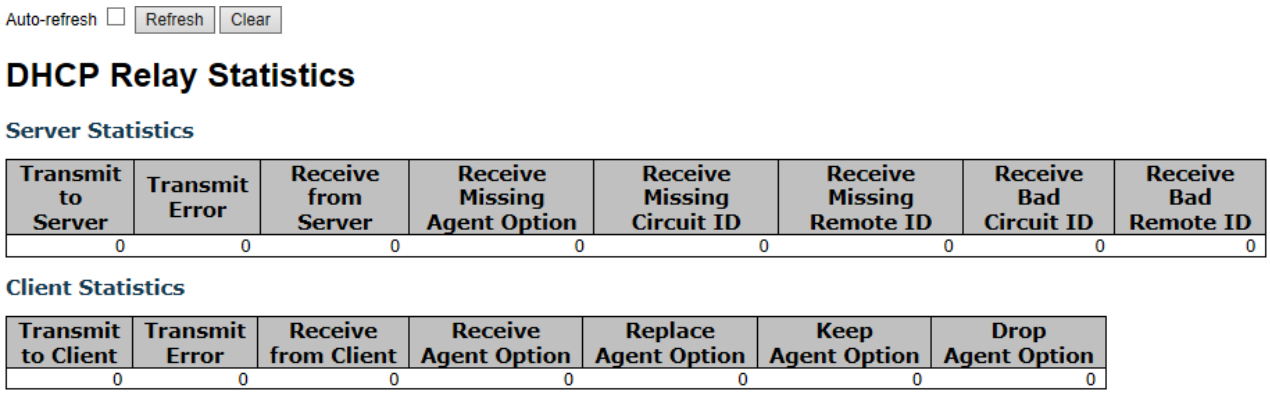


Figure 38 – DHCP Relay Statistics

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

Client Statistics

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 with relay agent information option.
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.
Auto-refresh :	Auto-refresh Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page immediately.
Clear	Clear all statistics.

5.3 Port Setting

Port Setting allows managing of 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.

Port Configuration

Refresh

Port	Link	Speed		Flow Control			Maximum Frame Size	Power Control
		Current	Configured	Current Rx	Current Tx	Configured		
*			<>			☐	9600	<>
1		Down	Auto	✗	✗	☐	9600	Disabled
2		Down	Auto	✗	✗	☐	9600	Disabled
3		Down	Auto	✗	✗	☐	9600	Disabled
4		Down	Auto	✗	✗	☐	9600	Disabled
5		Down	Auto	✗	✗	☐	9600	Disabled
6		Down	Auto	✗	✗	☐	9600	Disabled
7		Down	Auto	✗	✗	☐	9600	Disabled
8		Down	Auto	✗	✗	☐	9600	Disabled
9		1Gfdx	Auto	✗	✗	☐	9600	Disabled
10		Down	Auto	✗	✗	☐	9600	Disabled
11		Down	Auto	✗	✗	☐	9600	Disabled
12		Down	Auto	✗	✗	☐	9600	Disabled
13		Down	Auto	✗	✗	☐	9600	Disabled
14		Down	Auto	✗	✗	☐	9600	Disabled
15		Down	Auto	✗	✗	☐	9600	Disabled
16		Down	Auto	✗	✗	☐	9600	Disabled
17		Down	1000-X_AMS	✗	✗	☐	9600	Disabled
18		Down	1000-X_AMS	✗	✗	☐	9600	Disabled
19		Down	1000-X_AMS	✗	✗	☐	9600	Disabled
20		Down	1000-X_AMS	✗	✗	☐	9600	Disabled

Save Reset

Figure 39 – Port Configuration

Label	Description
Port	This is the logical port number for this row.
Link	The current link state is shown by different colors. Green indicates the link is up, and red means that it is down.
Current Link Speed	Indicates the current link speed of the port
Configured Link Speed	Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are: **Disabled**—disables the switch port operation. **Auto**—port auto negotiating speed with the link partner and selects the highest speed that is compatible with the link partner. **10Mbps HDX**—forces the cu port in 10Mbps half duplex mode. **10Mbps FDX**—forces the cu port in 10Mbps full duplex mode. **100Mbps HDX**—forces the cu port in 100Mbps half duplex mode. **100Mbps FDX**—forces the cu port in 100Mbps full duplex mode. **1Gbps FDX**—forces the port in 1Gbps full duplex **SFP_Auto_AMS**—automatically determines the speed of the SFP. Note: There is no standardized way to do SFP auto detect, so here it is done by reading the SFP rom. Due to the missing standardized way of doing SFP auto detect some SFPs might not be detectable. The port is set in AMS mode with SFP preferred. Cu port is set in **Auto** mode. **100-FX**—SFP port in 100-FX speed. Copper port disabled. **100-FX_AMS**—port in AMS mode with SFP preferred. SFP port in 100-FX speed. **1000-X**—SFP port in 1000-X speed. Copper port disabled. **1000-X_AMS**—port in AMS mode with SFP preferred. SFP port in 1000-X speed.
Flow Control	When **Auto Speed** is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The **Current Rx** column indicates whether pause frames on the port are obeyed, and the **Current Tx** column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the **Configured** column to use flow control. This setting is related to the setting for Configured Link Speed.
Maximum Frame Size	Enter the maximum frame size allowed for the switch port, including Frame Check Sequence (FCS).
Power Control	The Usage column shows the current percentage of the power consumption per port. The Configured column allows for changing the power savings mode parameters per port. **Disabled**: All power savings mechanisms disabled. **ActiPHY**: Link down power savings enabled. **PerfectReach**: Link up power savings enabled. **Enabled**: Both link up and link down power savings enabled.
Refresh	Click to refresh the page immediately.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.3.2 Port Trunk

5.3.2.1 Configuration

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

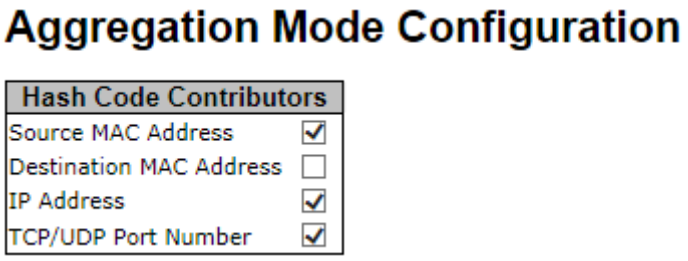


Figure 40 - Aggregation Mode Configuration

Label	Description
Source MAC Address	The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, **Source MAC Address** is enabled.
Destination MAC Address	The **Destination MAC Address** can be used to calculate the destination port for the frame. Check to enable the use of the **Destination MAC Address**, or uncheck to disable. By default, **Destination MAC Address** is disabled.
IP Address	The **IP address** can be used to calculate the destination port for the frame. Check to enable the use of the **IP Address**, or uncheck to disable. By default, I**P Address** is enabled.
TCP/UDP Port Number	The **TCP/UDP Port Number** can be used to calculate the destination port for the frame. Check to enable the use of the **TCP/UDP Port Number**, or uncheck to disable. By default, **TCP/UDP Port Number** is enabled.

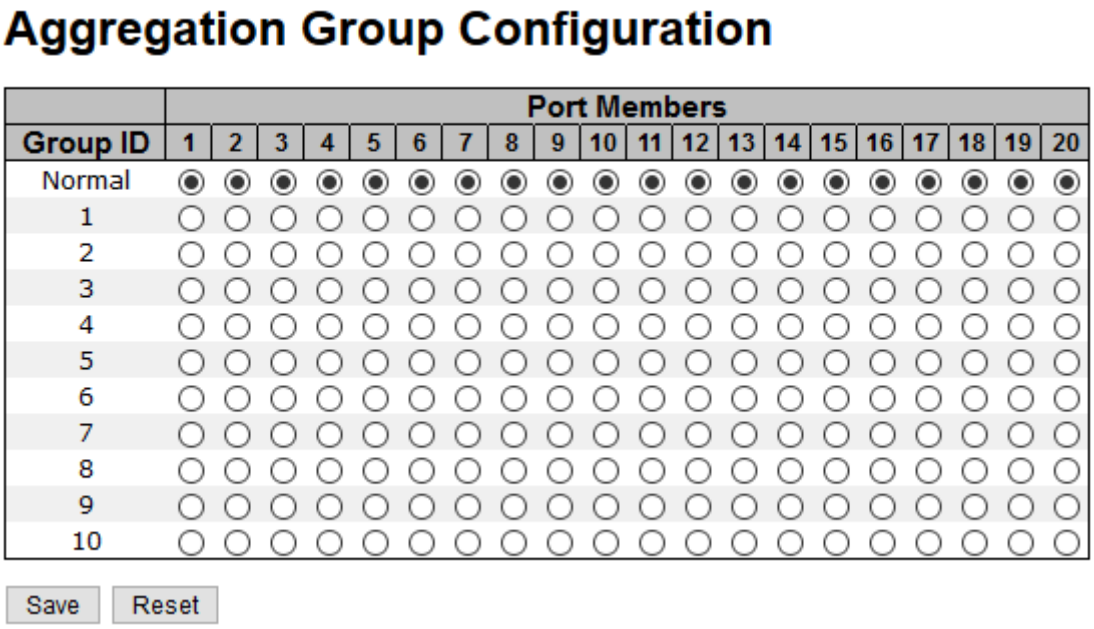


Figure 41 - Aggregation Group Configuration

Label	Description
Group ID	Indicates the ID of each aggregation group. **Normal** means no aggregation. Only one group ID is valid per port.

Label	Description
Port Members	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.3.2.2 LACP Port

The Link Aggregation Control Protocol (LACP), an IEEE 802.3ad standard protocol, allows bundling several physical ports together to form a single logical port. Note that LACP and Static aggregation can't be both enabled on the same ports.

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

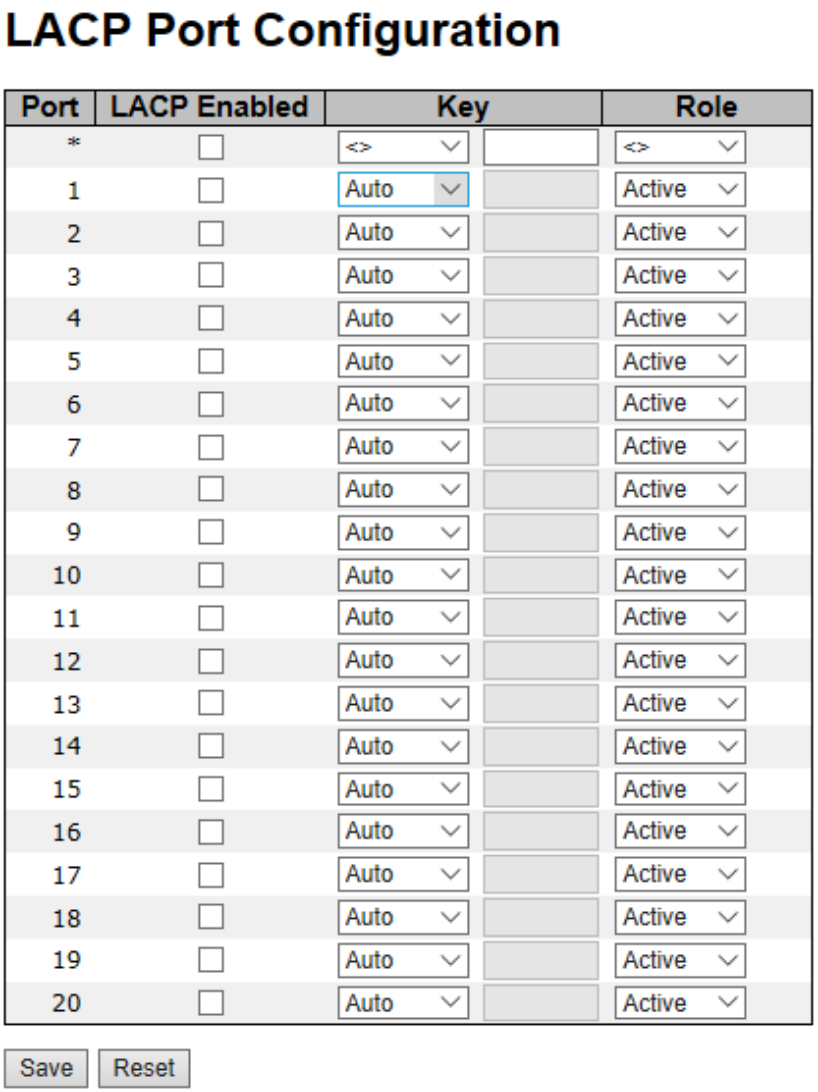


Figure 42 – LACP Port Configuration

Label	Description
Port	The switch port number.
LACP Enabled	Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. Up to 32 aggregations are supported (if stackable).
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 the user 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	Indicates LACP activity status. **Active** will transmit LACP packets every second; while **Passive** will wait for a LACP packet from a partner (speak if spoken to).
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.3.2.3 LACP System Status

This page provides a status overview for all LACP instances.

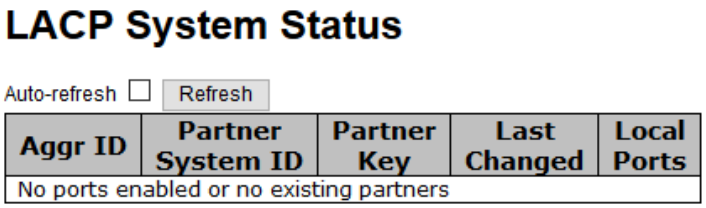
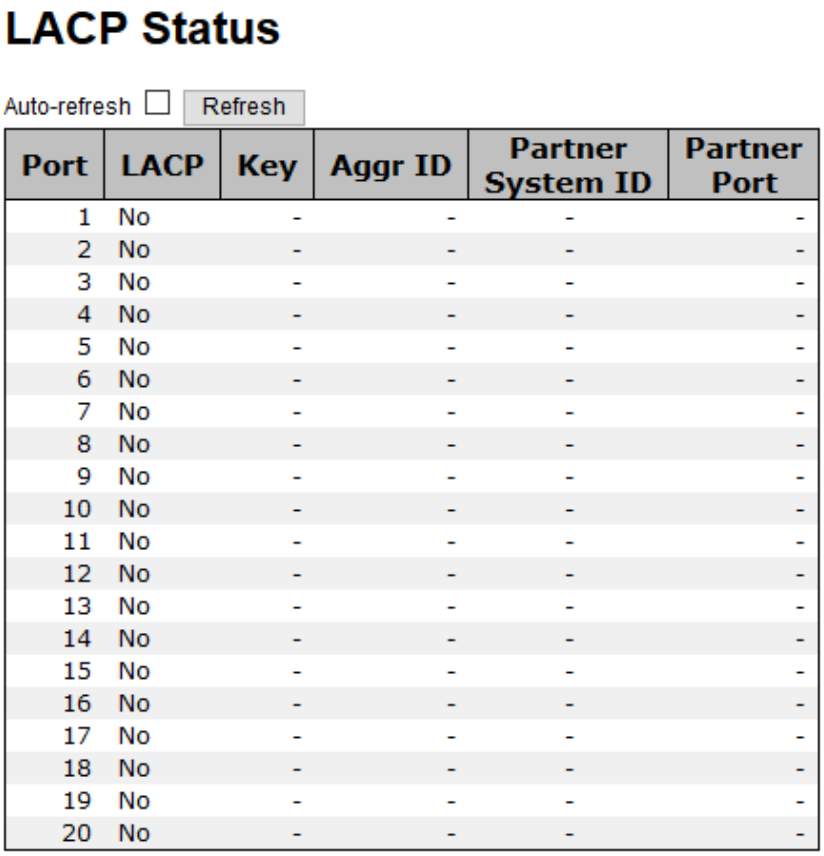


Figure 43 – LACP System Status

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 changed.
Local Ports	Shows which ports are a part of this aggregation for this switch.
Refresh	Click to refresh the page immediately.
Auto-refresh	Check to enable an automatic refresh of the page at regular Intervals.

5.3.2.4 LACP Port Status

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



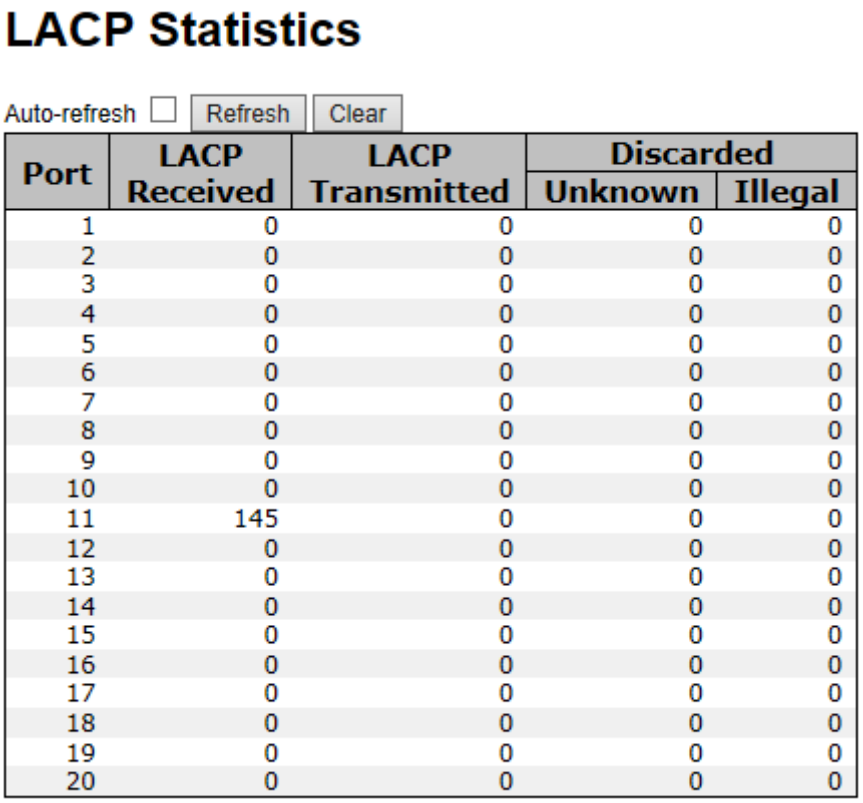
Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	No	-	-	-	-
6	No	-	-	-	-
7	No	-	-	-	-
8	No	-	-	-	-
9	No	-	-	-	-
10	No	-	-	-	-
11	No	-	-	-	-
12	No	-	-	-	-
13	No	-	-	-	-
14	No	-	-	-	-
15	No	-	-	-	-
16	No	-	-	-	-
17	No	-	-	-	-
18	No	-	-	-	-
19	No	-	-	-	-
20	No	-	-	-	-

Figure 44 - LACP Status

Label	Description
Port	Switch port number.
LACP	**Yes** means LACP is enabled and the port link is up. **No** means that 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 and is in disabled LACP status.
Key	The key assigned to this 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.

5.3.2.5 LACP Port Statistics

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



Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	145	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0

Figure 45 - LACP Statistics

Label	Description
Port	Switch port number.
LACP Received	The number of LACP frames received at each port.
LACP Transmitted	The number of LACP frames sent from 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.

5.3.3 Loop Protection

Loop protection increases the efficiency of STP, RSTP, and MSTP by preventing ports from moving into a forwarding state that would result in a loop opening up in the network. Spanning-tree protocol loop protection can be configured to improve the stability of Layer 2 networks. It is recommended to configure loop protection only on non-designated interfaces such as the root or alternate interfaces. Otherwise, if loop protection is configured on both sides of a designated link, then certain STP configuration events (such as setting the root bridge priority to an inferior value in a topology with many loops) can cause both interfaces to transition to blocking mode. When you enable loop protection, you must configure at least one action [10] (Log Only, Shutdown Port (block), or both (Shutdown Port and Log)).
This page allows the user to inspect the current Loop Protection configurations, and possibly change them as well.

5.3.3.1 Configuration

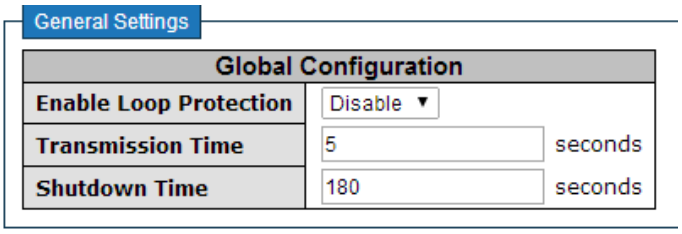


Figure 46 – Loop Protection

Label	Description
Enable Loop Protection	Controls whether loop protections is enabled (as a whole).
Transmission Time	The interval between each loop protection PDU sent to each port. The value must be between 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).

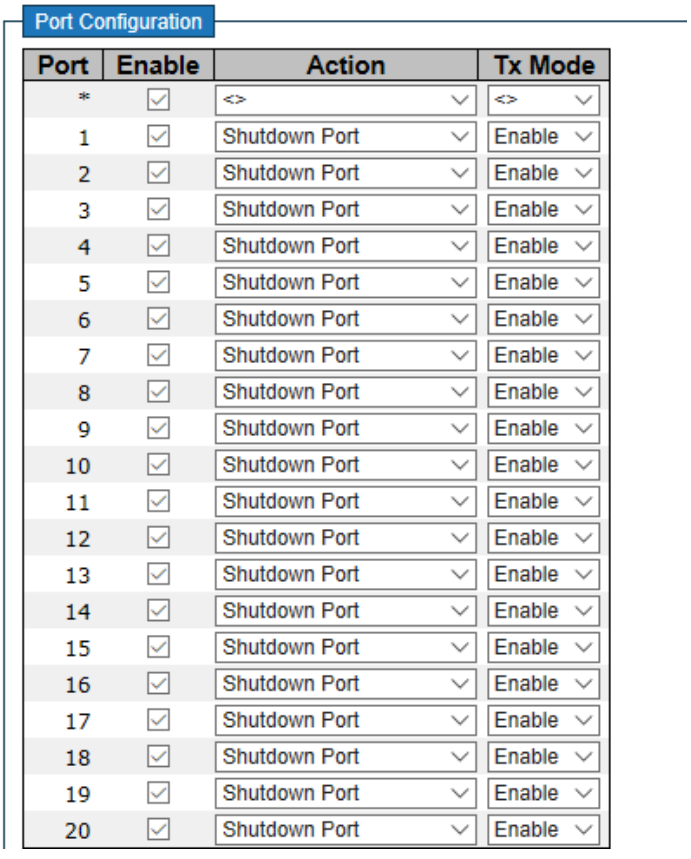


Figure 47 - Port Configuration

Label	Description
Port	The switch port number of the port.
Enable	Controls whether loop protection is enabled on this switch port.
Action	Configures the action to take when a loop is detected. Valid values are **Shutdown Port, Shutdown Port and Log,** or **Log Only**
Tx Mode	Controls whether the port is actively generating loop protection PDUs or only passively look for looped PDUs.
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values

5.3.3.2 Status

This page displays the loop protection port status the ports of the switch.

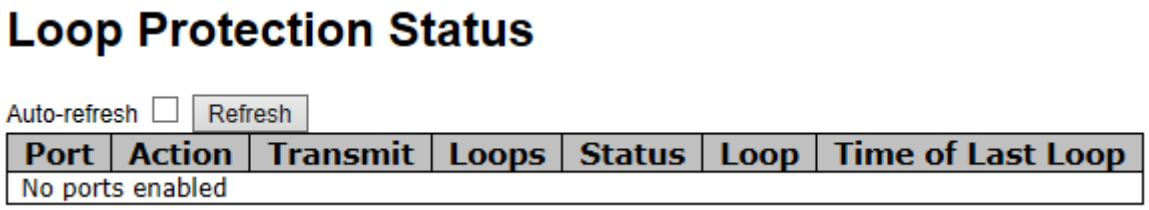


Figure 48 - Loop Protection Status

Label	Description
Port	The switch port number of the port.
Action	The currently configured port action
Transmit Mode	The currently configured port transmit mode.
Loops	The number of loops detected on this port.
Status	The current loop protection status of the port.
Loop	Whether a loop is currently detected on the port.
Time of Last Loop	The time of the last loop event detected.
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values

5.4 Redundancy

5.4.1 iRing

iRing Protocol is a very fast network redundancy protocol that provides link fail-over protection with very fast self-healing recovery.

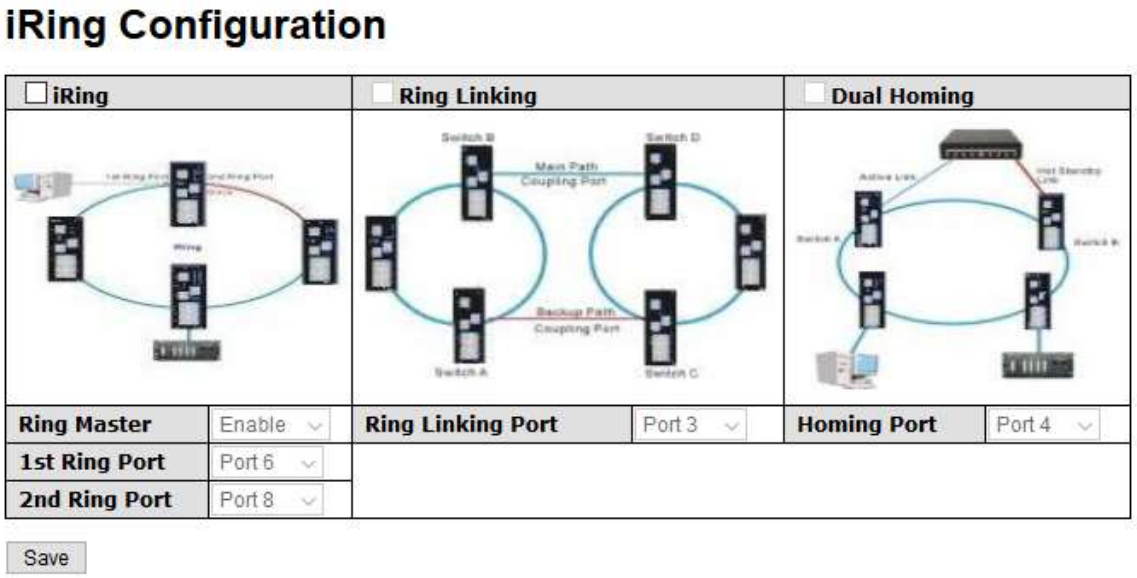


Figure 49 - iRing Configuration

Label	Description
iRing	Check to enable iRing topology.
Ring Master	Only one ring master is allowed in a ring. However, if more than one switch is 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 ring port
2nd Ring Port	The backup ring port
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	Used 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 (e.g., a backbone switch). The two links work in active/backup mode, and connect each ring to the normal switches in RSTP mode.
Save	Click to apply the configurations.

5.4.2 iChain

iChain is an easy use and powerful network redundancy protocol. The recovery speed of iChain is very quickly. It provides the add-on network redundancy topology for any backbone network, the upper LAN could be iRing, iBridge, RSTP, Single Switch, or any backbone.

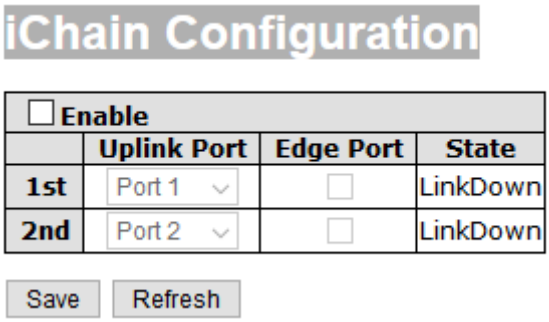


Figure 50 - iChain Configuration

Label	Description
Enable	Check to enable iChain function
Uplink Port	There are two uplink ports for every devices in the chain. The user must specify the ports according to topology of network.
Edge Port	Only the edge (head or tail) device needs to specify edge port. The user must specify the edge port according to topology of network.
State	There three states for uplink port: Link Down, Blocking, and Forwarding.
Save	Click to apply the configurations.
Refresh	Click to refresh the page immediately.

5.4.3 iBridge

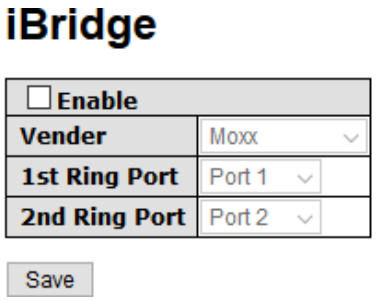


Figure 51 – iBridge

Label	Description
Enable	Check to enable iBridge function
1st Ring Port	The first port connecting to the bridge
2nd Ring Port	The second port connecting to the bridge
Vender	The list of the supported vendors is: • Moxx • Advantexx • Hitshmaxx
Save	Click to apply the configurations.

5.4.4 RSTP

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol (STP). It provides faster convergence of spanning tree after a topology change. The system also supports STP and will detect a connected device that is running STP or RSTP protocol automatically. RSTP is enabled by default.

This page allows a user to configure STP system settings. The settings are used by all STP Bridge instances in the switch.

5.4.4.1 RSTP Bridge Setting

The RSTP function can be disabled or STP or RSTP enabled, and their parameters set for each port via the RSTP Port Setting interface.

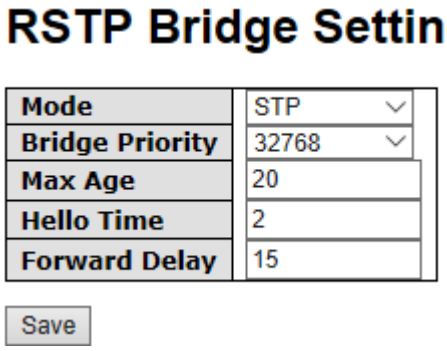


Figure 52 - RSTP Bridge Setting interface

Label	Description
Mode	The RSTP function must be enabled or disabled before configuring any of the related parameters. Valid values are **Disable**, **STP**, and **RSTP (default)**.
Bridge Priority (0-61440)	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the Multiple Spanning Tree Instances (MSTI) number, concatenated with the 6-byte MAC address of the switch forms a *Bridge Identifier*. For `MSTP` operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
Max Age (6-40)	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2
Hello Time (1-10)	The time that the Control Switch sends out the BPDU (Bridge Protocol Data Unit) packet to verify the current status of RSTP. Enter a value between 1 and 10.
Forwarding Delay (4-30)	The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

NOTE: Follow this rule to configure the MAX Age, Hello Time, and Forward Delay Time:

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

5.4.4.2 RSTP Port Setting

This page allows the user to configure the current RSTP port configurations, and change them as well.

This page contains settings for physical and aggregated ports.

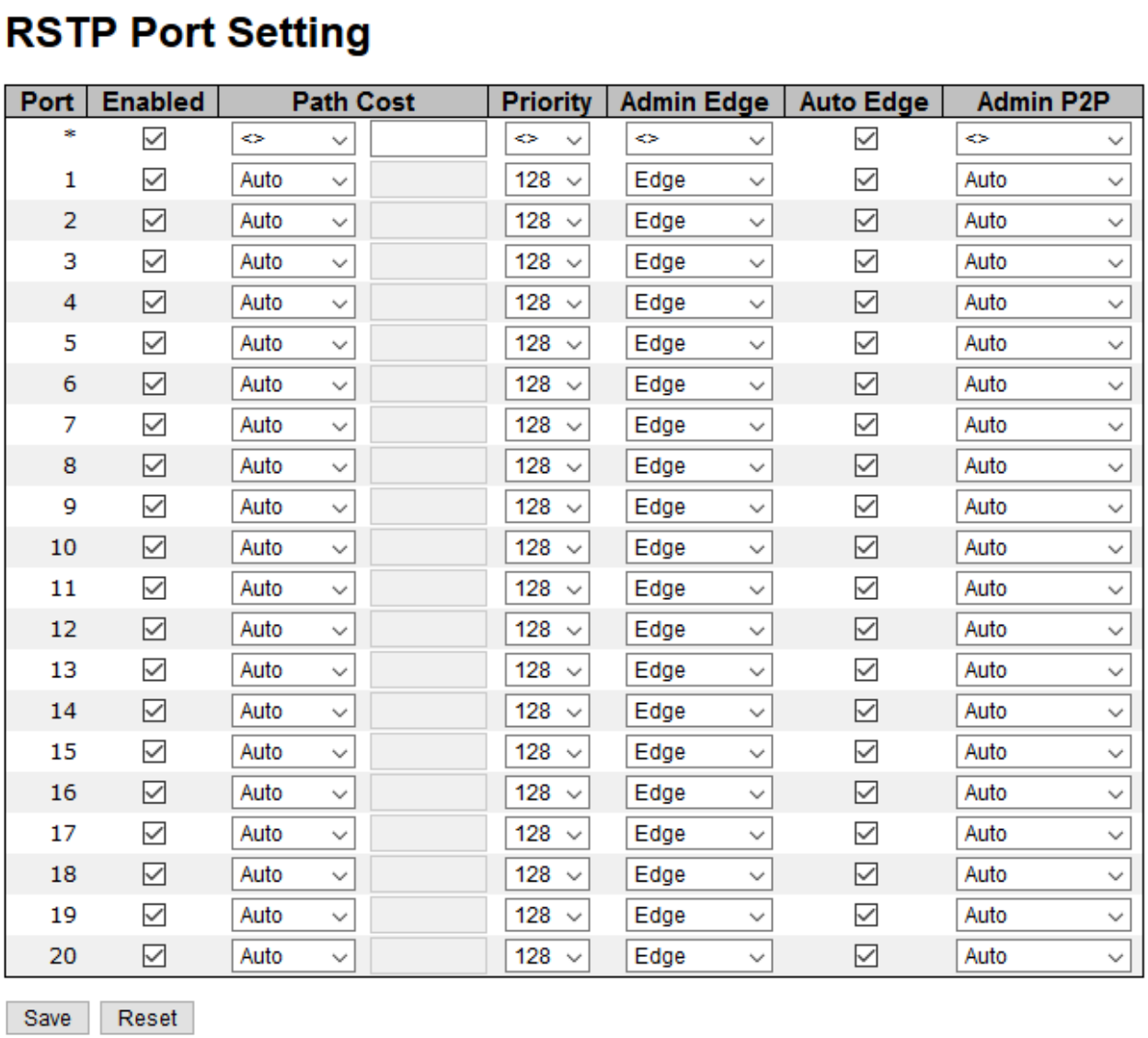


Figure 53 - RSTP Port Setting

Label	Description
Port	The switch port number of the logical RSTP port
Enabled	It shows whether RSTP is enabled on this switch port.
Path Cost	The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D 2004 recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority (0-240)	Enter which port should be blocked by setting the priority on the LAN. Enter a number between 0 and 240. The value of priority must be a multiple of 16.
Admin Edge	Admin Edge is the port which is directly connected to end stations. Controls whether the *operEdge* flag should start as set or cleared. (The initial *operEdge* state when a port is initialized).
Auto Edge	Controls whether the bridge should enable automatic edge detection on the bridge port. This allows *operEdge* to be derived from whether BPDU's are received on the

Label	Description
	port or not.
Admin P2P	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 apply the configurations.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.4.4.3 RSTP Bridge Status

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

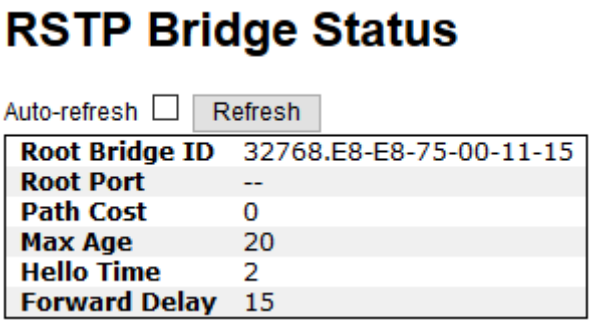
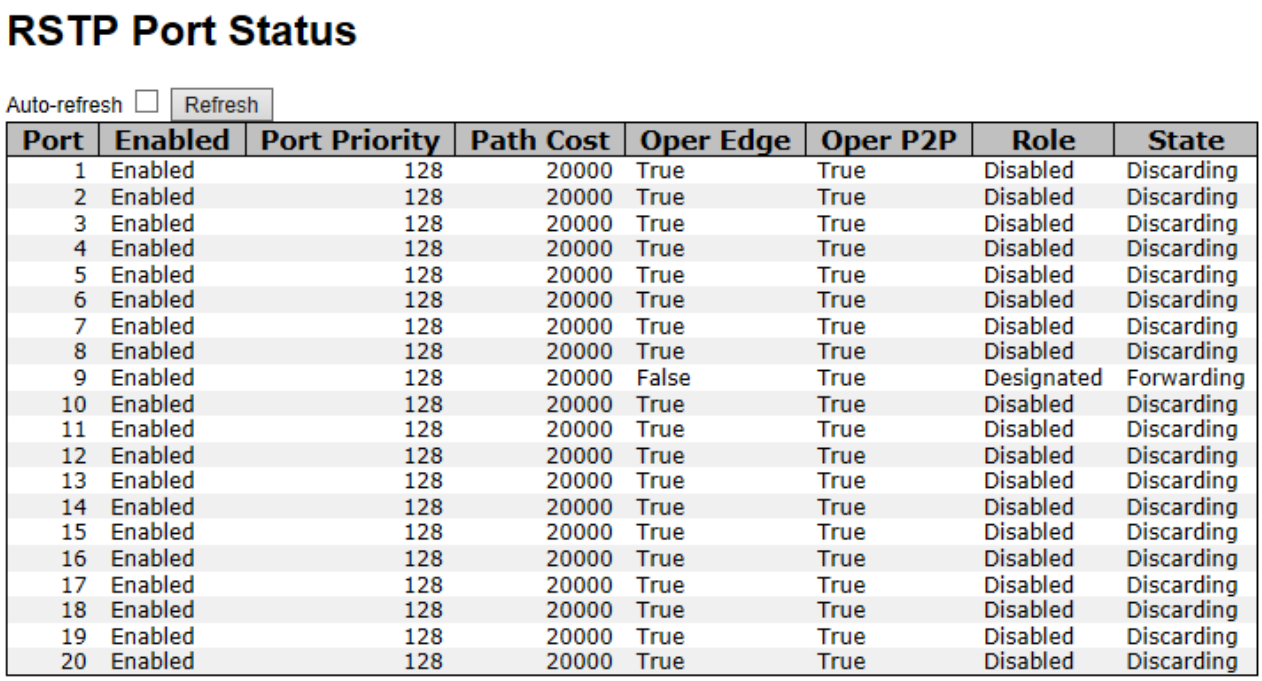


Figure 54 - RSTP Bridge Status

Label	Description
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page immediately.
Root Bridge ID	The Bridge ID of this Bridge instance.
Root Port	The switch port currently assigned the root port role.
Path Cost	Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Max Age	The maximum age of information defined in this device..
Hello Time	The time that the Control Switch sends out the BPDU (Bridge Protocol Data Unit).
Forward Delay	The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode).

