NT4008 Industrial Ethernet Managed Switch Series

Software Guide | July 2021

LP1161 | Revision B

COPYRIGHT

SOFTWARE LICENSE

Software supplied with each Red Lion® product remains the exclusive property of Red Lion. Red Lion grants with each unit a perpetual license to use this software with the express limitations that the software may not be copied or used in any other product for any purpose. It may not be reverse engineered, or used for any other purpose other than in and with the computer hardware sold by Red Lion.

Red Lion Controls, Inc.
20 Willow Springs Circle
York, PA 17406

CONTACT INFORMATION:

AMERICAS

Inside US: +1 (877) 432-9908
Outside US: +1 (717) 767-6511
Hours: 8 am-6 pm Eastern Standard Time
(UTC/GMT -5 hours)

ASIA-PACIFIC

Shanghai, P.R. China: +86 21-6113-3688 x767
Hours: 9 am-6 pm China Standard Time
(UTC/GMT +8 hours)

EUROPE

Netherlands: +31 33-4723-225
France: +33 (0) 1 84 88 75 25
Germany: +49 (0) 1 89 5795-9421
UK: +44 (0) 20 3868 0909
Hours: 9 am-5 pm Central European Time
(UTC/GMT +1 hour)

Website: www.redlion.net
Support: support.redlion.net

Table of Contents

Preface

Disclaimer

Portions of this document are intended solely as an outline of methodologies to be followed during the maintenance and operation of the NT4008 Industrial Ethernet Managed Switch Series equipment. It is not intended as a step-by-step guide or a complete set of all procedures necessary and sufficient to complete all operations.

While every effort has been made to ensure that this document is complete and accurate at the time of release, the information that it contains is subject to change. Red Lion Controls, Inc. is not responsible for any additions to or alterations of the original document. Industrial networks vary widely in their configurations, topologies, and traffic conditions. This document is intended as a general guide only. It has not been tested for all possible applications, and it may not be complete or accurate for some situations.

Users of this document are urged to heed warnings and cautions used throughout the document.

Trademark Acknowledgments

Red Lion Controls acknowledges and recognizes ownership of the following trademarked terms used in this document.

- Ethernet is a registered trademark of Xerox Corporation.
- PROFINET® is a registered trademark of PROFIBUS and PROFINET International (PI).

All other company and product names are trademarks of their respective owners.

Document History and Related Publications

The hard copy and electronic media versions of this document are revised only at major releases and therefore, may not always contain the latest product information. Tech Notes and/or product addendums will be provided as needed between major releases to describe any new information or document changes.

The latest online version of this document and all product updates can be accessed through the Red Lion web site at www.redlion.net/support/documentation.

Additional Product Information

Additional product information can be obtained by contacting the local sales representative or Red Lion through the contact numbers and/or support e-mail address listed on the inside of the front cover.

Chapter 1 Security Best Practices

Introduction

It is more important than ever to secure network devices from unauthorized access, both within and outside of your organization. Red Lion Controls strongly recommends immediately changing all default user accounts and passwords, as well as disabling protocols that are not needed in your application.

Protocols and user names with their default passwords are listed in the table below:

PROTOCOLS/USERS	DEFAULT NAME	DEFAULT PASSWORD
User Login	admin	admin
SNMP v1/v2c	read community	public
SNMP v1/v2c	write community	private
SNMP v1/v2c	trap community	public

Some protocols are enabled by default for the best overall out of the box experience. However, if any in this group will not be used or needed in your network, then these should be disabled to prevent unexpected behavior, unauthorized access or usage. These protocols are listed in the table below:

PROTOCOLS
SNMP
LLDP

Default Passwords

User Passwords

The NT4008 ships from the factory with a default ***admin*** user account. Red Lion strongly recommends creating a new user with administrative privileges before the unit is deployed.

At a minimum, the default password for the ***admin*** user should be changed. The first time a login is made with the admin account the user will be prompted to change the default password.

SNMP v1/v2c Community Names

The NT4008 ships with default Community Names for SNMP v1/v2c operation. SNMP v1/v2c traffic, per the standard, is neither hashed nor encrypted. Therefore, it is Red Lion's recommendation that customers requiring SNMP use SNMP v3, which offers more secure SNMP communication.

If SNMP v1/v2c is required in your application, Red Lion strongly recommends changing the default SNMP credentials before deployment.

See the Disabling Unused Protocols section if SNMP will not be used.

Legacy Protocols

When multiple revisions of a protocol are supported, Red Lion enables the most secure revision by default and disables legacy (unsecure) versions of the protocol. We strongly recommend leaving the older revisions disabled.

LEGACY PROTOCOL	SECURE PROTOCOL EQUIVALENT
HTTP	HTTPS

LEGACY PROTOCOL	SECURE PROTOCOL EQUIVALENT
Telnet	SSH

Disabling Unused Protocols

Certain network protocols are enabled by default for the best overall out of the box experience. However, some of these protocols and devices have the capability of configuring and/or reading network settings or causing unexpected network behavior. These protocols and devices should be disabled when they are not being utilized in your network to prevent unexpected behavior, unauthorized access and/or control of your network and individual network devices.

The following protocols meet these criteria:

- SNMP
- LLDP

Chapter 2 Introduction

NT4008 Series Key Features

Red Lion's NT4008 Gigabit Managed Industrial Ethernet switches are certified to meet PROFINET PNIO v2.34 conformance class B (CC-B), RT Class 1 standards to ensure seamless integration into PROFINET networks using standard PLC configuration and management tools. A GSDML file is provided.

Housed in rugged IP30 metal enclosures, the NT4008 switches offer -40 to 75 ˚C operating temperature, redundant 12-58 VDC power inputs, reverse polarity protection, LED link and activity status indication, a configurable alarm contact, and are certified for use in hazardous, marine and rail applications.

Two port configurations are available:

- Eight 10/100/1000 RJ45 ports
- Six 10/100/1000 RJ45 ports and two dual mode SFP slots for optional 100Base or 1000Base SFP transceivers

The NT4008 series is designed for ease of installation and years of trouble free operation with a robust feature set that includes DHCP Server, SNMP v1/v2c/v3, IGMP v1/v2/v3, LLDP, MRP, RSTP, MSTP, Fast Ring and Chain protocols, VLANs, MAC/IP port security, ACL, QoS, Syslog, NTP, LACP/LAG (static and dynamic link aggregation), port mirroring, sFlow, and Multicast/Broadcast storm protection.

For use in MRP topologies, MRM (MRP Manager) or MRC (MRP Client) configurations are available.

PART NUMBER	DESCRIPTION	TOTAL PORTS	10/100/1000 BaseT(X)	100/1000 SFP	MRP MANAGER
NT-4008-000-PN-C	8-port Gigabit Managed Industrial Ethernet Switch (8 10/100/1000BaseT RJ45 ports, PNIO CC-B, MRC	8	8		MRC
NT-4008-000-PN-M	8-port Gigabit Managed Indsutrial Ethernet Switch (8 10/100/1000BaseT RJ45 ports), PNIO CC-B, MRM	8	8		MRM
NT-4008-DM2-PN-C	8-port Gigabit Managed Industrial Ethernet Switch (6 10/100/1000BaseT RJ45 ports, 2 Dual Mode 100/1000Base SFP expansion slots, PNIO CC-B, MRC	8	6	2	MRC
NT-4008-DM2-PN-M	8-port Gigabit Managed Industrial Ethernet Switch (6 10/100/1000BaseT RJ45 ports, 2 Dual Mode 100/1000Base SFP expansion slots, PNIO CC-B, MRM	8	6	2	MRM

SFP transceivers are sold separately.

Summary of Features

FEATURE	DESCRIPTION
Alarms and Events	Supports Alarms, Alarm Relay Contact, Event Logging, and Syslog
Bridging and Forwarding	IEEE 802.1D/802.1Q transparent bridging Dynamic data switching Store-and-forward wire-speed switching Frame buffering MAC address learning • Configurable aging time or aging disable • Per-port learning modes: auto, disabled, secure (static only) • Learning-disabled VLANs MAC address table capacity up to: • 16K MAC addresses • 1024 static MAC addresses
Configuration Management	• Save, restore, activate, and delete configurations • Reset factory defaults • Import and export configurations
DHCP	DHCP IPv4 and DHCP IPv6 Client DHCP Client supports Option 61 client identifier DHCP Relay Agent supports Option 82 circuit and remote identifiers DHCP Server supports: • Option 12 client name • Option 60 vendor class identifier • Option 43 vendor specific information DHCP Snooping
Diagnostics	Front panel view: browser displays port and LED status Ping and traceroute VeriPHY cable diagnostics
IP Multicast Filtering and Routing	IGMP: IPv4 Internet Group Management Protocol • IGMPv1 (IETF RFC 1112) • IGMPv2 (IETF RFC 2236) • IGMPv3 (IETF RFC 3376) MLD: IPv6 Multicast Listener Discovery • MLDv1 (IETF RFC 2710) • MLDv2 (IETF RFC 3810) Options • Snooping, Querier, Proxy, Leave Proxy • Profiles: To limit multicast ranges per port • Control of unregistered multicast flooding SSM: Source-Specific Multicast (IETF RFC 3569, 4604, 4607)
L2 Redundancy Protocols	Media Redundancy Protocol • MRC (MRP client) • MRM (MRP manager) on specific models Spanning Tree Protocols • STP • RSTP • MSTP Ring Protocol • Ring and Chain (RingV2) with fast fault recovery Loop Protection
L3 Static IP Routing	Capacity up to: • 32 static routes
Link Aggregation (Port Trunking)	Supports static or dynamic port groups (LACP). Capacity up to: • 4 LAG groups • 8 ports per group

FEATURE	DESCRIPTION
	• Configurable destination port selection algorithm
Link Layer Discovery Protocol	LLDP advertises information about a device and neighboring devices • LLDP • LLDP-MED
Maintenance	Restart Reset to factory defaults Firmware upgrade Active and alternative firmware images
Network Security	Port Security • Limits the number of MACs using a port • Management of limit violations IP Source Guard • Limits the number of IPs using a port ACL: Access Control List • Matches: MAC address, IP address, TCP/UDP port, Class of Service, and other criteria • Actions: deny ingress, permit ingress, filter egress, redirect, rate limit, mirror, log, port shutdown, count matching frames, and other actions ARP Inspection
Port Configuration	Configurable • Port enable/disable • Speed • Duplex • Flow Control • Priority Flow Control • Maximum Frame Size • Excessive Collision Mode • Frame Length Check • Port Description
PROFINET	MRP: Media Redundancy Protocol MRC: Media Redundancy Client (all models) MRM: Media Redundancy Manager (select models)
Quality of Service and Traffic Management	CoS (IEEE 802.1Q) and Differentiated Services (DiffServ/DSCP) Ingress Port Frame Classification Ingress Port Policing (rate limiting, flow control) Ingress Port Policing per QoS Queue Egress Port Scheduling (Strict, Deficit Weighted Round Robin, Strict+DWRR) Egress Port Shaping (rate limiting per queue and port) Egress Port Tag Remarking (reclassification of QoS on egress) DSCP enable, classification, and rewriting DSCP-Based QoS DSCP Translation DSCP Classification (CoS to DSCP mapping) Storm Policing (control storming of broadcast, multicast, and unknown unicast) WRED (Weighted Random Early Detection congestion avoidance) QoS Control List: assignment of QoS values based on frame content • Source/Destination MAC • VLAN tag and CoS priority values • VLAN double-tagging values Frame Type and values (EtherType, LLC, SNAP, IPv4, IPv6)
Switch Management and Security	Management Interfaces • Console port session with automatic logout after inactivity • IPv4 and IPv6 access • Up to 4 Telnet and SSH sessions with automatic logout after inactivity • Up to 20 HTTP and HTTPS sessions • SNMP v1, v2c, and v3 • Access managed by user's VLAN and IP address

FEATURE	DESCRIPTION
	Date and Time • Manual or NTP (Network Time Protocol) • Time Zone and Daylight Saving Time User Management • Up to 20 user accounts • Users are assigned to one of 15 privilege levels • Privilege levels grant access to specific switch features SNMP Security • SNMPv2 community strings • SNMPv3 users with MD5 or SHA passwords RMON • Statistics, history, alarms, and events System Information Contact, name, and location
Traffic Monitoring	Port Mirroring • Mirrors frames from ingress ports to analysis ports • Rmirror: Remote mirroring access across switches • Mirroring as an ACL action SFlow • Exports packet samples and interface counters
Virtual Local Area Networks	IEEE 802.1Q VLAN IDs from 1 to 4094 Management Access VLANs Standard VLAN tagging Double Tagging (QinQ, VLAN Stacking) SVL: Shared VLAN Learning MAC-based VLAN assignment Protocol-based VLAN assignment IP Subnet-based VLAN assignment ACL filtering by VLAN tag and priority Learning-disabled VLANs

Description of Features

The switch provides a wide range of advanced performance enhancing features. Flow control eliminates the loss of packets due to bottlenecks caused by port saturation. Broadcast storm suppression prevents broadcast traffic storms from overwhelming the network. Untagged access, tagged (trunk), hybrid, and protocol-based VLANs provide traffic security and efficient use of network bandwidth. CoS priority queuing ensures the minimum delay for moving real-time multimedia data across the network, while IP multicast filtering and routing provides support for real-time network applications.