5.4.4.4 RSTP Port Status

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



RSTP Port Status

Auto-refresh ☐ Refresh

Port	Enabled	Port Priority	Path Cost	Oper Edge	Oper P2P	Role	State
1	Enabled	128	20000	True	True	Disabled	Discarding
2	Enabled	128	20000	True	True	Disabled	Discarding
3	Enabled	128	20000	True	True	Disabled	Discarding
4	Enabled	128	20000	True	True	Disabled	Discarding
5	Enabled	128	20000	True	True	Disabled	Discarding
6	Enabled	128	20000	True	True	Disabled	Discarding
7	Enabled	128	20000	True	True	Disabled	Discarding
8	Enabled	128	20000	True	True	Disabled	Discarding
9	Enabled	128	20000	False	True	Designated	Forwarding
10	Enabled	128	20000	True	True	Disabled	Discarding
11	Enabled	128	20000	True	True	Disabled	Discarding
12	Enabled	128	20000	True	True	Disabled	Discarding
13	Enabled	128	20000	True	True	Disabled	Discarding
14	Enabled	128	20000	True	True	Disabled	Discarding
15	Enabled	128	20000	True	True	Disabled	Discarding
16	Enabled	128	20000	True	True	Disabled	Discarding
17	Enabled	128	20000	True	True	Disabled	Discarding
18	Enabled	128	20000	True	True	Disabled	Discarding
19	Enabled	128	20000	True	True	Disabled	Discarding
20	Enabled	128	20000	True	True	Disabled	Discarding

Figure 55 - RSTP Port Status

Label	Description
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click to refresh the page immediately.
Port	The switch port number of the logical RSTP port
Enabled	It shows whether RSTP is enabled or disabled on this switch port.
Port Priority	Which ports should be blocked by priority in LAN. A number 0 through 240. The value of priority must be the multiple of 16.
Path Cost	The cost of the path to the other bridge from this transmitting bridge at the specified port. A number 1 through 200000000.
OperEdge	When **True**, OperEdge is enabled, the port is configured as an edge port and directly connected to an end station and cannot create a bridging loop. **False** means that OperEdge is disabled.
OperP2P	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. It is served by a point-to-point LAN segment), or it can be connected to two or more bridges (i.e. It is served by a shared medium LAN segment). OperP2P shows the P2P status of the link to be manipulated administratively. **True** means P2P enabling. False means P2P disabling.
Role	The Role of each port is Disabled or Designated.
State	The State of each port is Discarding or Forwarding.

5.4.5 MSTP

5.4.5.1 Bridge Settings

This page allows the user to configure STP system settings. The settings are used by all STP Bridge instances in the switch.

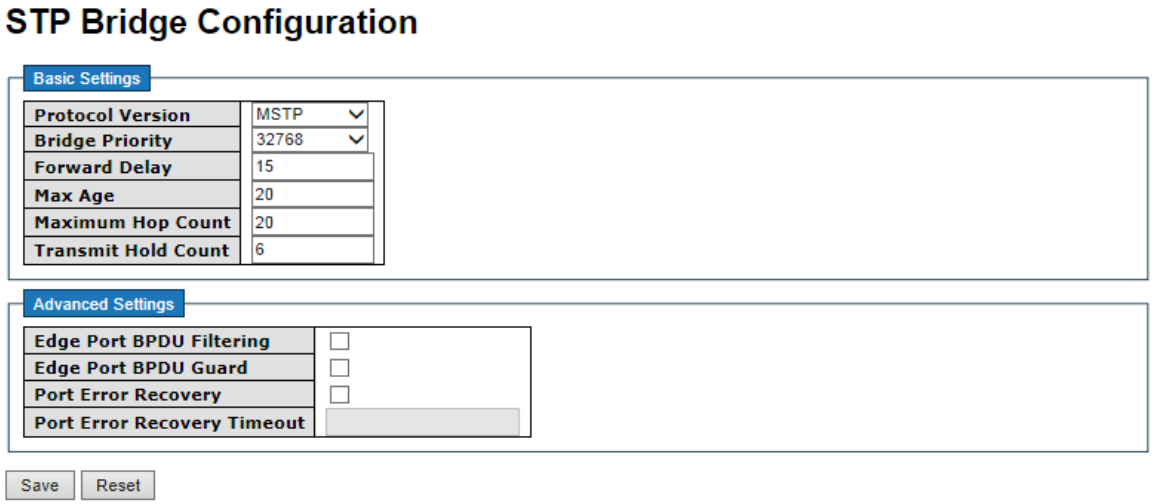


Figure 56 - STP Bridge Configuration

Label	Description
Protocol Version	The version of the STP protocol. Valid values include STP, RSTP, and MSTP.
Bridge Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a *Bridge Identifier*. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
Forward Delay	The delay used by STP bridges to transit root and designated ports to forwarding (used in STP compatible mode). The range of valid values is 4 to 30 seconds.
Max Age	The maximum time the information transmitted by the root bridge is considered valid. The range of valid values is 6 to 40 seconds, and **Max Age** must be <= (FwdDelay-1)*2.
Maximum Hop Count	This defines the initial value of remaining hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. The range of valid values is 4 to 30 seconds, and MaxAge must be <= (FwdDelay-1)*2.
Transmit Hold Count	The number of BPDUs a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. The range of valid values is 1 to 10 BPDUs per second.
Advanced Settings	
Edge Port BPDU Filtering	Controls 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.

Label	Description
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).
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.4.5.2 MSTI Mapping

This page allows the user to inspect the current Multiple Spanning Tree Instances (MSTI) bridge instance priority configurations, and possibly change them as well.

Switches participating in MST instances must be constantly configured with the same MST configuration information. The collection of switches which have the same MST information form an MST region.

Within each MST region, MSTP maintains multiple STIs. Instance 0 is known as IST. All other instances are numbered from 1 to 15. The IST is the only spanning tree instance that sends and receives the MST configuration messages, all other instance information are encapsulated in MST BPDUs. Thus, in MSTP there are two contexts of operation, one in the context of the entire topology called Common and Internal Spanning Tree (CIST), which is the default spanning tree instance for MSTP, and the other in the context of each individual spanning tree context, that is, MSTI. [6]

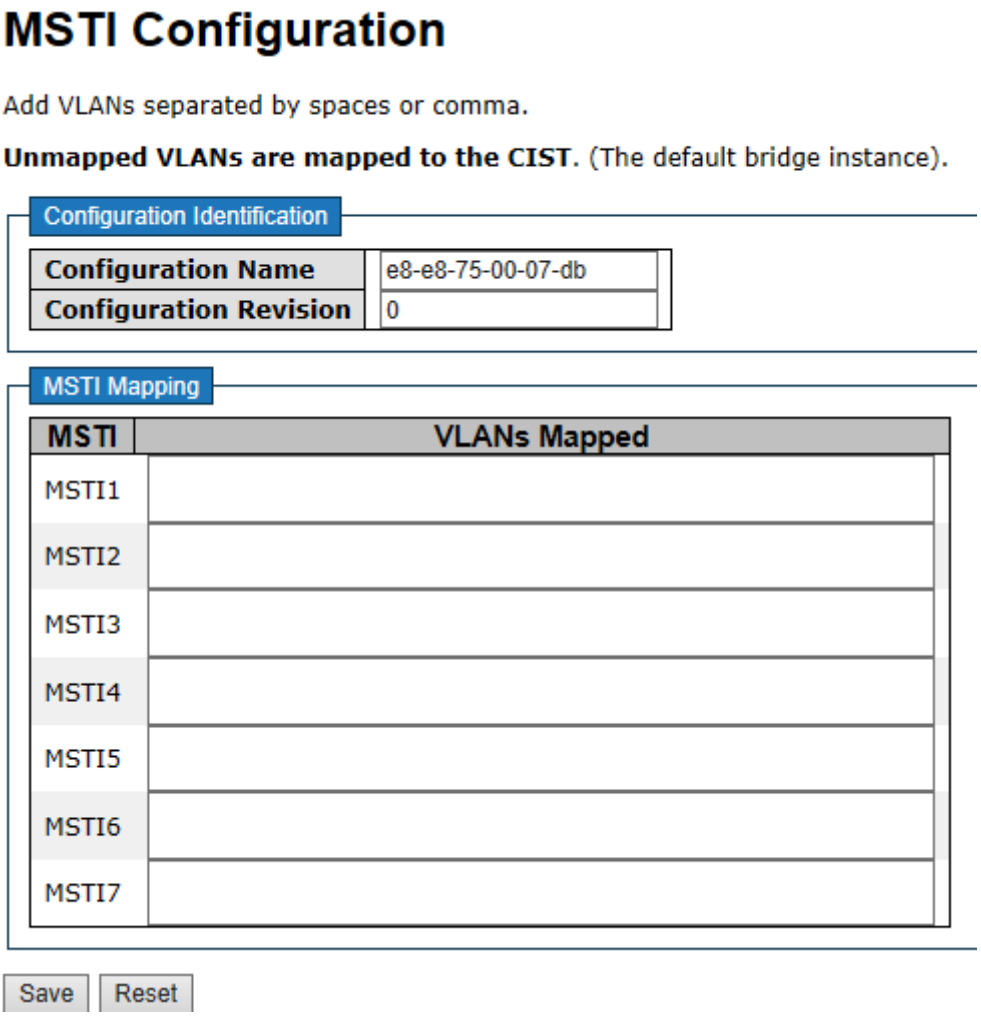


Figure 57 - MSTI Configuration

Label	Description
Configuration Name	The name which identifies the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configurations in order to share spanning trees for MSTIs (intra-region). The name should not exceed 32 characters.
Configuration Revision	Revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
MSTI Mapping	
MSTI	The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
VLANs Mapped	The list of VLANs mapped to the MSTI. The VLANs can be given as a single (**xx**, xx being between 1 and 4094) VLAN, or a range **(xx-yy)**, each of which must be separated with comma and/or space. A VLAN can only be mapped to *one* MSTI. An unused MSTI should just be left empty. (I.e. not having any VLANs mapped to it.) Example: `2,5,20-40`.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.4.5.3 MSTI Priorities

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

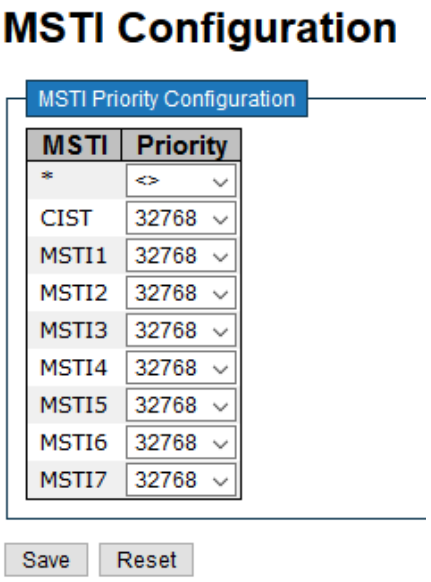


Figure 58 - MSTI Configuration

Label	Description
MSTI	The bridge instance. CIST is the default instance, which is always active.
Priority	Indicates bridge priority. The lower the value, the higher the priority. The bridge priority, MSTI instance number, and the 6-byte MAC address of the switch forms a Bridge Identifier.
Save	Click to save changes
Reset	Click to undo any changes made locally and revert to previously saved values

5.4.5.4 CIST Ports

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

This page contains settings for physical and aggregated ports.

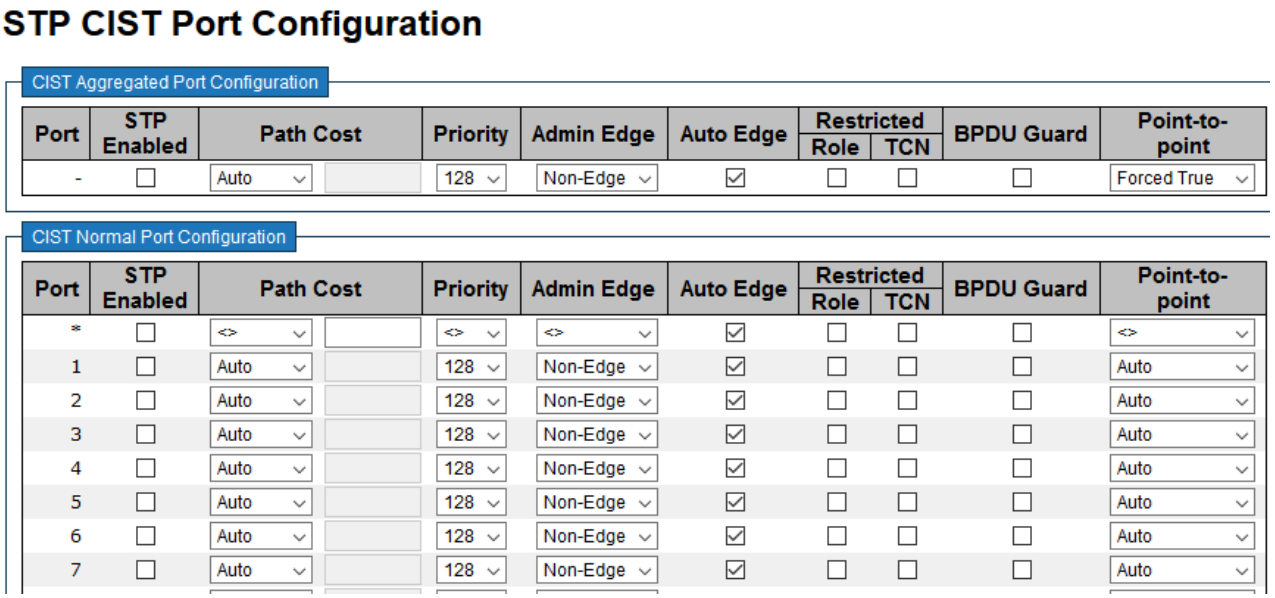


Figure 59 – STP MSTI Port Configuration

Label	Description
Port	The switch port number of the logical STP port
STP Enabled	Check to enable STP for the port
Path Cost	Configures the path cost incurred by the port. **Auto** will set the path cost according to the physical link speed by using the 802.1D-recommended values. **Specific** allows the user to enter a user-defined value. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range of valid values is 1 to 200000000.
Priority	Configures the priority for ports having identical port costs. (See above).
Admin Edge	Configures the operEdge flag should start as set or cleared.(the initial operEdge stated when a port is initialized).
Auto Edge	Check to enable the bridge to detect edges at the bridge port automatically. This allows **operEdge** to be derived from whether BPDUs are received on the port or not.

Restricted	
Role	When enabled, the port will not be selected as root port for CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an alternate port after the root port has been selected. If set, spanning trees will lose connectivity. It can be set by a network administrator to prevent bridges outside a core region of the network from influencing the active spanning tree topology because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
TCN	When enabled, the port will not propagate received topology change notifications and topology changes to other ports. If set, it will cause temporary disconnection after changes in an active spanning trees topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges outside a core region of the network from causing address flushing in that region because those bridges are not under the full control of the administrator or is the physical link state for the attached LANs transitions frequently.
BPDU Guard	If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port **Edge** status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.
Point-to-Point	Configures whether the port connects to a point-to-point LAN rather than a shared medium. This can be configured automatically or set to true or false manually. Transiting to forwarding state is faster for point-to-point LANs than for shared media.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.4.5.5 MSTI Ports

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

An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains MSTI port settings for physical and aggregated ports.

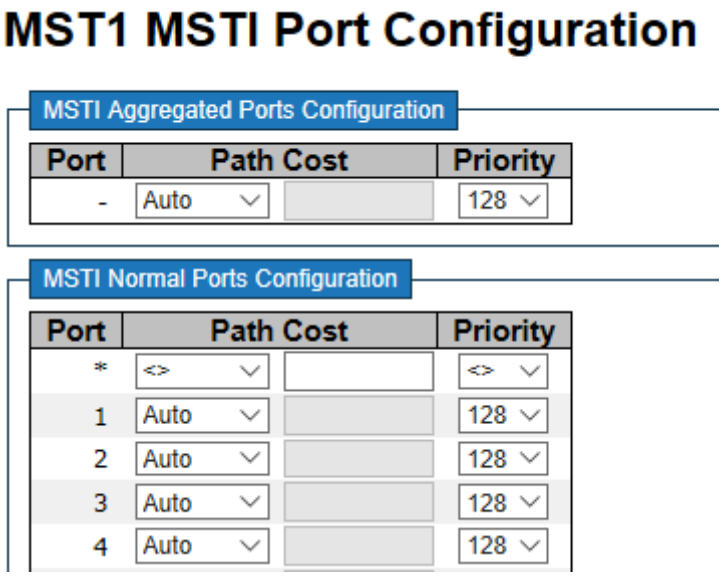


Figure 60 –MSTI Port Configuration

Label	Description
Port	The switch port number of the corresponding STP CIST (and MSTI) port
Path Cost	Configures the path cost incurred by the port. **Auto** will set the path cost according to the physical link speed by using the 802.1D-recommended values. **Specific** allows the user to enter a user-defined value. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range of valid values is 1 to 200000000.
Priority	Configures the priority for ports having identical port cost. (See above).
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.4.5.6 Bridge Status

This page shows the status for all STP bridge instances.

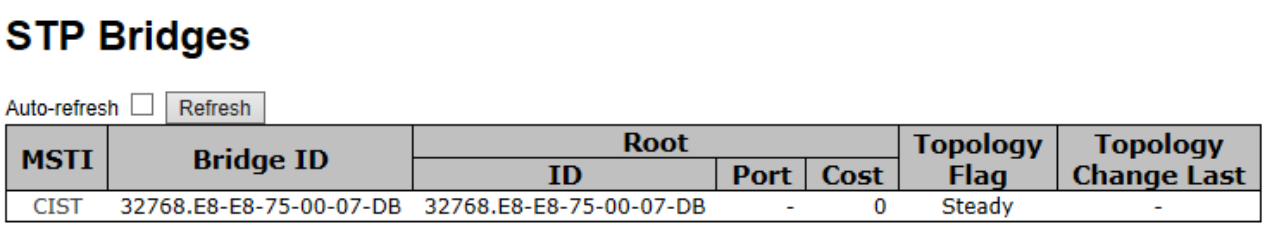


Figure 61 - STP Bridges

Label	Description
MSTI	The bridge instance. Can also be linked to the STP detailed bridge status.
Bridge ID	The bridge ID of this bridge instance.
Root ID	The bridge ID of the currently selected root bridge.
Root Port	The switch port currently assigned the root port role.
Root Cost	Root path cost. For a root bridge, this is zero. For other bridges, it is the sum of port path costs on the least cost path to the Root Bridge.
Topology Flag	The current state of the Topology Change Flag for the bridge instance.
Topology Change Last	The time since last Topology Change occurred.
Refresh	Click to refresh the page immediately.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.

5.4.5.7 Port Status

This page displays the STP port status for the currently selected switch.

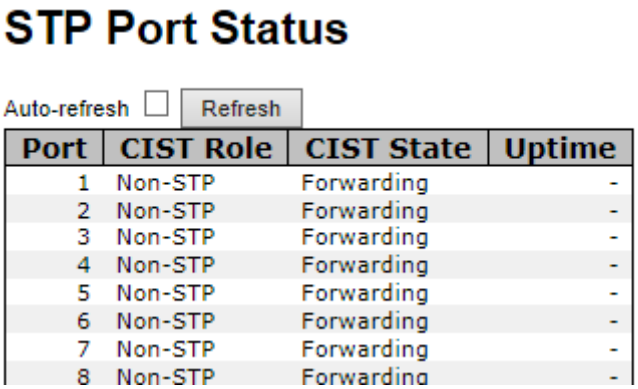


Figure 62 - STP Port Status

Label	Description
Port	The switch port number to which the following settings will be applied.
CIST Role	The current STP port role of the CIST port. The values include: **AlternatePort**, **BackupPort**, **RootPort**, **DesignatedPort**, and **Non-STP**.
CIST State	The current STP port state of the CIST port. The values include: **Blocking**, **Learning**, and **Forwarding**.
Uptime	The time since the bridge port was last initialized
Refresh	Click to refresh the page immediately.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.

5.4.5.8 Port Statistics

This page displays the STP port statistics for the currently selected switch.

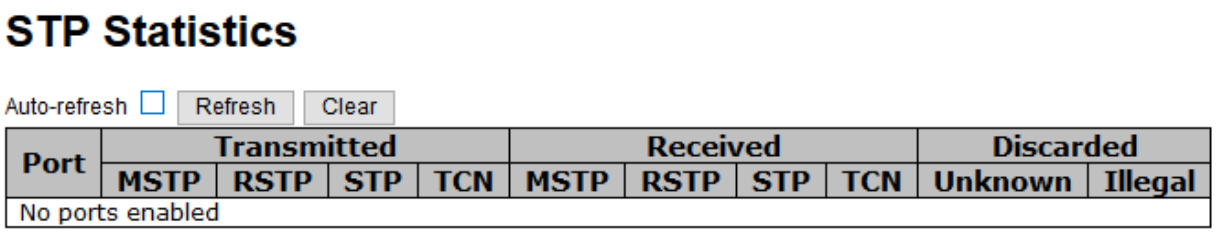


Figure 63 - STP Statistics

Label	Description
Port	The switch port number to which the following settings will be applied.
MSTP	The number of MSTP configuration BPDU's received/transmitted on the port.
RSTP	The number of RSTP configuration BPDU's received/transmitted on the port
STP	The number of legacy STP configuration BPDU's received/transmitted on the port
TCN	The number of (legacy) topology change notifications BPDU's received/transmitted on the port.
Discarded Unknown	The number of unknown spanning tree BPDUs received (and discarded) on the port.
Discarded Illegal	The number of illegal spanning tree BPDU's received (and discarded) on the port.
Refresh	Click to refresh the page immediately.
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals.

5.4.6 MRP

5.4.6.1 Introduction

MRP (Media Redundancy Protocol) is an industry standard for high-availability Ethernet networks. MRP allows 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).

5.4.6.2 Configuration

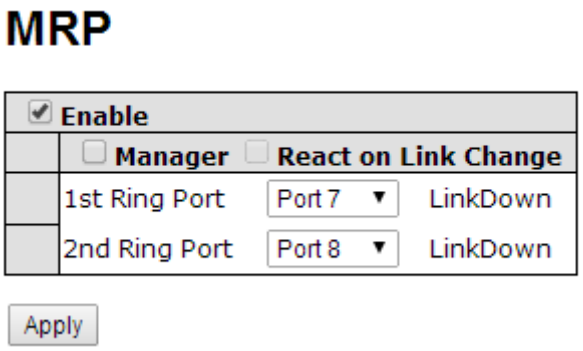


Figure 64 - MRP

Label	Description
Enable	Enables the MRP function.
Manager	Every MRP topology needs a MRP manager, and can only have one manager. If two or more switches are set to be Managers at the same time, the MRP topology will fail.
React on Link Change (Advanced mode)	Faster mode. Enabling this function will ensure MRP topology a more rapid converge. This function only can be set by the MRP manager switch.
1st Ring Port	Chooses the port that connects to the MRP ring.
2nd Ring Port	Chooses the port that connects to the MRP ring.

5.4.7 Fast Recovery

Fast Recovery is a function for port redundancy. The port has the highest recovery priority (the lowest number) will be the active port, others will be blocked (if included).

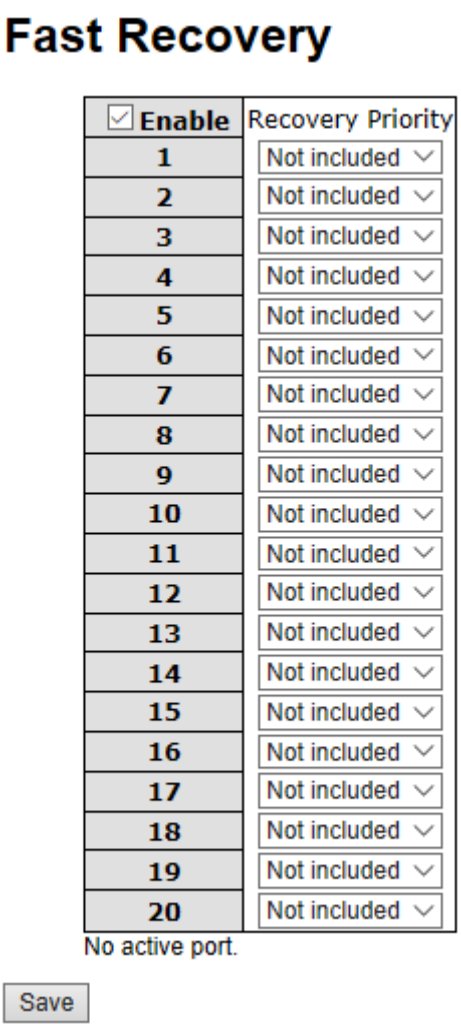


Figure 65 - Fast Recovery

Label	Description
Enable	Enables fast recovery mode
Recovery Priority	The port has the highest recovery priority (the lowest number) will be the active port, others will be blocked (if included).
Save	Click to save the configurations.

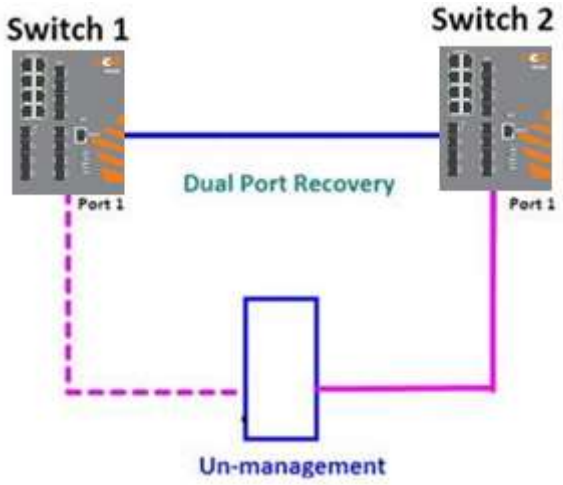
5.4.8 Dual Port Recovery

Dual Port Recovery mode is defined to work with unmanaged devices/switches or ring of switches. This feature can be set to on single port of switches on both sides of unmanaged ring. The iES20GF in Dual Port Recovery mode will provide redundant links.

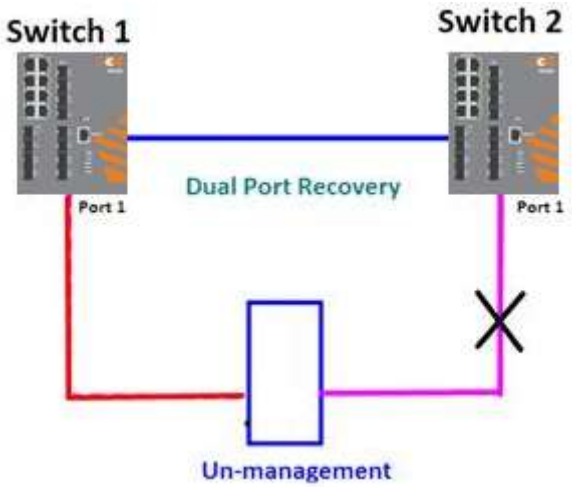
5.4.8.1 Introduction

Dual Port Recovery is an iS5 Communication Proprietary solution for interoperability issues with unmanaged devices like unmanaged switches. Dual Port Recovery allows Ethernet switches in ring configuration with unmanaged devices to recover from failure rapidly to ensure seamless data transmission. A dual port recovery ring can support up to 5 unmanaged devices and will enable a back-up link in 40ms (adjustable to min 20ms (recommended is 40ms).

This protocol is based on sending specific messages (BPDU format) from each port on both sides of unmanaged chain. The Dual Port Recovery feature can be executed with other redundancy protocols on same device.

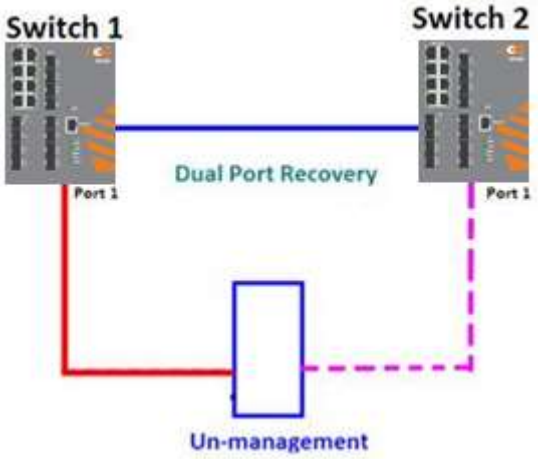


In Dual Port Recovery function if link of port in "Forwarding" state goes down, the "backup" port is changing its state to be forwarding, like in picture below. The disconnected port changes its status to "No Link"



When link of port 1 on switch 2 returns back to be link up, the switch 1 port 1 is in "forwarding" state

and in this case the "No Link" port is changing its status to be "Blocking" port.



5.4.8.2 Configuration

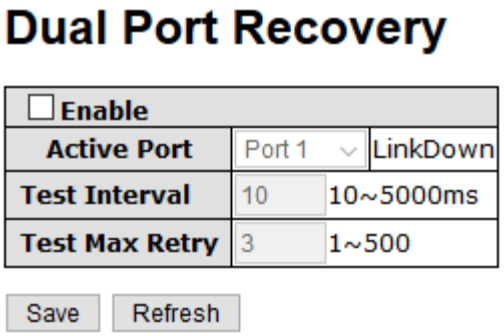


Figure 66 – Dual Port Recovery

Label	Description
Enable	Activate the Dual Port Recovery mode.
Active Port	Choosing the port which connects to the unmanaged switch/ring of switches. Note: User need to select one port to be Active Port on each of two devices of each side.
Test Interval	Setting Interval time for sending keep alive messages (10-5000 ms default 10) Note: Test interval should be the same on both sides.
Test Max Retry	Set the maximum number of lost frames to start Dual Port Recovery mechanism (1-500 retries default 3)Note: Test Max Retry should be the same on both sides.
Apply	Click **Apply** to activate the configurations.

5.5 VLAN

5.5.1 VLAN Membership

The VLAN membership configuration for the switch can be monitored and modified here. Up to 4096 VLANs are supported. This page allows for adding and deleting VLAN's as well as adding and deleting port members of each VLAN.

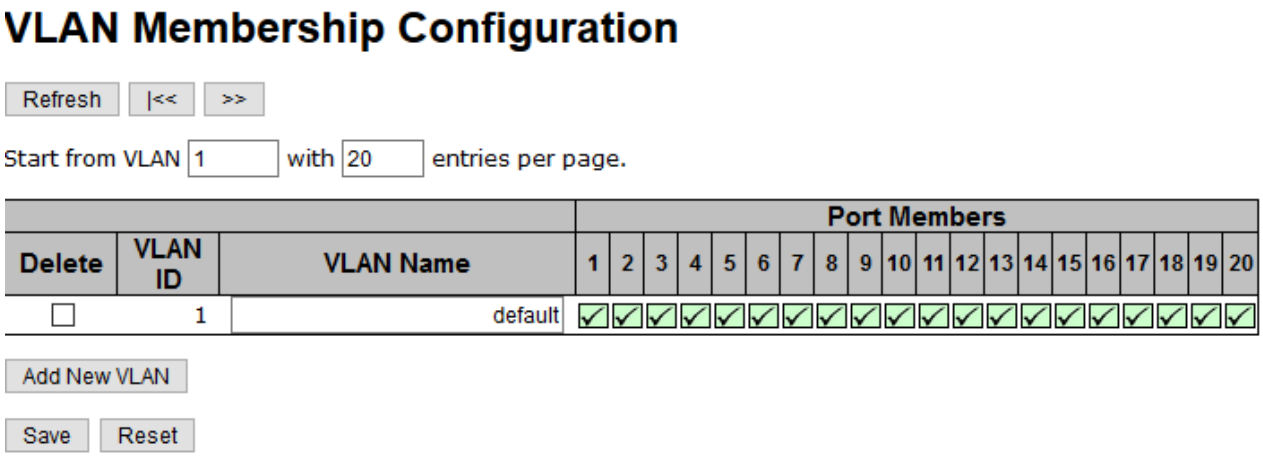


Figure 67 -VLAN Membership Configuration

5.5.1.1 Navigating the VLAN Table

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

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking **Refresh** will update the displayed table starting from that or the closest next VLAN Table match.

The **>>** will use the last entry of the currently displayed VLAN 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 I << to start over.

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	Indicates the ID of this particular VLAN.
VLAN Name	Indicates the name of the VLAN. Maximum length of the VLAN Name String is 32. VLAN Name can be null. If it is not null, it must contain alphabets or numbers. At least one alphabet must be present in a non-null VLAN name. VLAN name can be edited for the existing VLAN entries or it can be added to the new entries.
Port Members	A row of check boxes for each port is displayed for each VLAN ID. To include a port in a VLAN, check the box as ✓. To include a port in a forbidden port list, check the box as shown ✗. To remove or exclude the port from the VLAN, make sure the box is unchecked as shown . By default, no ports are members, and for every new VLAN entry all boxes are unchecked.

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

5.5.2 Ports Configuration

This page is used for configuring the switch port VLAN.

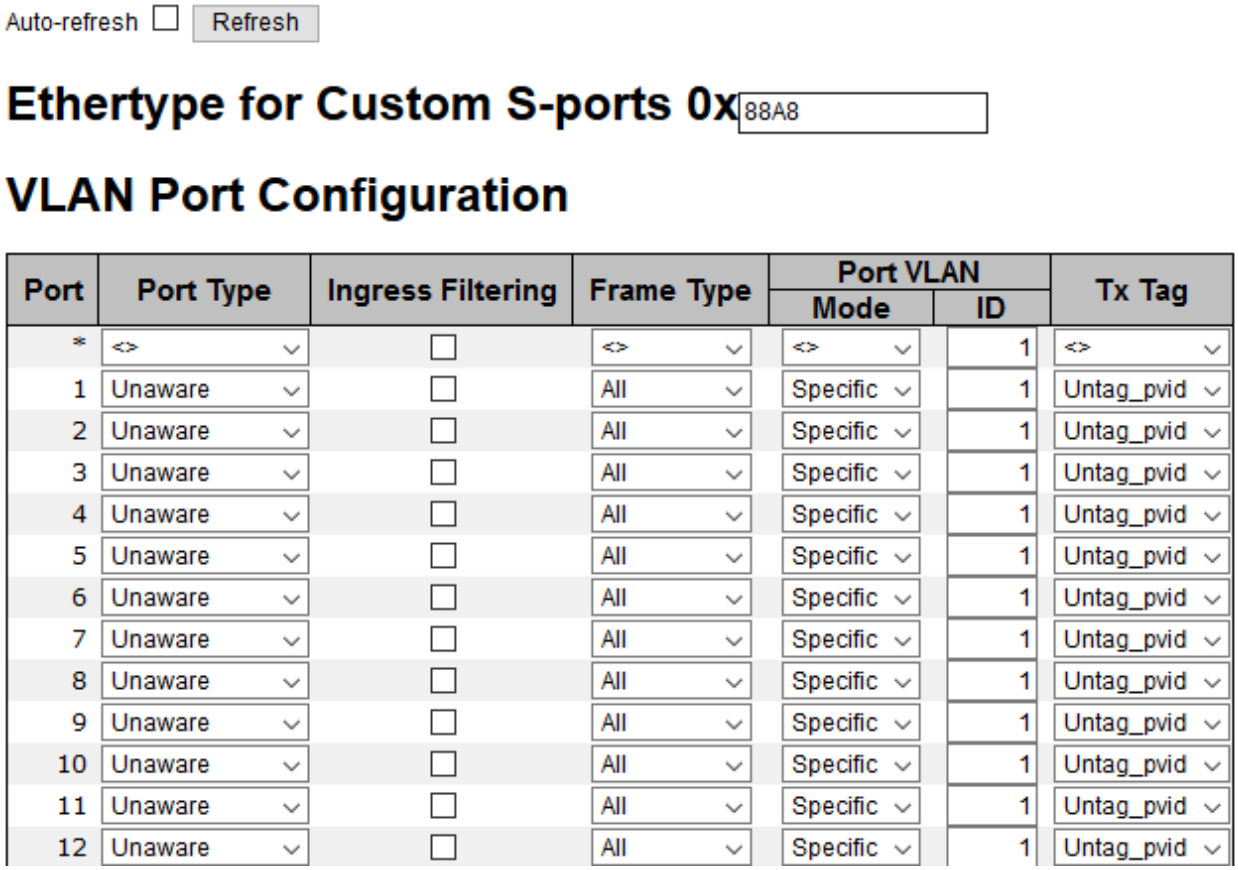


Figure 68 - VLAN Port Configuration

Label	Description
Ethertype for custom S-Ports	This field specifies the Ether type used for custom S-ports. This is a global setting for all custom S-ports.
Port	This is the logical port number of this row.
Port type	Port can be one of the following types: **Unaware**, **Custom** (**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.

Label	Description
Ingress Filtering	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.
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. The options are: **Untag_pvid**: all VLANs except the configured PVID will be tagged. **Tag_all**: all VLANs are tagged. **Untag_all**: all VLANs are untagged.

5.5.2.1 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 Tag protocol identifier (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 forwarded.	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.

	Ingress action	Egress action
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: If the tagged frame contains a TPID of 0x8100, it will be forwarded. 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.**

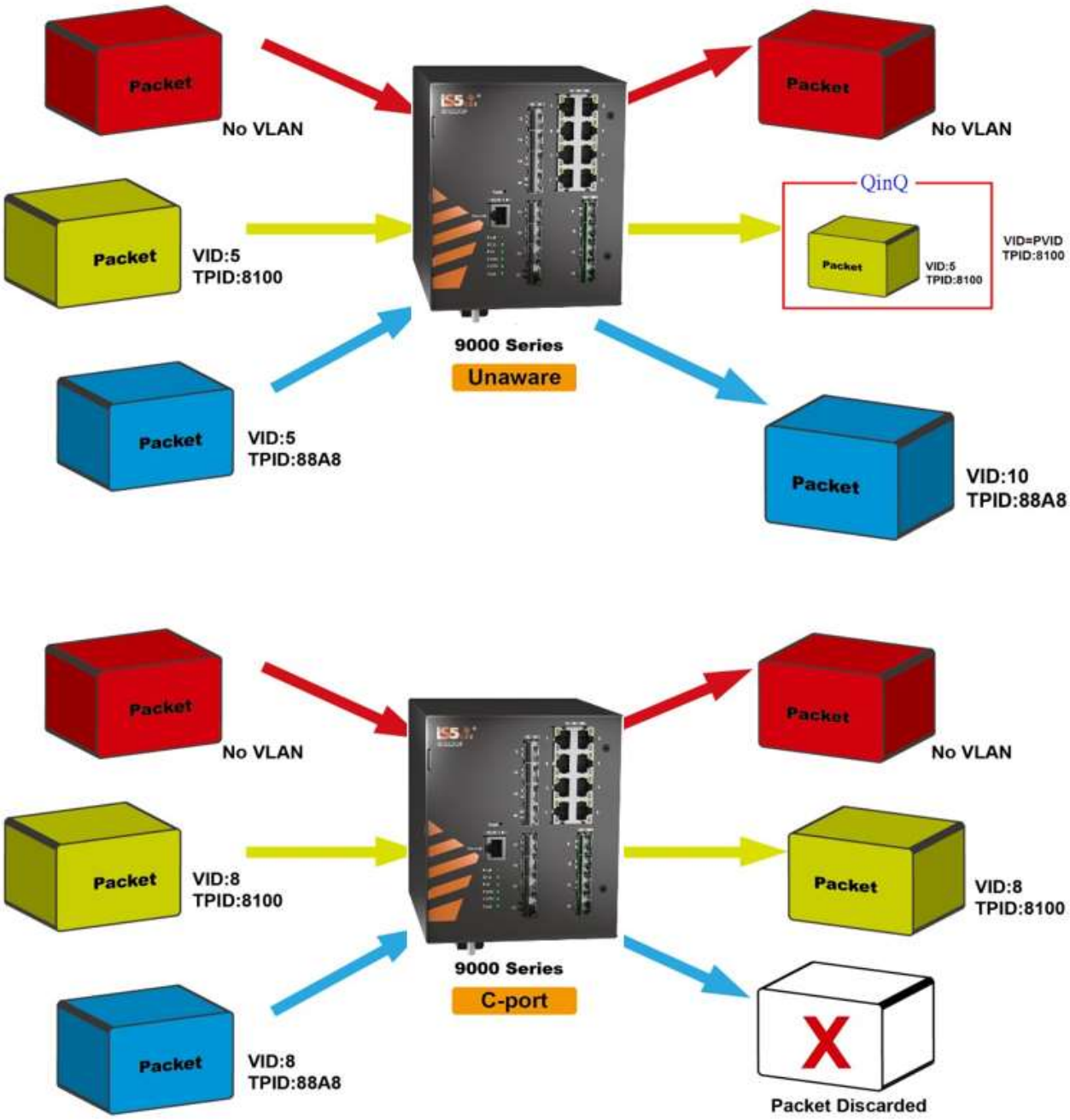


Figure 69 - Unaware and C-port Port Types

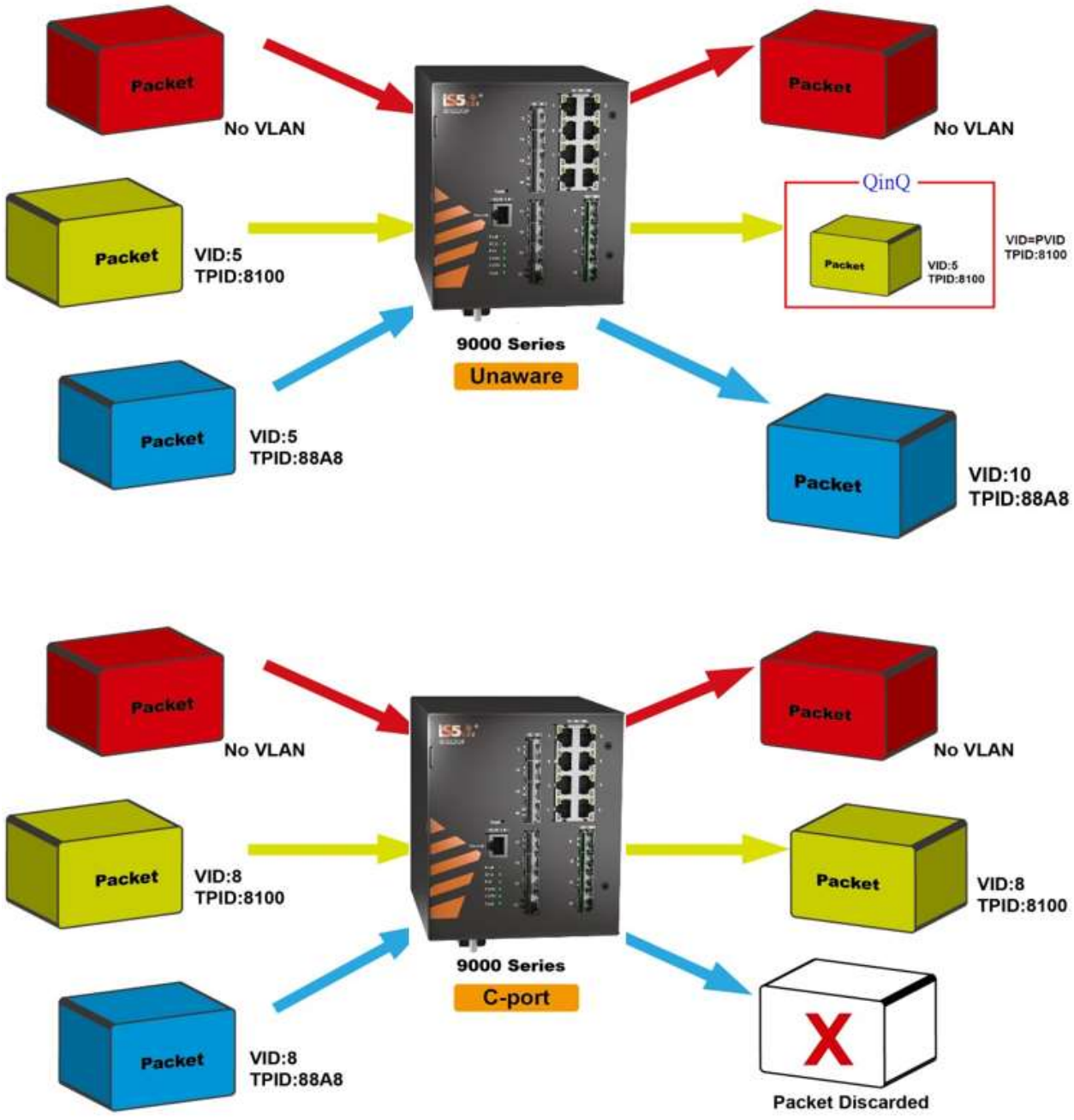


Figure 70 - S-port and S-custom Port Types

5.5.2.2 Examples of VLAN Settings

VLAN Access Mode:

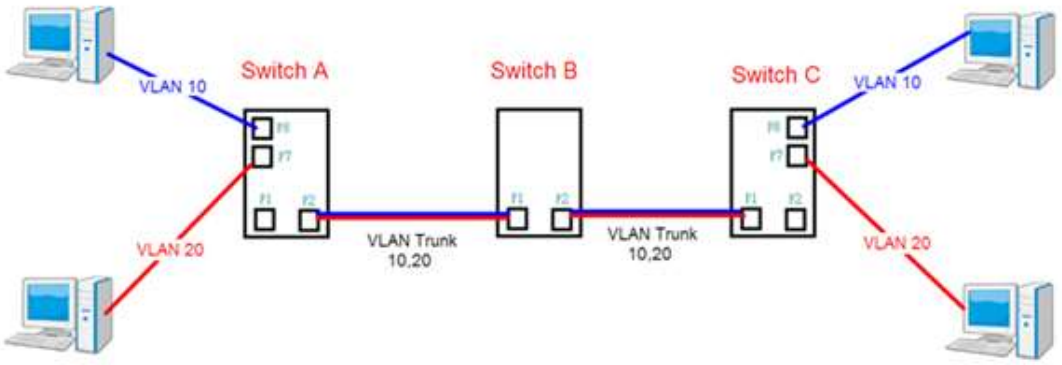


Figure 71 - VLAN Access Mode topology

Switch A,

Port 7 is VLAN Access mode = Untagged 20

Port 8 is VLAN Access mode = Untagged 10

Below are the switch settings.

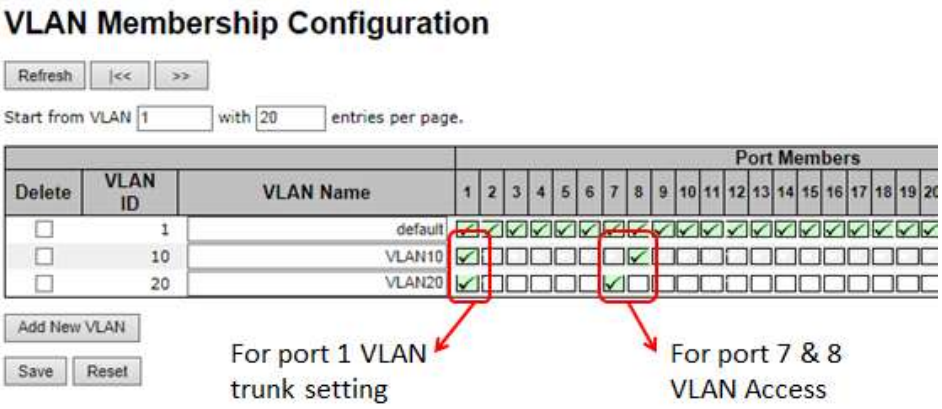


Figure 72 - VLAN Membership Configuration

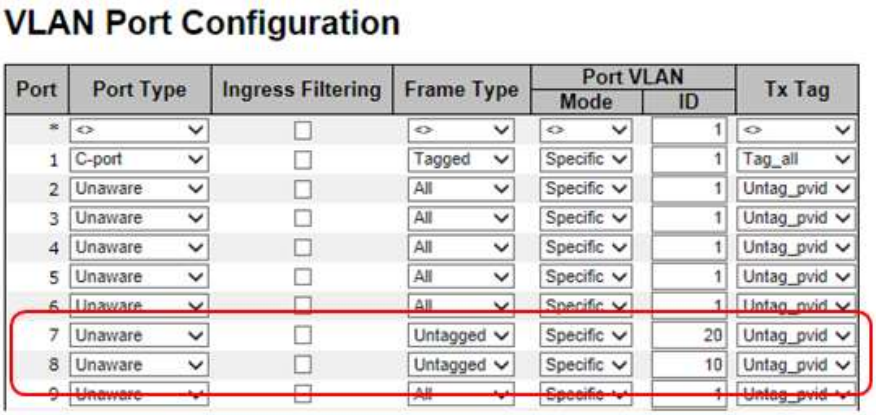
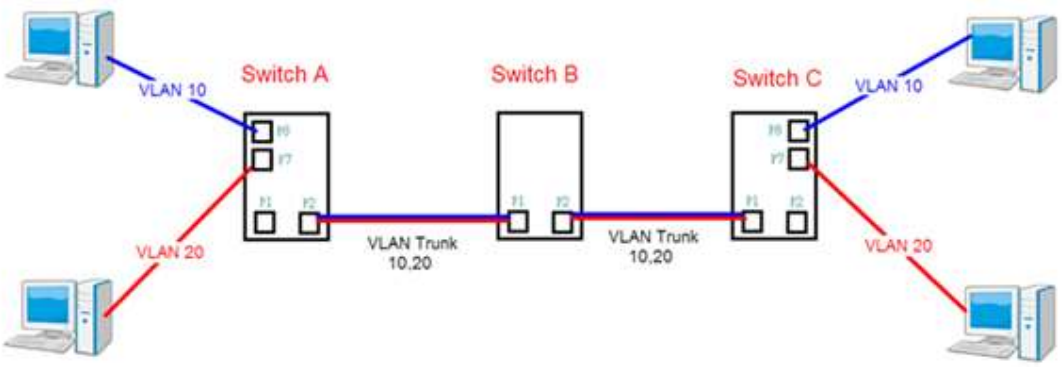


Figure 73 - VLAN Port Configuration

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.

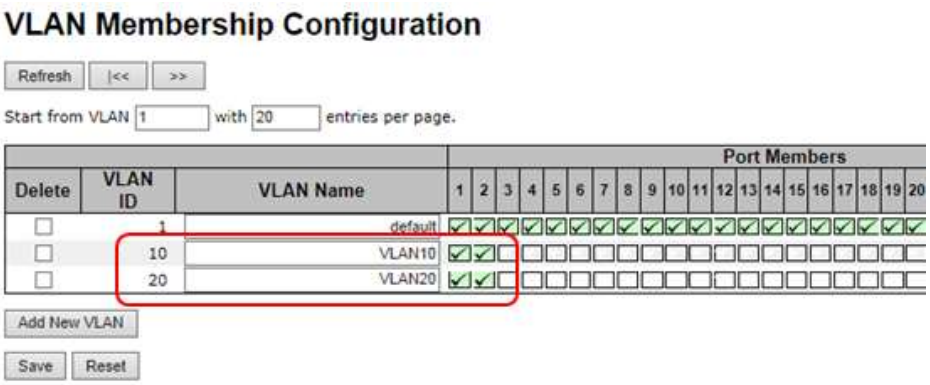


Figure 74 - VLAN Membership Configuration

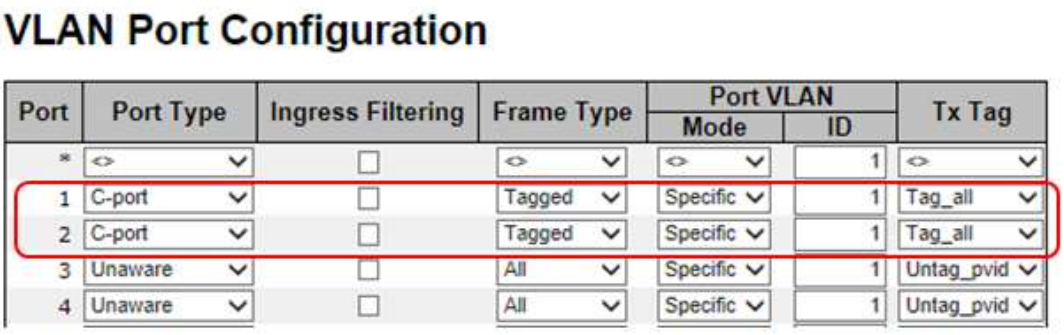


Figure 75 - VLAN Port Configuration

VLAN Hybrid Mode:

Port 1 VLAN Hybrid mode = untagged 10

Tagged 10, 20

Below are the switch settings.

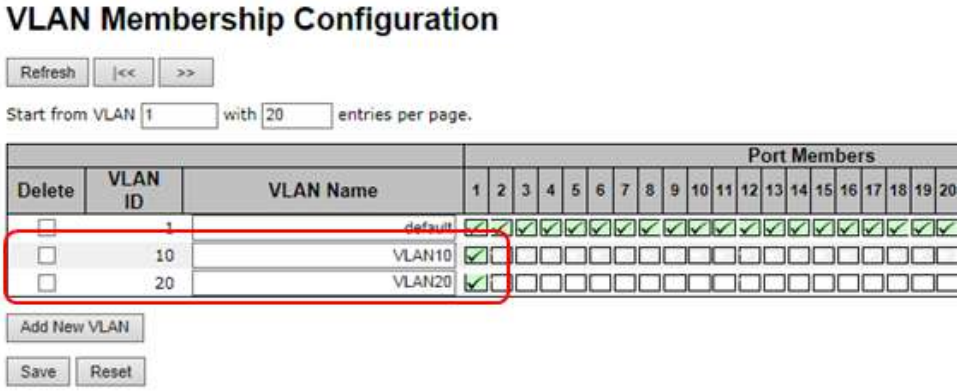


Figure 76 - VLAN Membership Configuration

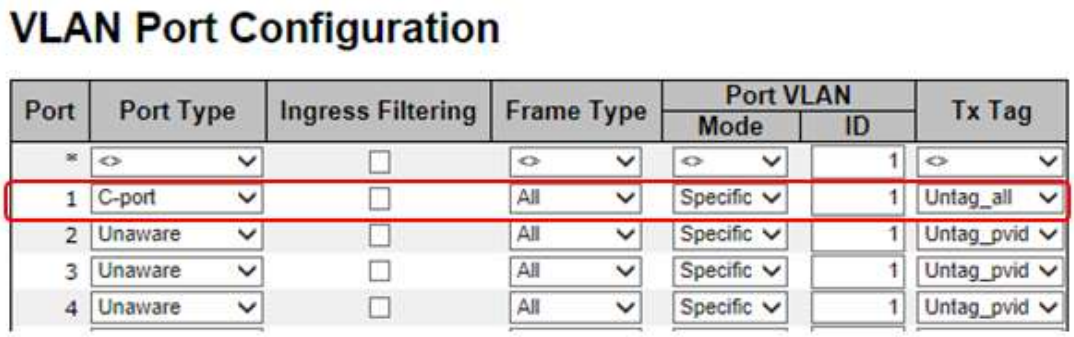
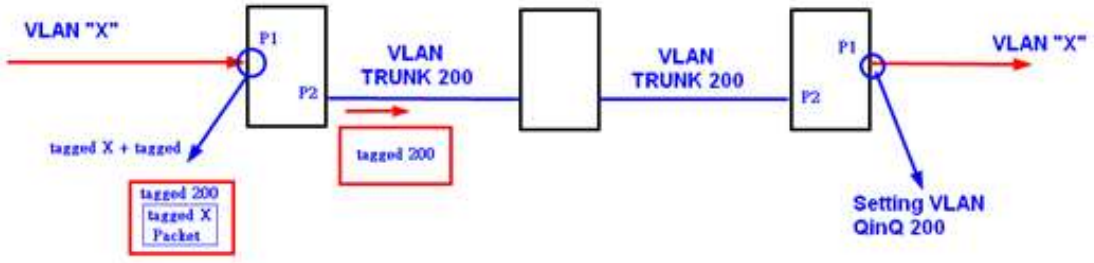


Figure 77 - VLAN Port Configuration

VLAN QinQ Mode:

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

VLAN "X" = Unknown VLAN



iES20GF Port 1 VLAN Settings:

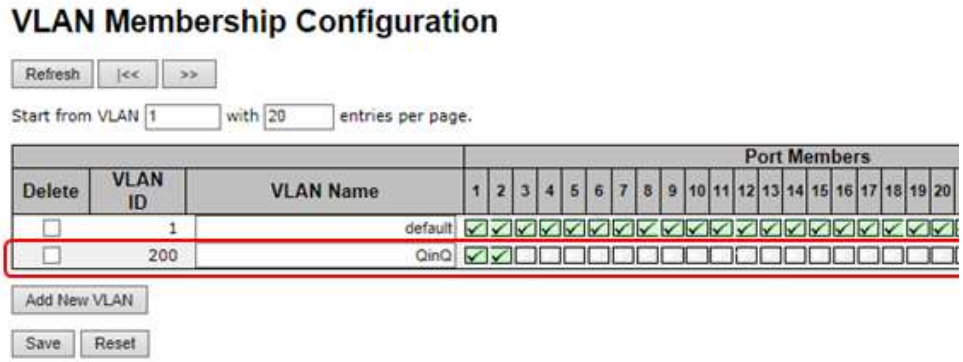


Figure 78 - VLAN Membership Configuration

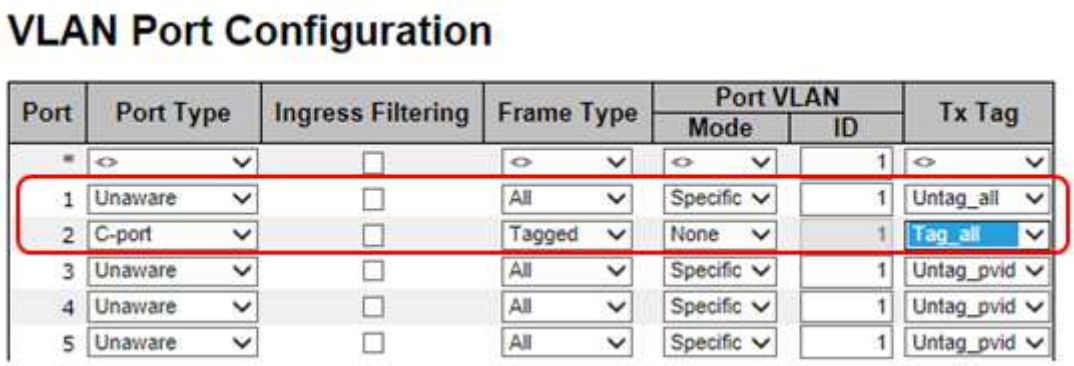


Figure 79 - VLAN Port Configuration

VLAN ID Settings

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

iES20GF VLAN Settings:

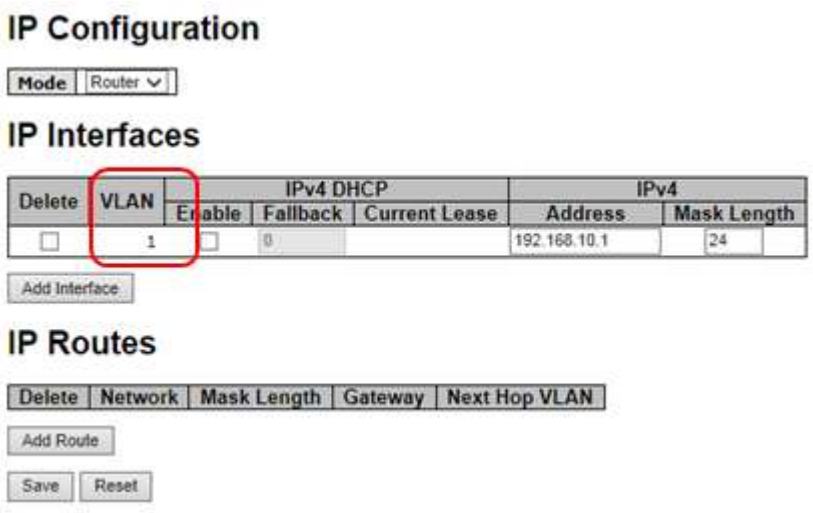


Figure 80 – IP Configuration

5.5.3 Private VLAN

A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains, allowing the user to isolate the ports on the switch from each other.
This page is used for configuring the private VLAN membership configuration.

5.5.3.1 Private VLAN Membership Configuration

Private VLANs can be added or deleted, and port members of each private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and private VLAN IDs can be identical. A port must be a member of both a VLAN and a private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and private VLAN 1.

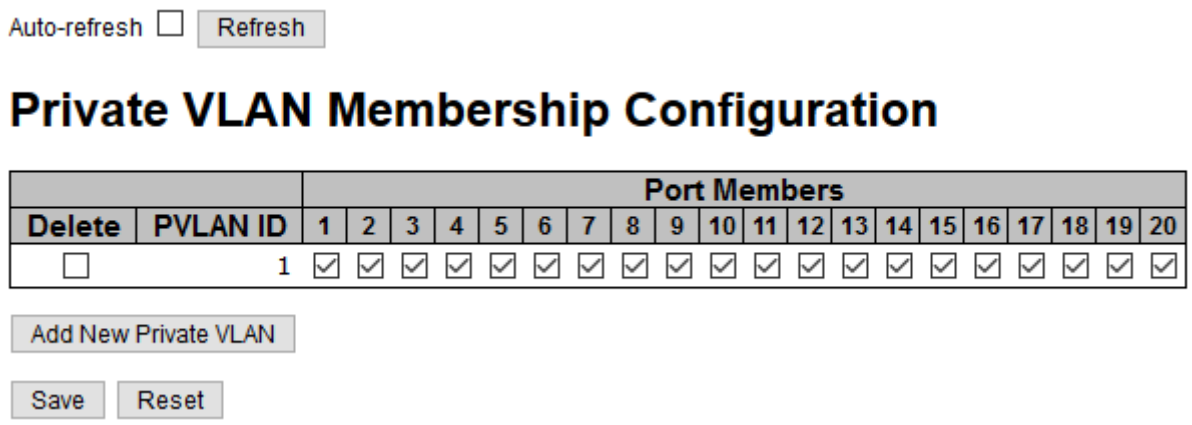


Figure 81 – Private VLAN Membership Configuration

A VLAN-unaware port can only be a member of one VLAN, but it can be a member of multiple private VLANs.

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Private VLAN ID	Indicates the ID of this particular private VLAN.
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 Private VLAN	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.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page immediately

5.5.3.2 Port Isolation Configuration

This page is used for enabling or disabling port isolation on ports in a Private VLAN (PVLAN). An isolated port cannot communicate with other ports within the same PVLAN.

A port member of a VLAN can be isolated from other isolated ports on the same VLAN and Private VLAN.

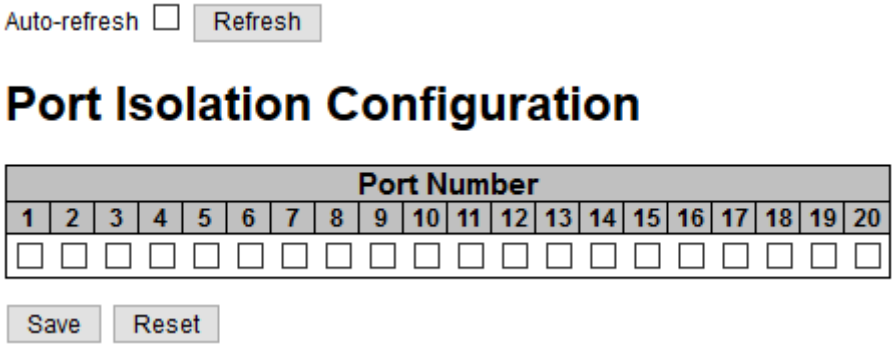


Figure 82 – Port Isolation Configuration

Label	Description
Port Number	A check box is provided for each port of a private VLAN. 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.
Refresh	Click to refresh the page immediately.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.6 SNMP

SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture and enables network management systems to learn of network problems by receiving traps or change notices from network devices implementing SNMP.

5.6.1 SNMP System Configurations

Configure SNMP on this page.

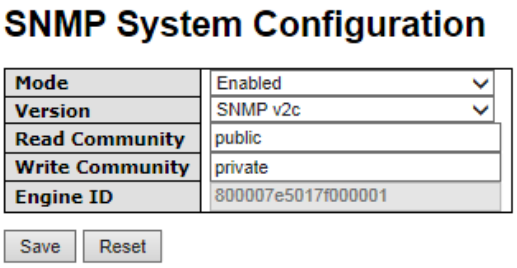


Figure 83 – SNMP System Configuration

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	Indicates the read community string for permitting access to SNMP agent. The allowed string length is 0 to 255, and only ASCII characters from 33 to 126 are allowed. The field is applicable only when SNMP version is SNMPv1 or SNMPv2c. SNMPv3 uses User-based Security Model (USM) for authentication and privacy, and the community string will be associated with SNMPv3 communities table. It provides more flexibility to configure security name than a SNMPv1 or SNMPv2c community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.
Write Community	Indicates the write community string to permit access to SNMP agent. The allowed string length is 0 to 255, and only ASCII characters from 33 to 126 are allowed. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 uses USM for authentication and privacy and the community string will be associated with SNMPv3 community table.
Engine ID	Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

5.6.1.1 SNMP Trap Configuration

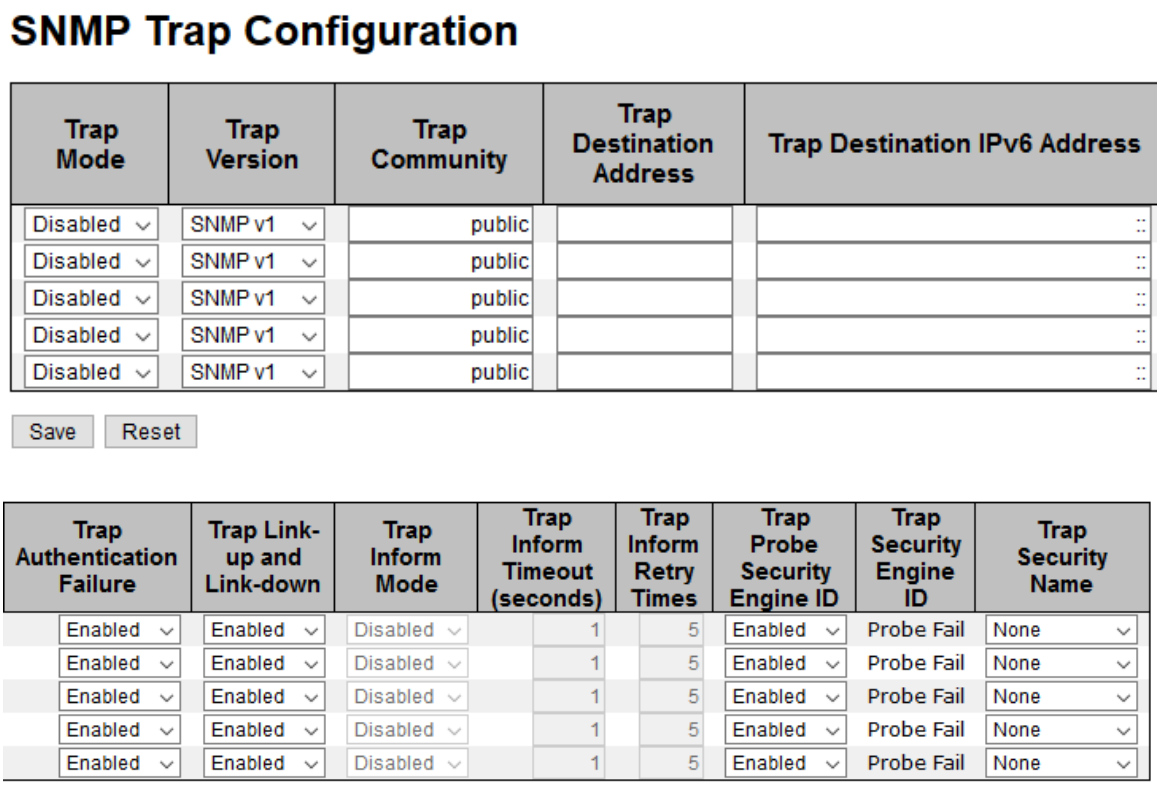


Figure 84 – SNMP Trap Configuration

Label	Description
Trap Mode	Indicates existing SNMP mode operation. 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	Indicates the community access string when sending SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126. community string. In addition to community string, a particular range of source addresses can be used to restrict source subnet.
Trap Destination Address	Indicates the SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w').
Trap Destination IPv6 Address	Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.

Label	Description
Trap Authentication Failure	Indicates that the SNMP entity is permitted to generate authentication failure traps. Possible modes are: **Enabled:** Enable SNMP trap authentication failure. **Disabled:** Disable SNMP trap authentication failure.
Trap Link-up and Link-down	Indicates the SNMP trap link-up and link-down mode operation. Possible modes are: **Enabled**: Enable SNMP trap link-up and link-down mode operation. **Disabled**: Disable SNMP trap link-up and link-down mode operation.
Trap Inform Mode	Indicates the SNMP trap inform mode operation. Possible modes are: **Enabled**: Enable SNMP trap inform mode operation. **Disabled**: Disable SNMP trap inform mode operation.
Trap Inform Timeout (seconds)	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.
Trap Inform Retry Times	Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.
Trap Probe Security Engine ID	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: Enabled: Enable SNMP trap probe security engine ID mode of operation. Disabled: Disable SNMP trap probe security engine ID mode of operation.
Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When **Trap Probe Security Engine ID** is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed.
Trap Security Name	Indicates the SNMP trap security name. SNMPv3 traps and informs using (user-based security method (USM) for authentication and privacy. A unique security name is needed when traps and informs are enabled.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.6.2 SNMP Community Configurations

This page allows the user to configure SNMPv3 community table. The entry index key is **Community.**

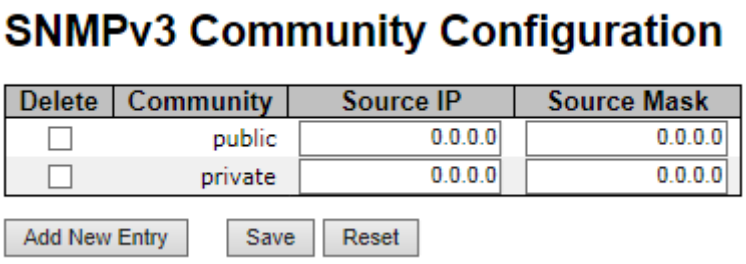


Figure 85 – SNMPv3 Community Configuration

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Community	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.
Source IP	Indicates the SNMP source address.
Source Mask	Indicates the SNMP source address mask.
Add New Entry	Click to add a new community configuration.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.6.3 SNMP User Configurations

This page allows the user to configure SNMPv3 user table. The entry index keys are **Engine ID** and **User Name**.

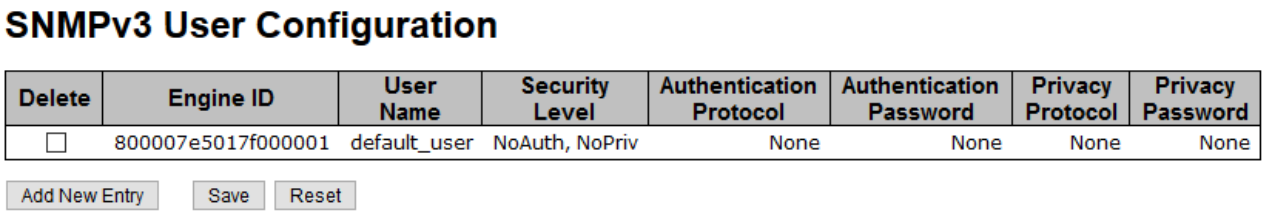


Figure 86 – SNMPv3 User Configuration

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number(in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user; otherwise it's remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Label	Description
Security Level	Indicates the security model that this entry should belong to. Possible security models include: **NoAuth, NoPriv**: no authentication and none privacy **Auth, NoPriv**: Authentication and no privacy **Auth, Priv**: Authentication and privacy 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 Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols include: **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 that this entry should belong to. Possible privacy protocols include: **None**: no privacy protocol **DES**: an optional flag to indicate that this user is using DES authentication protocol **AES**: An optional flag to indicate that this user uses AES 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.