Some of the key features are briefly described in the following sections.

Alarms and Events

Event Logging

The switch logs alarms and important system events as they occur. The most recent events are visable via the web interface. Events include:

- System startup and shutdown
- Port links going up and down
- Alarm LED state change

Alarms and Alarm Relay Contact

Certain system events (such as a port going link down or loss of a power input) can be configured to trigger an alarm. Alarms engage the Alarm Relay Contact on the exterior of the switch and are displayed on the web interface.

Syslog

The Syslog protocol, as specified in RFC-3164 and RFC-5424, allows sending system events to a remote logging device, known as a Syslog Collector or Server.

Bridging and Forwarding

The switch supports IEEE 802.1D/802.1Q transparent bridging.

MAC Address Table

A MAC address table facilitates data switching by learning MAC addresses on specific interfaces (ports and VLANs), and filtering or forwarding traffic based on this information. The address table is commonly called an FDB (forwarding database), an ARL (address resolution logic) table, or a FIB (forwarding information base).

MAC Learning

Normally, a given MAC address is learned on a particular interface (VLAN and port). This happens every time a frame enters the port with the given MAC address set as the **source** address. The MAC/VLAN/Port combination is stored in the MAC address table.

When a frame enters the switch the **destination** MAC address in the frame is checked against the table and the frame is forwarded to the appropriate port. If the destination MAC is not in the table, then the frame is forwarded to all ports in the VLAN.

Aging Time

The configurable Aging Time determines how long that MAC will remain in the table. If the MAC is not seen again on that interface, then after the aging time elapses, the MAC is removed (aged out) from the table. When aging is disabled, a learned MAC is never aged out.

Port MAC Learning Mode

The MAC learning mode of a port can be one of three modes.

- **Auto:** MACs are learned automatically when an unknown source MAC is seen. This is the default mode.
- **Disable:** Learning is disabled for all MACs. No source MAC entering the port is learned and traffic sent to that MAC therefore floods to ports in the VLAN.
- **Secure:** Learning is disabled for all MACs, except for MACs in the Static MAC Address Table. This allows traffic to flow to only authorized MACs on authorized ports.

Static MAC Address Table

A static MAC address can be assigned to a specific interface on the switch. A static address will not be learned dynamically on any other interface. As a result, all traffic having that particular MAC destination will forward only to the assigned interface. Static addresses can be used to provide network security by restricting traffic for a known host to a specific interface or to ensure that a MAC destination is always known to the switch even if traffic from the device is rarely seen on that interface and would normally age out.

Learning-disabled VLANs

If learning is disabled on a VLAN, then no source MAC addresses arriving on that VLAN are stored in the MAC address table. As a result, all frames entering a port in the VLAN will forward to every port in that VLAN. The only exception would be any static MAC addresses.

Static MAC Addresses

A static MAC address can be assigned to a specific interface on the switch. A static address will not be learned dynamically on any other interface. As a result, all traffic having that particular MAC destination will forward only to the assigned interface. Static addresses can be used to provide network security by restricting traffic for a known host to a specific interface or to ensure that a MAC destination is always known to the switch even if traffic from the device is rarely seen on that interface.

Store-and-Forward and Buffering

The switch copies each frame into its memory before forwarding them to another port. This ensures that all frames are a standard Ethernet size and have been checked for corruption using a cyclic redundancy check (CRC). This prevents bad frames from entering the network and wasting bandwidth.

To avoid dropping egressing frames on congested ports, the switch queues up frame buffers and transmits them when able within the limits of the available frame buffers.

Configuration Management

A switch configuration consists of all the options that can be modified by a user. A user with the appropriate privilege can:

- Modify the configuration and apply changes dynamically to the switch
- Save the current configuration to a persistent file so that this configuration is applied when the switch reboots
- Restore the current configuration to the last saved configuration
- Reset the configuration to factory defaults
- Export the configuration to a computer where it can be edited
- Import a configuration

This switch can manage multiple configurations. This includes creating, deleting, and activating (applying) configurations.

An imported configuration can be saved as a new configuration or it can replace or be merged into an existing configuration.

The running-config is not persistent. It is the currently active configuration and can be modified and saved as the new startup-config.

This switch begins with two persistent configurations:

- startup-config: this configuration is applied at boot up. It is copied to the running-config.
- default-config: this is the factory default configuration and can never be modified.

DHCP

DHCP (Dynamic Host Configuration Protocol) simplifies network configuration by automatically assigning IP addresses from a DHCP server to connected DHCP capable devices (DHCP clients).

This switch can be configured as a:

- DHCP client, with Option 61
- DHCP relay agent, with Option 82
- DHCP server, with Option 12, 43, 60, 61, and others

The switch also supports DHCP Snooping.

DHCP Client

The switch will automatically obtain an IP assignment from a DHCP server, and fallback to a pre-configured IP address if unable to get an IP from a server. Communication between the client and server can optionally go through a DHCP Relay Agent.

DHCP Option 61 allows a client to specify its unique client identifier. A server can assign a unique IP address to the client based on this identifier.

DHCP Relay Agent

A DHCP Relay Agent brokers DHCP traffic between a DHCP client and DHCP server.

It is not always practical to have a DHCP server on every subnet of a network. A relay agent enables a client on one network interface or VLAN to communicate with a server on a different interface or VLAN. This enables the use of one centralized DHCP server across multiple networks.

DHCP Option 82 allows a relay agent to have a unique Relay Agent ID and to have unique Relay Agent Circuit IDs for each port of the switch. This information is passed on to the DHCP server when a DHCP client is requesting an IP from the server. A DHCP server can assign a unique IP address based on the identity of the relay agent and the identity of the relay agent port that the client communicates through. As a consequence, a device on a specific relay agent port can receive a specific IP address and, if the device is replaced, the replacement receives the same IP address as the original device.

DHCP Server

A DHCP Server allows DHCP Client devices to automatically obtain an IP assignment from the server. IP assignments can be set up as a pool of IP addresses available to any client device; or specific IP addresses based on the clients Client ID (Option 61), or Relay Agent ID and Relay Agent Circuit ID (Option 82).

DHCP Snooping

DHCP snooping is a security enhancement that prevents malicious DHCP attacks. It tracks how trusted DHCP servers assign IP addresses to clients and uses this information to block DHCP traffic from untrusted DHCP servers, as well as other malicious DHCP traffic.

IP Multicast Filtering and Routing

IGMP

IGMP (Internet Group Management Protocol) is a protocol that manages how multicast traffic is routed across a network. Without IGMP, all multicast traffic is forwarded across the entire network. With IGMP, an IGMP-aware client can request specific multicast group data from a data provider. An IGMP-aware router or switch can intelligently route the multicast traffic from the data provider to only the ports where the clients are connected. This reduces unneeded network traffic.

Port Filtering Profiles

This switch supports access control lists for IGMP. It can be configured per-port to:

- Permit or deny all multicast traffic
- Permit or deny traffic for specific multicast groups
- Limit the number of multicast groups (channels)

IGMP and MLD Snooping

When IGMP Snooping (for IPv4) or MLD Snooping (for IPv6) is enabled on an interface, the switch snoops IGMP or MLD protocol traffic to route the multicast traffic. Various options are configurable including:

- IGMP version

- IGMP mode: Snooping, Querier, Proxy, and Leave Proxy
- Allowing or disallowing the flooding of unregistered multicast traffic.
- Enabling Source Specific Multicast (SSM), which allows a client to request multicast traffic from a specific provider.

Multicast Static Routing

Multicast traffic may be routed to specific ports via an entry in the Static MAC table. This ensures that a client will receive multicast data, even if it does not support the IGMP protocol.

L2 Redundancy Protocols

This switch can be connected to other devices using a Spanning Tree Protocol, a Ring & Chain (Ring V2) protocol, or Media Redundancy Protocol (described under PROFINET). A Loop Protection protocol can be enabled to detect network loops and shutdown and/or log this event.

Spanning Tree Protocols

STP establishes a simple connected active network topology (a spanning tree) from the arbitrary connections between the bridges (switches) of a bridged network. STP will set some ports to forwarding and others to blocking to prevent network loops. The bridges in the network will exchange sufficient information to automatically derive the spanning tree.

The switch supports these spanning tree protocols:

- **Spanning Tree Protocol (STP, IEEE 802.1D and IEEE 802.1Q-2014):** This protocol provides loop detection. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. If the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.
- **Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w and IEEE 802.1Q-2014):** This protocol reduces the convergence time for network topology changes to about 3 to 5 seconds, compared to 30 seconds or more for the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but will still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.
- **Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s and IEEE 802.1Q-2005):** This protocol is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group (as sometimes occurs with IEEE 802.1D STP). MSTP will interoperate with RSTP and STP devices.

Ring & Chain (RingV2)

Ring & Chain provides for very quick fail-over (in milliseconds) to a redundant network path when a link in the current network path goes down. The topology of the network must be either a ring or a chain. The setup for Ring & Chain is described in detail in the chapter “Ring Version 2”.

Loop Protection

Loop protection is a protocol that sends frames (PDUs) out selected ports and listens for these PDUs to detect when there is a loop in a connected network. If a loop is found, this event can be logged and the port can be shutdown for a configurable amount of time.

L3 Static IP Routing

The switch supports Layer 3 Static IP routing.

- Routing to statically configured hosts or subnet addresses is provided based on gateway and the distance (for IPv4) or next hop VLAN (for IPv6) specified in the static routing table.

Link Aggregation (Port Trunking)

Multiple ports can be combined (aggregated) into a group that behaves like a single connection. Groups can be manually set up or dynamically configured using the Link Aggregation Control Protocol (LACP – IEEE 802.3-2005). The additional ports dramatically increase the throughput across any connection, and provide redundancy by redistributing the load if a port in the group should fail.

Link Layer Discovery Protocol

LLDP is specified by IEEE 802.1AB and IEEE 802.3-2012. LLDP is used by networking devices to advertise their identity, capabilities, and to determine their neighboring devices. It can be used by other applications and protocols to discover a network's topology.

Network Security

Access Control List

ACL provides actions such as filtering and mirroring of L2 frames and L3 packets (based on the MAC address and EtherType, the IP address and protocol, TCP/UDP port number or ToS/DSCP value). ACL can be used to improve performance by blocking unnecessary network traffic. It can also be used to implement security controls by preventing access from certain devices or restricting access to specific network resources or protocols.