5.6.4 SNMP Group Configurations

This page allows the user to configure SNMPv3 group table. The entry index keys are **Security Model** and **Security Name.**

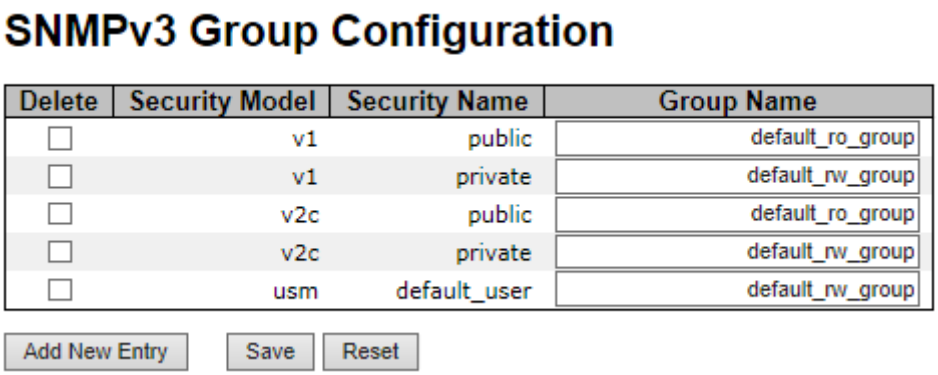


Figure 87 – SNMPv3 Group Configuration

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 included: **v1**: Reserved for SNMPv1. **v2c**: Reserved for SNMPv2c. **usm**: User-based Security Model (USM).
Security Name	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
Add New Entry	Click to add a new group configuration.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.6.5 SNMP View Configurations

This page allows the user to configure SNMPv3 view table. The entry index keys are **View Name** and **OID Subtree**.

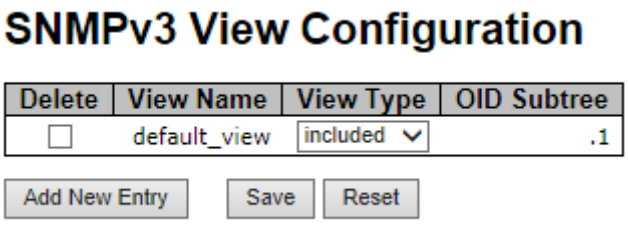


Figure 88 – SNMPv3 View Configuration

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and 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**: an optional flag to indicate that this view subtree should be included. **Excluded**: An optional flag to indicate that this view subtree should be excluded. Generally, if an entry's view type is **Excluded**, it should exist in another entry whose view type is **Included, and** its OID subtree oversteps the **Excluded** entry.
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk (*).
Add New Entry	Click to add a new view configuration.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.6.6 SNMP Access Configurations

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

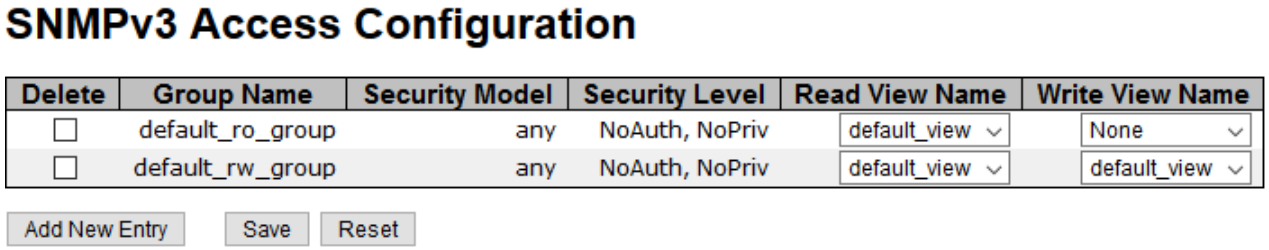


Figure 89 – SNMPv3 Access Configuration

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
Security Model	Indicates the security model that this entry should belong to. The 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. The security models include: **NoAuth, NoPriv**: no authentication and no privacy **Auth, NoPriv**: Authentication and no privacy **Auth, Priv**: Authentication and privacy
Read View Name	The names of the MIB view identifies the MIB objects for which this request may request the current values. The allowed string length is1 to 32, and only ASCII characters from 33 to 126 are allowed.

Label	Description
Write View Name	The names of the MIB view defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
Add New Entry	Click to add a new access configuration.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.7 Traffic Prioritization

5.7.1 Storm Control

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Storm Control is a feature which monitors incoming traffic levels over a 1-second traffic storm control interval and, during the interval, compares the traffic level with the configured traffic storm control level. When the ingress traffic reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends. [11]

There is a unicast storm, multicast storm, and a broadcast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

Storm control for the switch is configured on this page. The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch. Note: The Storm Control doesn't function in managed VLAN. For managed VLAN, use ACL (see 5.9.3 ACL) to limit traffic storms.

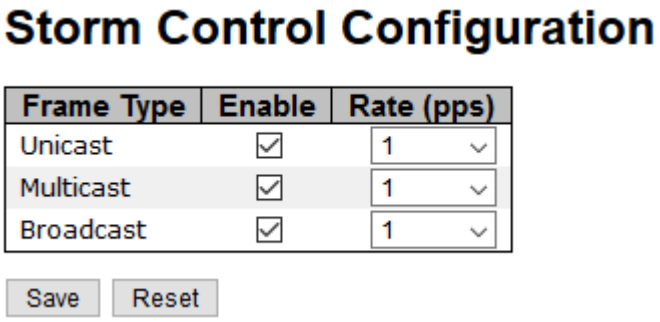


Figure 90 - QoS Port Storm Control

Label	Description
Frame Type	The settings in a particular row apply to the frame type listed here: Unicast, Multicast or Broadcast.
Rate	The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.7.2 Port Classification

Quality of service (QoS) is a method for achieving efficient bandwidth utilization between individual applications or protocols. QoS consists of the following key components:

- Classification—the process of distinguishing one type of traffic from another based upon access control lists (ACLs), Differentiated Services Code Point (DSCP), Class of Service (CoS), and other factors.
- Marking —used on traffic to convey specific information to a downstream device in the network, or to carry information from one interface in a device to another. When traffic is marked, QoS operations on that traffic can be applied.
- Shaping and policing— Shaping is the process of imposing a maximum rate of traffic, while regulating the traffic rate in such a way that downstream devices are not subjected to congestion. Shaping in the most common form is used to limit the traffic sent from a physical or logical interface. Policing is used to impose a maximum rate on a traffic class. If the rate is exceeded, then a specific action is taken as soon as the event occurs.
- Queuing used to prevent traffic congestion. Traffic is sent to specific queues for servicing and

scheduling based upon bandwidth allocation. Traffic is then scheduled or sent out through the port.

- Bandwidth—bandwidth allocation determines the available capacity for traffic that is subject to QoS policies.
- Trust—enables traffic to pass through the device, and the Differentiated Services Code Point (DSCP), precedence, or CoS values coming from the end points are retained in the absence of any explicit policy configuration. [9]

This page allows the user to configure the basic QoS Ingress Classification settings for all switch ports.

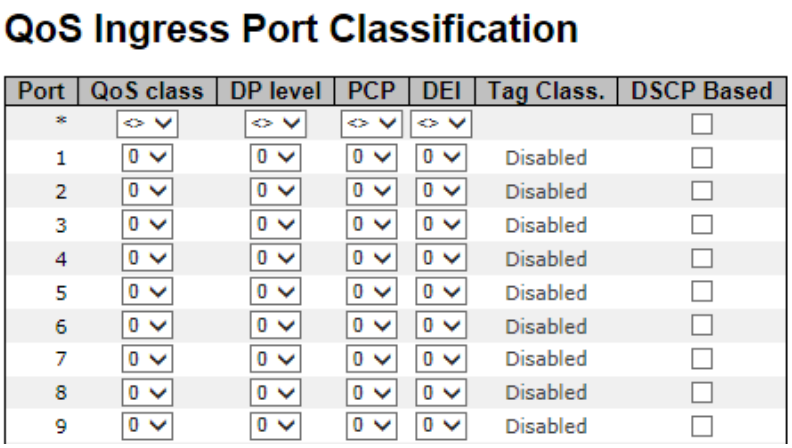


Figure 91 - QoS Ingress Port Classification

Label	Description
Port	The port number for which the configuration below
QoS Class	Controls the default QoS class Every incoming frame is 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. [1] 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 (DP) 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 (QoS Control List) QCL entry.
PCP	Controls the default PCP value. PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority. 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. DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag. 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.

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

5.7.3 Port Tag Remarking

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

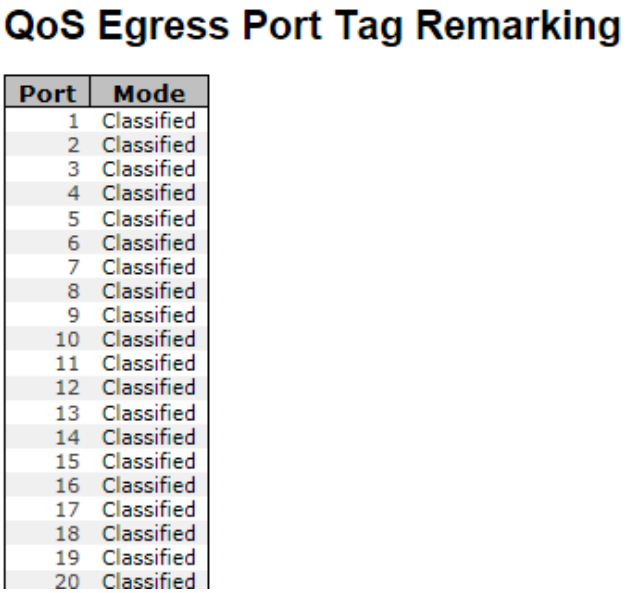


Figure 92 - QoS Egress Port Tag Remarking

Label	Description
Port	The logical port for the settings contained in the same row. Click 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.

5.7.4 Port DSCP

DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

This page allows the user to configure basic QoS Port DSCP Configuration settings for all switch ports.

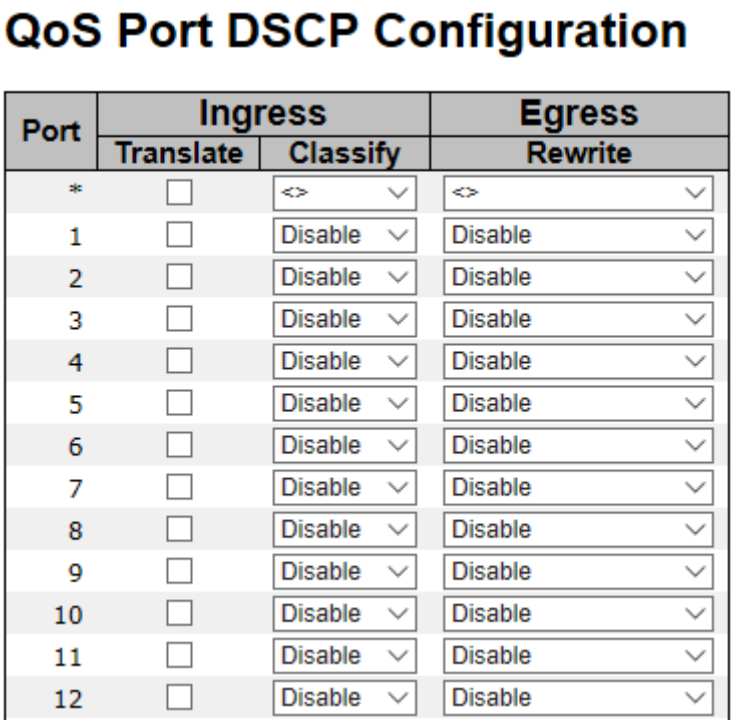


Figure 93 - QoS Port DSCP Configuration

Label	Description
Port	Shows the list of ports for which you can configure DSCP Ingress and Egress settings.
Ingress	**Ingress** settings allow you to change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: 1. **Translate** 2. **Classify**
Translate	Check to enable ingress translation
Classify	Classification has 4 different values. **Disable:** no Ingress DSCP classification **DSCP=0:** classify if incoming (or translated if enabled) DSCP is 0. **Selected:** classify only selected DSCP 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:**DSCP from the analyzer is remapped and the frame is remarked with remapped DSCP value.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.7.5 Port Policing

This page allows the user to configure Policer settings for all switch ports.

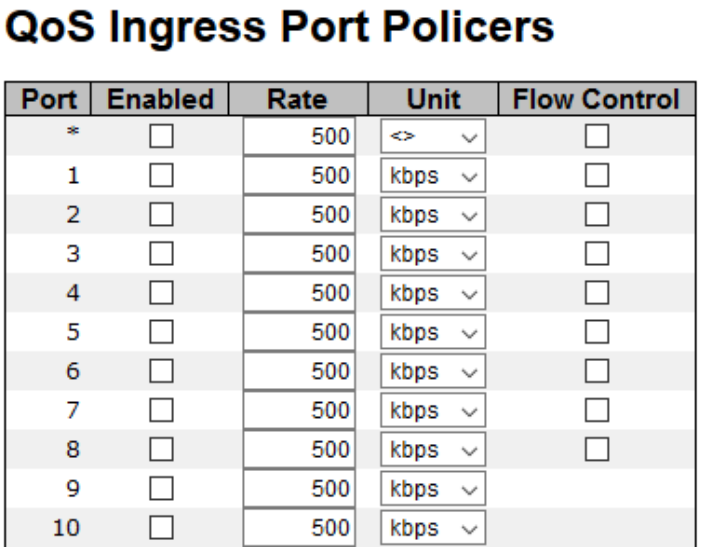


Figure 94 - QoS Ingress Port Policers

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 it is restricted to 1-13200 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 discarding frames.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.7.6 Queue Policing

This page allows the user to configure Queue Policer settings for all switch ports.

QoS Ingress Queue Policers

Port	Queue 0 Enable	Queue 1 Enable	Queue 2 Enable	Queue 3 Enable	Queue 4 Enable	Queue 5 Enable	Queue 6 Enable	Queue 7 Enable
*	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	☐	☐	☐	☐	☐	☐	☐

Figure 95 - QoS Ingress Queue Policers

Label	Description
Port	The port number for which the configuration below applies.
Enabled	Check to enable queue policer for individual switch ports
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.7.7 Port Schedulers

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

QoS Egress Port Schedulers

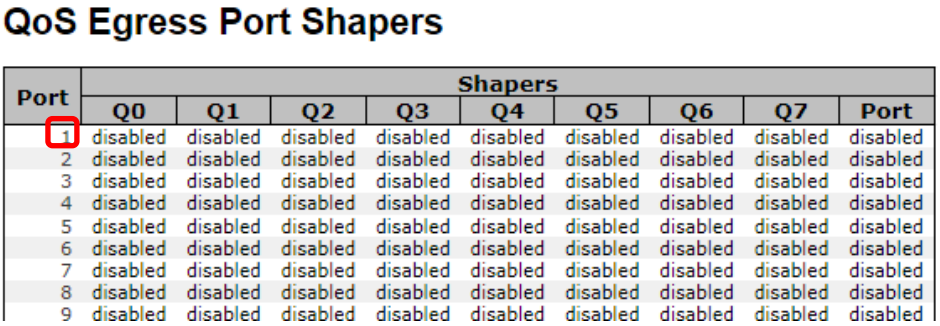
Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-

Figure 96 - QoS Egress Port Policers

Label	Description
Port	The logical port for the settings contained in the same row. Click the port number to configure the schedulers. Details for configuration can be found in the QoS Egress Port Scheduler and Shapers section.
Mode	Shows the scheduling mode for this port.
Weight	Shows the weight for this queue and port.

5.7.8 Port Shaping

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



QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

Figure 97 - QoS Egress Port Shapers

Label	Description
Port	The logical port for the settings contained in the same row. Click on the port number to configure the shapers. Details for configuration can be found in the QoS Egress Port Scheduler and Shapers section.
Shapers On	Shows **disabled** or actual port shaper rate - e.g. "800 Mbps"

5.7.8.1 QoS Egress Port Scheduler and Shapers

This page allows the user to configure Scheduler and Shapers for a specific port.

This is accessed by clicking specific port on the Port Scheduler or Shaping screen (Port 1 shown).

5.7.8.1.1 Strict Priority

In the **Scheduler Mode**, from the drop-down list, select **Strict Priority**.

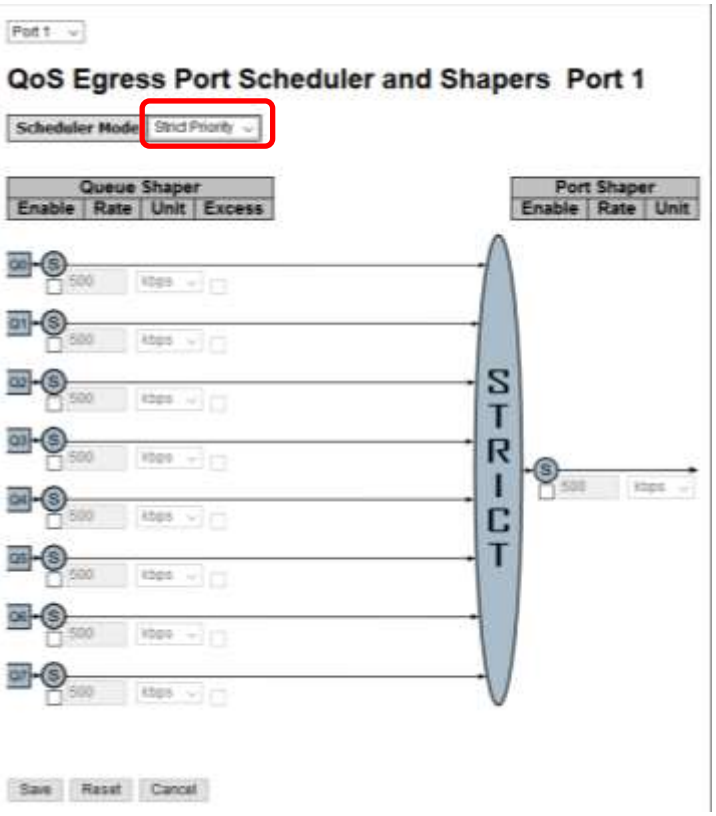


Figure 98 - QoS Ingress Port Scheduler and Shapers Port 1- Strict Priority

Label	Description
Scheduler Mode	Controls whether the scheduler mode is **Strict Priority** or **weighted** on this switch port
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** kbps**.** This value is restricted to: • 100 to 1000000 when the **Unit** is **kbps**, and 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 kbps**.** This value is restricted to: • 100 to 1000000 when the **Unit** is **kbps**, and 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 unit is **kbps**.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to the saved values.
Cancel	Click to undo any changes made locally and return to the previous page.

5.7.8.1.2Weighted

In the **Scheduler Mode**, from the drop-down list, select **Weighted**.

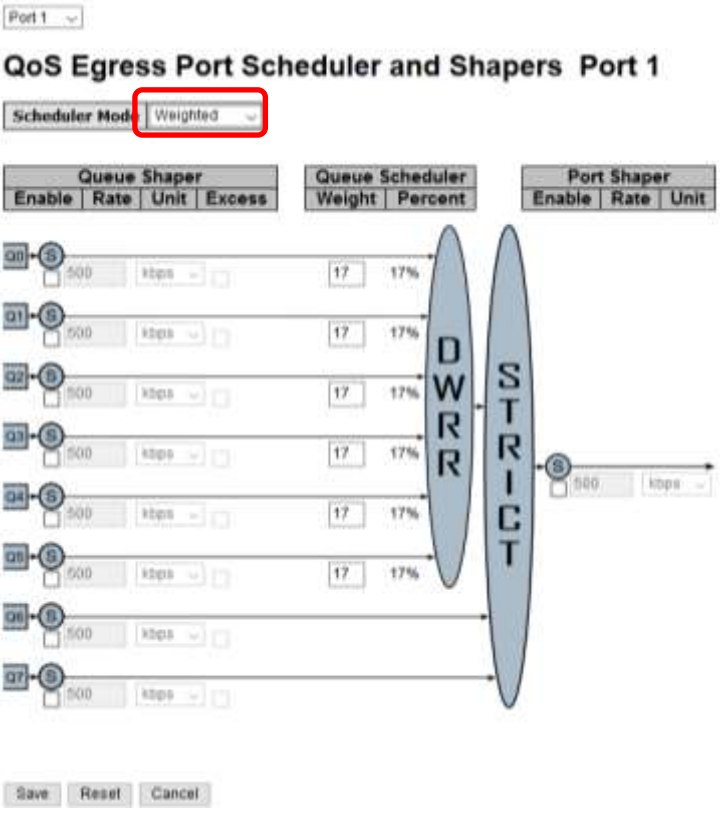


Figure 99 - QoS Egress Port Scheduler and Shapers Port 1 – Scheduler Mode Weighted

Label	Description
Scheduler Mode	Controls whether the scheduler mode is Strict Priority or Weighted on this switch port.
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 M bps. The default value is kbps.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Cancel	Click to undo any changes made locally and return to the previous page.

5.7.9 DSCP-Based QoS

This page allows the user to configure basic QoS DSCP-Based QoS Ingress Classification settings for all switches.

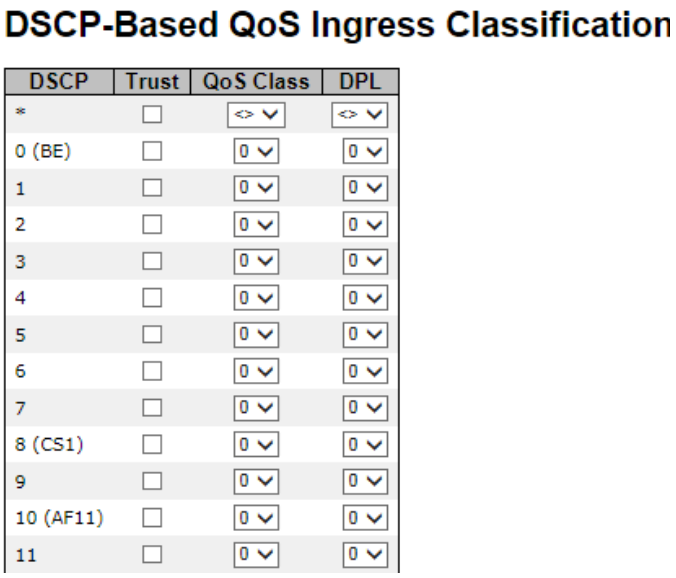


Figure 100 - QoS DSCP-Based QoS Ingress Classification

Label	Description
DSCP	Maximum number of supported DSCP values is 64
Trust	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level (DP level). DP level —Every incoming frame is classified to a DP level, which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP 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. A QoS class of 0 (zero) has the lowest priority.
DPL	Drop Precedence Level (0-3); a DP level of 0 (zero) corresponds to 'Committed' (Green)
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.7.10 DSCP Translation

To preserve the proper QoS Level of the packet and avoid high priority packets from being delayed or dropped, a DSCP translation policy for traffic can be used. When a DSCP translation policy is enabled, the QoS Level value is converted to a DSCP value according to the specified mapping rules. [8]

This page allows the user to configure basic QoS DSCP translation settings for all switches. DSCP translation can be done in **Ingress** or **Egress**.

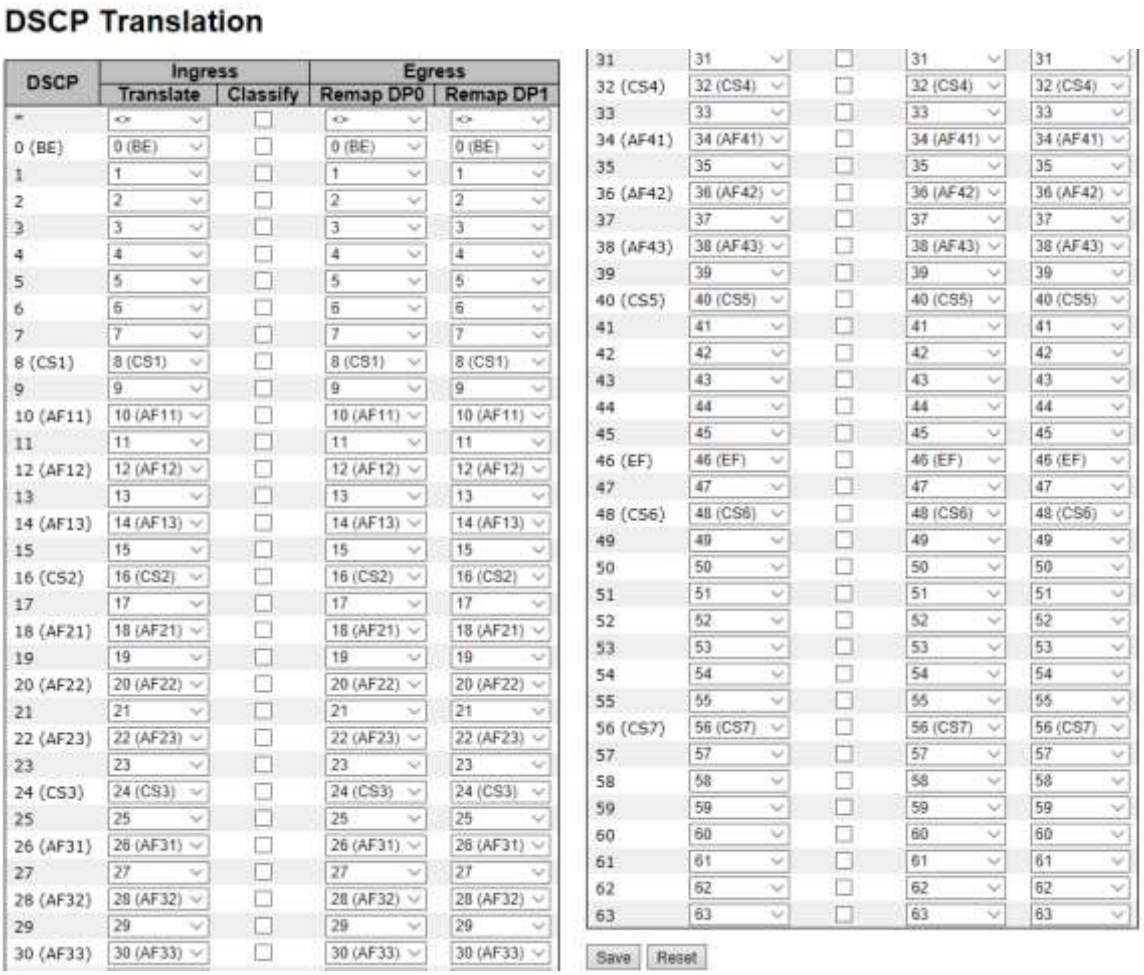


Figure 101 - DSCP Translation

Label	Description
DSCP	Maximum number of supported DSCP values is 64. Valid DSCP values are 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 configuration parameters for DSCP Translation: 1. **Translate:** DSCP can be translated to any of (0-63) DSCP values. 2. **Classify:** check to enable ingress classification
Egress	The configurable parameters for Egress side are as follows: 1. **Remap DP0** —controls the remapping for frames with DP level 0. Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63. 2. **Remap DP1** —controls the remapping for frames with DP level 1. Select the DSCP value from select menu to which you want to remap. DSCP value ranges form 0 to 63.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.7.11 DSCP Classification

This page allows the user to configure the mapping of QoS class to DSCP value.

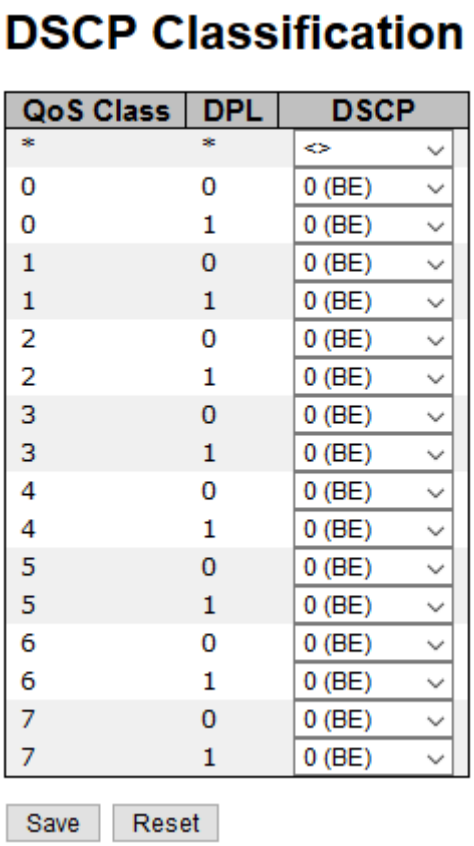


Figure 102 - DSCP Classification

Label	Description
QoS Class	Actual QoS class. A QoS class of 0 (zero) has the lowest priority.
DPL	Actual Drop Precedence Level.
DSCP	Select the classified DSCP value (0-63)
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.7.12 QoS Control List

This page shows the QoS Control List (QCL), which is made up of the QCEs. Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch. Click on the plus sign (as seen below in the right corner) to add a new QCE to the list.

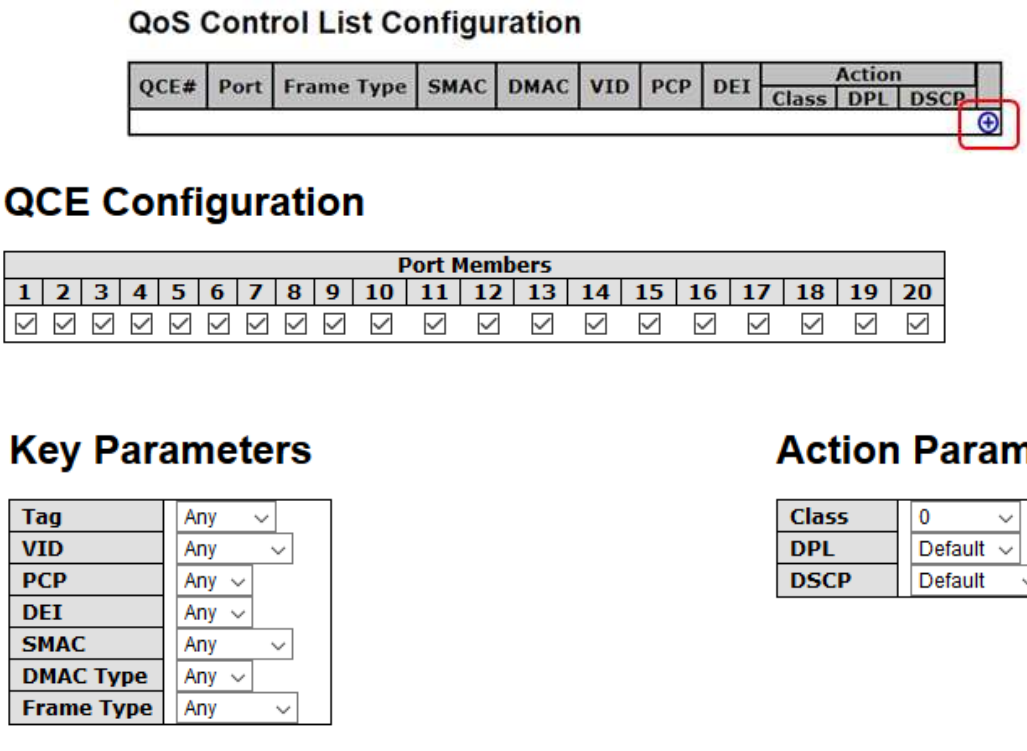


Figure 103 - QoS Control List Configuration

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**: value of tag, can be **Any**, **Untag** or **Tag**. **VID**: valid value of VLAN ID, can be any value from 1 to 4095 or **Any**, a specific value **(Specific)** or a **Range** of VIDs. **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 **0, 1** or **Any** **SMAC**: Source MAC Address, can be **specific** (xx-xx-xx, 24 MS bits OUI) or **Any** **DMAC Type**: Destination MAC type, can be **unicast** (**UC**), **multicast** (**MC**), **broadcast** (**BC**) or **Any** **Frame Type** can be values such as **Any, Ethernet, LLC, SNAP, IPv4, IPv6**
Frame Type	
Any	Allow all types of frames
Ethernet	Valid Ethernet values can range from 0x600 to 0xFFFF or Any' but excluding 0x800(IPv4) and 0x86DD(IPv6). The default value is Any.

Label	Description
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 Control: valid values can range from 0x00 to 0xFF or Any. The default value is Any.
SNAP	**PID**: valid PID (aka ethernet type) values can range from 0x00 to 0xFFFF or Any. The default value is Any.
IPv4	**Protocol** IP Protocol Number: (0-255, TCP or UDP) or Any **Source IP**: specific Source IP address in value/mask format or Any. IP and mask are in the format of 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**: Ipv4 frame fragmented options include 'yes', 'no', and 'any'. **DSCP** (Differentiated Code Point): 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.
IPv6	**Protocol IP protocol number**: Other (0-255), TCP, UDP, or Any **Source IP IPv6 source address**: (a.b.c.d) or Any, 32 LS bits **DSCP (Differentiated Code Point)**: 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 (0-3) 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.

5.7.13 QoS Statistics

This page provides the statistics of individual queues for all switch ports.

Queuing Counters

Auto-refresh ☐ Refresh Clear

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	2124	41811	0	0	0	0	0	0	0	0	0	0	0	0	0	33980
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	570891	2266	0	0	0	0	0	0	0	0	0	0	0	0	0	411057
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	8210194	38198	0	0	0	0	0	0	0	0	0	0	0	0	0	194
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	75069	8737967	0	0	0	0	0	0	0	0	0	0	0	0	0	403538
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 104 - QoS Statistics

Label	Description
Port	The logical port number for the statistics displayed. Click a port number to see detailed port statistics. See 5.7.13.1 for an example of Detailed Port Statistics Port
Qn	There are 8 QoS queues per port. Q0 is the lowest priority.
Rx / Tx	The number of received and transmitted packets per queue.
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.

5.7.13.1 Detailed Port Statistics Port 7

On Figure 104 QoS Statistics, go to Port 9 (identified with a red rectangle) and click it. The following page appears.

Detailed Port Statistics Port 9

Port 9 Auto-refresh Refresh Clear

Receive Total		Transmit Total	
Rx Packets	572128	Tx Packets	414178
Rx Octets	121665738	Tx Octets	155829801
Rx Unicast	502990	Tx Unicast	374735
Rx Multicast	63744	Tx Multicast	38816
Rx Broadcast	5394	Tx Broadcast	627
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	334853	Tx 64 Bytes	35391
Rx 65-127 Bytes	2081	Tx 65-127 Bytes	88543
Rx 128-255 Bytes	39531	Tx 128-255 Bytes	187091
Rx 256-511 Bytes	187479	Tx 256-511 Bytes	2769
Rx 512-1023 Bytes	8184	Tx 512-1023 Bytes	81187
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	19197
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	572128	Tx Q0	2273
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	411905
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	1		

Figure 105 - Detailed Port Statistics Port 9

5.7.14 QCL Status

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

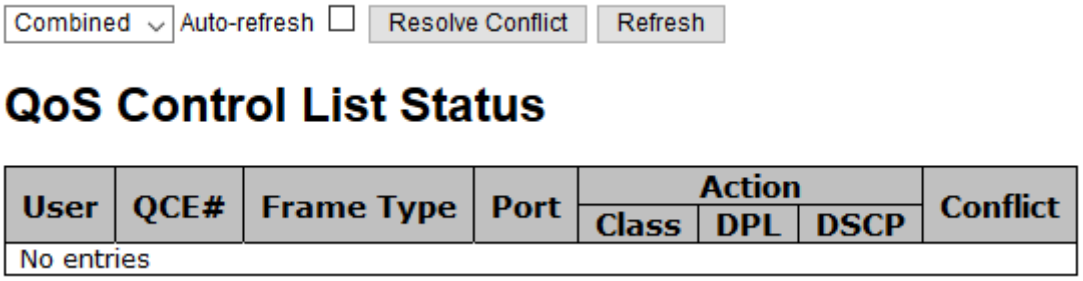


Figure 106 - QoS Control List Status

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 be 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.
QCL status	Select one of the following to be displayed: **Combined**: Show both static and conflict entries. **Static:** Show static entries. **Conflict:** Show conflict entries.
Clear	Clear all statistics counters.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page.

5.8 Multicast

5.8.1 IGMP Snooping Basic Configuration

Internet Group Management Protocol (IGMP) is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IPv4 multicast specification, such as ICMP for unicast connections.

IGMP Snooping is the process of listening to IGMP network traffic. The feature allows a network switch to listen to the IGMP conversation between hosts and routers. By listening to these conversations, the switch maintains a map of which links need which IP multicast (IPMC) streams.

This page provides IGMP Snooping related configurations.

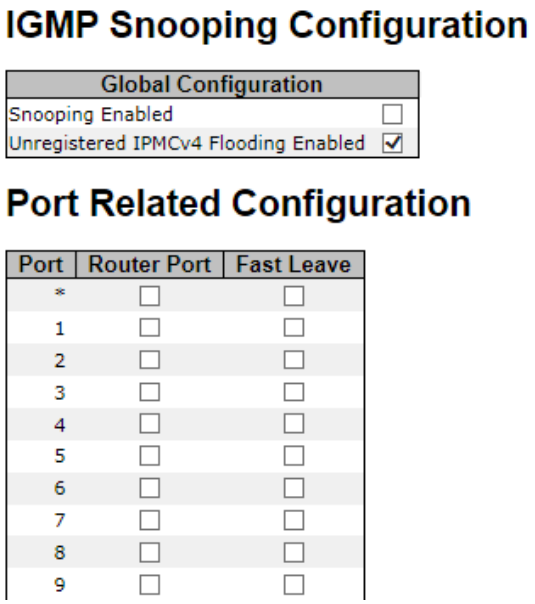


Figure 107 - IGMP Snooping Configuration

Label	Description
Snooping Enabled	Check to enable global IGMP snooping
Unregistered IPMCv4 Flooding enabled	Check to enable unregistered IPv4 MultiCast (IPMCv4) traffic flooding. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.
Router Port	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. Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.8.2 IGMP Snooping VLAN Configurations

Each page shows up to 99 entries from the VLAN 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 VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The **VLAN** input field allows the user to select the starting point in the VLAN Table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest VLAN Table match.

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

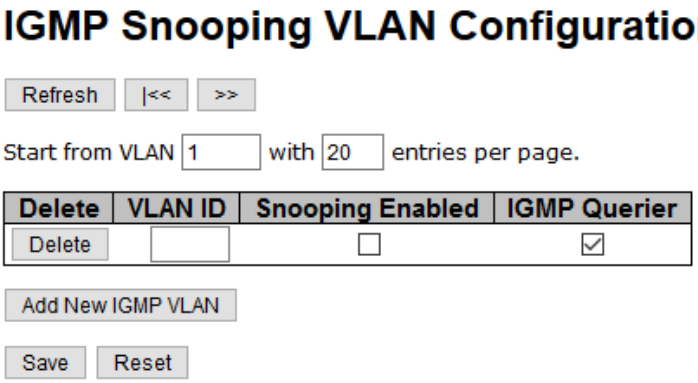


Figure 108 - IGMP Snooping VLAN Configuration

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.
Snooping Enabled	Check to enable IGMP snooping for individual VLAN. Up to 32 VLAN's can be selected.
IGMP Querier	Enable the IGMP Querier in the VLAN.
Add New IGMP VLAN	Click to add a new entry into the table.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.8.3 IGMP Snooping Status

This page provides IGMP Snooping status.

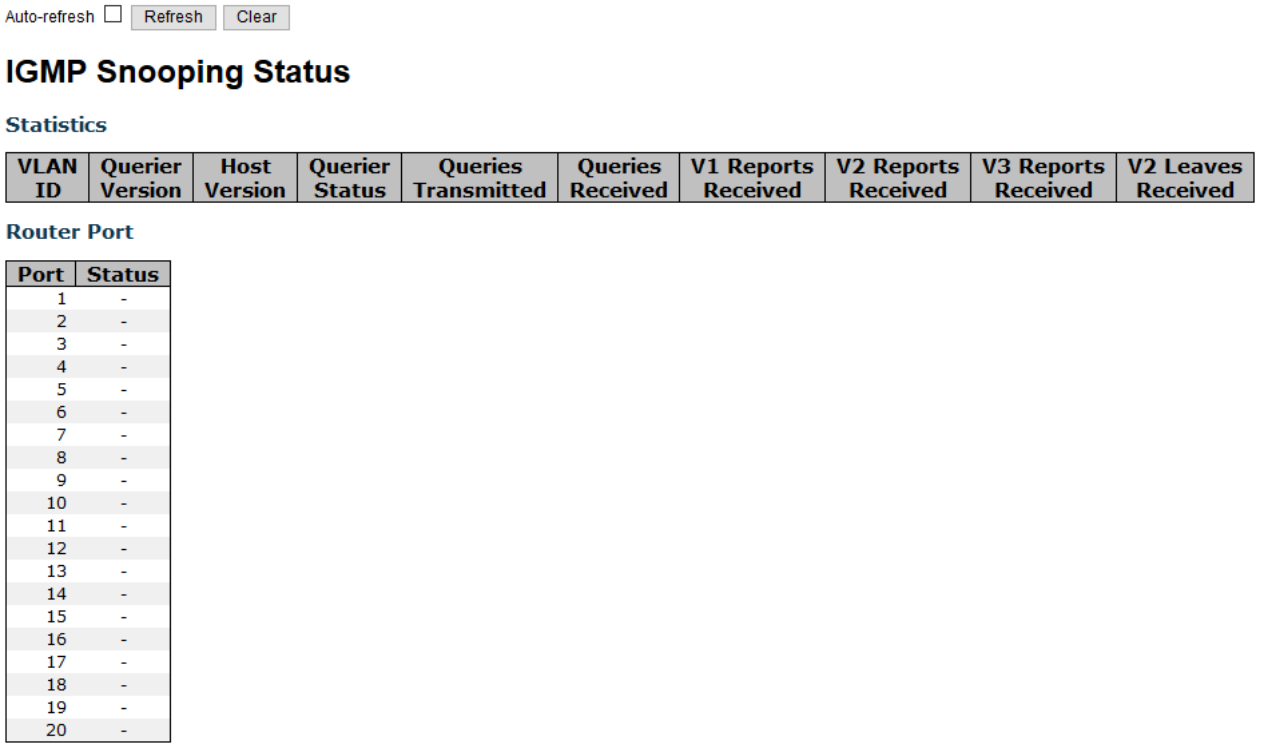


Figure 109 - IGMP Snooping Status

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 **DISABLED. DISABLE** denotes that the specific interface is administratively disabled.
Queries Transmitted	The number of transmitted Queries.
Queries Received	The number of Received Queries.
V1 Reports Received	The number of received V1 reports.
V2 Reports Received	The number of received V2 reports.
V3 Reports Received	The number of received V3 reports.
V2 Leaves Received	The number of received V2 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.
Router Port	Port number on the switch.
Router Port Status	Indicates whether a specific port is a router port or not

5.8.4 IGMP Snooping Group Information

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

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

The **Start from VLAN** and **group** input fields allow the user to select the starting point in the IGMP Group Table. Clicking **Refresh** will update the displayed table starting from that or the next closest IGMP Group Table match. In addition, the two input fields will—upon clicking **Refresh**—assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

Use the |<< button to start over.

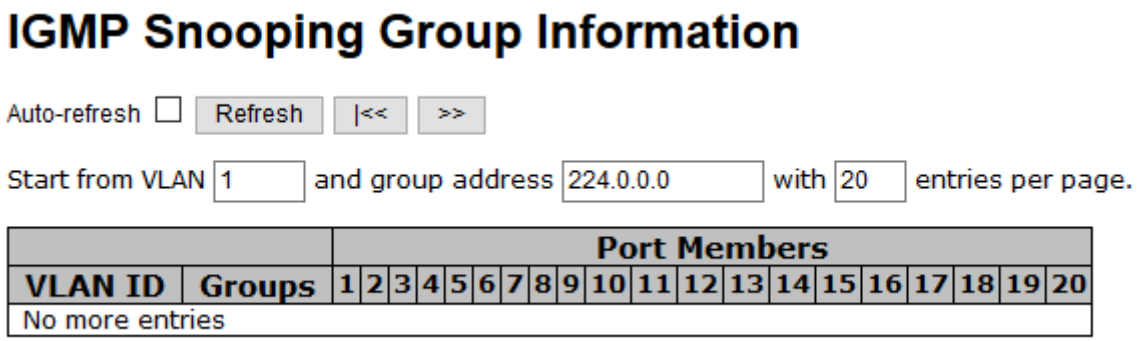


Figure 110 - IGMP Snooping Group Information

Label	Description
VLAN ID	The VLAN ID of the group.
Groups	The group address of the group displayed.
Port Members	Selected ports under this group.
Auto-refresh ☑	Automatic refresh occurs every 3 seconds.
Refresh	Refreshes the displayed table starting from the input fields.
|<<	Updates the table, starting with the first entry in the IGMP Group Table.
>>	Updates the table, starting with the entry after the last entry currently

5.9 Security

5.9.1 Remote Control Security Configuration

Remote Control Security allows the user to limit the remote access of management interface. When enabled, the request of client which is not in the allow list will be rejected.

Figure 111 - Remote Control Security Configuration

Label	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
Port	Port number of the device connecting to remote client. The options are **Any** or **Port 1, Port2**, etc.
IP	IP address of remote client. Keep this field "0.0.0.0" —it means "Any IP".
Web	Check this item to enable Web management interface..
Telnet	Check this item to enable Telnet management interface.
SNMP	Check this item to enable SNMP management interface.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.
Add new entry	Click to add a new entry

5.9.2 Device Binding

Device Binding effectively binds the IP/MAC address of the device connected with the switch port. If the IP/MAC address of the connecting device does not match the switch port binding information, the device will be blocked for security. Additionally, the bound device also benefits from a collection of active network traffic protection and maintenance tools — Alive Check, Stream Check, and DoS/DDoS auto-prevention.

This page provides Device Binding related configuration.

Device Binding

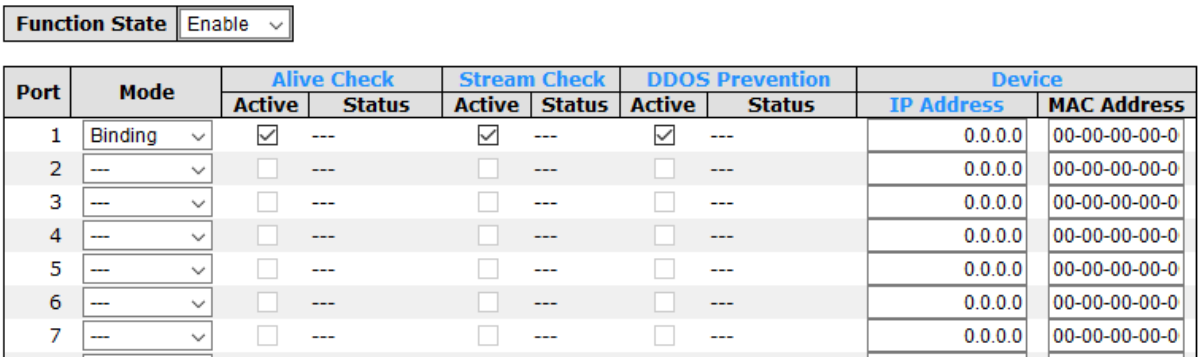


Figure 112 - Device Binding

Label	Description
Function State	Enable/Disable Device Binding.
Port	Port number of remote client.
Mode	Indicates the per-port Device Binding operation. Possible modes are: **---:** Disable. **Scan**: Scan IP/MAC automatically, but no binding function. **Binding**: Enable binding function. Under this mode, any IP/MAC not matching the entry will not be allowed to access the network. Add a checkmark to make Active Alive Check, Stream Check, and DoS/DDoS auto-prevention. **Shutdown**: Shutdown of the port (No Link).
Alive Check Active	Enable/Disable Alive Check. When enabled, switch will ping the device continually.
Alive Check Status	Indicates the Alive Check status. Possible options are: **---:** Disable. **Got Reply**: Got ping reply from device, that means the device is still alive. **Lost Reply**: Lost ping reply from device, that means the device might have been not available.
Stream Check Active	Enable/Disable Stream Check. When enabled, switch will detect the stream change(getting low) from device.
Stream Check Status	Indicates the Stream Check status. Possible statuses are: **---**: Disable. **Normal**: The stream is normal. **Low**: The stream is getting low.
DDOS Prevention Active	Enable/Disable DDOS Prevention. When enabled, switch will monitor the device for DDOS attack (from device).
DDOS Prevention Status	Indicates the DDOS Prevention status. Possible options are: **---**: Disable. **Analysing**: Analyse the packet throughput for initialization. **Running**: Function ready. **Attacked**: DDOS attack happened.
Save	Click to save changes.

5.9.2.1 Advanced Configurations

5.9.2.1.1Alias IP Address

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

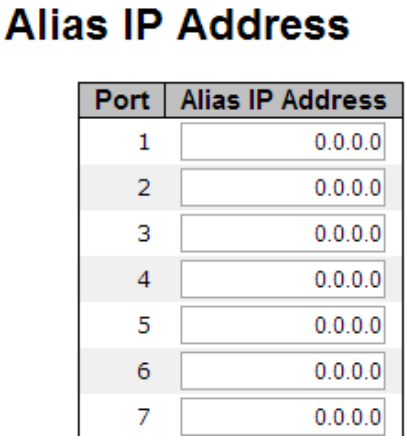


Figure 113 - Alias IP Address

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

5.9.2.1.2 Alive Check

You can use ping commands to check port link status. If port link fails, you can set actions from the list.

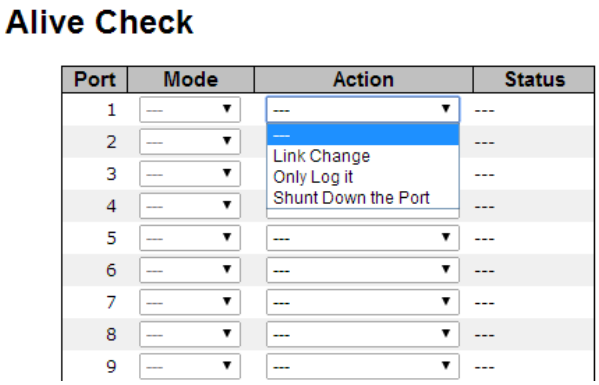


Figure 114 - Alive Check

Label	Description
Mode	Enable/Disable Alive Check of the port.
Action	Indicates the action when alive check failed. Possible actions are: **---:** Do nothing. **Link Change**: Link down the port, and link up once. Only Log it **Shunt Down the Port**: Shut down the port(No Link), and log the event. **Only Log it:** Just log the event.
Status	Indicates the Alive Check status. Possible statuses are: **---:** Disable. **Analysing:** Analyse the packet throughput for initialization. **Running**: Function ready. **Attacked**: DDOS attack happened.

5.9.2.1.3 DDOS Prevention

This page provides DDOS Prevention configurations. The switch can monitor ingress packets, and perform actions when DDOS attack occurred on this port. Configure the settings to achieve maximum protection.

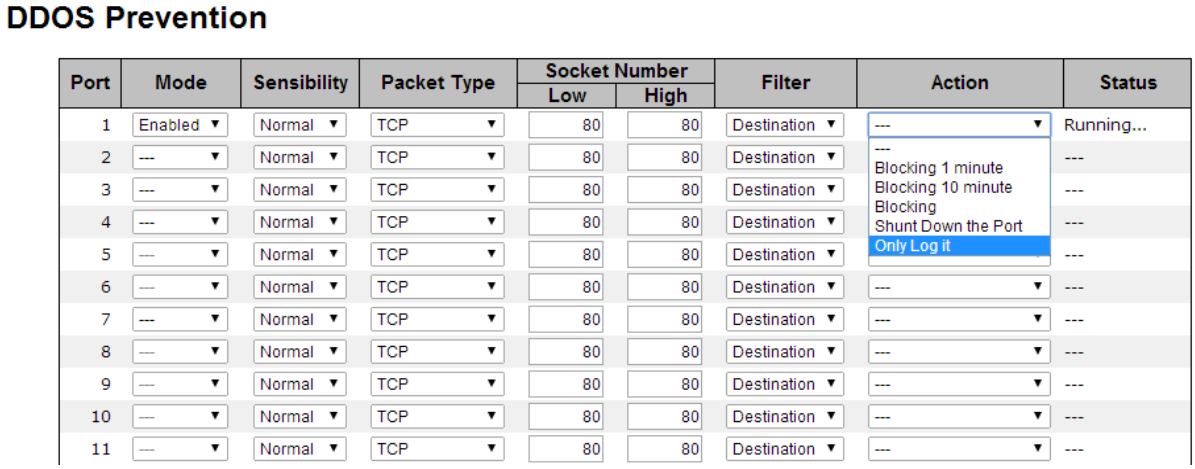


Figure 115 - DDoS Prevention

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 of numbers, from low to high, or a single number. In this case, please insert the same number.
Filter	If packet type is UDP (or TCP), 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 forwarding for 1 minute and logs the event **Blocking 10 minute**: blocks forwarding for 10 minutes and logs 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
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

5.9.2.1.4 Device Description

This page allows the user to configure device description settings.

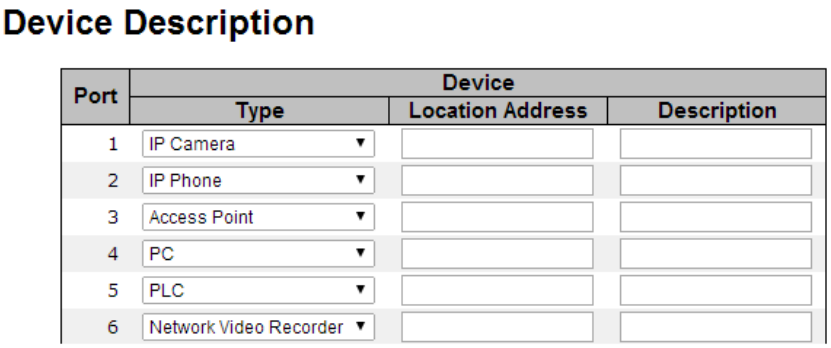


Figure 116 - Device Description

Label	Description
Device Type	Indicates device types. Possible types are: --- (no specification), **IP Camera**, **IP Phone**, **Access Point**, **PC**, **PLC**, and **Network Video Recorder**
Location Address	Indicates location information of the device. The information can be used for Google Mapping.
Description	Device descriptions

5.9.2.1.5 Stream Check

This page allows the user to configure Stream Check settings.

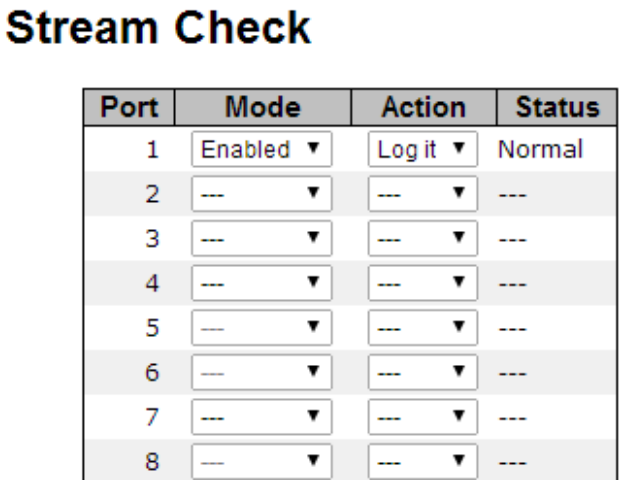


Figure 117 - Steam Check

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
Status	Indicates the Stream Check status. Possible statuses are: ---: disables Stream Check Normal: Stream Check is enabled

5.9.3 ACL

5.9.3.1 Ports

This page allows the user to configure the Access Control Entry (ACE) of each switch port. These parameters will affect frames received on a port unless the frame matches a specific ACE.

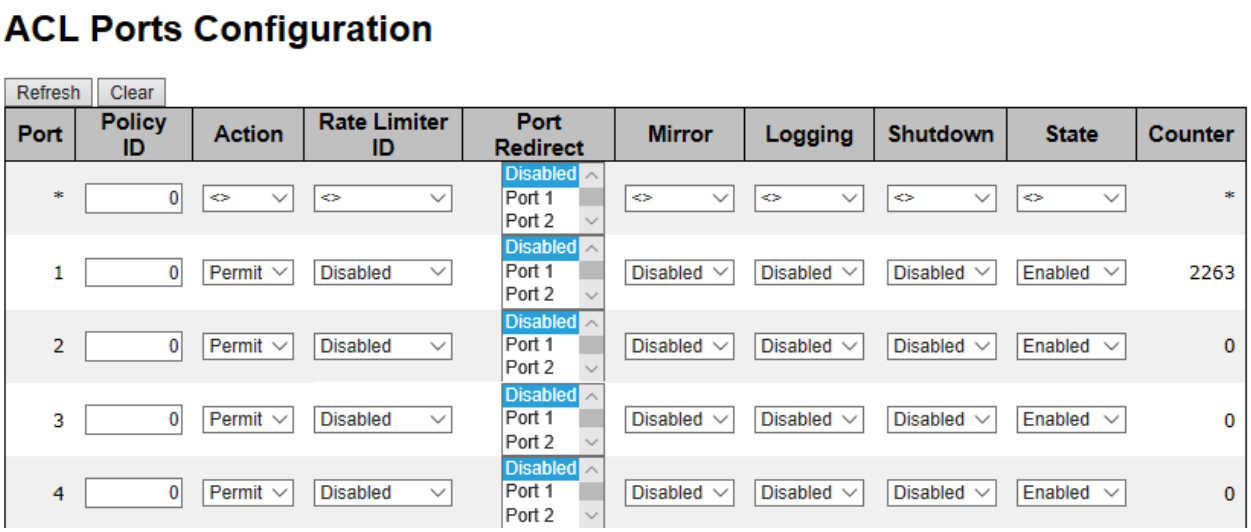


Figure 118 - ACL Ports Configuration

Label	Description
Port	The logical port for the settings contained in the same row.
Policy ID	Select the policy to apply to this port. The allowed values are `0` through `255`. The default value is 0.
Action	Select to **Permit** or **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 16**. The default value is Disabled.
Port Redirect	Select which port frames are redirected on. The allowed values are **Disabled** or a specific port number and it can't be set when action is permitted. The default value is **Disabled**.
Mirror	Specify the mirror operation of this port. The allowed values are: **Enabled**: Frames received on the port are mirrored. **Disabled**: Frames received on the port are not mirrored. The default value is "Disabled".
Logging	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.

Label	Description
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**.
State	Specify the state of this port. The allowed values are: **Enabled**: To re-open ports by changing the volatile port configuration of the ACL user module. **Disabled**: To close ports by changing the volatile port configuration of the ACL user module. The default value is **Enabled**.
Counter	Counts the number of frames that match this ACE.
Refresh	Click to refresh the page immediately.
Clear	Clear all statistics counters.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.9.3.2 Rate Limiter

This page allows the user to configure the rate limiter for the ACL of the switch.

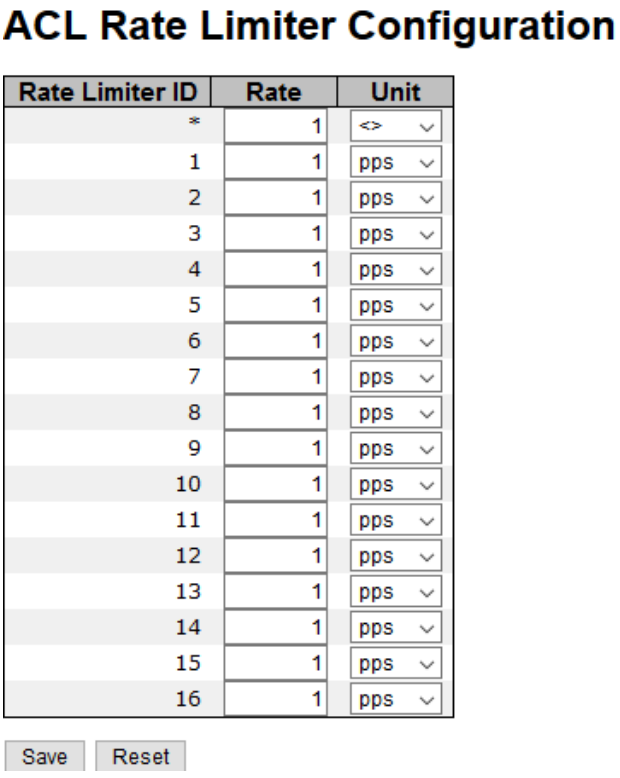


Figure 119 - ACL Rate Limiter Configuration

Label	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate	The allowed values are: 0-3276700 in pps or 0, 100, 200, 300, ..., 1000000 in kbps.

Unit	Specify the rate unit. The allowed values are: **pps**: packets per second. **kbps**: Kbits per second.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.9.3.3 Access Control List

This page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes an ACE that is defined. The maximum number of ACEs is 512 on each switch. Click on the lowest plus sign to add a new ACE to the list. The reserved ACEs used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed and the priority is highest.

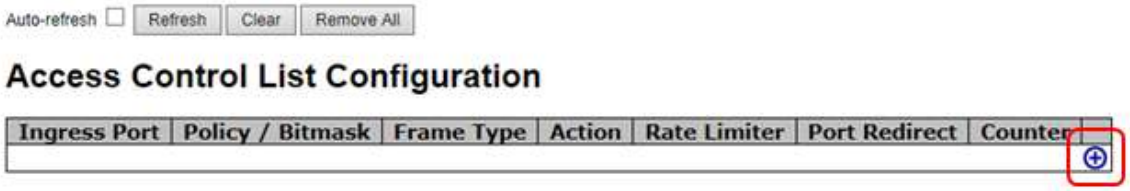


Figure 120 - ACL Control List Configuration

If you click the "+" sign, the following default ACE Configuration appears.

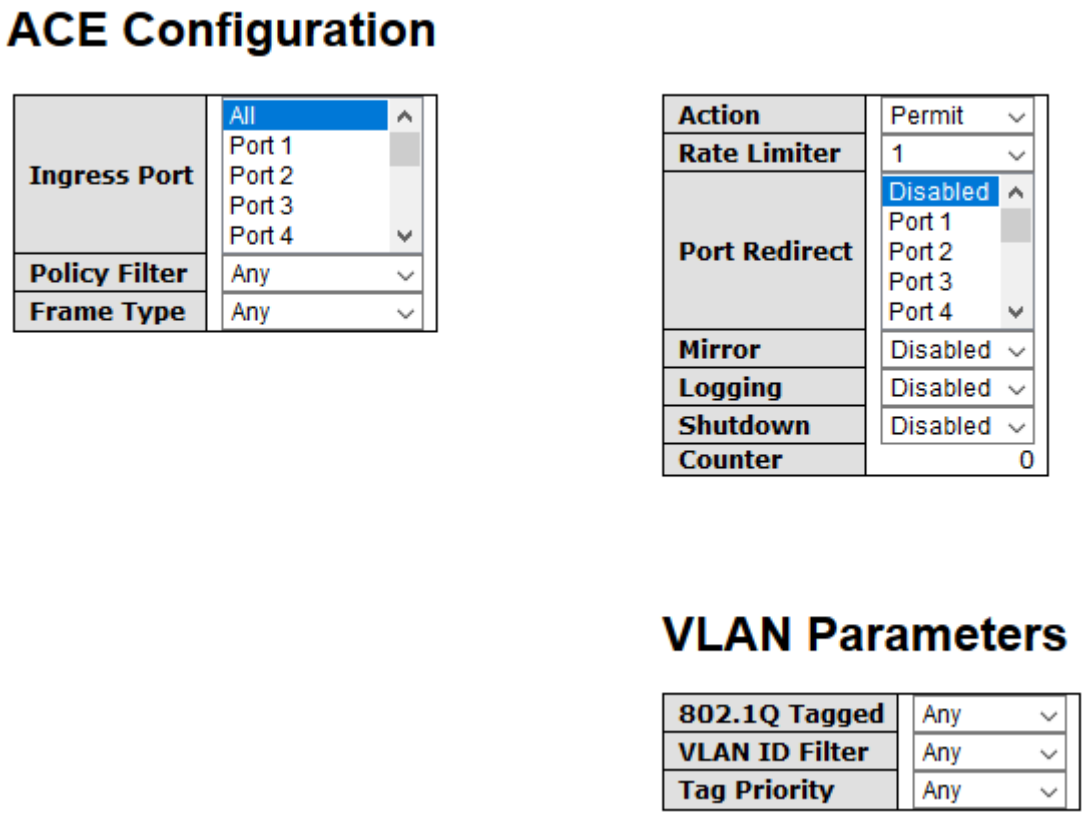


Figure 121 - Default ACE Configuration

An ACE consists of several parameters. These parameters vary with the frame type you have selected. First select the ingress port for the ACE, then the Policy Filter (if specific chosen, Policy Value and Policy Bitmask fields appear) and then the frame type. Different parameter options are displayed according to the frame type you have selected.

An ACE consists of several parameters. These parameters vary according to the selected frame type. First select the Ingress Port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type selected.

A frame that hits this ACE matches the configuration that is defined here.

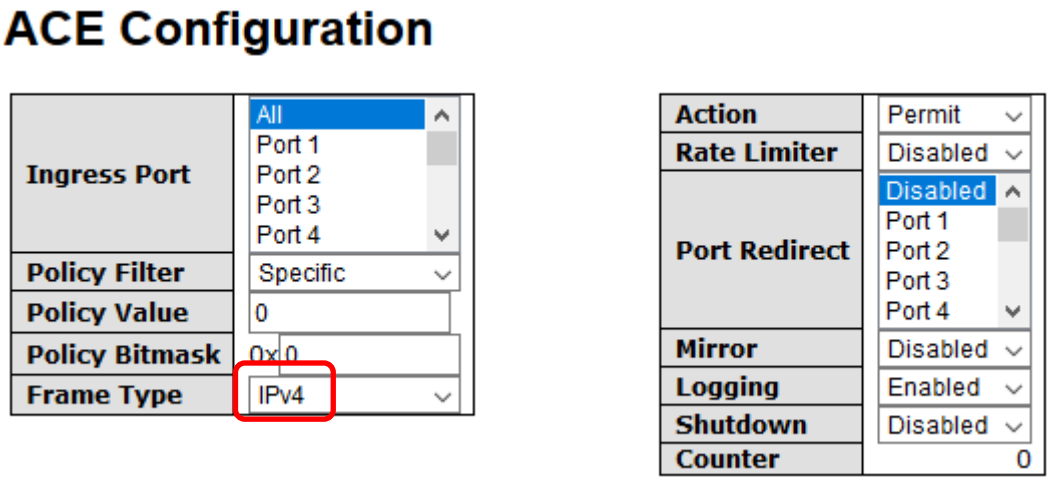


Figure 122 - ACE Configuration

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 Filter	Specify the policy number filter for this ACE. **Any:** No policy filter is specified. (policy filter status is "don't-care".) **Specific:** If you want to filter a specific policy with this ACE, choose this value. Two fields —policy value and bitmask appear. • **Policy Value**: Enter a range between 0 and 255. • **Policy Bitmask**: Enter a range between 0x0 and 0xff.
Frame Type	Indicates the frame type for this 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 describes 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 taken 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 16. **Disabled** means the rate limiter operation is disabled.

Label	Description
Port Redirect	Frames that hit the ACE are redirected to the port number specified here. The allowed range is the same as the switch port number range. `Disabled` indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted.
Mirror	Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are: **Enabled**: Frames received on the port are mirrored. **Disabled**: Frames received on the port are not mirrored. The default value is **Disabled**.
Logging	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.

5.9.3.3.1 MAC Parameters

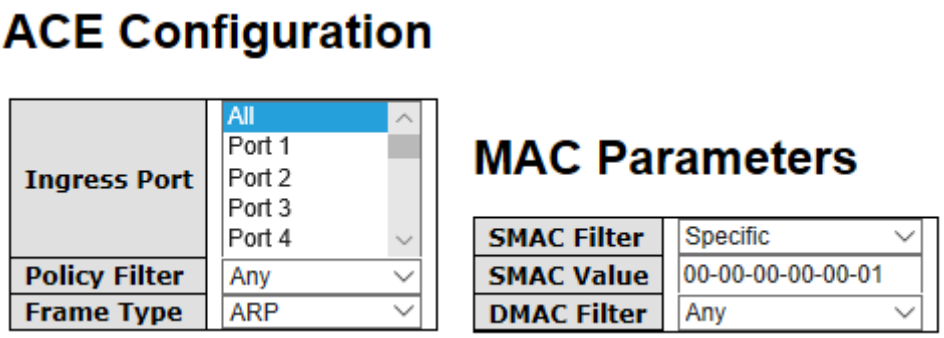


Figure 123 - MAC Parameters

Label	Description
SMAC Filter	(Only displayed when the frame type is Ethernet Type or ARP.) Specify the source MAC filter for this ACE. **Any**: No SMAC filter is specified. (SMAC filter status is "don't-care".) **Specific**: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering an SMAC value appears.
SMAC Value	When **Specific** is selected for the SMAC filter, enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.
DMAC Filter	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.

5.9.3.3.2 VLAN Parameters

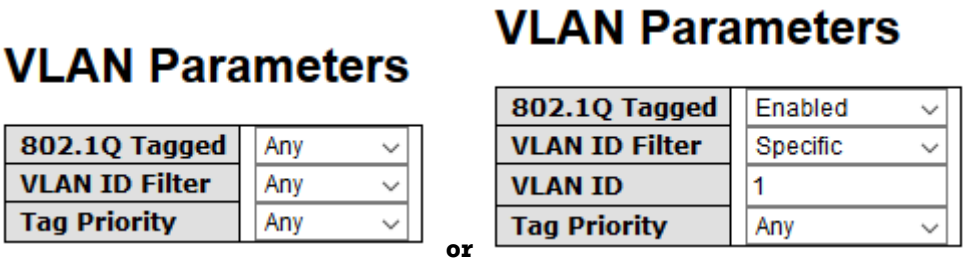


Figure 124 - VLAN Parameters (default values or with Filter "Specific")

Label	Description
802.1Q Tagged	Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are: **Any**: Any value is allowed ("don't-care"). **Enabled**: Tagged frame only. **Disabled**: Untagged frame only. The default value is Any.
VLAN ID Filter	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, the user 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 numbers are in the range from 0 to 7 **Any** means that no tag priority is specified (tag priority is "**don't-care**").

5.9.3.3.3 IP Parameters

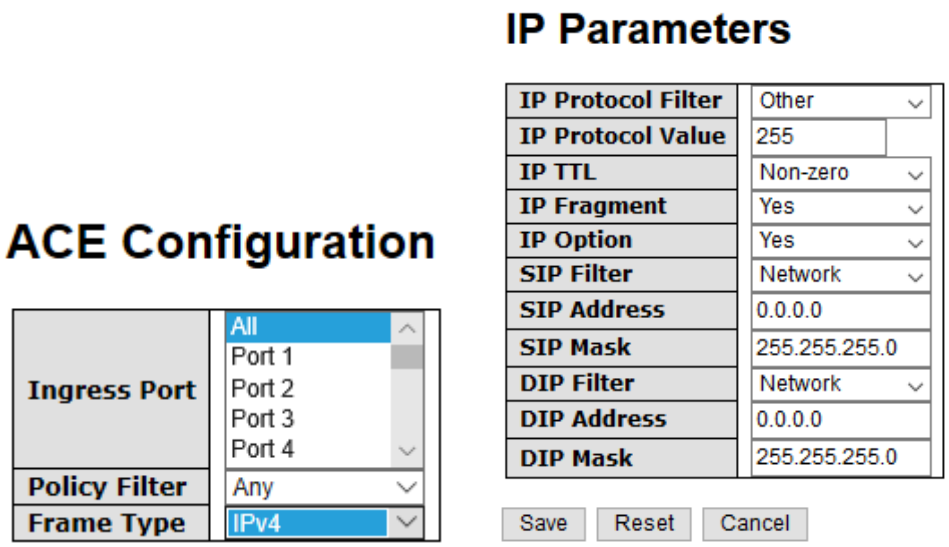


Figure 125 - IP Parameters

The IP parameters are available to be configured when Frame Type of IPv4 is selected (see Figure 122 - ACE Configuration).

Label	Description
IP Protocol Filter	Specifies the IP protocol filter for the ACE **Any:** no IP protocol filter is specified ("**don't-care**"). **Other:** 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, go to the Help file.
IP Protocol Value	**Other** allows the user 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 (TTL) 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 (SIP) 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.

Label	Description
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.

5.9.3.3.4 ARP Parameters

The ARP (Address Resolution Protocol) parameters are available to be configured when Frame Type of ARP is selected (see below).

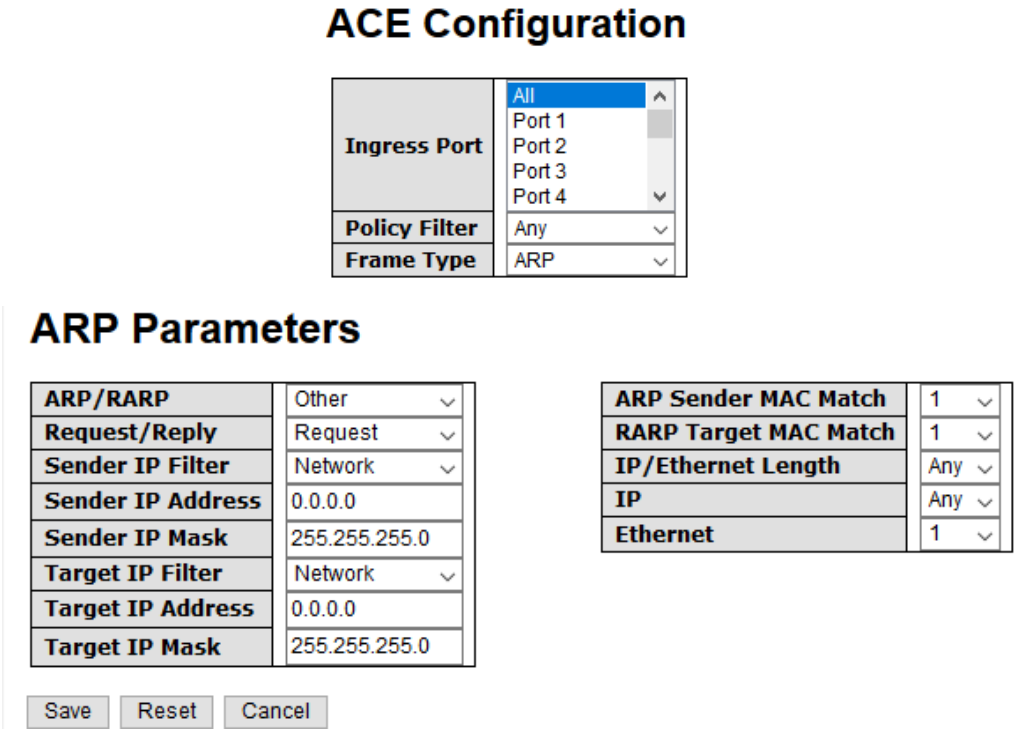


Figure 126 - ARP Parameters

Label	Description
ARP/RARP	Specifies the available ARP/RARP opcode (OP) flag for the ACE. RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP. **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.