The ACL is a list of Access Control Entries. Each entry defines the frame content to match on and the actions to take on a match.

ARP Inspection

ARP Inspection prevents security attacks based on ARP packets. When the switch receives an ARP packet, the source MAC address in the frame is compared against the known MAC addresses found in either a Dynamic Table (drawn from DHCP Snooping) or a Static Table. If the source MAC is not know, the ARP is ignored.

On this switch, ARP Inspection can be enabled per-port or per-VLAN. Additionally, the ARP can be logged.

IP Source Guard

Access to ports can be controlled using IP Source Guard, which restricts traffic sources to a small number of IP/MAC addresses or to any IP/MAC addresses configured in a static table. More complex IP and MAC filtering is available through the Access Control List.

Port Security

Port Security limits which devices can communicate through the port by examining the source MAC address on frames.

On this switch, each port can be configured to allow traffic from 0 to 1023 unique source MAC addresses. When this number is exceeded, the violating frame is simply dropped, the port can be shutdown (and re-enabled later), or some additional quota of source MACs can be used for a limited time.

Port Configuration

Each port on the switch can be configured to support different modes of operation. You can configure:

- Administrative Status
- Auto-Negotiation or Speed plus Duplex Mode
- Flow Control
- Priority Flow Control
- Maximum Frame Size
- Excessive Collision Mode
- Frame Length Check
- Port Description

Administrative Status

The Admin Status allows a port to be disabled so that no traffic can enter or leave the port.

Auto-Negotiation

In Auto-Negotiation mode, two connected ports automatically detect and use the best speed and duplex mode that they have in common. Both ports should have auto-negotiation enabled.

Full-Duplex

Full-duplex operation allows simultaneous communication between a pair of connected ports using point-to-point media (dedicated channel). Full-duplex operation does not require that transmitters defer, nor do they monitor or react to received activity, as there is no contention for a shared medium in this mode.

Use full-duplex mode on ports whenever possible to double the throughput of switch connections.

Half-Duplex

In half-duplex mode, the CSMA/CD media access ports share a common transmission medium. To transmit, a port waits (defers) for a quiet period on the medium (when no other port is transmitting) and then sends the intended message in bit-serial form. If, after initiating a transmission, the message collides with that of another port, then each transmitting port intentionally transmits for an additional predefined period to ensure propagation of the collision throughout the system. The port remains silent for a random amount of time (back-off) before attempting to transmit again.

Flow Control

Flow control may be enabled to pause network traffic during periods when port buffering thresholds are exceeded. It is intended to prevent loss of packets. Flow control is based on the IEEE 802.3x standard (now incorporated in IEEE 802.3-2002).

Flow control is generally left disabled in favor of using modern protocols and traffic management techniques (like QoS and packet resends). However, it may be very helpful when configuring ports that communicate with a single end device that has limited traffic processing capabilities.

Priority Flow Control

PFC (IEEE 802.1Qbb) is similar to Flow Control, but it can be enabled per CoS priority in the entering frames. Traffic can be paused for some CoS priority and not for others.

Maximum Frame Size

This is the maximum frame size allowed for this port, including the FCS field. This is related to the MTU, but not the same value.

Excessive Collision Mode

When sending a frame, if there is a collision on the link, after 16 collisions the frame will be discarded.

Frame Length Check

If the length of the frame does not match the length field in the frame, then the frame is dropped. This can be used to eliminate corrupt or malicious frames.

Port Description

A user friendly description can be assigned to this port.

PROFINET

PROFINET is an industrial Ethernet protocol for networked devices. It provides a mechanism for device configuration, data exchange and device management. It is designed for proactive maintenance and to minimize downtime of your assets. This switch is a PROFINET PNIO V2.34, Conformance Class B (CC-B), RT Class 1 device. A CC-B device includes real-time data exchange, alarms and diagnostics, network topology support, and SNMP support.

A PROFINET device receives its IP configuration from a PROFINET controller. The configuration values can be determined dynamically based on the location of the device within the network topology, according to the setup defined at the server.

This switch also supports the Media Redundancy Protocol (MRP), which implements a ring topology with a heal time of less than 200 ms. This switch can operate as an MRP client (MRC). The -M models of this switch can also operates as an MRP manager (MRM).

Quality of Service and Traffic Management

QoS is a general term referring to various mechanisms that manage the priority and resources available to critical network traffic. It is particularly important for time-critical traffic, especially when a network is congested. The switch supports a rich set of features for managing QoS.

QoS Through Prioritization

QoS can provide different priorities to different applications, users, or data flows. QoS guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as Voice over IP, high resolution images, online games and IP-TV, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication. Prioritization helps to ensure that time-sensitive traffic is given preference over less critical traffic when a network is congested. QoS mechanisms are not required in the absence of network congestion.

QoS is typically implemented by categorizing traffic into 8 priority levels and by assigning a drop precedence which indicates whether a frame at a given priority may be dropped when traffic is congested.

The 8 priority levels corresponds to 8 priority **queues** in the actual hardware of this switch.

QoS Through Rate Limiting

Rate Limiting controls the maximum rate of (non-critical) traffic transmitted or received on an interface. Rate limiting may be configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that exceeds the acceptable rate can be dropped or subjected to further filtering.

Ingress Prioritization

For incoming traffic, the switch prioritizes traffic using CoS values and ToS/DiffServ values.

- **CoS**: The priority of an L2 frame can be specified by the IEEE 802.1p value inside an 802.1Q VLAN tag of an Ethernet frame. This is commonly known as the Class of Service (CoS).
- **ToS/DiffServ**: The priority of an L3 IP packet can be specified by the ToS/DiffServ field in the IP header. This field may have different values known as ToS (Type of Service), IP Precedence, or DSCP (Differentiated Services Codepoint) values.
- **Default Classification**: The priority of all incoming traffic on a port can be set to a default value.
- **Remapped Classification:** The priority of incoming traffic can also be remapped through a table that converts the frame's priority into a different priority. For this switch, re-mapping is found under Port Classification (for CoS), DSCP Translation (DSCP), and ACL entries.

Access Control Lists

Access Control Lists can search the content of frames and packets and perform particular actions on the matching traffic. These actions include denying, permitting, mapping traffic into a priority queue, applying a CoS marking, or mirroring the traffic.

Policing

A policer manages excessive rates of ingress traffic. It can limit traffic at a port or priority queue level. It can drop traffic or enable flow control.

Shaping

The shaper manages egress traffic rates for a port and egress traffic rates for each priority queue.

Scheduling

For outgoing traffic, the switch uses eight priority queues that are serviced either by Strict Priority, a Weighted Round Robin (WRR) algorithm, or a combination of both. The Queue & Scheduler can also force traffic with particular CoS values to particular priority queues.

Storm Policing

Storm Policing can block or rate limit traffic that is broadcast, unknown unicast, or multicast.

Egress Re-Prioritization

At the tail end of QoS management, the priority of a frame leaving a port can be modified. This allows the frame to be handled internally at one priority and then passed onto the network at a different priority.

On this switch egress re-prioritization can be configured under Port Classification/Port Tag Remarking for 802.1p CoS values and Port DSCP/DSCP Translation for DSCP values.

QoS Control List

The QoS Control List provides finer control of the priority of ingressing frames. A QCE (entry) in the list can look for specific frame field values (including MAC addresses, frame types, or priority). When a match is found, the frame's priority can be set to specific values.

Weighted Random Early Detection

WRED is a mechanism for randomly dropping ingressing frames before they are placed into a priority queue. It is enabled globally per-priority queue. Each queue is assigned a minimum and maximum threshold (percentage of traffic). As traffic approaches the maximum value frames are randomly dropped.

Switch Management

These are the various methods and protocols used to configure and monitor the switch.

Management Interfaces

Secure management interfaces are available and unsecured interfaces are provided for backwards compatibility with less secure clients. Management access can be limited to specific IP addresses.

A command line interface is available through the Console port on the exterior of the switch, and through the Secured Shell (SSH) and unsecured Telnet network protocols.

A graphical interface is available over the Hypertext Transfer Protocol Secure (HTTPS) and the unsecured Hypertext Transfer Protocol (HTTP).

Available management protocols which cooperate with external applications include Simple Network Management Protocol (SNMP), Remote Network Monitoring (RMON), and PROFINET (described separately above).

User Management

User accounts can be created to manage access to the management interfaces and to manage the privileges available to a user. Each user is assigned to a specific privilege level. The privilege level grants the user specific permissions to view and modify the switch configuration and to view and modify status information.

Date and Time

The date and time can be set manually or dynamically by enabling NTP (Network Time Protocol) which takes its time from an NTP server. The time can be further configured to a specific Time Zone and for a specific Daylight Saving Time adjustment.

SNMP

SNMP (Simple Network Management Protocol) is a protocol used to monitor and manage the switch. SNMP defines a method of granting specific users access to specific areas of the switch configuration and status information. This switch supports SNMPv1, v2c, and v3. In short, SNMPv2c adds performance and error-handling improvements and SNMPv3 adds authentication and encrypts SNMP network traffic.

The switch supports sending traps (notifications) to SNMP Trap Stations. The SNMP traps are: coldStart, warmStart, linkUp, linkDown, authenticationFailure, entConfigChange, newRoot, topologyChange, lldpRemTablesChange, risingAlarm, fallingAlarm, ipTrapInterfacesLink, psecTrapGlobalsMain, and psecTrapInterfaces. SNMP Traps are sent to all trap stations when the corresponding trap is enabled.

RMON

RMON (Remote Networking Monitoring) is a protocol that allows the switch to send specific data to an RMON application. The application uses this data to monitor traffic and analyze protocols on the LAN.

The RMON groups supported by the switch are statistics, history, alarm, and event.

Traffic Monitoring

Port Mirroring

The switch can unobtrusively mirror (copy and transmit) traffic from any port to a designated analysis port. A protocol analyzer or RMON probe can be attached to the latter port to perform traffic analysis, such as verifying connection integrity. This is typically used to troubleshoot and debug a network, and is disabled during normal operations.

This switch supports standard port mirroring where the source port and analysis port are on the same switch. It also supports remote mirroring which directs the mirrored traffic to an analysis port on a different switch. This port is called a reflector port and it is tied to a specific VLAN.

ACL entries can also be used to mirror specific frames that match very specific criteria.

sFlow

sFlow is a protocol that monitors traffic through sampling frames rather than mirroring frames. This reduces the amount of diagnostic traffic on the network.

sFlow sends the sampled frames and port counters from this switch (an agent) to a specific receiver where both are identified by an IP address. The rate of sampling of frames and counters is configurable per-port.

Virtual Local Area Networks

Overview of VLANs

VLANs (Virtual Local Area Networks) facilitate easy administration of logical groups of devices that can communicate as if they were physically on the same LAN. A port can be assigned to one or more specified VLANs. The switch forwards traffic (broadcast, multicast, or unicast) only between ports that belong to the same VLAN.

The switch supports tagged VLANs as specified by IEEE 802.1Q. A frame entering the switch can have a VLAN tag or a default VLAN can be applied to it. Any traffic entering a port can be discarded if it does not have a VLAN tag that matches a port's VLAN membership. Traffic leaving the switch can be configured to have a VLAN tag or be untagged.

By default, all ports belong to VLAN 1 (VID=1) and are set to untag the frame on egress.

Ports can be assigned to VLANs either manually (using Static VLANs) or dynamically using GVRP (GARP VLAN Registration Protocol) on switches that support GVRP.

By segmenting your network into VLANs, you can:

- Eliminate broadcast storms which severely degrade performance in a flat network.
- Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the physical network wiring.
- Provide data security by restricting all traffic to the originating VLAN, except where a connection is explicitly defined via the switch's routing service.
- Use protocol-based VLANs to assign traffic of a specific protocol to a specific VLAN.
- Use VLAN translation to replace a specific VLAN ID of incoming traffic with a different VLAN ID.
- Use private VLANs (port isolation) to restrict a group of ports to have one common uplink port. These ports cannot send or receive traffic between themselves (they are isolated from each other); they may only exchange traffic with the designated uplink port.