Label	Description
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. Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets. An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.
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 Sender MAC 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 Target 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 target MAC address **1**: RARP frames where THA is equal to the target MAC address **Any**: any value is allowed ("**don't-care**")
IP/Ethernet Length	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**").

5.9.3.3.5 ICMP Parameters

ICMP Parameters can be configured when:

- Frame Type is IPv4
- IP Protocol Filter is Internet Control Message Protocol (ICMP)

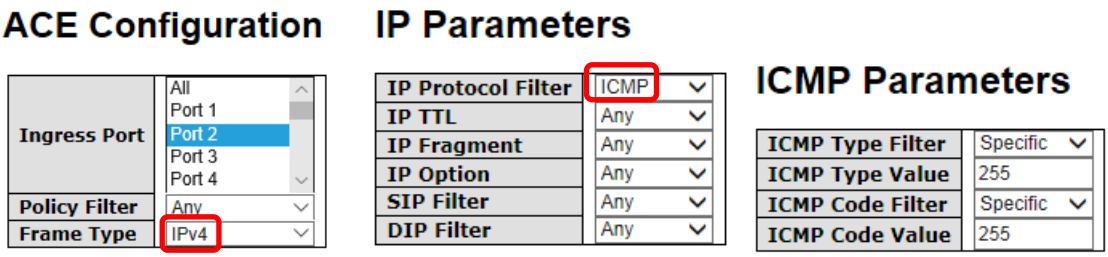


Figure 127 - ICMP Parameters

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.

5.9.3.3.6 TCP /UDP Parameters

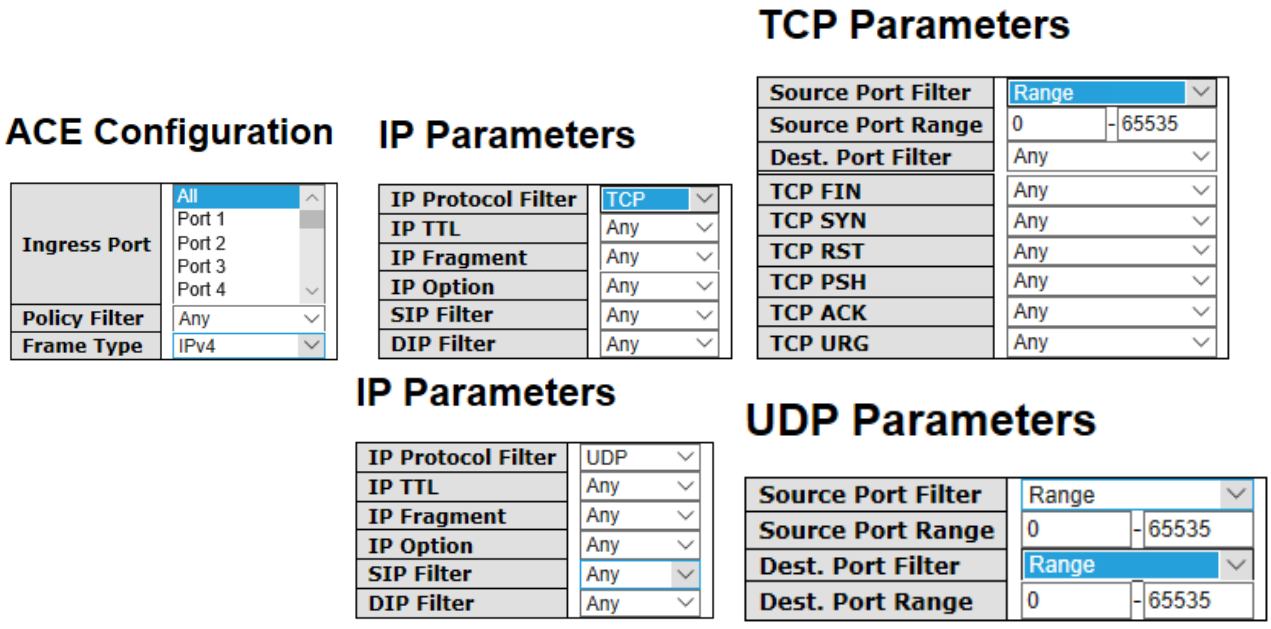


Figure 128 - TCP / UDP Parameters

Set Frame Type to IPv4 to access IP Parameters.

TCP Parameters can be configured when IP Protocol Filter is set to TCP.

Similarly, UDP Parameters can be configured when IP Protocol Filter is set to UDP.

Label	Description
TCP/UDP Source Port 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 Port No.	When **Specific** is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535. A frame 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 range.
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 range.

Label	Description
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**").

5.9.3.3.7 Ethernet Type Parameters

The Ethernet Type parameters can be configured only when Frame Type **Ethernet Type** is selected.

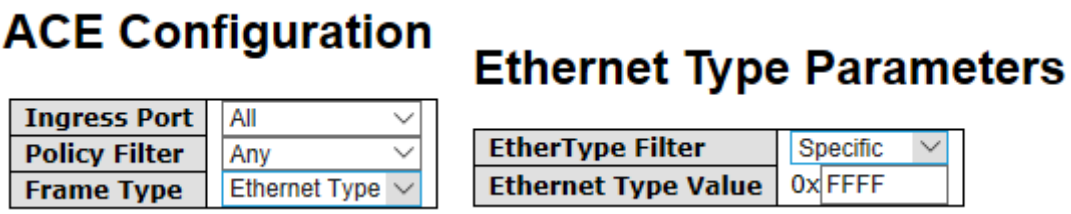
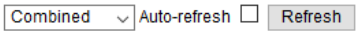


Figure 129 - Ethernet Type Parameters

Label	Description
EtherType Filter	Specify the Ethernet type filter for this ACE. **Any**: No EtherType filter is specified (EtherType filter status is "don't-care"). **Specific**: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering a EtherType value appears.
Ethernet Type Value	When **Specific** is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is from 0x600 to 0xFFFF excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits such ACE matches this EtherType value.

5.9.3.4 ACL Status

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

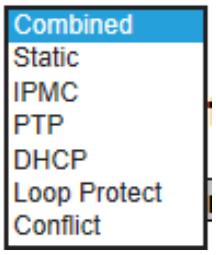


ACL Status

User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
No entries										

Figure 130 - ACL Status

Label	Description
User	Indicates the ACL user.
Ingress Port	Indicates the ingress port to which the ACE will apply. **All**: the ACE will match all ports. **Port n**: the ACE applies to this port number, where n is the number of the switch port.
Frame Type	Indicates the frame type of the ACE. **Any**: The ACE will match any frame type. **EType**: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. **ARP**: The ACE will match ARP/RARP frames. **IPv4**: The ACE will match all IPv4 frames. **IPv4/ICMP:** The ACE will match IPv4 frames with ICMP protocol. **IPv4/UDP**: The ACE will match IPv4 frames with UDP protocol. **IPv4/TCP**: The ACE will match IPv4 frames with TCP protocol. **IPv4/Other**: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. **IPv6**: The ACE will match all IPv6 standard frames.
Action	Indicates the forwarding action of the ACE. **Permit**: Frames matching the ACE may be forwarded and learned. **Deny**: Frames matching the ACE are dropped.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When **Disabled** is displayed, the rate limiter operation is disabled.
Port Redirect	Frames that match the ACE are copied to the port number specified here. The allowed range is the same as the switch port number range. Disabled indicates that the port copy operation is disabled.
Mirror	Specify the mirror operation of this port. The allowed values are: **Enabled**: Frames received on the port are mirrored. **Disabled**: Frames received on the port are not mirrored. The default value is **Disabled**.
CPU	Forwards packet that matches the specific ACE to CPU.
CPU Once	Forwards first packet that matches the specific ACE to CPU.
Counter	The counter indicates the number of times the ACE was hit by a frame.
Conflict	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Label	Description
Select ACL	Select one of the following to be displayed:  **Combined**: Shows both static and conflict entries in the ACL. **Static:** Shows static entries in the ACL. **IPMC:** Shows IPv4 MultiCast (IPMC)entries in the ACL. **DHCP:** Shows DHCP entries in the ACL **Loop Protect:** Shows Loop-protect entries in the ACL. Loop protect feature can prevent Layer2 loops by sending loop protect protocol packets and shutting down interfaces in case they receive loop protect packets originated from themselves. The feature works by checking source MAC address of received loop protect packet against MAC addresses of loop protect enabled interfaces. If the match is found, loop protect disables the interface which received the loop protect packet. Log message warns about this event and interface is marked with a loop protect comment by system. **Conflict:** Show conflict entries in the ACL.
Refresh	Click to refresh the page.
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals.

5.9.4 AAA

Authentication, authorization, and accounting (AAA) is an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA provides a modular way of performing the following services:

- Authentication—Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and depending on the selected security protocol—encryption. Authentication is the way a user is identified prior to being allowed access to the network and network services.
- Authorization—provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, and Telnet. AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the user's actual capabilities and restrictions. The database can be located locally on the access server or router or it can be hosted remotely on a RADIUS or TACACS+ security server. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user.
- Accounting—provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes. Accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. When AAA accounting is activated, the network access server reports user activity to the RADIUS or TACACS+ security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server. [12]

5.9.4.1.1 Common Server Configuration

This page allows the user to configure the Authentication Servers.

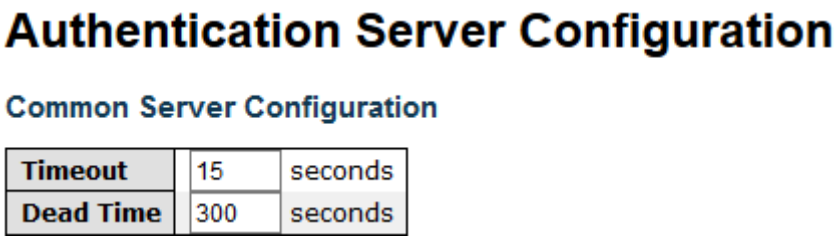


Figure 131 - Common Server Configuration

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

5.9.4.1.2 RADIUS Authentication Server Configuration

Remote Authentication Dial-In User Service (RADIUS) is a network protocol that provides security to networks against unauthorized access. RADIUS secures a network by enabling centralized authentication of dial-in users and authorizing their access to use a network service.

The table has one row for each RADIUS Authentication Server and a number of columns.

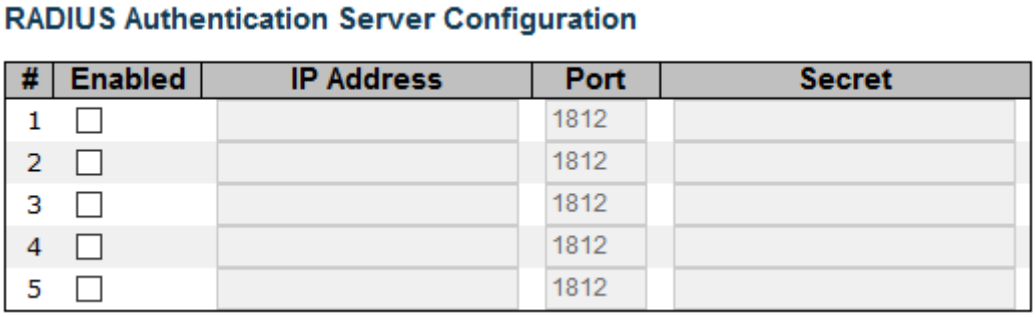


Figure 132 - RADIUS Authentication Server Configuration

Label	Description
#	The RADIUS Authentication Server number for which the configuration below applies.
Enabled	Enable the RADIUS Authentication Server by checking this box
IP Address	The IP address of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation.
Port	The UDP port to be used 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 - up to 29 characters long - shared between the RADIUS Authentication Server and the switch.

5.9.4.1.3 RADIUS Accounting Server Configuration

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

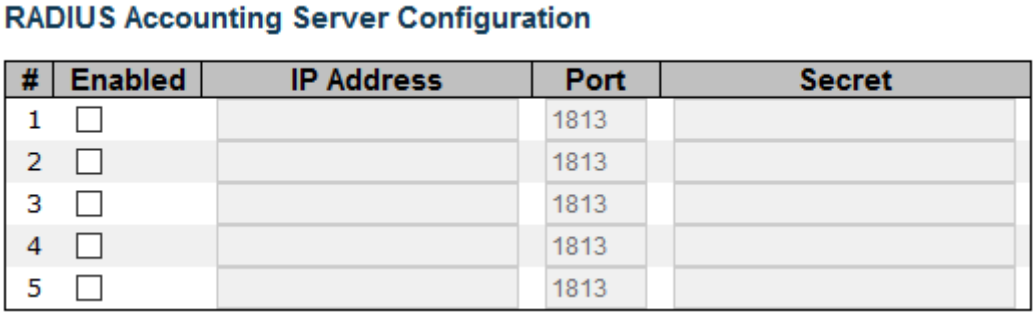


Figure 133 - RADIUS Accounting Server Configuration

Label	Description
#	The RADIUS Accounting Server number for which the configuration below applies.
Enabled	Enable the RADIUS Accounting Server by checking this box
IP Address	The IP address of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation.
Port	The UDP port to be used on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.

Label	Description
Secret	The secret - up to 29 characters long - shared between the RADIUS Authentication Server and the switch.

5.9.4.1.4TACACS+ Authentication Server Configuration

TACACS+ is an acronym for Terminal Access Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting services. This switch has TACACS+ authentication server configuration.

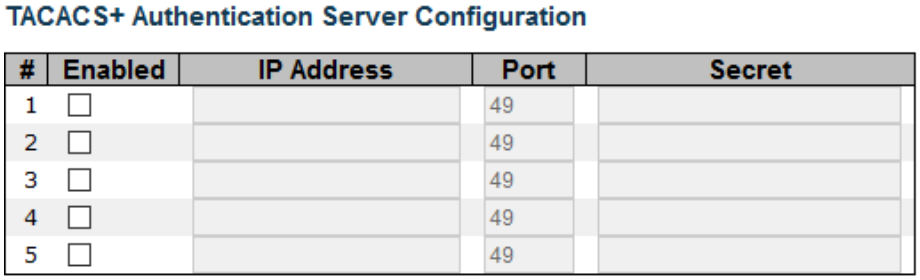


Figure 134 - TACACS+ Authentication Server Configuration

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

Label	Description
#	The TACACS+ Authentication Server number for which the configuration below applies.
Enabled	Enable the TACACS+ Authentication Server by checking this box
IP Address	The IP address of the TACACS+ Authentication Server. IP address is expressed in dotted decimal notation.
Port	The TCP port to be used on the TACACS+ Authentication Server. If the port is set to 0 (zero), the default port (49) is used on the TACACS+ Authentication Server.
Secret	The secret - up to 29 characters long - shared between the RADIUS Authentication Server and the switch.

5.9.4.2 RADIUS Overview

This page provides an overview of the status of the RADIUS servers configurable on the authentication configuration page.

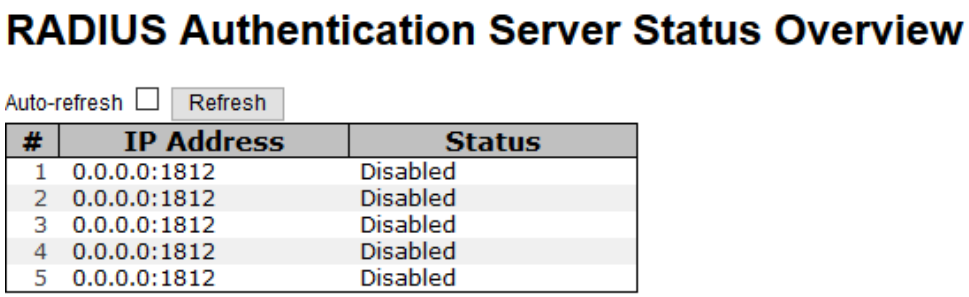


Figure 135 - Radius Authentication Server Status Configuration

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. For example, 0.0.0.0:1812.

Label	Description
Status	The current status of the server. This field takes one of the following values: **Disabled:** The server is disabled. **Not Ready:** The server is enabled, but IP communication is not yet up and running. **Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead** (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Refresh	Click to refresh the page immediately.
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals.

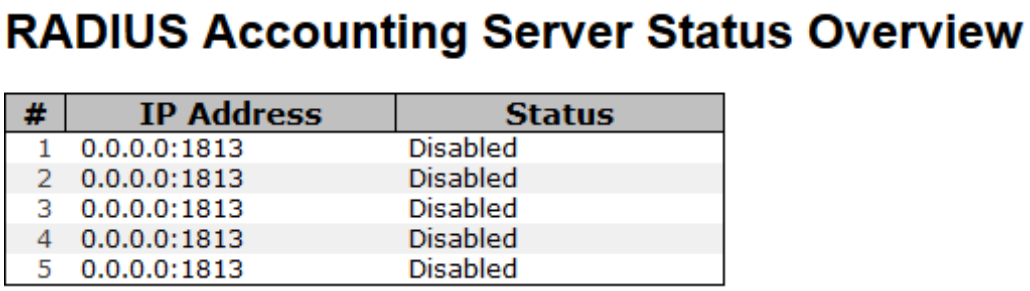


Figure 136 - Radius Accounting Server Status Configuration

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. For example, 0.0.0.0:1812.
Status	The current status of the server. This field takes one of the following values: **Disabled:** The server is disabled. **Not Ready:** The server is enabled, but IP communication is not yet up and running. **Ready:** The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead** (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

5.9.4.3 RADIUS Details

This page provides detailed statistics for a particular RADIUS server. Use the server select box to switch between the servers to have shown details for them.

The statistics map as shown in Figure 137 and Figure 138is based on the MIB named specified in RFC4668 - RADIUS Authentication Client MIB. [3] For reference for RFC4668 Names and their Descriptions as shown in the header in the tables below, see RFC4668 Section 7 Definitions.

In RADIUS authentication, clients send Access-Requests, and servers reply with **Access-Accepts**, **Access-Rejects**, and **Access-Challenges** (as shown in the Receive Packets cell). Typically, Network

Access Server (NAS) devices implement the client function. RADIUS authentication servers implement the server function, and thus would be expected to implement the RADIUS authentication server MIB.

5.9.4.3.1 RADIUS Authentication Server Statistics

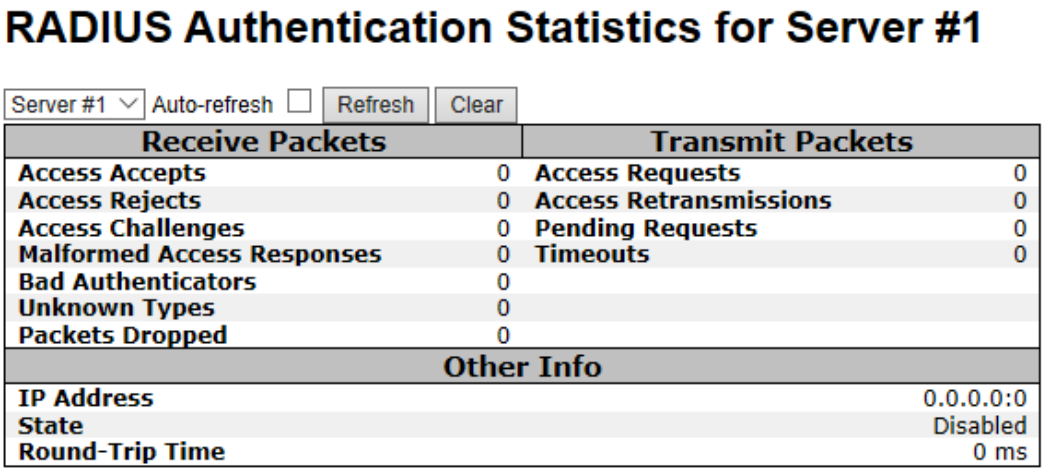


Figure 137 - Radius Authentication Statistics for Server #1

Label	Description
Server #n ↓	The server select drop down box determines which server's information is shown by selecting server #n. Where 'n' is a server, 1 to 5.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page immediately.
Clear	Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

Packet Counters: RADIUS authentication server packet counter. There are seven receive and four transmit counters (see below for details).

Rx/Tx	Name	RFC4668 Name [3]	Description
Rx	**Access Accepts**	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	**Access Rejects**	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	**Access Challenges**	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	**Malformed Access Responses**	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
Rx	**Bad Authenticator**	radiusAuthClientExtBadAuthentica	The number of RADIUS Access-Response packets containing invalid authenticators or Message

Rx/Tx	Name	RFC4668 Name [3]	Description
	s	tors	Authenticator attributes received from the server.
Rx	**Unknown Types**	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Rx	**Packets Dropped**	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx	**Access Requests**	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	**Access Retransmissions**	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx	**Pending Requests**	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Tx	**Timeouts**	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.

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

Name	RFC4668 Name [4]	Description
IP Address	-	IP address and UDP port for the authentication server in question.
State	-	Shows the state of the server. It takes one of the following values: **Disabled**: The selected server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead** (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

5.9.4.3.2 RADIUS Accounting Server Statistics

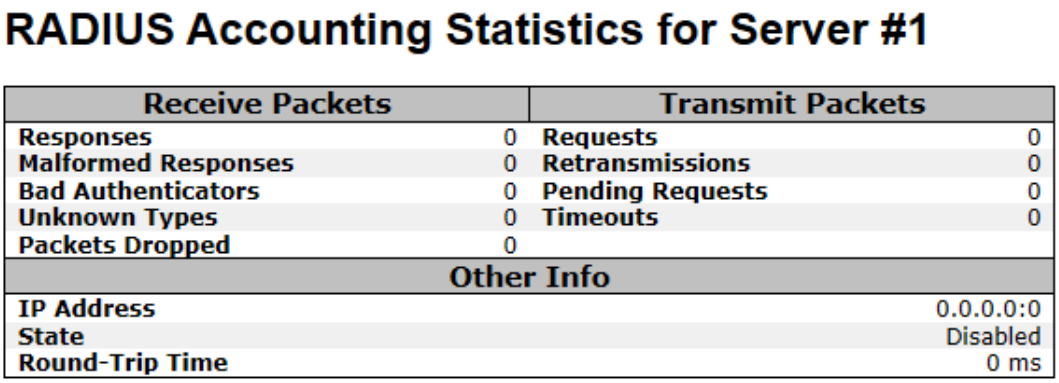


Figure 138 - Radius Accounting Statistics for Server #1

The statistics map is based on the MIB named in RFC4670 - RADIUS Accounting Client MIB. [4]. As per RFC4670 Section 5, In RADIUS accounting, clients send Accounting-Requests, and servers reply with Accounting-Responses. The RADIUS accounting servers implement the server function, and thus would be expected to implement the RADIUS accounting server MIB.

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

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

Rx/Tx	Name	RFC4670 Name [4]	Description
Rx	Responses	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
Rx	Malformed Responses	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
Rx	Bad Authenticators	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.

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

Name	RFC4668 Name	Description [4]
IP Address	-	IP address and UDP port for the authentication server in question.
State	-	Shows the state of the server. It takes one of the following values: **Disabled**: The selected server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept 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.

Label	Description
Auto-refresh ☐	Check this box to refresh the page automatically. Automatic refresh occurs
Refresh	Click to refresh the page immediately.
Clear	Clears the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

5.9.5 NAS (802.1x)

5.9.5.1 Network Access Server Configuration

This page allows the user to configure the IEEE 802.1X and MAC-based authentication system and port settings. Network Access Server stands for NAS.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers (the backend servers) determine whether the user is allowed access to the network. They are configured at **Security** → **AAA** page (see 5.9.4.)

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, which makes MAC-based authentication is less secure than 802.1 X authentications.

5.9.5.1.1 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 [2] (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 back-end authentication server requests from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

5.9.5.1.2 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.

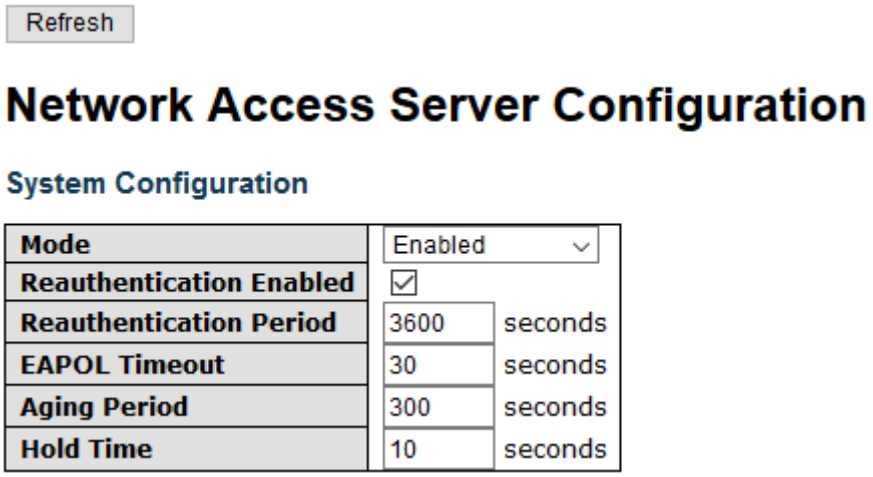


Figure 139 - Network Access Server Configuration

5.9.5.1.3System Configuration

Label	Description
Mode	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed to forward frames.
Reauthentication Enabled	If checked, clients are re-authenticated after the interval specified by the Re-authentication Period. Re-authentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port. For MAC-based ports, re-authentication 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 **Re-authentication is Enabled**. 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.
Aging 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 "**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.

5.9.5.1.4Port Configuration

The table has one row for each port on the switch and a number of columns.

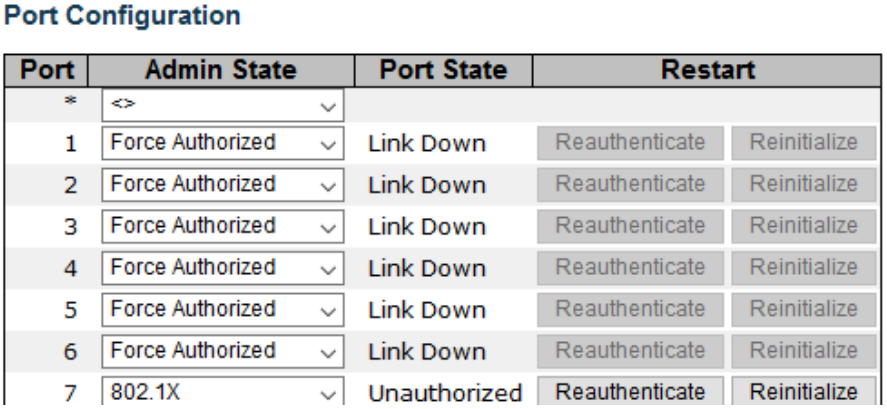


Figure 140 - Network Access Server Port Configuration

Label	Description
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: **1. Force Authorized** **2. Force Unauthorized** **3. 802.1X** **4. MAC-based Auth.** All modes are explained below.
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.
802.1X	In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs [2]. Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it. When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant. *Note:* Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.
MAC-based Auth.	Unlike 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

Label	Description
	802.1X standard. The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.
Port State	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.

5.9.5.2 NAS Switch

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

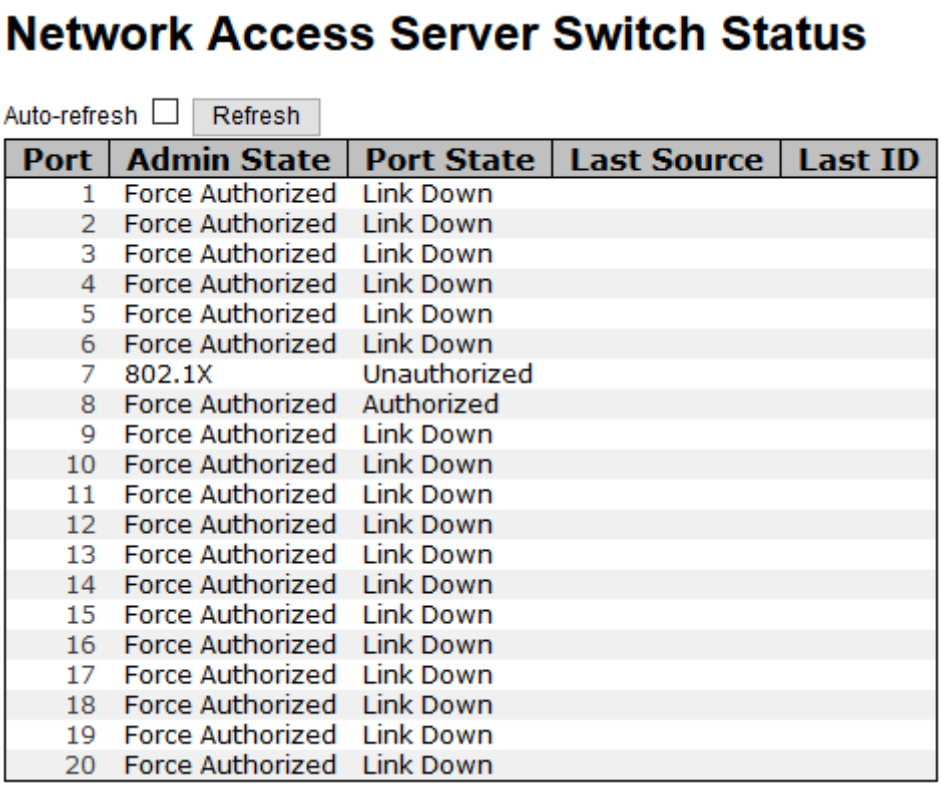


Figure 141 - Network Access Server Switch Status

Label	Description
Port	The switch port number. Click a port number to navigate to detailed NAS 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.

5.9.5.3 NAS Port

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only . Use the port select box to select which port details to be displayed.

Note that Port counters are shown only for ports with Authorized port state such Port 20 (refer to Figure 141- Network Access Server Switch Status). Port 1 does not show Port counters.

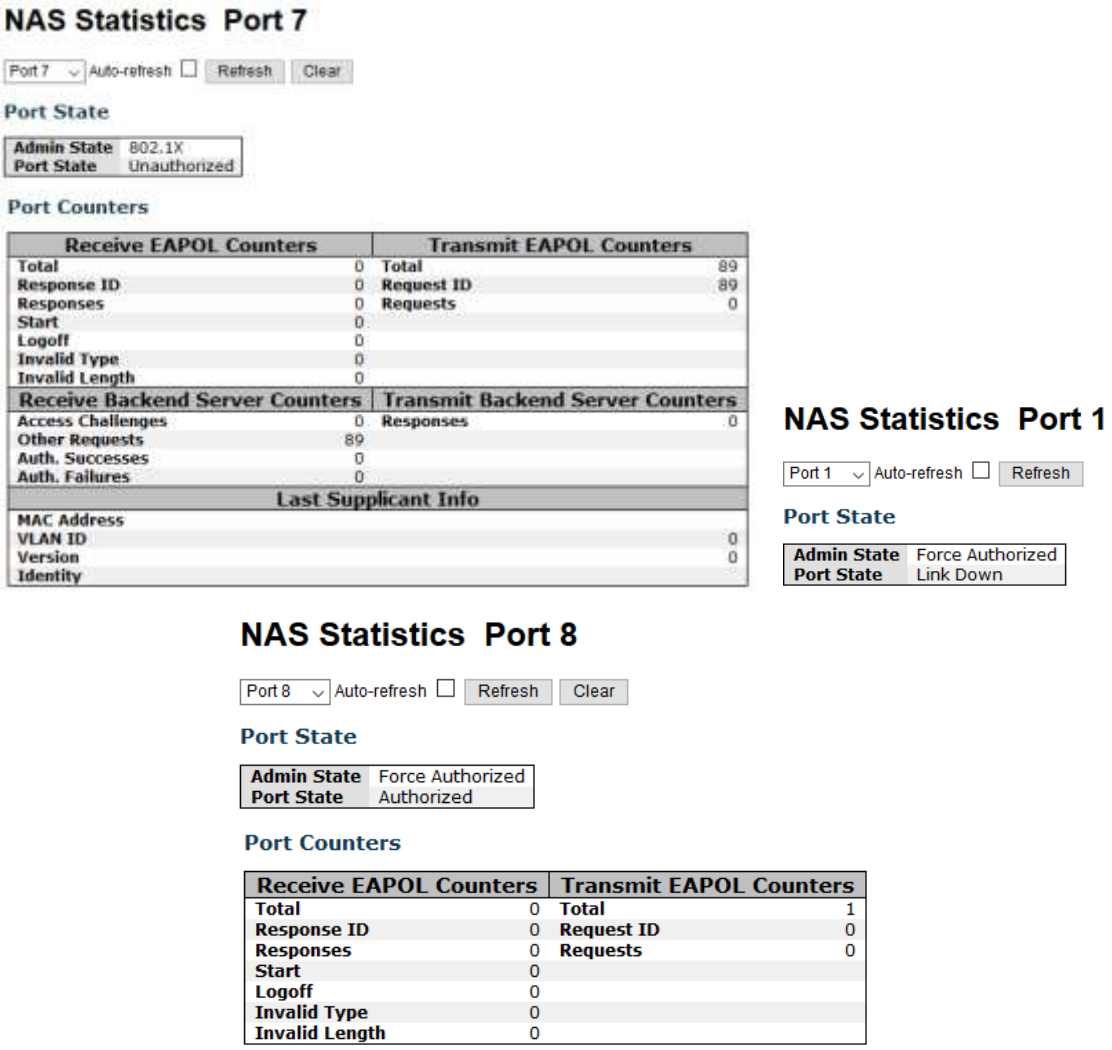


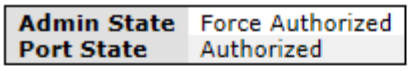
Figure 142 - NAT Statistics Admin State Force Authorized

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.
Port n ↓	The port select drop down box determines which port's information is shown by selecting port 'n'. Where 'n' is a valid port number.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page immediately.
Clear	This button is available in the following modes: • Force Authorized • Force Unauthorized • 802.1X Click to clear the counters for the selected port

5.9.5.3.1 EAPOL Counters

These supplicant frame counters are available for the following administrative states:

- **Force Authorized**
- **Force Unauthorized**
- **802.1X**



Port Counters

Receive EAPOL Counters		Transmit EAPOL Counters	
Total	0	Total	1
Response ID	0	Request ID	0
Responses	0	Requests	0
Start	0		
Logoff	0		
Invalid Type	0		
Invalid Length	0		

Figure 143 – EAPOL Counters Admin State Force Authorized

Rx/Tx	Name	IEEE Name	Description
Rx	**Total**	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	**Response ID**	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
Rx	**Responses**	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
Rx	**Start**	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	**Logoff**	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
Rx	**Invalid Type**	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	**Invalid Length**	dot1xAuthEapLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	**Total**	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	**Request ID**	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
Tx	**Requests**	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

5.9.5.3.2 Backend Server Counters

These backend (RADIUS) frame counters are available for the following administrative states:

- **802.1X**
- **MAC-based Auth.**

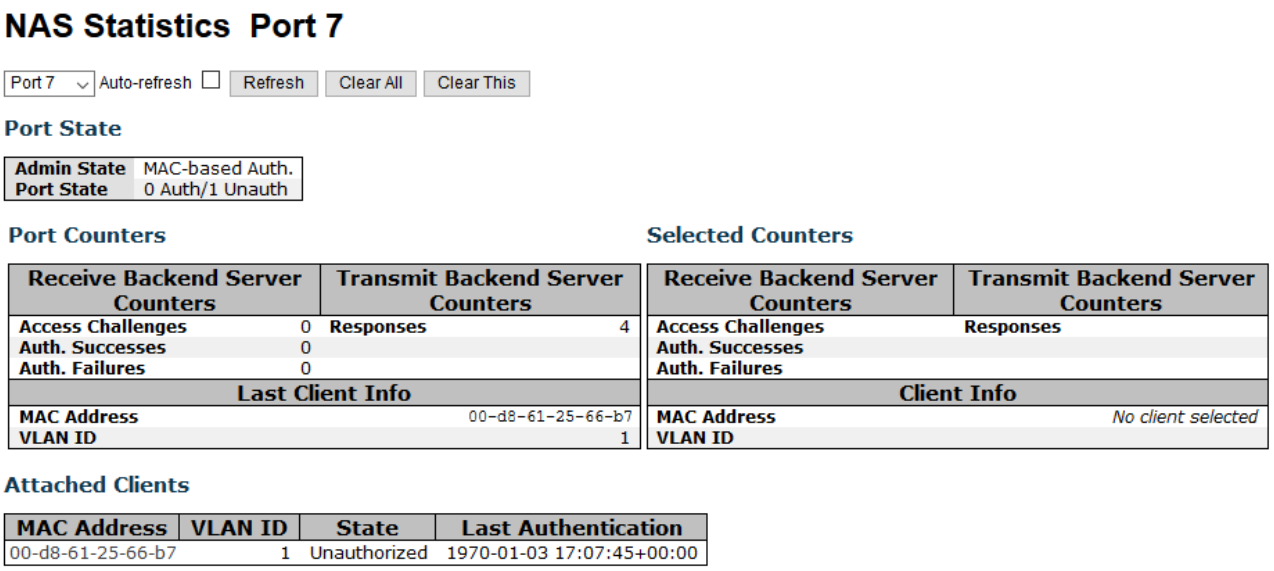


Figure 144 - NAT Statistics Admin MAC-based Auth.

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.
Port n ↓	The port select drop down box determines which port's information is shown by selecting port 'n'. Where 'n' is a valid port number.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page immediately.
Clear	This button is available in the following modes: • Force Authorized • Force Unauthorized • 802.1X Click to clear the counters for the selected port
Clear All	This button is available in the following modes: • MAC-based Auth.X Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared, however.
Clear This	This button is available in the following modes: • MAC-based Auth.X Click to clear only the currently selected client's counters.

Backend (RADIUS) Frame Counters table

Rx/Tx	Name	IEEE Name	Description
Rx	**Access Challenges**	dot1xAuthBackend AccessChallenges	**802.1X-based**: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch. **MAC-based**: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).
Rx	**Other Requests**	dot1xAuthBackend OtherRequestsToSupplicant	**802.1X-based**: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method. **MAC-based**: Not applicable.
Rx	**Auth. Successes**	dot1xAuthBackend AuthSuccesses	**802.1X- and MAC-based**: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.
Rx	**Auth. Failures**	dot1xAuthBackend AuthFails	**802.1X- and MAC-based**: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.
Tx	**Responses**	dot1xAuthBackend Responses	**802.1X-based:** Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted. **MAC-based:** Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.

5.9.5.3.3 Last Supplicant/ Client Info

Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:

- **802.1X**
- **MAC-based Auth.**

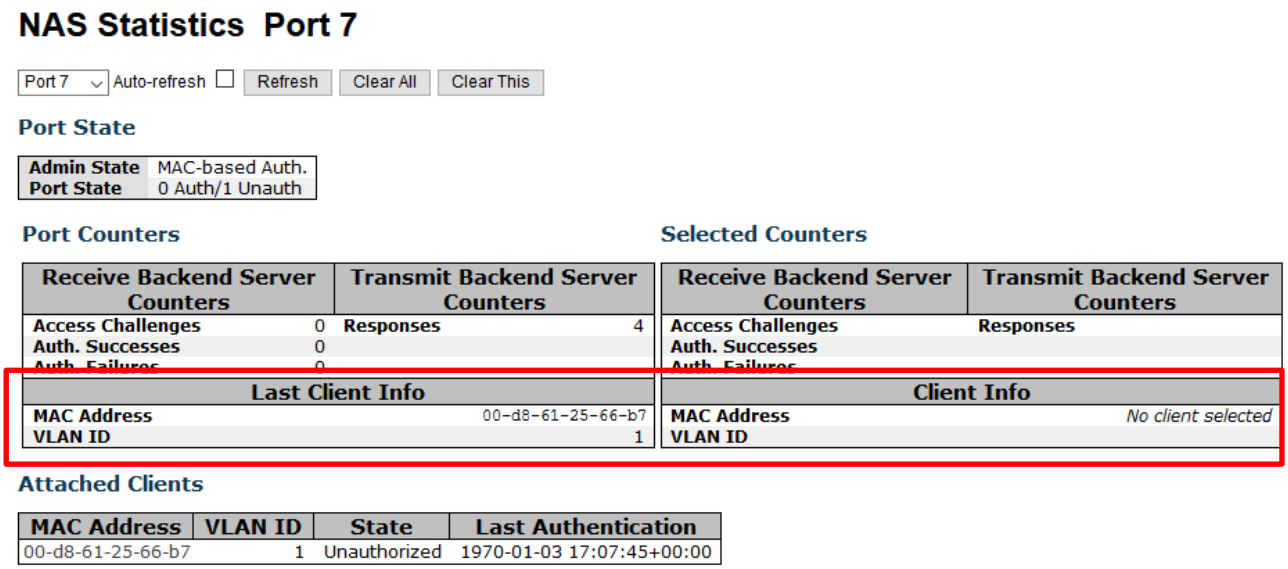


Figure 145 - Last Supplicant/ Client Info Admin State MAC-based Auth.

Name	IEEE Name	Description
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
VLAN ID	-	The VLAN ID on which the last frame from the last supplicant/client was received.
Version	dot1xAuthLastEapolFrameVersion	**802.1X-based**: The protocol version number carried in the most recently received EAPOL frame. **MAC-based**: Not applicable (as shown on Figure 145)
Identity	-	**802.1X-based**: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. **MAC-based**: Not applicable (as shown on Figure 145).

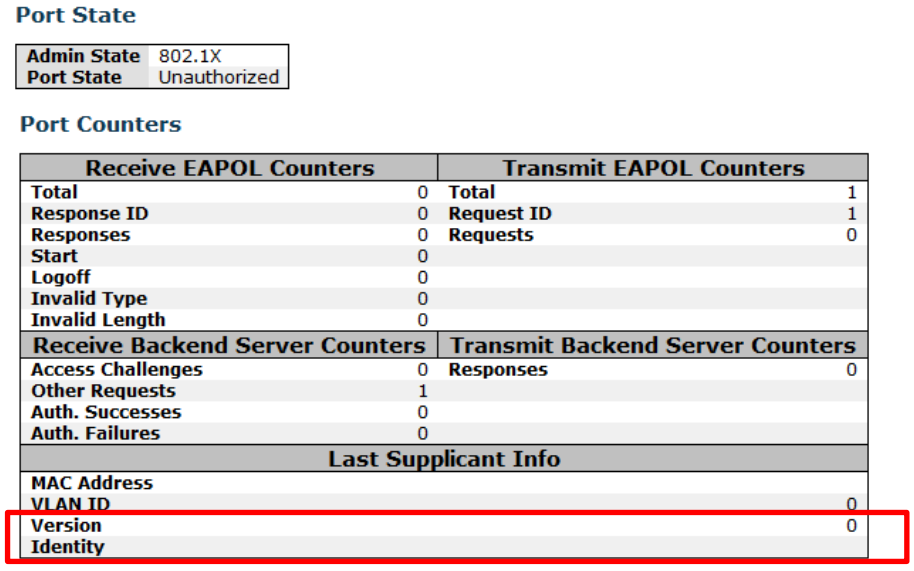


Figure 146 - Last Supplicant/ Client Info Admin State 802.1X-based.

5.9.5.3.4 Selected Counters and Attached Clients

The Selected Counters table is visible when the port is in the MAC-based Auth. state. The table is identical to and is placed next to the Port Counters table, and it will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses (shown as Attached Clients) from the table below.

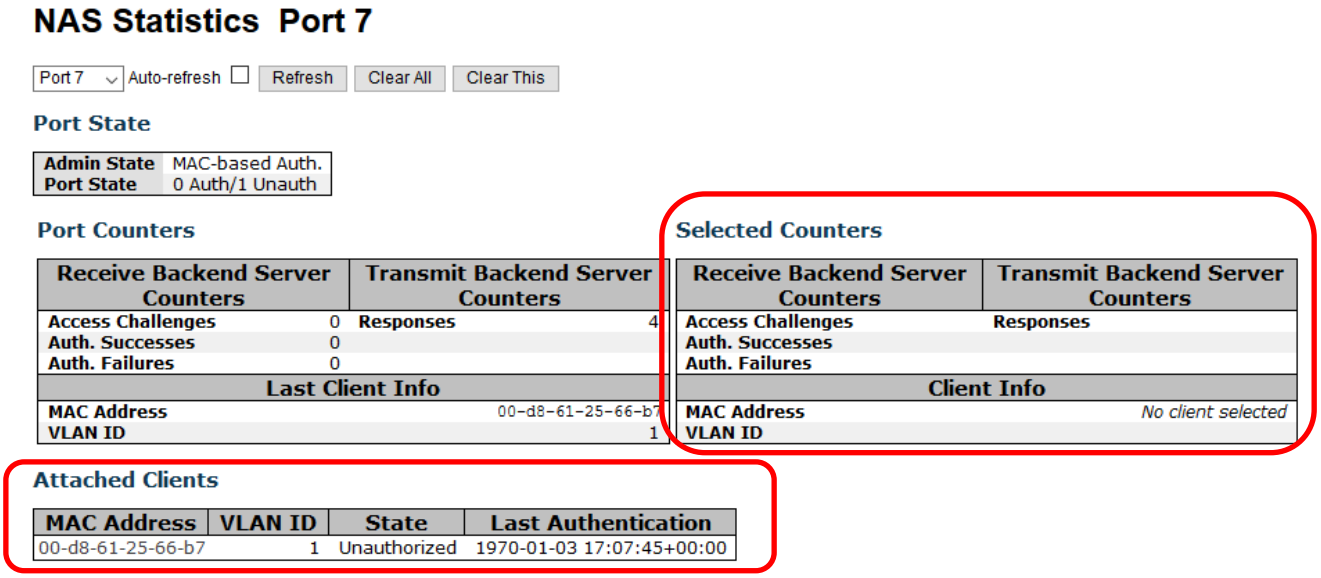


Figure 147 – Selected Counters / Attached Clients

Label	Description
MAC Address	For MAC-based Auth., this column holds the MAC address of the attached client. Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows "No clients attached".
VLAN ID	This column holds the VLAN ID of the corresponding client that is currently secured through the Port Security module.
State	The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.
Last Authentication	Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

5.10 Warning

5.10.1 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. Select the events to cause the fault alarm, then click **Save** to save the changes.

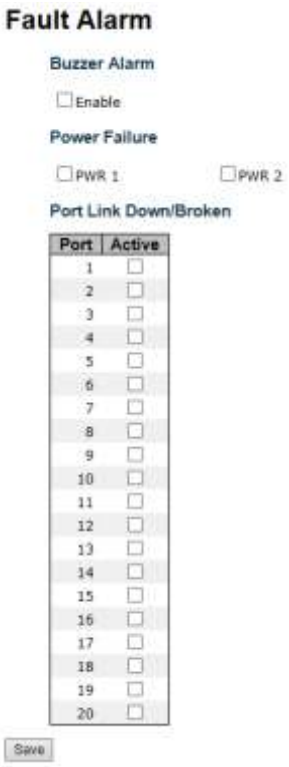


Figure 148 - Fault Alarm

Label	Description
Buzzer Alarm	?
Power Failure	Fault alarm when any selected power failure. This switch support dual powers.
Port Link Down/Broken	Fault alarm when any selected port link down/broken.
Save	Click to save changes.

5.10.2 System Warning

5.10.2.1 SYSLOG Setting

The SYSLOG is a protocol that transmits event notifications across networks. For more details, refer to RFC 3164 - The BSD SYSLOG Protocol [5].

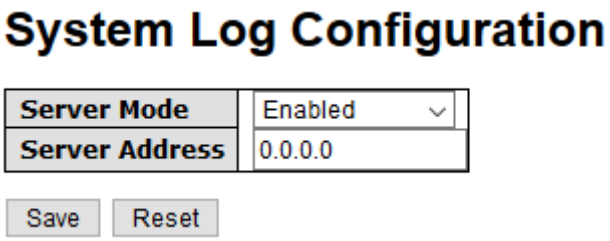


Figure 149 - System Log Configuration

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. 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
Server Address	Indicates the IPv4 host address of syslog server. If the switch provides DNS functions, it also can be a host name.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.10.2.2 SMTP Settings

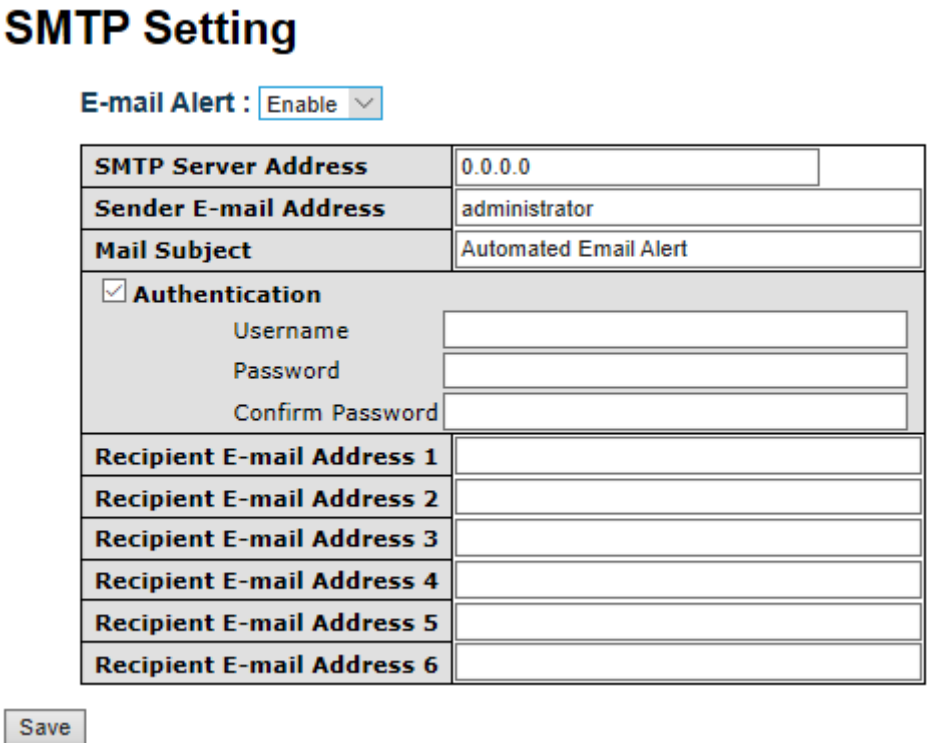


Figure 150 - SMTP Settings

Label	Description
E-mail Alarm	Enables or disables transmission of system warnings by e-mail.
SMTP Server Address	The SMTP server IP address(or domain name address).
Sender E-mail Address	Sender email 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, allows a total number of six recipients.
Save	Click to save changes

5.10.2.3 Event Selection

SYSLOG is the warning method supported by the system. Check the corresponding box to enable the system event warning method you want. Please note that the checkbox cannot be checked when SYSLOG is disabled.

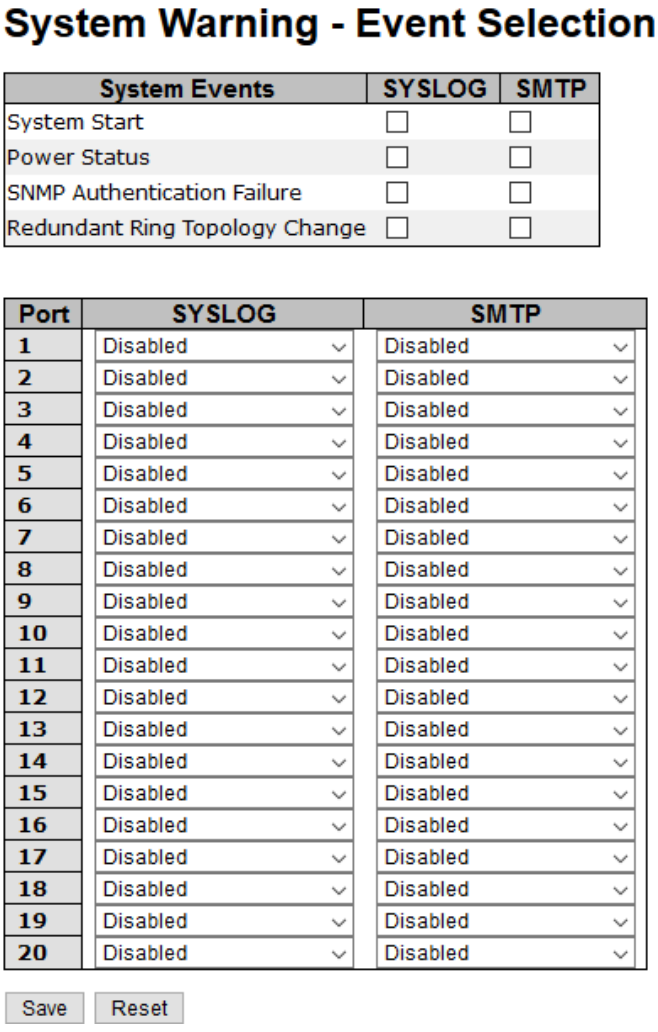


Figure 151 - System Warning - Event Selection

SYSLOG is the warning method supported by the system. Check the corresponding box to enable the system event warning you want. Please note that the checkboxes cannot be added when SYSLOG is disabled.

Label	Description
System Start	Alerts when the system is restarted.
Power Status	Alerts when power is up or down.
SNMP Authentication Failure	Alerts when SNMP authentication fails.
Redundant Ring Topology	Alerts when there is a ring topology change.
SYSLOG Port Event	Select the SYSLOG event for a specific port number. Options are: • Disable • Link Up • Link Down • Link Up & Link Down
SMTP Port Event	Select the SMTP event for a specific port number. Options are: • Disable • Link Up • Link Down • Link Up & Link Down
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.11 Monitor and Diagnostic

5.11.1 MAC Table

5.11.1.1 MAC Address Table Configuration

The MAC address table can be configured on this page. Set timeouts for entries in the dynamic MAC table and configure the static MAC table here.

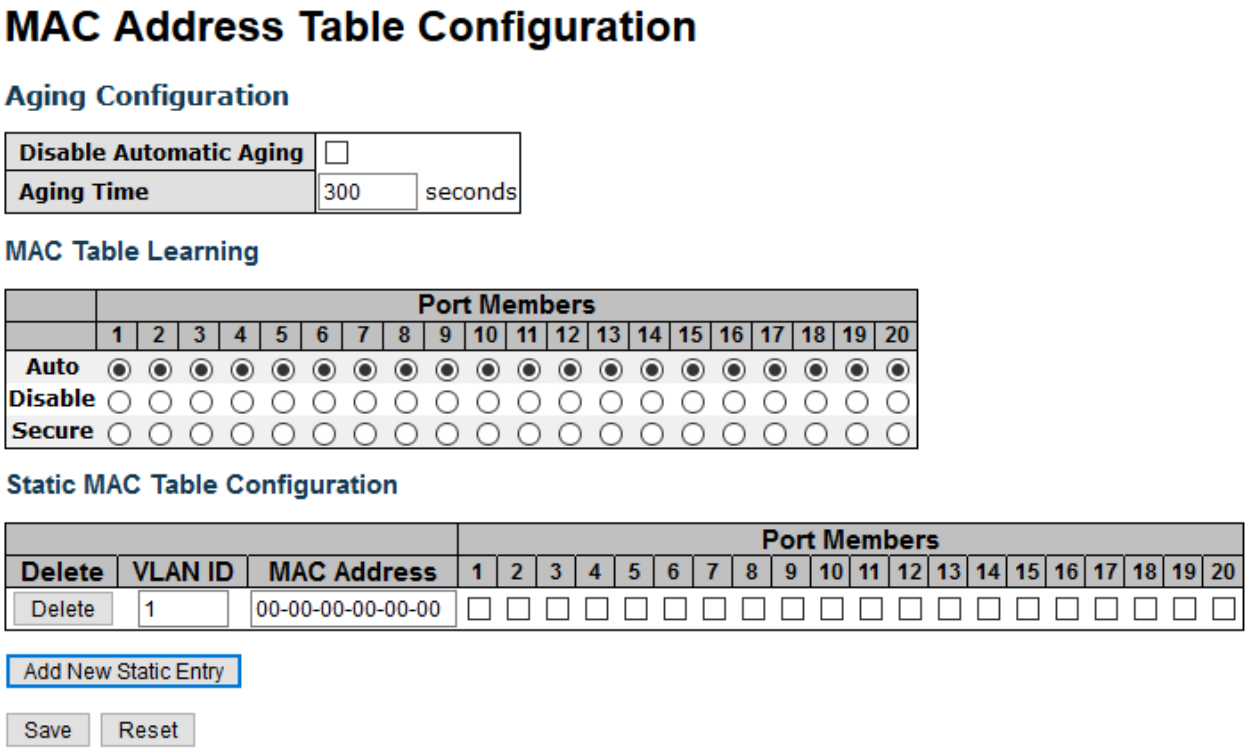


Figure 152 - MAC Address Table Configuration

5.11.1.1.1 Aging Configuration

By default, dynamic entries are removed from the MAC after 300 seconds. This removal is called aging.

You can configure aging time by entering a value in the box of **Age Time.** The allowed range is 10 to 1000000 seconds. You can also disable the automatic aging of dynamic entries by checking **Disable Automatic Aging**.

5.11.1.1.2 MAC Table Learning

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.

The port can be configures to learn dynamically the MAC address based upon the following settings:

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.

5.11.1.1.3 Static MAC Table Configurations

The static entries in the MAC table are shown in this table. The static MAC table can contain up to 64 entries. The entries are for the whole stack, not for individual switches. 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.
Add New Static Entry	Click to add a new entry to the static MAC table. specify the VLAN ID, MAC address, and port members for the new entry. Click **Save** to save the changes.

5.11.1.2 MAC Address Table

Entries in the MAC Table are shown on this page. The MAC Address Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Each page shows up to 999 entries from the MAC table, 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 the **Refresh** button will update the displayed table starting from that or the closest next MAC table match. In addition, the two input fields will – upon clicking **Refresh** - assume the value of the first displayed entry, allows for continuous refresh with the same start address.

The **>>** will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When it reaches the end, the text "**no more entries**" is shown in the displayed table. Use the **|<<** button to start over.

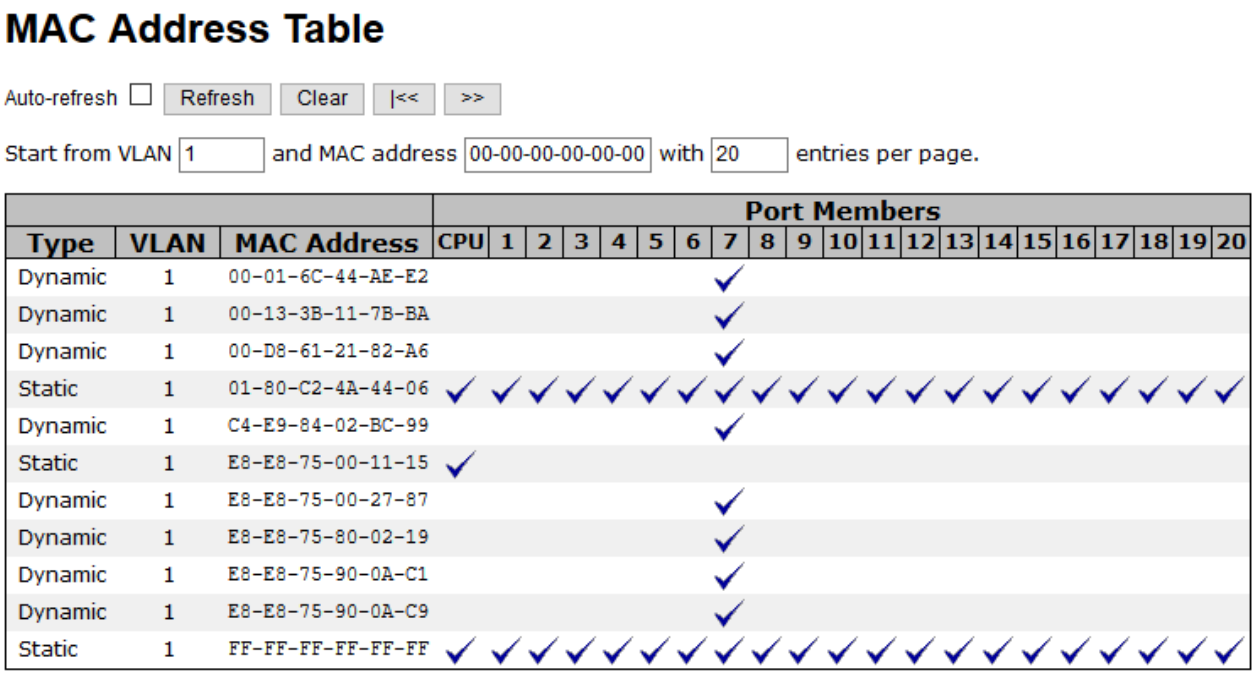


Figure 153 - MAC Address Table

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.
Auto-refresh ☐	Automatic refresh occurs every 3 seconds.
Clear	Flushes all dynamic entries
|<<	Updates the table starting from the first entry in the MAC Table, i.e. the entry with the lowest VLAN ID and MAC address.
>>	Updates the table, starting with the entry after the last entry currently displayed.

5.11.2 Port Statistic

5.11.2.1 Traffic Overview

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

Port Statistics Overview

Auto-refresh ☐ Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	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	81462	58566	17276805	24519463	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	558	3036	77712	744163	0	0	0	0	192
16	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0

Figure 154 - Port Statistics Overview

Label	Description
Port	The logical port for the settings contained in the same row. Click on a port to go to that ports Detailed Statistics page.
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. Automatic refresh occurs every 3 seconds at regular intervals.
Refresh	Click to refresh the page immediately.
Clear	Clears the counters for all ports.

5.11.2.2 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 totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.

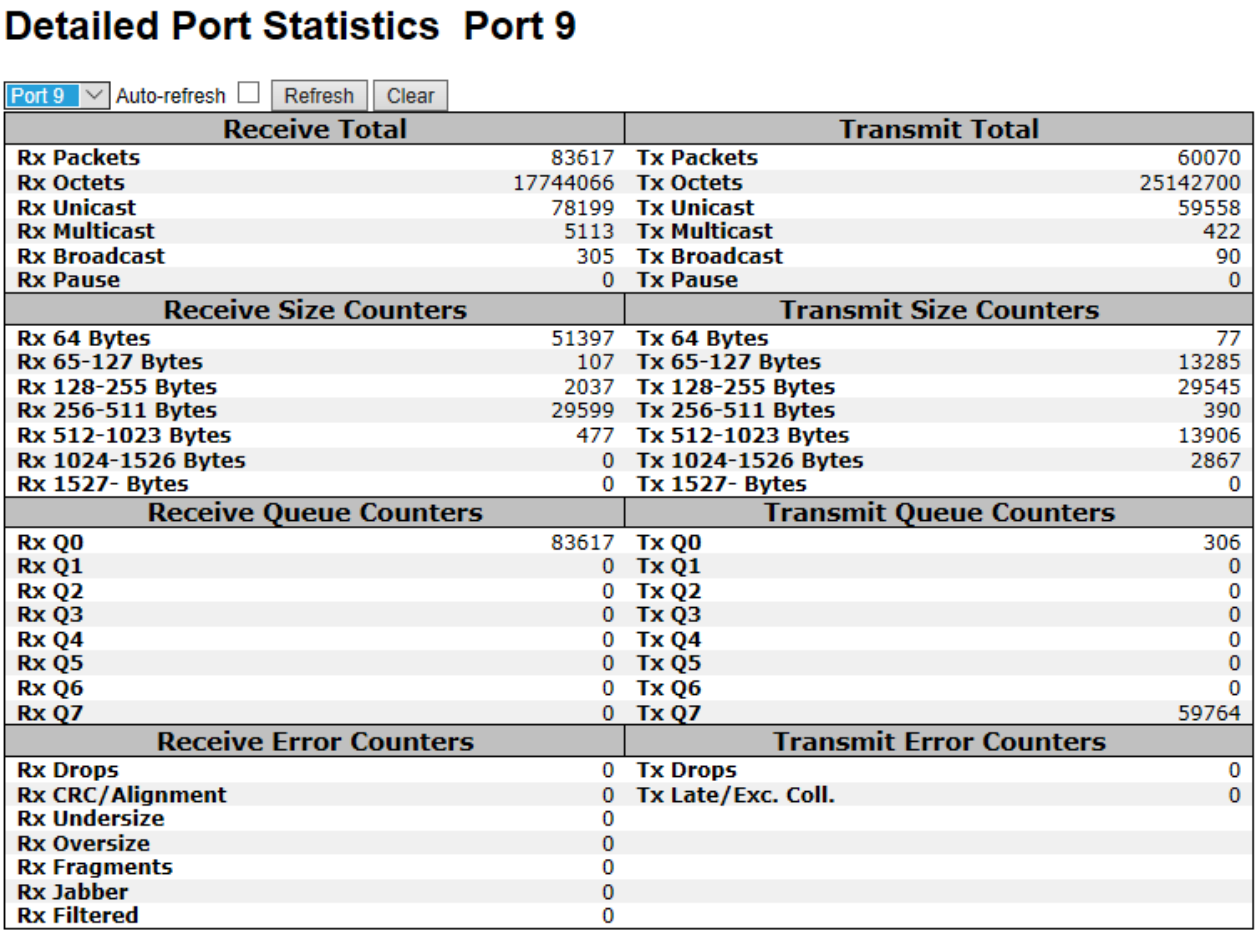


Figure 155 - Detailed Post Statistics

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,
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 and Tx Size Counters	The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.
Rx and Tx Queue Counters	The number of received and transmitted packets per input and output queue.
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.

5.11.3 Port Monitoring

You can configure port mirroring on this page. 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 is selected as follows:

- All frames received on a given port (also known as ingress or source mirroring).
- All frames transmitted on a given port (also known as egress or destination mirroring).

Port to mirror is also known as the mirror port. Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this port.

Disabled option disables mirroring.

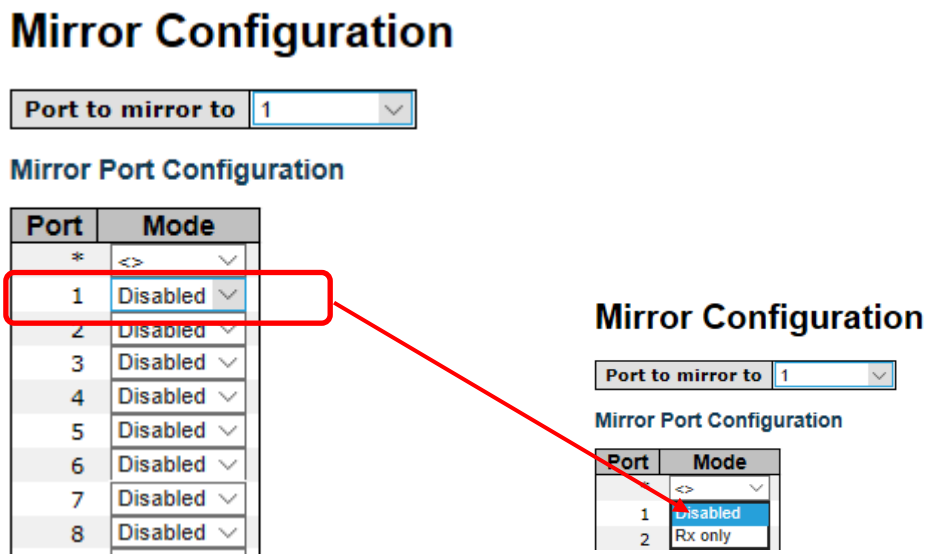


Figure 156 - Mirror Configuration

Label	Description
Port	The logical port for the settings contained in the same row.
Mode	Select mirror mode. **Disabled**—neither frames transmitted nor frames received are mirrored **Rx only**—Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored. **Tx only**—Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored. **Enabled**—Frames received and frames transmitted are mirrored on the mirror port.

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

Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror **port** Tx frames. Because of this, the **Mode** for the selected **mirror port** (which in the Figure above is Port 1) is limited to **Disabled** or **Rx only**.

5.11.4 System Log Information

This page provides switch system log information.

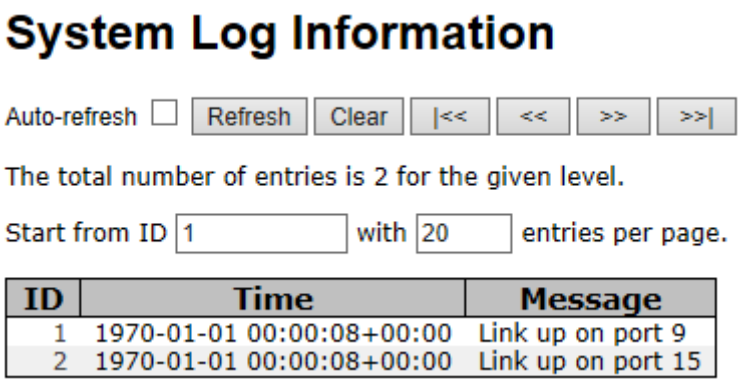


Figure 157 - System Log Information

Label	Description
ID	The ID (>= 1) of the system log entry
Message	The message of the system log entry.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
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.

5.11.5 VeriPHY Cable Diagnostics

This page is used for running the VeriPHY Cable Diagnostics for 10/100 and 1G copper ports.

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 is only accurate for cables of length 7 - 140 meters.

10 and 100 Mbps ports will be linked down while running VeriPHY. Therefore, running VeriPHY on a 10 or 100 Mbps management port will cause the switch to stop responding until VeriPHY is complete.

This page allows the user to perform VeriPHY cable diagnostics.

VeriPHY Cable Diagnostics

Port All

Start

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

Figure 158 - VeriPHY Cable Diagnostics

Press **Start** to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically. Results can be viewed 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 complete.

Label	Description
Port	The port for which VeriPHY Cable Diagnostics is requested
Cable Status	Port: port number Pair: the status of the cable pair OK - Correctly terminated pair Open - Open pair Short - Shorted pair Short A - Cross-pair short to pair A Short B - Cross-pair short to pair B Short C - Cross-pair short to pair C Short D - Cross-pair short to pair D Cross A - Abnormal cross-pair coupling with pair A Cross B - Abnormal cross-pair coupling with pair B Cross C - Abnormal cross-pair coupling with pair C Cross D - Abnormal cross-pair coupling with pair D Length: the length (in meters) of the cable pair

5.11.6 SFP Monitor

SFP modules with DDM (Digital Diagnostic Monitoring) function can measure the temperature of the apparatus, helping you monitor the status of connection and detect errors immediately. through DDM Web interface, event alarms can be managed and set up.

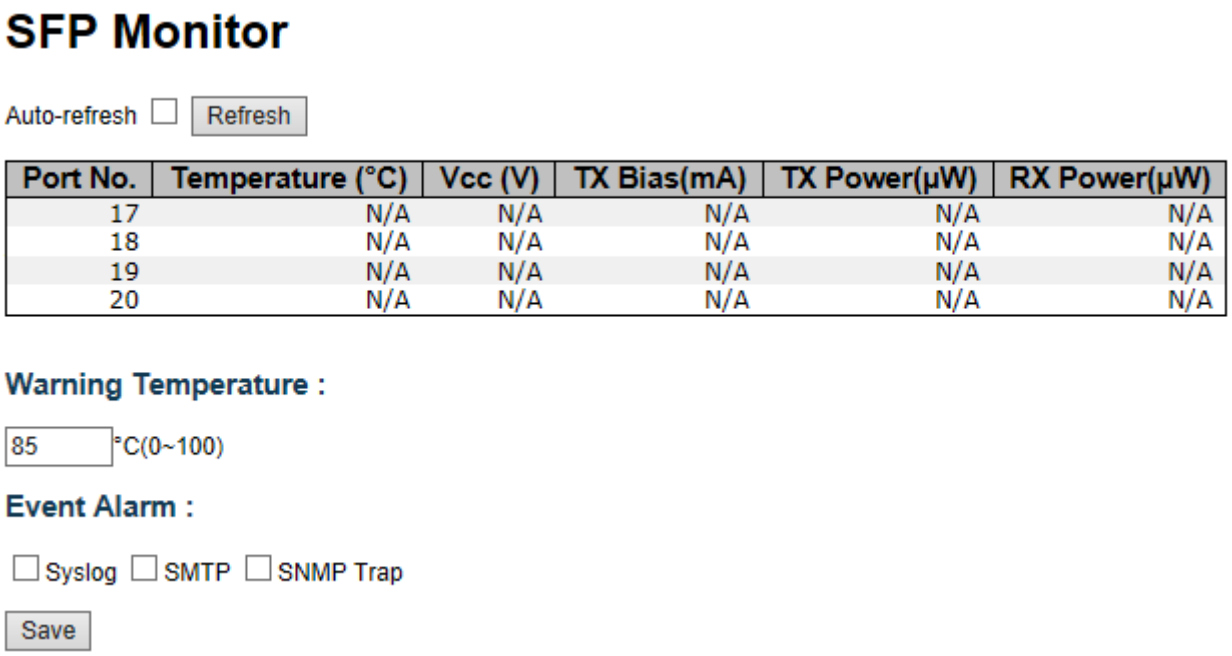


Figure 159 - SFP Monitor

5.11.7 Ping

Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP echo reply.

This page allows the user to issue ICMP packets to troubleshoot IP connectivity issues.