If switch ports are configured to transmit and receive untagged frames, then their connected devices are able to communicate throughout the LAN. Using Tagged VLANs, the switch has the ability to take non-tagged packets in some ports, add a VLAN tag to the packet, and send it out to tagged ports on the switch. VLANs can also be configured to accept tagged packets in tagged ports, strip the tags off the packets, and then send the packets back out to other untagged ports. This allows a network administrator to set up the switch to support devices on the network that do not support VLAN tagged packets. The administrator can also set up the ports to discard any packets that are tagged or to discard any packets that are untagged, based on a hybrid VLAN of both tagged and untagged ports and by using the VLAN Ingress Filter on the switch.

For each switch port there is one port VLAN ID (PVID) setting. If an incoming frame is untagged and untagged frames are being accepted, then that frame be assigned to the port VLAN ID. Subsequent switch routing and treatment will be in accordance with that VLAN. By configuring PVIDs properly and configuring for all frames to exit untagged, the switch can achieve a 'port VLAN' configuration in which all frames in and out are untagged, thus not requiring external devices to be VLAN cognizant.

Port VLAN Modes

To understand how a VLAN configuration will perform, first look at the port on which the frame enters the switch, then the VLAN ID (VID) (if the frame is tagged) or the PVID (if the frame is untagged). The VLAN defined by the VID or PVID defines a VLAN group with a membership of specific ports. This membership determines whether a port is included or excluded regarding frame egress from the switch.

Overlapping VLANs give the user the ability to have one or more ports share two or more VLAN groups. For information and examples on implementation, refer to VLAN Configuration.

Port Modes

Many switches have 3 predefined VLAN modes for ports. Access and Trunk mode are pre-configured for specific purposes and are not highly configurable. Hybrid mode is fully configurable.

Ports in **Access Mode** are configured to work well with end devices that do not support VLANs.

Ports in **Trunk Mode** are configured to concentrate traffic from different VLANs and pass it on to another Trunk Mode port on another switch. These switches could be part of a network backbone or of an up-link. In this configuration, all VLAN tags are generally preserved on ingressing traffic and egressing traffic.

Ports in **Hybrid Mode** mode have the most options for accepting and preserving VLAN tags. On this switch, this includes options for handling VLAN C-tags and S-tags for tunneling (described below) or for forcing all ingressing traffic into one VLAN regardless of any frame's VLAN tag (the port is said to be VLAN-unaware).

IEEE 802.1Q Tunneling (QinQ, VLAN Stacking)

This feature is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to retain customer-specific VLAN (C-tag) and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting a Service Provider VLAN (SPVLAN or S) tag into the customer's frames when they enter the service provider's network, and then stripping the S-tag when the frames leave the network.

System Defaults

The switch's default configuration can be restored using the web interface or CLI. Under the web menu item Configuration Management→Activiate, select default-config to reset the configuration. The CLI command "reload defaults" will do the same.

The following table lists some of the basic system defaults.

FUNCTION	PARAMETER	DEFAULT
Console Port Connection	Baud Rate Data bits Stop bits Parity Flow Control Local Console Timeout	115200 bps 8 1 None None 10 minutes
IP Settings	Management Access VLAN IP Address PROFINET DHCP	VLAN 1 PROFINET assigned DHCP Client, Server, Relay Agent: Disabled Fallback IP Address: 192.168.1.201 Netmask: 255.255.255.0
Switch Authentication	Default user name Default password	Username "admin" Password "admin" Password must be changed on first login

FUNCTION	PARAMETER	DEFAULT
Switch Management	SSH Telnet HTTPS HTTP IP Access Managment SNMP SNMP Communities SNMP Users SNMP Groups SNMP Views SNMP Access default_rw_group	Enabled Disabled Enabled Disabled Disabled Enabled public, private default_view default_ro_group
Port Configuration	Speed Flow Control Maximum Frame Size Excessive Collision Mode Frame Length Check	Auto Disabled 10240 Discard Disabled
Link Aggregation (Port Trunking)	Static Groups LACP (all ports)	None Disabled
Quality of Service	Storm Policing Port Policing Queue Policing Queue Shaping Scheduling Port Shaping	Disabled Disabled Disabled Disabled Strict Priority Disabled
MAC Address Table	Aging Time	300 seconds
L2 Redundancy Protocols	MRP Spanning Tree RingV2 Loop Protection	PROFINET assigned Disabled Disabled Disabled
LLDP	Mode	Enabled
Virtual LANs	Default VLAN PVID Port Mode Acceptable Frame Type Ingress Filtering	1 1 Access All Enabled
IP Multicast Filtering and Routing	IGMP Snooping MLD Snooping Unregistered MC Flooding Proxy Leave Proxy	Enabled Enabled Enabled Disabled Disabled
Alarms and Events	Logging Port Link Down Alarms Power Alarm Syslog	Enabled Disabled Disabled Disabled
NTP	Clock Synchronization	Disabled

Chapter 3 Web Interface

This chapter describes using the Red Lion Controls NT4008 switch web interface and presents the menu tree view broken down into major functional groups.

The switches are password protected by a login security system. You can login to the switch with the user name and password provided below.

All of the switches have the same default user name (admin) and password (admin). You are required to change the password at the first login. Additional user accounts can be added and configured to have different privilege levels.

Web Browser Support

IE 7 (or newer version) with the following default settings is recommended:

Language Script	Latin based
Web page font	Times New Roman
Plain text font	Courier New
Encoding	Unicode (UTF-8)
Text size	Medium

Firefox with the following default settings is recommended:

Web page font	Times New Roman
Encoding	Unicode (UTF-8)
Text size	Medium

Google Chrome with the following default settings is recommended:

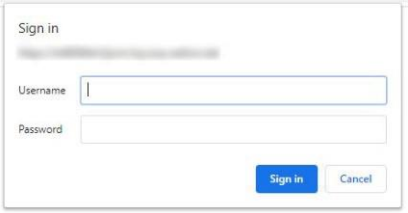
Web page font	Times New Roman
Encoding	Unicode (UTF-8)
Text size	Medium

Accessing the Web Software Interface

Launch a web browser and enter the IP address of the device into the address bar. PROFINET is enabled by default with 192.168.1.201 as the fallback address.

Login

The following login screen will appear:

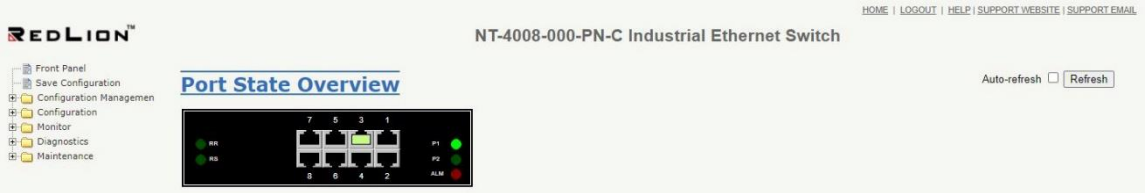


Username: Login user name. The maximum length is 32 characters. Default username: admin

Password: Login password. The maximum length is 32 characters. Default password: admin

When logging in for the first time using the default credentials, you will be prompted to change the password.

Upon successfully logging in a screen similar to the one below will appear.



Navigation

All main screens of the web interface can be reached by clicking on hyperlinks in the five main folders in the menu tree on the left side of the system home screen:

- **Configuration Management:** Restart the system, Save and Restore, and Configure HTTP Import and Export.
- **Configuration:** Configure the system, interfaces and filters.
- **Monitor:** Display statistics, status and contents of memory.
- **Diagnostics:** Ping, traceroute, and VeriPHY.
- **Maintenance:** Factory reset, firmware upgrade, and image selection.

You can find more detailed information in the navigation drop-down menu, or by displaying a screen's help window by navigating to the screen and clicking the "HELP" link located in the top-right.

Home Screen Information and Links

System, user and support information is available in the upper-right corner on the home screen.

HOME: Returns to the Front Panel page.

LOGOUT: Logout from the web interface.

HELP: Displays a help page for the active page.

SUPPORT WEBSITE: Go to the Red Lion website NT4008 support page(s)

SUPPORT EMAIL: Opens the default email client with the Red Lion support email address set.

Using the Online Help

Each screen has a Help page containing information relevant to the current screen. The help pages are displayed in a new web browser window. To close a help page, simply close the containing window.

Each page of Configuration/Status/System functions has a corresponding help page.

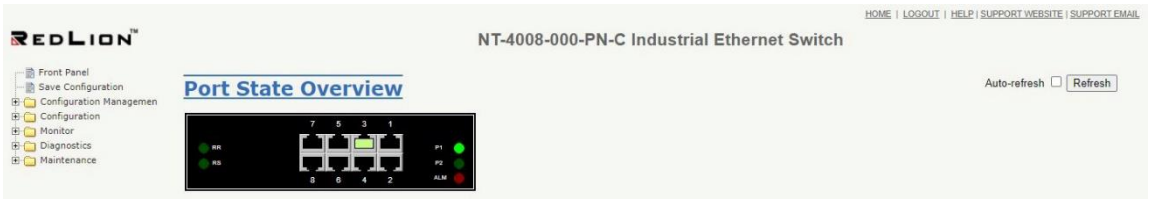
Ending a Session

A user must click on LOGOUT and close the web browser to end a session. This prevents unauthorized access to the system with the user's login name and password.

Organization

The tree view is a menu within the web interface. It offers users quick navigation to the desired page for viewing data or changing configuration parameters.

After logging onto a NT4008 switch, the home page (Front Panel) will be displayed. On the left hand side of the screen is a list of configurable settings supported by the NT4008 switch. Below is a list of these settings with a description of their purpose.



Front Panel: Graphic of the switch front panel displaying device and port status information. Port status is displayed when moving the cursor to a port icon.

Save Configuration: Saves the active running configuration to the startup configuration.

Configuration Management: Configuration Management is used to restart the switch, save and restore a configuration, configure HTTP import and export, as well as activate and delete configurations.

Configuration: The Configuration page is used to set or change switch configuration parameters.

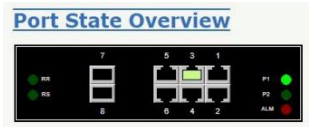
Monitor: Monitor is used to query system data to view and monitor switch operating statistics.

Diagnostics: Diagnostics are used for ping, traceroute, and VeriPHY.

Maintenance: Maintenance is used to upgrade switch operating software, restart the device, and reset the device to factory defaults.

Front Panel

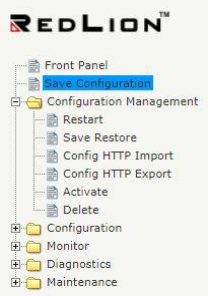
This page displays the real status of the system's panel.



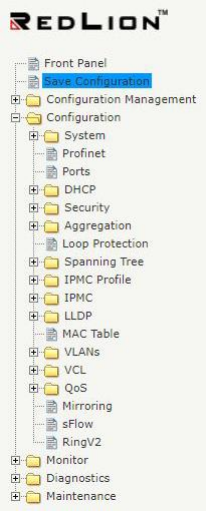
Save Configuration

This page is used to save the current running configuration to the startup configuration. By doing this, the current settings will be restored after a device reset or a power cycle.

Configuration Management Menu

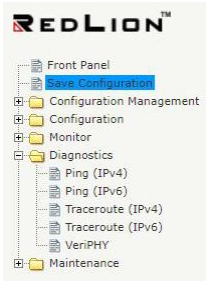


Configuration Menu

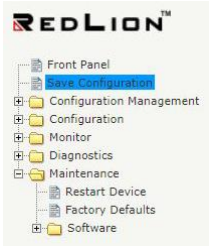


Monitor Menu

Diagnostics Menu

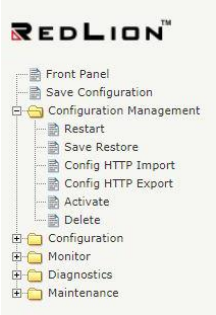


Maintenance Menu



Chapter 4 Configuration Management

This chapter lists the configuration related functions available for Red Lion Controls NT4008 switch models.