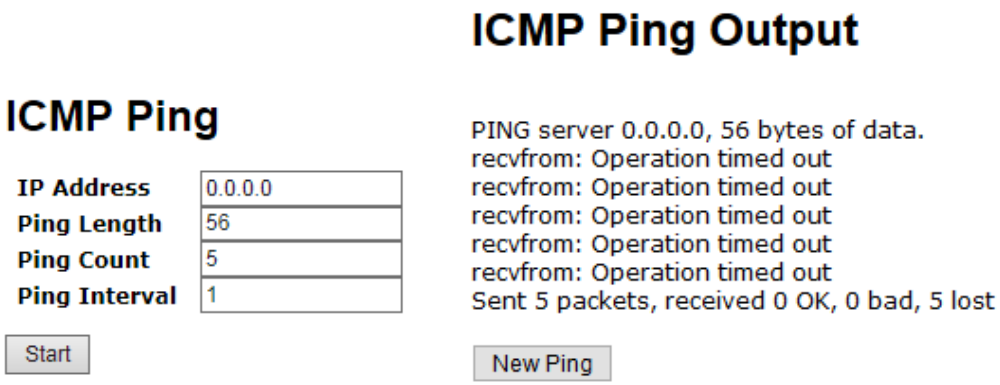


Figure 160 - ICMP Ping

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 (see the second part of the figure above).

Click **New Ping** to return to **ICMP Ping** screen.

The following properties of the issued ICMP packets can be configured:

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 count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.

5.11.8 Ping6

This page allows the user to issue ICMPv6 Ping packets to troubleshoot IP connectivity issues.

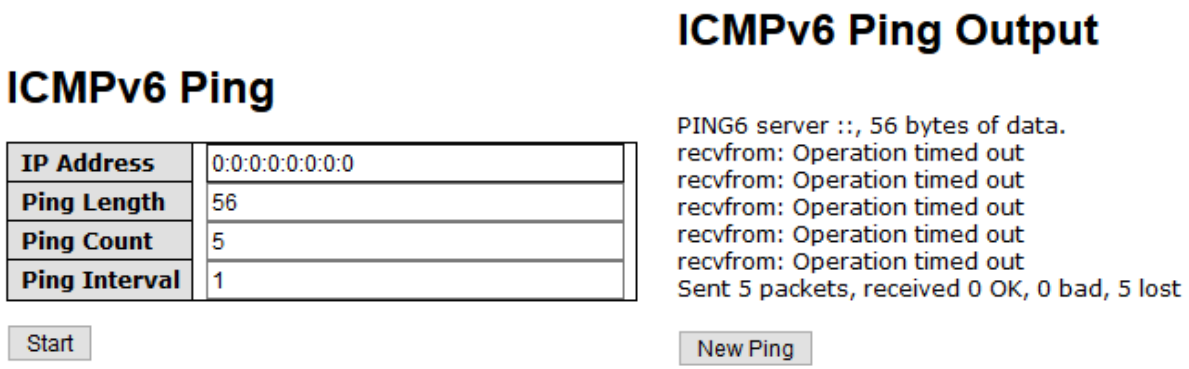


Figure 161 – ICMPv6 Ping

Label	Description
IP Address	The destination IP Address
Ping Length	The payload size of the ICMPv6 packet. Values range from 8 to 65,535 bytes. [7]
Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.

5.12 Factory Defaults

You can reset the configuration of the stack switch on this page. The IP configuration and/or User/Password are retained only if the respective boxes are checked when the switch is restored to factory defaults.

Figure 162 - Factory Defaults

Label	Description
Yes	Click to reset the configuration to factory defaults.
No	Click to return to the **System Information** page without resetting.

5.13 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.

Figure 163 - System Reboot - Restart Device

Label	Description
Yes	Click to reboot device.
No	Click to return to the **System Information** page without rebooting.

6. CLI MANAGEMENT

6.1 Command Line Interface Setup

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

1. Start **Tara Term VT** (or other terminal emulator) application.

or the app from Command Prompt

2. Go to **Setup** menu and select **Serial Port**.

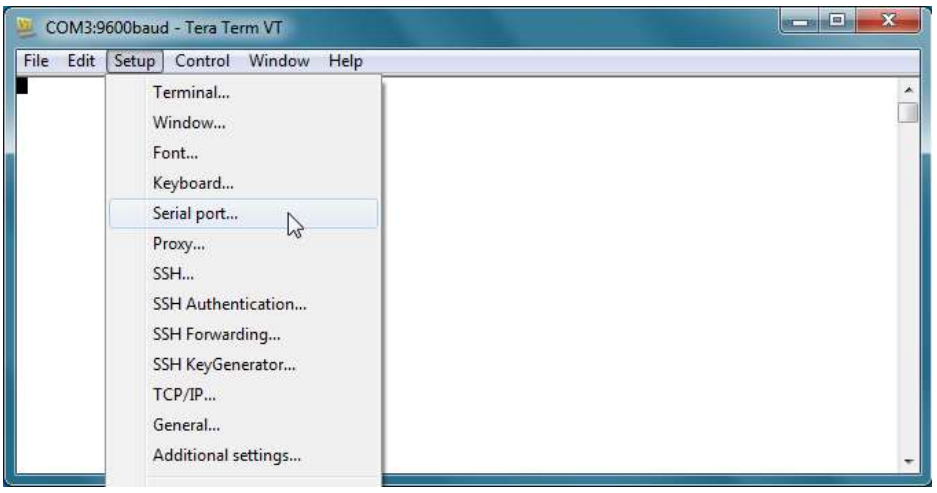


Figure 164 – Tera Term VT, Setup Menu

3. Select the COM Port used by your PC to connect to the Console Port. Set the rest of the properties to **115200 for Baud rate, 8 for Data bits, None for Parity, 1 bit for Stop and none for Flow control**. Then, click **OK**.

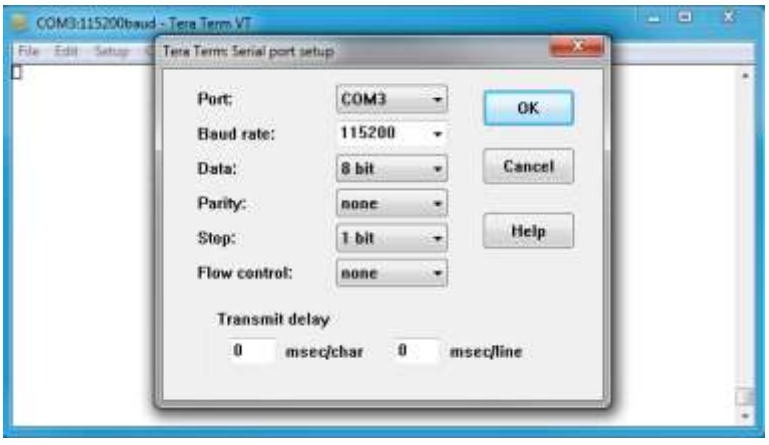


Figure 165 – Tera Term VT, Serial port setup

4. Press "**Enter**" for the Console login screen to appear. Use the keyboard to enter the Console Username and Password which is same as for Web management (**admin** for both), then press "**Enter**".

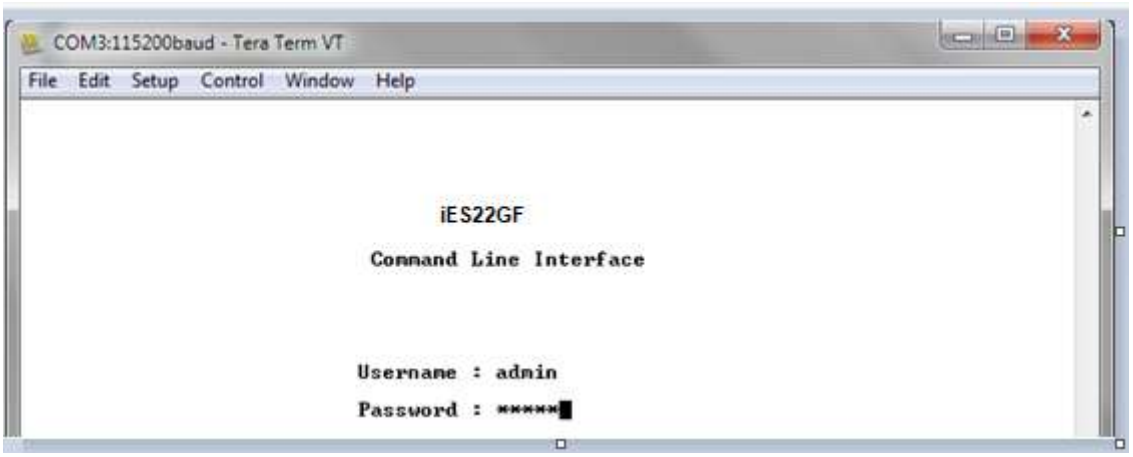


Figure 166 - iES20GF Command Line Interface - Tera Term VT

6.1.2 CLI Management by Telnet

You 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 the console via Telnet.

1. Connect your PC to one of the Ethernet ports of the switch via an Ethernet cable.
2. Telnet to the IP address of the switch from the Windows "**Run"** command (or from the MS-DOS prompt).

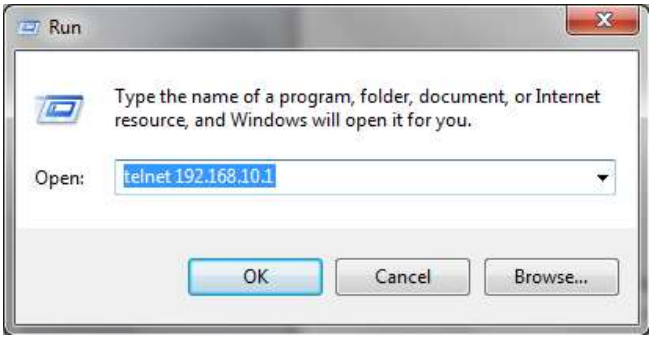


Figure 167 - Telnet Command Prompt

3. The Console login screen appears. Use the keyboard to enter the Console Username and Password, then press "Enter". This is the same as the Web Browser password. The default Username is "admin" and the default Password is "admin".

Figure 168 - iES20GF Command Line Interface - Telnet

6.1.3 Command Groups

```
Welcome to iES20GF Command Line Interface.
Type 'help' or '?' to get help.
>
?
General Commands:
-----------------
Help/?: Get help on a group or a specific command
Up    : Move one command level up
Logout: Exit CLI

Command Groups:
---------------
System      : System settings and reset options
IP          : IP configuration and Ping
Port        : Port management
MAC         : MAC address table
VLAN        : Virtual LAN
PVLAN       : Private VLAN
Security    : Security management
STP         : Spanning Tree Protocol
Aggr        : Link Aggregation
LACP        : Link Aggregation Control Protocol
LLDP        : Link Layer Discovery Protocol
QoS         : Quality of Service
Mirror      : Port mirroring
Config      : Load/Save of configuration via TFTP
Firmware    : Download of firmware via TFTP
Loop Protect : Loop Protection
IPMC        : MLD/IGMP Snooping
Fault       : Fault Alarm Configuration
Event       : Event Selection
DHCPServer  : DHCP Server Configuration
iRing       : iRing Configuration
iChain      : iChain Configuration
iBridge     : iBridge Configuration
Fastrecovery : Fast-Recovery Configuration
DualPort    : Dual Port Recovery Configuration
RCS         : Remote Control Security
SFP         : SFP Monitor Configuration
DeviceBinding: Device Binding Configuration
Modbus      : Modebus TCP Configuration
Mrp: MRP Configuration
Auto-Logout  : Auto-Logout Timer Configuration
RSTP        : RSTP Configuration
Show        : Show Configuration

Type '<group>' to enter command group, e.g. 'port'.
Type '<group> ?' to get list of group commands, e.g. 'port ?'.
Type '<command> ?' to get help on a command, e.g. 'port mode ?'.
Commands may be abbreviated, e.g. 'por co' instead of 'port configuration'.
>
```

Figure 169 - Command Groups Printout

6.1.3.1 system

>system ?
Available Commands:

System Configuration [all | (port <port_list>)]
System Log Configuration
System Timezone Configuration
System Version
System Log Server Mode [enable|disable]
System Name [<name>]
System Timezone Offset [<offset>]
System Contact [<contact>]
System Log Server Address [<ip_addr_string>]
System Timezone Acronym [<acronym>]
System Description [<description>]
System DST Configuration
System Log Level [info|warning|error]
System DST Mode [disable|recurring|non-recurring]
System Location [<location>]
System DST start <week> <day> <month> <date> <year> <hour> <minute>
System Log Lookup [<log_id>] [all|info|warning|error]
System DST end <week> <day> <month> <date> <year> <hour> <minute>
System Log Clear [all|info|warning|error]
System DST Offset [<dst_offset>]
System Reboot
System Restore Default [keep_ip]
System Load
System INTP [enable|disable]
System Banner Title [<title>]
System Banner Message [<message>]
System>

6.1.3.2 IP

>IP ?
Available Commands:

IP Configuration
IP DHCP [enable|disable]
IP Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]
IP Ping <ip_addr_string> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]
IP SNTP Mode [enable|disable]
IP SNTP Server1 Add [<ip_addr_string>]
IP SNTP Server2 Add [<ip_addr_string>]
IP SNTP Server1 Delete
IP SNTP Server2 Delete
IP IPv6 AUTOCONFIG [enable|disable]
IP IPv6 Setup [<ipv6_addr>] [<ipv6_prefix>] [<ipv6_router>]
IP IPv6 State <ipv6_addr> [enable|disable]
IP IPv6 Ping6 <ipv6_addr> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]
IP IPv6 SNTP Server1 Add [<ipv6_addr>]
IP IPv6 SNTP Server2 Add [<ipv6_addr>]
IP IPv6 SNTP Server1 Delete
IP IPv6 SNTP Server2 Delete
>

6.1.3.3 port

>port ?
Available Commands:

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

6.1.3.4 MAC

>mac ?
Available Commands:

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

6.1.3.5 VLAN

>vlan ?
Available Commands:

VLAN Configuration [<port_list>]
VLAN PVID [<port_list>] [<vid>|none]
VLAN FrameType [<port_list>] [all|tagged|untagged]
VLAN IngressFilter [<port_list>] [enable|disable]
VLAN tx_tag [<port_list>] [untag_pvid|untag_all|tag_all]
VLAN PortType [<port_list>] [unaware|c-port|s-port|s-custom-port]
VLAN EtypeCustomSport [<etype>]
VLAN Add <vid>|<name> [<ports_list>]
VLAN Forbidden Add <vid>|<name> [<port_list>]
VLAN Delete <vid>|<name>
VLAN Forbidden Delete <vid>|<name>
VLAN Forbidden Lookup [<vid>] [(name <name>)]
VLAN Lookup [<vid>] [(name <name>)] [combined|static|nas|all]
VLAN Name Add <name> <vid>
VLAN Name Delete <name>
VLAN Name Lookup [<name>]
VLAN Status [<port_list>] [combined|static|nas|mstp|all|conflicts]
>

6.1.3.6 pvlan

>pvlan ?
Available Commands:

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

6.1.3.7 security

>security ?

Command Groups:

Switch : Switch security
Network : Network security
AAA : Authentication, Authorization and Accounting

Type '<group>' to enter command group
Type '<group> ?' to get group help

>security
Type 'up' to move up one level or '/' to go to root level

6.1.3.7.1 Security switch

Security>switch ?

Command Groups:

Security Switch Password : System password
Security Switch Privilege: Privilege level
Security Switch Auth : Authentication
Security Switch SSH : Secure Shell
Security Switch TELNET : Telnet management
Security Switch HTTPS : Hypertext Transfer Protocol over Secure Socket Layer
Security Switch RMON : Remote Network Monitoring

Type '<group>' to enter command group
Type '<group> ?' to get list of group commands
Type '<group> <command> ?' to get help on a command

6.1.3.7.1.1 Security Switch password

Security/Switch>
Security/Switch>password ?
Description:

Set the system password.

Syntax:

Security Switch Password <username> <password>

Parameters:

<username>: Username string.
<password>: System password string. Use 'clear' or "" to clear the string
Security/Switch>

6.1.3.7.1.2 Security Switch privilege

Security/Switch>privilege ?
Available Commands:

Security Switch Privilege Level Configuration
Security Switch Privilege Level Group <group_name>
[<cro>] [<crw>] [<sro>] [<srw>]
Security Switch Privilege Level Current

6.1.3.7.1.3 Security Switch authentication

Security/Switch>auth ?
Available Commands:

Security Switch Auth Configuration
Security Switch Auth Method [console|telnet|ssh|web] [none|local|radius|tacacs+] [enable|disable]
]
Security/Switch/Auth> configuration

Auth Configuration:
==========

Client	Authentication Method	Local Authentication Fallback
console	local	Disabled
telnet	local	Disabled
ssh	local	Disabled
web	local	Disabled

6.1.3.7.1.4 Security Switch SSH

Security/Switch/Auth>up
Security/Switch>ssh ?
Available Commands:

Security Switch SSH Configuration
Security Switch SSH Mode [enable|disable]:

6.1.3.7.1.5 Security Switch TELNET

Security/Switch>TELNET ?
Available Commands:

Security Switch TELNET Configuration
Security Switch TELNET Mode [enable|disable]
Security/Switch>

6.1.3.7.1.6 Security Switch HTTPS

Security/Switch>HTTPS ?
Available Commands:

Security Switch HTTPS Configuration
Security Switch HTTPS Mode [enable|disable]
Security/Switch>

6.1.3.7.1.7 Security Switch RMON

Security/Switch>rmon ?
Available Commands:

Security Switch RMON Statistics Add <stats_id> <data_source>
Security Switch RMON Statistics Delete <stats_id>
Security Switch RMON Statistics Lookup [<stats_id>]
Security Switch RMON History Add <history_id> <data_source> [<interval>] [<buckets>]
Security Switch RMON History Delete <history_id>
Security Switch RMON History Lookup [<history_id>]
Security Switch RMON Alarm Add <alarm_id> <interval> <alarm_variable> [absolute|delta]
<rising_threshold> <rising_event_index> <falling_threshold>
<falling_event_index> [rising|falling|both]
Security Switch RMON Alarm Delete <alarm_id>
Security Switch RMON Alarm Lookup [<alarm_id>]
Security Switch RMON Event Add <event_id> [none|log|trap|log_trap] [<community>]
[<description>]
Security Switch RMON Event Delete <event_id>
Security Switch RMON Event Lookup [<event_id>]
Security/Switch>

6.1.3.7.2Security network

Security>network ?

Command Groups:

Security Network Psec : Port Security Status
Security Network NAS : Network Access Server (IEEE 802.1X)
Security Network ACL : Access Control List
Security Network DHCP : Dynamic Host Configuration Protocol

6.1.3.7.1.1 Security Network psec

Security/Network>psec ?
Available Commands:

Security Network Psec Switch [<port_list>]
Security Network Psec Port [<port_list>]
Security/Network>

6.1.3.7.1.2 Security Network NAS

Security/Network>nas ?
Available Commands:

Security Network NAS Configuration [<port_list>]
Security Network NAS Mode [enable|disable]
Security Network NAS State [<port_list>] [auto|authorized|unauthorized|macbased]
Security Network NAS Reauthentication [enable|disable]
Security Network NAS ReauthPeriod [<reauth_period>]
Security Network NAS EapolTimeout [<eapol_timeout>]
Security Network NAS Agetime [<age_time>]
Security Network NAS Holdtime [<hold_time>]
Security Network NAS Authenticate [<port_list>] [now]
Security Network NAS Statistics [<port_list>] [clear|eapol|radius]
Security/Network>

6.1.3.7.1.3 Security Network ACL

Security/Network>acl ?
Available Commands:

Security Network ACL Configuration [<port_list>]
Security Network ACL Action [<port_list>] [permit|deny] [<rate_limiter>]
[<port_redirect>] [<mirror>] [<logging>] [<shutdown>]

Security Network ACL Policy [<port_list>] [<policy>]
Security Network ACL Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]
Security Network ACL Add [<ace_id>] [<ace_id_next>]
[(port <port_list>)] [(policy <policy> <policy_bitmask>)]
[<tagged>] [<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_redirect>] [<mirror>] [<logging>] [<shutdown>]
Security Network ACL Delete <ace_id>
Security Network ACL Lookup [<ace_id>]
Security Network ACL Clear
Security Network ACL Status [combined|static|loop_protect|dhcp|ipmc|conflicts]
Security Network ACL Port State [<port_list>] [enable|disable]
Security/Network>

6.1.3.7.1.4 Security Network DHCP

Security/Network>DHCP ?
Available Commands:

Security Network DHCP Relay Configuration
Security Network DHCP Relay Mode [enable|disable]
Security Network DHCP Relay Server [<ip_addr>]
Security Network DHCP Relay Information Mode [enable|disable]
Security Network DHCP Relay Information Policy [replace|keep|drop]
Security Network DHCP Relay Statistics [clear]
Security/Network>

6.1.3.7.3Security AAA

Security> AAA ?
Available Commands:

Security AAA Configuration
Security AAA Timeout [<timeout>]
Security AAA Deadtime [<dead_time>]
Security AAA RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>]
[<server_port>]
Security AAA ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>]
[<server_port>]
Security AAA TACACS+ [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>]
[<server_port>]
Security AAA Statistics [<server_index>]
Security>

6.1.3.8 STP

>stp ?
Available Commands:

STP Configuration
STP Version [<stp_version>]
STP Txhold [<holdcount>]
STP MaxHops [<maxhops>]
STP MaxAge [<max_age>]
STP FwdDelay [<delay>]
STP CName [<config-name>] [<integer>]
STP bpduFilter [enable|disable]

STP bpduGuard [enable|disable]
STP recovery [<timeout>]
STP Status [<msti>] [<stp_port_list>]
STP Msti Priority [<msti>] [<priority>]
STP Msti Map [<msti>] [clear]
STP Msti Add <msti> <vid-range>
STP Port Configuration [<stp_port_list>]
STP Port Mode [<stp_port_list>] [enable|disable]
STP Port Edge [<stp_port_list>] [enable|disable]
STP Port AutoEdge [<stp_port_list>] [enable|disable]
STP Port P2P [<stp_port_list>] [enable|disable|auto]
STP Port RestrictedRole [<stp_port_list>] [enable|disable]
STP Port RestrictedTcn [<stp_port_list>] [enable|disable]
STP Port bpduGuard [<stp_port_list>] [enable|disable]
STP Port Statistics [<stp_port_list>] [clear]
STP Port Mcheck [<stp_port_list>]
STP Msti Port Configuration [<msti>] [<stp_port_list>]
STP Msti Port Cost [<msti>] [<stp_port_list>] [<path_cost>]
STP Msti Port Priority [<msti>] [<stp_port_list>] [<priority>]
>

6.1.3.9 SNMP

>snmp ?
Available Commands:

SNMP Configuration
SNMP Mode [enable|disable]
SNMP Version [1|2c|3]
SNMP Read Community [<community>]
SNMP Write Community [<community>]
SNMP Trap Mode [enable|disable]
SNMP Trap Version [1|2c|3]
SNMP Trap Community [<community>]
SNMP Trap Destination [<ip_addr_string>]
SNMP Trap IPv6 Destination [<ipv6_addr>]
SNMP Trap Authentication Failure [enable|disable]
SNMP Trap Link-up [enable|disable]
SNMP Trap Inform Mode [enable|disable]
SNMP Trap Inform Timeout [<timeout>]
SNMP Trap Inform Retry Times [<retries>]
SNMP Trap Probe Security Engine ID [enable|disable]
SNMP Trap Security Engine ID [<engineid>]
SNMP Trap Security Name [<security_name>]
SNMP Engine ID [<engineid>]
SNMP Community Add <community> [<ip_addr>] [<ip_mask>]
SNMP Community Delete <index>
SNMP Community Lookup [<index>]
SNMP User Add <engineid> <user_name> [MD5|SHA]
    [<auth_password>] [DES] [<priv_password>]
SNMP User Delete <index>
SNMP User Changekey <engineid> <user_name>
    <auth_password> [<priv_password>]
SNMP User Lookup [<index>]
SNMP Group Add <security_model> <security_name> <group_name>
SNMP Group Delete <index>
SNMP Group Lookup [<index>]
SNMP View Add <view_name> [included|excluded] <oid_subtree>
SNMP View Delete <index>
SNMP View Lookup [<index>]
SNMP Access Add <group_name> <security_model> <security_level>

```
    [<read_view_name>] [<write_view_name>]
SNMP Access Delete <index>
SNMP Access Lookup [<index>]
>
```

6.1.3.10 aggr

```
>aggr ?
Available Commands:

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

6.1.3.11 lacp

```
>lacp ?
Available Commands:

LACP Configuration [<port_list>]
LACP Mode [<port_list>] [enable|disable]
LACP Key [<port_list>] [<key>]
LACP Prio [<port_list>] [<prio>]
LACP System Prio [<sysprio>]
LACP Role [<port_list>] [active|passive]
LACP Status [<port_list>]
LACP Statistics [<port_list>] [clear]
LACP Timeout [<port_list>] [fast|slow]
>
```

6.1.3.12 lldp

```
>lldp ?
Available Commands:

LLDP Configuration [<port_list>]
LLDP Mode [<port_list>] [enable|disable]
LLDP Statistics [<port_list>] [clear]
LLDP Info [<port_list>]
>
```

6.1.3.13 qos

```
>qos ?
Available Commands:

QoS Configuration [<port_list>]
QoS Port Classification Class [<port_list>] [<class>]
QoS Port Classification DPL [<port_list>] [<dpl>]
QoS Port Classification PCP [<port_list>] [<pcp>]
QoS Port Classification DEI [<port_list>] [<dei>]
QoS Port Classification Tag [<port_list>] [enable|disable]
QoS Port Classification Map [<port_list>] [<pcp_list>] [<dei_list>] [<class>] [<dpl>]
QoS Port Classification DSCP [<port_list>] [enable|disable]
QoS Port Policer Mode [<port_list>] [enable|disable]
QoS Port Policer Rate [<port_list>] [<rate>]
QoS Port Policer Unit [<port_list>] [kbps|fps]
QoS Port Policer FlowControl [<port_list>] [enable|disable]
QoS Port QueuePolicer Mode [<port_list>] [<queue_list>] [enable|disable]
```

QoS Port QueuePolicer Rate [<port_list>] [<queue_list>] [<bit_rate>]
QoS Port Scheduler Mode [<port_list>] [strict|weighted]
QoS Port Scheduler Weight [<port_list>] [<queue_list>] [<weight>]
QoS Port Shaper Mode [<port_list>] [enable|disable]
QoS Port Shaper Rate [<port_list>] [<bit_rate>]
QoS Port QueueShaper Mode [<port_list>] [<queue_list>] [enable|disable]
QoS Port QueueShaper Rate [<port_list>] [<queue_list>] [<bit_rate>]
QoS Port QueueShaper Excess [<port_list>] [<queue_list>] [enable|disable]
QoS Port TagRemarking Mode [<port_list>] [classified|default|mapped]
QoS Port TagRemarking PCP [<port_list>] [<pcp>]
QoS Port TagRemarking DEI [<port_list>] [<dei>]
QoS Port TagRemarking Map [<port_list>] [<class_list>] [<dpl_list>] [<pcp>] [<dei>]
QoS Port DSCP Translation [<port_list>] [enable|disable]
QoS Port DSCP Classification [<port_list>] [none|zero|selected|all]
QoS Port DSCP EgressRemark [<port_list>] [disable|enable|remap_dp_unaware|remap_dp_aware]
QoS DSCP Map [<dscp_list>] [<class>] [<dpl>]
QoS DSCP Translation [<dscp_list>] [<trans_dscp>]
QoS DSCP Trust [<dscp_list>] [enable|disable]
QoS DSCP Classification Mode [<dscp_list>] [enable|disable]
QoS DSCP Classification Map [<class_list>] [<dpl_list>] [<dscp>]
QoS DSCP EgressRemap [<dscp_list>] [<dpl_list>] [<dscp>]
QoS Storm Unicast [enable|disable] [<packet_rate>]
QoS Storm Multicast [enable|disable] [<packet_rate>]
QoS Storm Broadcast [enable|disable] [<packet_rate>]
QoS QCL Add [<qce_id>] [<qce_id_next>]
  [<port_list>]
  [<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type>]
  [(etype [<etype>]) |
  (LLC [<DSAP>] [<SSAP>] [<control>]) |
  (SNAP [<PID>]) |
  (ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) |
  (ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])]
  [<class>] [<dp>] [<classified_dscp>]
QoS QCL Delete <qce_id>
QoS QCL Lookup [<qce_id>]
QoS QCL Status [combined|static|conflicts]
QoS QCL Refresh
>

6.1.3.14 mirror

>mirror ?
Available Commands:

Mirror Configuration [<port_list>]
Mirror Port [<port>|disable]
Mirror Mode [<port_cpu_list>] [enable|disable|rx|tx]
>

6.1.3.15 config

>config ?
Available Commands:

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

6.1.3.16 firmware

>firmware ?
Available Commands:

Firmware Load <ip_addr_string> <file_name>
Firmware IPv6 Load <ipv6_server> <file_name>
Firmware Information
Firmware Swap
>

6.1.3.17 loop protect

>loop protect ?
Available Commands:

Loop Protect Configuration
Loop Protect Mode [enable|disable]
Loop Protect Transmit [<transmit-time>]
Loop Protect Shutdown [<shutdown-time>]
Loop Protect Port Configuration [<port_list>]
Loop Protect Port Mode [<port_list>] [enable|disable]
Loop Protect Port Action [<port_list>] [shutdown|shut_log|log]
Loop Protect Port Transmit [<port_list>] [enable|disable]
Loop Protect Status [<port_list>]
>

6.1.3.18 ipmc

>ipmc ?
Available Commands:

IPMC Configuration [igmp]
IPMC Mode [igmp] [enable|disable]
IPMC Flooding [igmp] [enable|disable]
IPMC VLAN Add [igmp] <vid>
IPMC VLAN Delete [igmp] <vid>
IPMC State [igmp] [<vid>] [enable|disable]
IPMC Querier [igmp] [<vid>] [enable|disable]
IPMC Fastleave [igmp] [<port_list>] [enable|disable]
IPMC Router [igmp] [<port_list>] [enable|disable]
IPMC Status [igmp] [<vid>]
IPMC Groups [igmp] [<vid>]
IPMC Version [igmp] [<vid>]
>

6.1.3.19 fault

>fault ?
Available Commands:

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

6.1.3.20 event

>event ?
Available Commands:

Event Configuration
Event Syslog SystemStart [enable|disable]
Event Syslog PowerStatus [enable|disable]
Event Syslog SnmpAuthenticationFailure [enable|disable]
Event Syslog RingTopologyChange [enable|disable]
Event Syslog Port [<port_list>] [disable|linkup|linkdown|both]
Event SMTP SystemStart [enable|disable]

Event SMTP PowerStatus [enable|disable]
Event SMTP SnmpAuthenticationFailure [enable|disable]
Event SMTP RingTopologyChange [enable|disable]
Event SMTP Port [<port_list>] [disable|linkup|linkdown|both]
>

6.1.3.21 dhcpserver

>dhcpserver ?
Available Commands:

DHCPServer Mode [enable|disable]
DHCPServer Setup [<ip_start>] [<ip_end>] [<ip_mask>] [<ip_router>] [<ip_dns>] [<ip_tftp>] [<lease>] [<bootfile>]
DHCPServer Client List
DHCPServer Client AddStatic <mac_addr> <ip_addr>
DHCPServer Client Delete <no.>
DHCPServer Client SetStatic <no.>
>

6.1.3.22 iRing

>iring ?
Available Commands:

iRing Mode [enable|disable]
iRing Master [enable|disable]
iRing 1stRingPort [<port>]
iRing 2ndRingPort [<port>]
iRing Ring-Linking Mode [enable|disable]
iRing Ring-Linking Port [<port>]
iRing Dual-Homing Mode [enable|disable]
iRing Dual-Homing Port [<port>]
>

6.1.3.23 ichain

>ichain ?
Available Commands:

iChain Configuration
iChain Configuration
iChain Mode [enable|disable]
iChain 1stUplinkPort [<port>]
iChain 2ndUplinkPort [<port>]
iChain EdgePort [1st|2nd|none]
>

6.1.3.24 ibridge

>ibridge ?
Available Commands:

iBridge Configuration
iBridge Mode [enable|disable]
iBridge 1stRingPort [<port>]
iBridge 2ndRingPort [<port>]
iBridge Vender [moxx|advantexx|hirschmaxx]
>

6.1.3.25 fastrecovery

>fastrecovery ?

Available Commands:

Fastrecovery Mode [enable|disable]
Fastrecovery Port [<port_list>] [<fr_priority>]
>

6.1.3.26 dualport

>dualport ?
Available Commands:

DualPort Configuration [enable|disable]
DualPort Port <port>
DualPort Interval <integer>
DualPort Retry <integer>
DualPort TimeoutDelay <integer>
DualPort DebugMessage [enable|disable]
>

6.1.3.27 rcs

>rcs ?
Available Commands:

RCS Mode [enable|disable]
RCS Add [<ip_addr>] [<port_list>] [web_on|web_off] [telnet_on|telnet_off] [snmp_on|snmp_off]
RCS Del <index>
RCS Configuration

6.1.3.28 sfp

>sfp ?
Available Commands:

SFP syslog [enable|disable]
SFP temp [<temperature>]
SFP Info

6.1.3.29 MRP

>mrp ?
Available Commands:

MRP Configuration
MRP Mode [enable|disable]
MRP Manager [enable|disable]
MRP React [enable|disable]
MRP 1stRingPort [<mrp_port>]
MRP 2ndRingPort [<mrp_port>]
MRP Parameter MRP_TOPchgT [<value>]
MRP Parameter MRP_TOPNRmax [<value>]
MRP Parameter MRP_TSTshortT [<value>]
MRP Parameter MRP_TSTdefaultT [<value>]
MRP Parameter MRP_TSTNRmax [<value>]
MRP Parameter MRP_LNKdownT [<value>]
MRP Parameter MRP_LNKupT [<value>]
MRP Parameter MRP_LNKNRmax [<value>]

6.1.3.30 devicebinding

>devicebinding ?
Available Commands:

DeviceBinding Mode [enable|disable]
DeviceBinding Port Mode [<port_list>] [disable|scan|binding|shutdown]
DeviceBinding Port DDOS Mode [<port_list>] [enable|disable]
DeviceBinding Port DDOS Sensibility [<port_list>] [low|normal|medium|high]
DeviceBinding Port DDOS Packet [<port_list>]
[rx_total|rx_unicast|rx_multicast|rx_broadcast|tcp|udp]
DeviceBinding Port DDOS Low [<port_list>] [<socket_number>]
DeviceBinding Port DDOS High [<port_list>] [<socket_number>]
DeviceBinding Port DDOS Filter [<port_list>] [source|destination]
DeviceBinding Port DDOS Action [<port_list>]
[do_nothing|block_1_min|block_10_mins|block|shutdown|only_log]
DeviceBinding Port DDOS Status [<port_list>]
DeviceBinding Port Alive Mode [<port_list>] [enable|disable]
DeviceBinding Port Alive Action [<port_list>] [do_nothing|link_change|shutdown|only_log]
DeviceBinding Port Alive Status [<port_list>]
DeviceBinding Port Stream Mode [<port_list>] [enable|disable]
DeviceBinding Port Stream Action [<port_list>] [do_nothing|only_log]
DeviceBinding Port Stream Status [<port_list>]
DeviceBinding Port Addr [<port_list>] [<ip_addr>] [<mac_addr>]
DeviceBinding Port Alias [<port_list>] [<ip_addr>]
DeviceBinding Port DeviceType [<port_list>] [unknown|ip_cam|ip_phone|ap|pc|plc|nvr]
DeviceBinding Port Location [<port_list>] [<device_location>]
DeviceBinding Port Description [<port_list>] [<device_description>]
>

6.1.3.31 modbus

>modbus ?
Available Commands:

Modbus Status
Modbus Mode [enable|disable]
>

6.1.3.32 auto-logout

>auto-logout ?
Available Commands:

Auto-Logout CLI [<timer>]
Auto-Logout Web [<timer>]
>

6.1.3.33 rstp

>RSTP ?
Available Commands:

RSTP Configuration
RSTP Mode [<rstp_mode>]
RSTP BridgePriority [<priority>]
RSTP HelloTime [<hello>]
RSTP MaxAge [<max_age>]
RSTP FwdDelay [<delay>]
RSTP Status [<stp_port_list>]
RSTP Port Configuration [<stp_port_list>]
RSTP Port Mode [<stp_port_list>] [enable|disable]
RSTP Port Edge [<stp_port_list>] [enable|disable]
RSTP Port AutoEdge [<stp_port_list>] [enable|disable]
RSTP Port P2P [<stp_port_list>] [enable|disable|auto]
RSTP Port Cost [<stp_port_list>] [<path_cost>]

RSTP Port Priority [<stp_port_list>] [<priority>]
>

6.1.3.34 show

>show ?
Available Commands:

Show Configuration Switch
Show Configuration Port <port_list>
>

7. APPENDIX A: IES20GF MODBUS INFORMATION

*Device ID/PLC is 1
*04 Read Input Register (3x) should be used.
*The returned values are in hex format

Address	Description
16	VendorName
48	ProductName
81	Version
85	MacAddress
256	SysName
512	SysDescription
768	SysLocation
1024	SysContact
4096	PortStatus: Port :1~VTSS_PORTS Value :0x0000 Link down 0x0001 Link up 0x0002 Disable 0xffff NoPort
4352	PortSpeed: Port :1~VTSS_PORTS Value :0x0000 10M-Half 0x0001 10M-Full 0x0002 100M-Half 0x0003 100M-Full 0x0004 1G-Half 0x0005 1G-Full 0xffff NoPort
4608	PortFlowCtrl : Port :1~VTSS_PORTS Value :0x0000 Off 0x0001 On 0xffff NoPort