Note: If you upload a configuration file to the device without IPv4 or IPv6 information on VLAN 1, the device will keep the currently configured IPv4 and IPv6 settings for VLAN 1. This only occurs on VLAN 1 and is a special case so that a user does not lose IP connectivity via the management VLAN.

Configuration

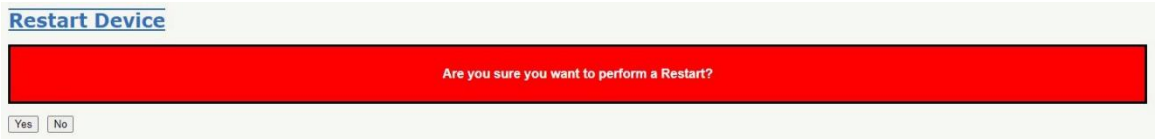
The switch stores its configuration in a number of text files in CLI format. The files are either virtual (RAM-based) or stored in flash on the switch.

The available files are:

- **Running-config:** A virtual file that represents the currently active configuration on the switch. This file is volatile.
- **Startup-config:** The startup configuration for the switch, read at boot time. If this file does not exist at boot time, the switch will start up in default configuration.
- **Default-config:** A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.
- Up to 31 other files, typically used for configuration backups or alternative configurations.

Restart

Use this screen to restart the system. After restart, the switch will boot normally.



Yes: Click to restart device.

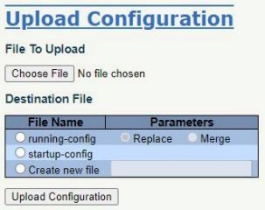
No: Click to return to the Port State page without restarting.

Save Restore

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

Config HTTP Import/Export

It is possible to upload a file from a computer to any file on the switch, except *default-config* which is read-only. Select the file to upload, select the destination file on the target, then click Upload Configuration.



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

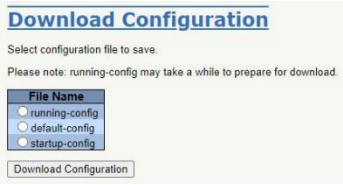
Replace Mode: The current configuration is fully replaced with the configuration in the uploaded file.

Merge Mode: The uploaded file is merged into *running-config*.

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

Config HTTP Export

Download any of the files on the switch to a computer. Select the file and click Download Configuration. Downloading *running-config* may take a little while to complete, as the file must be prepared.



Activate

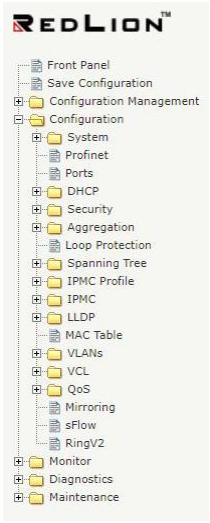
It is possible to activate any of the configuration files present on the switch, except for *running-config* which represents the currently active configuration. Select the file to activate and click Activate Configuration. This will initiate the process of completely replacing the existing configuration with the selected file.

Delete

It is possible to delete any of the writable files stored in flash, including *startup-config*. If this is done and the switch is rebooted without a prior Save operation, this effectively resets the switch to default configuration.

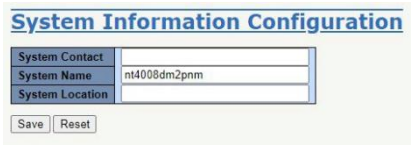
Chapter 5 Configuration

This chapter contains a listing of all functionality that can be configured for the Red Lion Controls NT4008 switch models.



System

Information



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

System Name: An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. The first or last character must not be a minus sign. The allowed string length is 0 to 63.

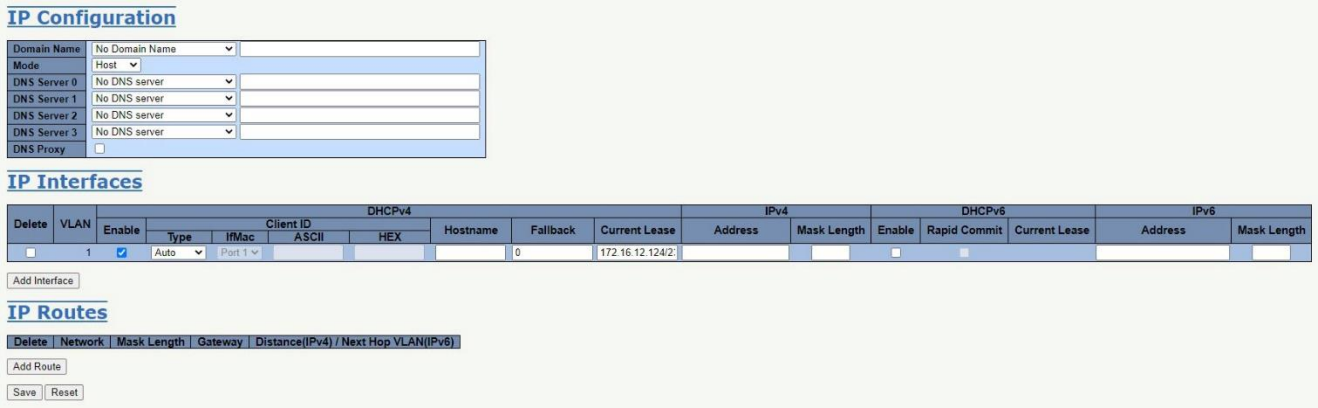
System Location: The physical location of this node(e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.

Buttons

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

IP

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



Domain Name: The name string of the local domain where the device belongs. Most queries for names within this domain can use short names relative to the local domain. The system then appends the domain name as a suffix to unqualified names. For example, if the domain name is set as 'example.com' and you specify the PING destination by the unqualified name as 'test', then the system will qualify the name to be 'test.example.com'. The following modes are supported:

No Domain Name: No domain name will be used.
Configured Domain Name: Explicitly specify the name of local domain. Make sure the configured domain name meets your organization's given domain.
From any DHCPv6 interface: The first domain name offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used.
From this DHCPv6 interface: Specify from which DHCPv6-enabled interface a provided domain name should be preferred.

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

DNS Server: This setting controls the DNS name resolution done by the switch. There are four servers available for configuration, and the index of the server presents the preference (lower index has higher priority) in doing DNS name resolution. The following modes are supported:

No DNS server: No DNS server will be used.
Configured IPv4: Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation. Make sure the configured DNS server is reachable (e.g. via PING) for activating DNS service.
Configured IPv6: Explicitly provide the valid IPv6 unicast (except linklocal) address of the DNS Server. Make sure the configured DNS server is reachable (e.g. via PING6) for activating DNS service.
From any DHCPv4 interface: The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used.
From this DHCPv4 interface: Specify from which DHCPv4-enabled interface a provided DNS server should be preferred.
From any DHCPv6 interface: The first DNS server offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used.
From this DHCPv6 interface: Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.

DNS Proxy: When DNS proxy is enabled, the system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network. Only IPv4 DNS proxy is currently supported.

Delete: Select this option to delete an existing IP interface.

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

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

IPv4 DHCP Client Identifier Type: The Type of Client Identifier is selectable, option: Auto, IF_MAC, ASCII, HEX. Default is Auto. When the type is Auto and the hostname is configured (not empty), then the hostname will be used in the DHCP option 61 field. If the hostname is empty, then the system MAC address will be used, in format xx-xx-xx-xx-xx-xx. Note: in either case, there is an extra byte 00 appended in front of the option 61 field. For example: xx-xx-xx-xx-xx-xx, option 61 value length would be 18. 0x00 stands for Not HW Address.

IPv4 DHCP Client Identifer IfMac: The interface name of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ifmac', the configured interface's hardware MAC address will be used in the DHCP option 61 field. For example: If port 2 is selected, the option 61 value would be the system's MAC plus 2. Note: In this case, there is an extra byte 01 appended in front of the option 61 field, like 01aabbcc010203, length 7. The 0x01 stands for Hardware type Ethernet.

IPv4 DHCP Client Identifer ASCII: The ASCII string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ascii', the ASCII string will be used in the DHCP option 61 field. Note: In this case, there is an extra byte 00 appended in front of the option 61 field. 0x00 stands for Not HW Address. Only lower-case characters are used.

IPv4 DHCP Client Identifer HEX: The hexadecimal string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type 'hex', the hexadecimal value will be used in the DHCP option 61 field. Note: In this case, the option 61 value would be the same as HEX without an extra byte.

IPv4 DHCP Hostname: The hostname of DHCP client. If DHCPv4 client is enabled, the configured hostname will be used in the DHCP option 12 field. When this value is empty string, the option 12 field uses the system's MAC.

IPv4 DHCP Fallback Timeout: The number of seconds for trying to obtain a DHCP lease. After this period expires, the IPv4 Address (below) is used as the IPv4 address of this interface. A value of zero disables the fallback mechanism, and DHCP will keep retrying until a valid lease is obtained. Allowed values are 0 to 4294967295 seconds.

IPv4 DHCP Current Lease: For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.

IPv4 Address: The IPv4 address of the interface in dotted decimal notation. If DHCP is enabled, this field configures the fallback address. The field may be left blank if IPv4 operation on the interface is not desired – or no DHCP fallback address is desired.

IPv4 Mask: The number of bits in the IPv4 network mask. This is also known as the bit-length of the prefix. For example, the subnetwork mask 255.255.255.0 has 24 bits in the prefix. Valid values are between 0 and 30 bits for an IPv4 address. If DHCP is enabled, this field configures the fallback

address network mask. The field may be left blank if IPv4 operation on the interface is not desired – or no DHCP fallback address is desired.

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

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

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

IPv6 Address: The IPv6 address of the interface. An IPv6 address is a 128-bit value represented as eight fields separated by a colon (:). Each field has 0 to 4 hexadecimal digits. For example, fe80::215:c5ff:fe03:4dc7. The characters :: may be used once in the address as a short hand for multiple zeros. For example, 1111:222:0:0:0:6:7:8 can be also be written as 1111:222::6:7:8. Any IPv6 address is allowed except for IPv4-compatible addresses and IPv4-mapped addresses.

IPv6 Mask: The number of bits in the IPv6 network mask. This is also known as the bit-length of the prefix. Valid values are between 1 and 128 bits for an IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.

Resolving IPv6 DAD: The link-local address is formed from an interface identifier based on the hardware address which is supposed to be uniquely assigned. Once the DAD (Duplicate Address Detection) detects the address duplication, the operation on the interface SHOULD be disabled. At this moment, manual intervention is required to resolve the address duplication. For example, check whether the loop occurs in the VLAN or if there is indeed another device occupying the same hardware address as the device in the VLAN. After making sure the specific link-local address is unique on the IPv6 link in use, delete and then add the specific IPv6 interface to restart the IPv6 operations on this interface.

Delete: Select this option to delete an existing IP route.

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

Mask Length: The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match in order to qualify for this route. Valid values are between 0 and 32 bits for IPv4 routes and 0 to 128 bits for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).

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

Distance (Only for IPv4): The distance value of route entry is used to provide the priority information of the routing protocols to routers. When two or more different routing protocols are involved and have the same destination, the distance value can be used to select the best path.

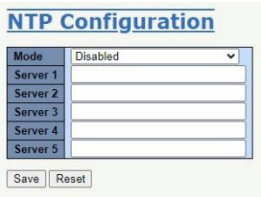
Next Hop VLAN (Only for IPv6): The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. The given VID ranges from 1 to 4095 and will be effective only when the corresponding IPv6 interface is valid. If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway. If the IPv6 gateway address is not link-local, the system ignores the next hop VLAN for the gateway.

Buttons

Add Interface: Click to add a new IP interface. A maximum of 8 interfaces are supported.
Add Route: Click to add a new IP route. A maximum of 32 routes are supported.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

NTP

Configure the NTP (Network Time Protocol) on this page.



Mode: The NTP mode operation. Possible modes are:

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

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

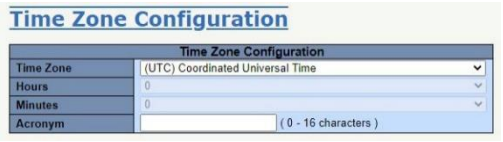
Buttons

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

Time

This page allows you to configure the Time Zone.

Time Zone Configuration



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

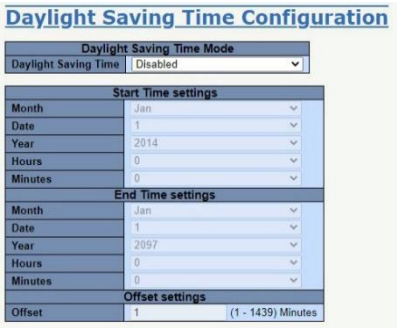
Hours: Number of hours offset from UTC. The field is only available when the manual time zone is used.

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

Acronym: User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range : Up to 16 characters) Notice the string '' is a special syntax that is reserved for null input.

Daylight Saving Time Configuration

This page is used to setup Daylight Saving Time Configuration.



Daylight Saving Time: This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select 'Disable' to disable the Daylight Saving Time configuration. Select 'Recurring' and configure the Daylight Saving Time duration to repeat the configuration every year. Select 'Non-Recurring' and configure the Daylight Saving Time duration for single time configuration. (Default : Disabled)

Recurring Configurations: start time settings.

Week: Select the starting week.
Day: Select the starting day.
Month: Select the starting month.
Hours: Select the starting hour.
Minutes: Select the starting minute.

Recurring Configurations: end time settings.

Week: Select the ending week number.
Day: Select the ending day.
Month: Select the ending month.
Hours: Select the ending hour.
Minutes: Select the ending minute.

Offset Settings

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

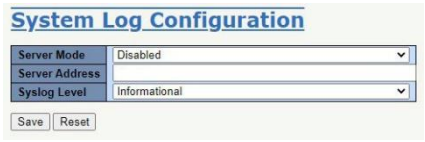
Date/Time Configuration

Buttons

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

Log

Configure the System Log on this page.



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

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

Server Address: The IPv4 host address of the syslog server. If DNS is configured, it can also be a domain name.

Syslog Level: Configure what kind of message will be sent to syslog server. Possible modes are:

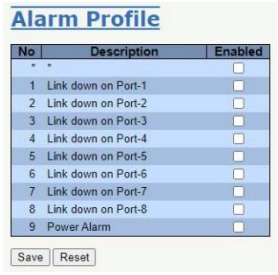
Error: Send the specific messages which severity code is less or equal than Error (3).
Warning: Send the specific messages which severity code is less or equal than Warning (4).
Notice: Send the specific messages which severity code is less or equal than Notice (5).
Informational: Send the specific messages which severity code is less or equal than Informational (6).

Buttons

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

Alarm Profile

Alarm Profile is provided here to enable/disable alarm.



No: Index of the Alarm Profile entry.

Description: Alarm Type Description.

Enabled: If an alarm entry is Enabled, then that alarm will be captured in alarm history or shown as current when it occurs. The alarm will trigger the Alarm LED light, Alarm Relay, and any existing and enabled SNMP traps.
Disabled: If an alarm entry is not Enabled, then that alarm will not be captured in alarm history or shown as current when it occurs. The alarm will not trigger the Alarm LED light, Alarm Relay, or any SNMP traps.

Note: If any alarm is enabled and triggered, the Alarm LED will turn on and the Alarm Output Relay will be enabled.

Buttons

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

PROFINET

Configure PROFINET on this page.

Mode: The PROFINET mode. Possible modes are:

Enabled: Enable PROFINET operation.
Disabled: Disable PROFINET operation.

Buttons

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

Ports

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

Port: This is the logical port number for this row.

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

Current Link Speed: Provides the current link speed of the port.

Configured Link Speed: Selects any available link speed for the given switch port. Only speeds supported by the specific port are 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 to 10Mbps, half-duplex mode.
10Mbps FDX: Forces the CU port to 10Mbps full-duplex mode.
100Mbps HDX: Forces the CU port to 100Mbps half-duplex mode.
100Mbps FDX: Forces the CU port to 100Mbps full duplex mode.
1Gbps FDX: Forces the port in 1Gbps, full duplex.

Advertise Duplex: When duplex is set as auto (i.e auto negotiation), the port will only advertise the specified duplex as either Fdx or Hdx to the link partner. By default, a port will advertise all the supported duplexes if the Duplex is set to Auto.

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

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

Notice: The 100FX standard doesn't support Auto Negotiation, so when in 100FX mode the flow control capabilities will always be shown as "disabled".

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

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

Excessive Collision Mode: Configure port transmit collision behavior.

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

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

Description: Port Description, max length 255 characters.

Buttons

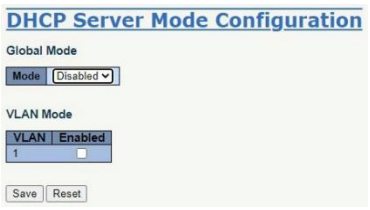
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
Refresh: Click to refresh the page. Any changes made locally will be undone.

DHCP

Server

Mode

This page configures global mode and VLAN mode to enable/disable DHCP server per system and per VLAN.



Global Mode: Configure operation mode to enable/disable DHCP server per system.

Mode: Configure the operation mode per system. Possible modes are:
Enabled: Enable DHCP server per system.
Disabled: Disable DHCP server per system.

VLAN Mode: Configure operation mode to enable/disable DHCP server per VLAN.

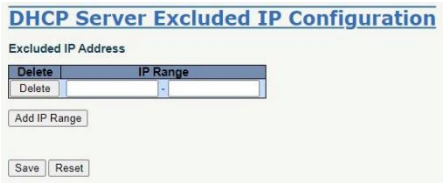
VLAN: Indicate the VLAN in which DHCP server is enabled or disabled.
Enabled: Indicate the operation mode per VLAN interface. Check Enabled to enable DHCP server to VLAN.

Buttons

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

Excluded IP

This page configures excluded IP addresses. DHCP server will not allocate these excluded IP addresses to DHCP client.



Excluded IP Address: Configure excluded IP addresses.

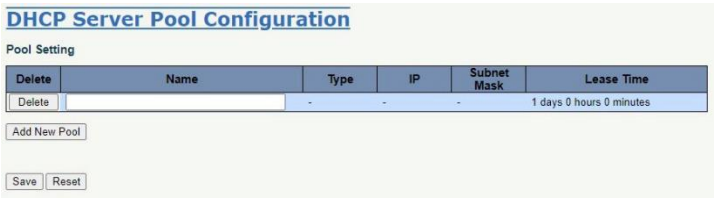
IP Range: Define the IP range to be excluded IP addresses. The first excluded IP must be smaller than or equal to the second excluded IP. If the IP range contains only one excluded IP, then you can just enter it in the first excluded IP field, the second field, or both.

Buttons

Add IP Range: Click to add a new excluded IP range.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

Pool

This page manages DHCP pools. According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client.



Add or delete pools.

Adding and naming a pool creates a new pool with the "default" configuration. If you want to configure all settings including type, IP subnet mask, and lease time, you can click the pool name to go into the configuration page.

Name: Configure the pool name that accepts all printable characters, except white space. If you want to configure the detail settings, you can click the pool name to go into the configuration page.

Type: Display pool type.

Network: Defines a pool of IP addresses to service more than one DHCP client.
Host: Services a specific DHCP client identified by client identifier or hardware address. If "-" is displayed, it means undefined.

IP: Display network number of the DHCP address pool. If "-" is displayed, it means undefined.

Subnet Mask: Display the subnet mask of the DHCP address pool. If "-" is displayed, it means undefined.

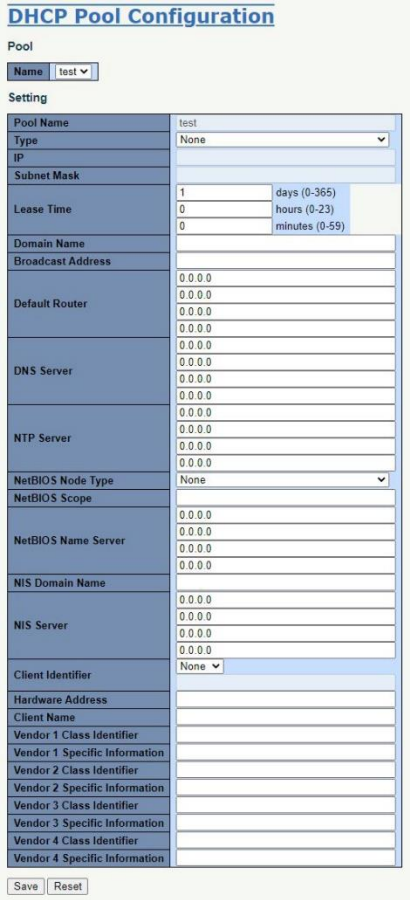
Lease Time: Display lease time of the pool.

Buttons

Add New Pool: Click to add a new DHCP pool.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

DHCP Pool Configuration

This page configures all settings of a DHCP pool.



Name: Select a pool by name.

Pool Name: Display the selected pool name.

Type: Specify the pool type.

Network: The pool defines a pool of IP addresses to service more than one DHCP client.
Host: The pool services for a specific DHCP client identified by client identifier or hardware address.

IP: Specify the network number of the DHCP address pool.

Subnet Mask: DHCP option 1. Specify the subnet mask of the DHCP address pool.

Lease Time: DHCP option 51, 58 and 59. Specify the lease time that allows the client to request a lease time for the IP address. If all are 0's, then it means the lease time is infinite.

Domain Name: DHCP option 15. Specify the domain name that client should use when resolving hostname via DNS.

Broadcast Address: DHCP option 28. Specify the broadcast address in use on the client's subnet.

Default Router: DHCP option 3. Specify a list of IP addresses for routers on the client's subnet.

DNS Server: DHCP option 6. Specify a list of Domain Name System name servers available to the client.

NTP Server: DHCP option 42. Specify a list of IP addresses indicating NTP servers available to the client.

NetBIOS Node Type: DHCP option 46. Specify the NetBIOS over TCP/IP Node Type for the client as described in RFC 1001/1002.

NetBIOS Scope: DHCP option 47. Specify the NetBIOS over TCP/IP Scope for the client as described in RFC 1001/1002.

NetBIOS Name Server: DHCP option 44. Specify a list of NBNS name servers listed in order of preference.

NIS Domain Name: DHCP option 40. Specify the name of the client's NIS domain.

NIS Server: DHCP option 41. Specify a list of IP addresses indicating NIS servers available to the client.

Client Identifier: DHCP option 61. Specify the client's unique identifier. This is used when the pool Type is Host. Select the type of client identifier:

None: Client identifier is not specified yet.
Name: The client identifier is a value other than a MAC address.
MAC: The client identifier is a MAC address.

Hardware Address: Specify the client's hardware (MAC). This is used when the pool Type is Host.

Client Name: DHCP option 12. Specify the name of client. This is used when the pool Type is Host.

Vendor *i* Class Identifier: DHCP option 60. Specify the client's vendor class identifier (vendor type). The DHCP server will deliver the corresponding option 43 specific information to a client that sends this option 60 vendor class identifier.

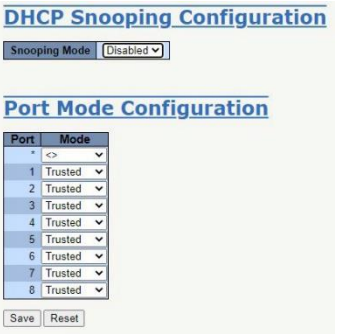
Vendor *i* Specific Information: DHCP option 43. Specify the vendor specific information corresponding to the option 60 vendor class identifier.

Buttons

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

Snooping

Configure DHCP Snooping on this page.



Snooping Mode: Indicates the DHCP snooping operation mode. Possible modes are:

Enabled: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports.
Disabled: Disable DHCP snooping mode operation.

Port Mode Configuration: Indicates the DHCP snooping port mode. Possible port modes are:

Trusted: Configures the port as trusted source of the DHCP messages.
Untrusted: Configures the port as untrusted source of the DHCP messages.

Buttons

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

Relay

A DHCP relay agent is used to forward and transfer DHCP messages between the clients and the server when they are not in the same subnet domain. It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of the GIADDR field to determine the assigned subnet. For such conditions, please make sure the VLAN interface IP address and the PVID (Port VLAN ID) are configured correctly.

Relay Mode: Indicates the DHCP relay mode operation. Possible modes are:

Enabled: Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.
Disabled: Disable DHCP relay mode operation.

Relay Server: Indicates the DHCP relay server IP address.

Relay Information Mode: Indicates the DHCP relay information mode operation options. The option 82 circuit ID is formatted as "[vlan_id][module_id][port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID (in a standalone device it is always equals 0; in a stackable device it represents the switch ID), and the last two characters are the port numbers. For example, "00030108" would mean the DHCP message receive from VLAN ID 3, switch ID 1, port No 8. The option 82 remote ID value is equal the switch MAC address. Possible modes are:

Enabled: Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled.
Disabled: Disable DHCP relay information mode operation.

Relay Information Policy: Indicates the DHCP relay information policy options. If the agent receives a DHCP message containing relay agent information when DHCP relay information mode operation is enabled, the policy will be enforced. The 'Replace' policy is invalid when relay information mode is disabled. Possible policies are:

Replace: Replace the original relay information when a DHCP message containing relay agent information is received.
Keep: Keep the original relay information when a DHCP message containing relay agent information is received.
Drop: Drop the package when a DHCP message containing relay agent information is received.

Buttons

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

Security

Switch

Users

This page provides an overview of the current users. The only way to login as another user on the web server is to close and reopen the browser.

User Name: The name identifying the user. This is also a link to Add/Edit User.

Privilege Level: The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, the user can access all groups, i.e. the user is granted full control of the device. Other value levels need to refer to each group's privilege level. The user's privilege should be same or greater than the group privilege in order to have the access level of that group. By default, most groups have privilege level 5, which is read-only access, while privilege level 10 is read-write access. System maintenance (software upload, factory defaults, etc.) requires privilege level 15. Generally, privilege level 15 can be used for an administrator accounts, privilege level 10 for standard user accounts, and privilege level 5 for a guest account.

Buttons

Add New User: Click to add a new user. The maximum number of users is 20.

Add User

User Name: A string identifying the user name. The allowed string length is 1 to 31. The valid user name allows letters, numbers and underscores.

Password: The password of the user. The allowed string length is 0 to 31. Any printable characters including spaces are accepted.

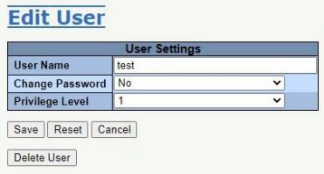
Password (again): The password of the user. The allowed string length is 0 to 31. Any printable character including spaces are accepted.

Privilege Level: The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. full control of the device is granted. Other values refer to each group privilege level. User's privilege should be the same or greater than the group privilege level to have the access of that group. By default, most groups with privilege level 5 have read-only access, and groups with privilege level 10 have read-write access. System maintenance (software upload, factory defaults, etc.) require user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account, and privilege level 5 for a guest account.

Buttons

Save: Click to save changes.
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 Users Configuration.

Edit User



User Name: A string identifying the user name. The allowed string length is 1 to 31. The valid user name allows letters, numbers and underscores.

Change Password: Select Yes to set a new password.

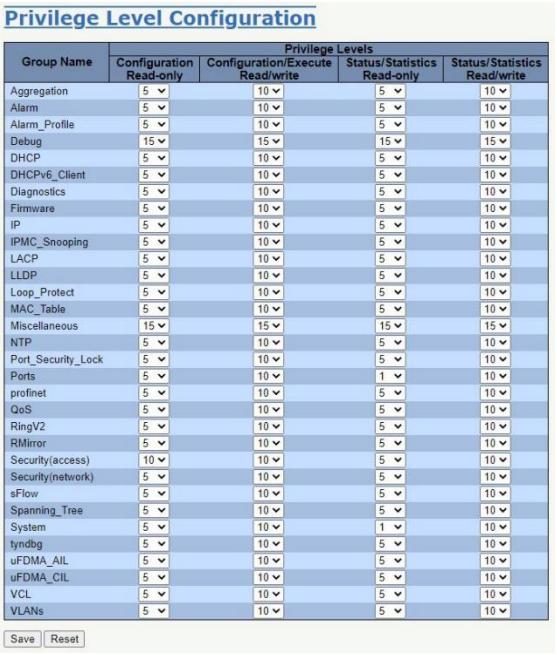
Privilege Level: The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, i.e. full control of the device is granted. Other values refer to each group privilege level. User's privilege should be the same or greater than the group privilege level to have the access of that group. By default, most groups with privilege level 5 have read-only access, and groups with privilege level 10 have read-write access. System maintenance (software upload, factory defaults, etc.) require user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account, and privilege level 5 for a guest account.

Buttons

Save: Click to save changes.
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 Users Configuration.
Delete User: Delete the current user. This button is only available for added users.

Privilege Levels

This page provides an overview of the privilege levels.



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

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

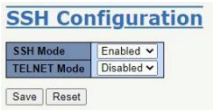
Privilege Levels: The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, the user can access all groups, i.e. the user is granted full control of the device. Other value levels need to refer to each group's privilege level. The user's privilege should be the same or greater than the group privilege in order to have the access level of that group. By default, most groups have privilege level 5 ,which is read-only access, while privilege level 10 is read-write access. System maintenance (software upload, factory defaults and etc.) requires privilege level 15. Generally, privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account, and privilege level 5 for a guest account.

Buttons

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

SSH/TELNET

Configure SSH / TELNET on this page.



Mode: The SSH and TELNET mode operation. Possible modes are:

Enabled: Enable SSH / TELNET mode operation.
Disabled: Disable SSH / TELNET mode operation. (TELNET is Disabled by Default.)

Buttons

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

HTTPS

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

Mode: Indicates the HTTPS mode operation. Possible modes are:

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

Automatic Redirect: Indicates the HTTPS redirect mode operation. It is only relevant when "HTTPS Mode Enabled" is selected. When redirect mode is enabled, the HTTP connection will redirect to an HTTPS connection automatically. Note that the browser may not allow this redirection because of security features, unless the switch certificate is trusted by the browser. The user needs to initialize the HTTPS connection manually in this case. Possible modes are:

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

Certificate Maintain: The operations for certificate maintenance. Possible operations are:

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

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

Certificate Upload: Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separate files for saving the certificate and private key, use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem. Note that the RSA certificate is recommended since most of the new browser versions have removed support for DSA in certificate, e.g. Firefox v37 and Chrome v39. Possible methods are:

Web Browser: Upload a certificate via the Web browser.

URL: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name>. For example, tftp://10.10.10.10/new_image_path/new_image.dat, http://username:password@10.10.10.10:80/new_image_path/new_image.dat. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), underscore(_). The maximum length is 63 and hyphen must not be the first character. A file name that only contains '.' is not allowed.

Certificate Status: Display the current status of the certificate on the switch. Possible statuses are:

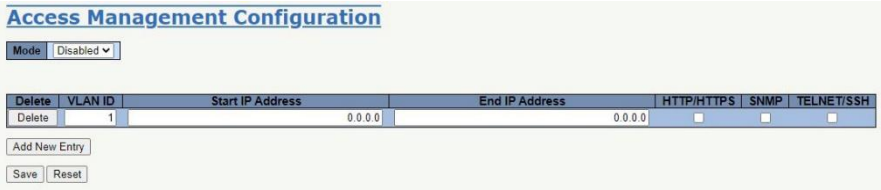
Switch secure HTTP certificate is present.
Switch secure HTTP certificate is not present.
Switch secure HTTP certificate is generating ....

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
Refresh: Click to refresh the page. Any changes made locally will be undone.

Access Management

Configure the access management table on this page. The maximum number of entries is 16. If the application's type matches any one of the access management entries, it will allow access to the switch.



Mode: The access management mode operation. Possible modes are:

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

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

VLAN ID: The VLAN ID for the access management entry.

Start IP Address: The start IP unicast address for the access management entry.

End IP Address: The end IP unicast address for the access management entry.

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

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

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

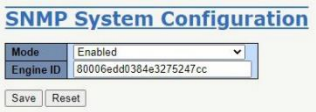
Buttons

Add New Entry: Click to add a new access management entry.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

SNMP

System

Configure SNMP on this page.



Mode: Indicates the SNMP mode operation. Possible modes are:

Enabled: Enable SNMP mode operation.
Disabled: Disable SNMP mode operation.

Engine ID: Indicates the SNMPv3 engine ID. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Only users on this Engine ID can access the device (local users), so changing the Engine ID will revoke access for all current local users.

Buttons

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

Trap: Destinations

Configure trap destinations on the Trap Configuration page. Configure trap detailed configuration on the SNMP Trap Configuration page.

Trap Destination Configurations: Configure trap destinations on this page.

Delete: Select this option to delete an existing trap destination.
Name: Indicates the Trap Configuration's name and the Trap Destination's name.
Enable: Indicates the trap destination mode operation. Possible modes are:
Enabled: Enable SNMP trap mode operation.
Disabled: Disable SNMP trap mode operation.
Version: Indicates the SNMP trap supported version. Possible versions are:
SNMPv1: Set SNMP trap supported version 1.
SNMPv2c: Set SNMP trap supported version 2c.
SNMPv3: Set SNMP trap supported version 3.
Destination Address: Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). It also allows a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash. Also indicates the SNMP trap destination IPv6 address. The IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros, but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
Destination Port: Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1-65535.

Buttons

Add New Entry: Click to add a new user.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

SNMP Trap Configuration: Configure SNMP trap on this page.

Trap Config Name: Indicates which trap Configuration's name for configuring. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Trap Mode: The SNMP mode operation. Possible modes are:
Enabled: Enable SNMP mode operation.
Disabled: Disable SNMP mode operation.
Trap Version: The SNMP supported version. Possible versions are:
SNMP v1: Set SNMP supported version 1.
SNMP v2c: Set SNMP supported version 2c.
SNMP v3: Set SNMP supported version 3.
Trap Community: The community access string when sending SNMP trap packet. The allowed string length is 0 to 63, and the allowed content is ASCII characters from 33 to 126.
Trap Destination Address: The SNMP trap destination address. It allow a valid IP address in dotted decimal notation ('x.y.z.w'). It can also use a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash. The SNMP trap destination IPv6 address. The IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
Trap Destination Port: The SNMP trap destination port. Then SNMP Agent will send SNMP messages via this port, the port range is 1-65535.
Trap Inform Mode: 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): The SNMP trap inform timeout. The allowed range is 0 to 2147.
Trap Inform Retry Times: The SNMP trap inform retry times. The allowed range is 0 to 255.
Trap Security Engine ID: 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. 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: The SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

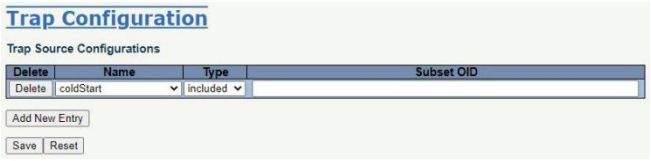
Buttons

Save: Click to save changes.

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

Trap: Sources

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



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

Name: The name for the entry.

Type: The filter type for the entry. Possible types are:

included: An optional flag to indicate a trap is sent for the given trap source is matched.
excluded: An optional flag to indicate a trap is not sent for the given trap source is matched.

Subset OID: The subset OID for the entry. The value should depend on the kind of trap name. For example, the ifIndex is the subset OID of linkUp and linkDown, 1000001 stands for port 1. A valid subset OID is one or more digital numbers (0-4294967295) or an asterisk (*) which are separated by dots(.). The first character must not begin with an asterisk(*) and the maximum of OID count must not exceed 63.

Buttons

Add New Entry: Click to add a new entry. The maximum entry count is 32.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

Communities

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

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

Community name: The security name to map the community to the SNMP Groups configuration. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Community secret: The community secret (access string) to permit access using SNMPv1 and SNMPv2c to the SNMP agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Source IP: The SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source prefix.

Source Prefix: The SNMP access source address prefix.

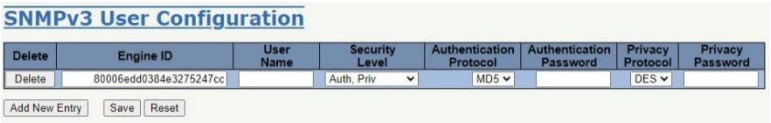
Buttons

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

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

Users

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



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

Engine ID: An octet string identifying the engine ID of an entry. The string must contain an even number of digits (in hexadecimal format) between 10 and 64 characters; 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. This 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 equals a system engine ID, then the user is local; otherwise it is a remote user.

User Name: A string identifying the user name for an entry. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Level: The security model for an entry. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.
Auth, NoPriv: Authentication and no privacy.
Auth, Priv: Authentication and privacy.
The value of security level cannot be modified if the entry already exists. For this reason, make sure that the value is set correctly from the start.

Authentication Protocol: The authentication protocol for an entry . Possible authentication protocols are:

None: No authentication protocol.
MD5: An optional flag to indicate that this user uses MD5 authentication protocol.
SHA: An optional flag to indicate that this user uses SHA authentication protocol.
The value of the security level cannot be modified if the entry already exists. The user must ensure that the value is set correctly before creating the entry.

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

Privacy Protocol: The privacy protocol that for an entry. Possible privacy protocols are:

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

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

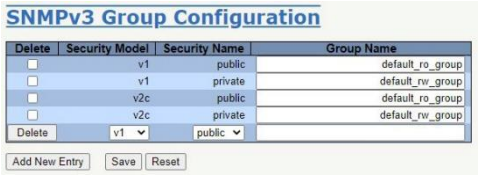
Buttons

Add New Entry: Click to add a new user entry.

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

Groups

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



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

Security Model: Indicates the security model that for an entry. Possible security models are:

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

Security Name: A string identifying the security name for an entry. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

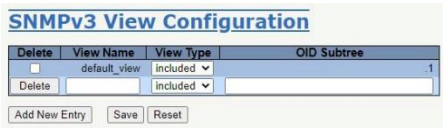
Group Name: A string identifying the group name for an entry. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Buttons

Add New Entry: Click to add a new group entry.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

Views

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



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

View Name: A string identifying the view name. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

View Type: The view type for an entry. Possible view types are:

included: An optional flag to indicate that this view subtree should be included.
excluded: An optional flag to indicate that this view subtree should be excluded.

OID Subtree: The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 64. The allowed string content is digital number or asterisk (*).

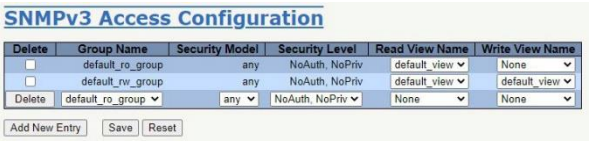
Buttons

Add New Entry: Click to add a new view entry.
Save: Click to save changes.

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

Access

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



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

Group Name: A string identifying the group name for an entry. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

Security Model: Indicates the security model for an entry. Possible security models are:

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

Security Level: Indicates the security model for an entry. Possible security models are:

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

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

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

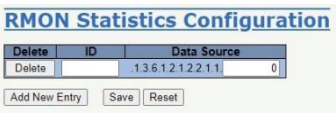
Buttons

Add New Entry: Click to add a new access entry.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

RMON

Statistics

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



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

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

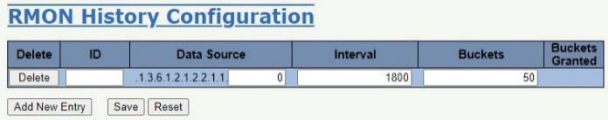
Data Source: The port ID that will be monitored. If in stacking switch, the value must add 1000000* (switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.

Buttons

Add New Entry: Click to add a new RMON statistics entry.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

History

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



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

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

Data Source: The port ID to be monitored. If using a stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.

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

Buckets: The maximum data entries associated this History control entry stored in RMON. The range is from 1 to 65535, default value is 50.

Buckets Granted: The number of data that will be saved in the RMON.

Buttons

Add New Entry: Click to add a new RMON history entry.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

Alarm

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

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

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

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

Variable: The particular variable to be sampled, the possible variables are:

InOctets: The total number of octets received on the interface, including framing characters.
InUcastPkts: The number of uni-cast packets delivered to a higher-layer protocol.
InNUcastPkts: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol.

InDiscards: The number of inbound packets that are discarded even the packets are normal.
InErrors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
InUnknownProtos: the number of the inbound packets that were discarded because of the unknown or un-support protocol.
OutOctets: The number of octets transmitted out of the interface, including framing characters.
OutUcastPkts: The number of unicast packets that request to transmit.
OutNUcastPkts: The number of broadcast and multicast packets that request to transmit.
OutDiscards: The number of outbound packets that are discarded event the packets is normal.
OutErrors: The number of outbound packets that could not be transmitted because of errors.
OutQLen: The length of the output packet queue (in packets).

Sample Type: The method of sampling the selected variable and calculating the value to be compared against the thresholds. Possible sample types are:

Absolute: Get the sample directly.
Delta: Calculate the difference between samples (default).

Value: The value of the statistic during the last sampling period.

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

Rising: Trigger alarm when the first value is larger than the rising threshold.
Falling: Trigger alarm when the first value is less than the falling threshold.
RisingOrFalling: Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).

Rising Threshold: Rising threshold value (-2147483648 to 2147483647).

Rising Index: Rising event index (1-65535).

Falling Threshold: Falling threshold value (-2147483648 to 2147483647)

Falling Index: Falling event index (1-65535).

Buttons

Adding New Entry: Click to add a new RMON alarm entry.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

Event

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

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

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

Desc: The string length is from 0 to 127, default is a null string.

Type: The notification of the event. The possible types are:

none: No SNMP log is created, no SNMP trap is sent.

log: Create SNMP log entry when the event is triggered.
snmptrap: Send SNMP trap when the event is triggered.
logandtrap: Create SNMP log entry and sent SNMP trap when the event is triggered.

Event Last Time: The value of sysUpTime at the time this event entry last generated an event.

Buttons

Add New Entry: Click to add a new RMON event entry.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

Network

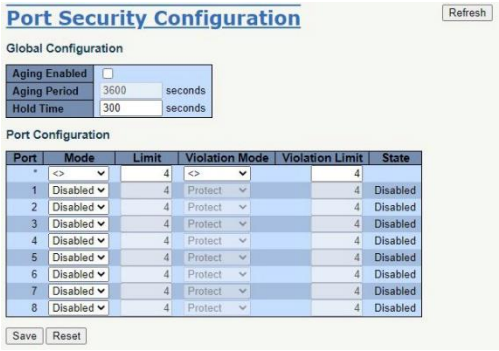
Port Security

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

Port Security allows limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If Port Security is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken depending on the violation mode. The four violation modes are described below.

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

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



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

Aging Period: If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying functionality for securing MAC addresses, they may have other requirements for the aging period. The underlying functionality will use the shortest requested aging period of all modules that have aging enabled. The Aging Period can be set to a number between 10 and 10000000 seconds with a default of 3600 seconds. The following example explains the benefits of enabling aging: If an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch having Port Security enabled, the end-host will be allowed to forward if it does not exceeded its limit. If the end-host logs off or powers down and aging was not enabled, the end-host would use resources on the switch and would still be allowed to forward. Aging prevents this. With aging enabled, a timer is started once the end-host is secured. When the timer expires, the switch will look for frames from the end-host. If no frames are seen within the next Aging Period, the switch assumes the end-host is disconnected and the corresponding resources are freed on the switch.

Hold Time: The hold time – measured in seconds – is used to determine how long a MAC address is held in the MAC table if it has been found to violate the limit. Valid range is between 10 and 10000000 seconds with a default of 300 seconds. The reason for holding a violating MAC address in the MAC table is primarily to ensure that the same MAC address doesn't give rise to continuous notifications (if notifications on violation count is enabled).

Port: The port number to which the configuration below applies.

Mode: Controls whether Port Security is enabled on this port. Notice that other modules may still use the underlying port security features without enabling Port Security on a given port.

Limit: The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1023. Default is 4. If the limit is exceeded, an action is taken corresponding to the violation mode. The switch has a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.

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

Protect: Do not allow more than Limit MAC addresses on the port, but take no further action.
Restrict: If Limit is reached, subsequent MAC addresses on the port will be counted and marked as violating. Such MAC addreses are removed from the MAC table when the hold time expires. At most Violation Limit MAC addresses can be marked as violating at any given time.
Shutdown: If Limit is reached, one additional MAC address will cause the port to be shut down. This implies that all secured MAC addresses will be removed from the port, and no new addresses will be learned. There are three ways to re-open the port:

1. In the "Configuration→Ports" page's "Configured" column, first disable the port, then restore the original mode.
2. Make a Port Security configuration change on the port.
3. Boot the switch.

Violation Limit: The maximum number of MAC addresses that can be marked as violating on this port. This number cannot exceed 1023. The default is 4. It is only used when Violation Mode is set to Restrict.

State: This column shows the current Port Security state of the port. The state takes one of four values:

Disabled: Port Security is disabled on the port.
Ready: The limit is not yet reached. This can be shown for all violation modes.
Limit Reached: Indicates that the limit is reached on this port. This is shown for all violation modes.
Shutdown: Indicates that the port is shut down by Port Security. This state is only shown if violation mode is set to Shutdown.

Buttons

Refresh: Click to refresh the page. Note that non-committed changes will be lost.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

ACL

Ports

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

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

Policy ID: Select the policy to apply to this port. The allowed values are 0 through 63. The default value is 0.

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

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

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

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

Enabled: Frames received on the port are mirrored.
Disabled: Frames received on the port are not mirrored.
The default value is "Disabled".

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

Enabled: Frames received on the port are stored in the System Log.
Disabled: Frames received on the port are not logged.
The default value is "Disabled".
Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.

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

Enabled: If a frame is received on the port, the port will be disabled.
Disabled: Port shut down is disabled.
The default value is "Disabled".
Note: The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).

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

Enabled: To reopen ports by changing the volatile port configuration of the ACL user module.
Disabled: To close ports by changing the volatile port configuration of the ACL user module.
The default value is "Enabled".

Counter: Counts the number of frames that match this ACE.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
Refresh: Click to refresh the page; any changes made locally will be undone.
Clear: Click to clear the counters.

Rate Limiters

Configure the rate limiter for the ACL of the switch.

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

Rate: The valid rate is 0 - 99, 100, 200, 300, ..., 1092000 in pps or 0, 100, 200, 300, ..., 1000000 in kbps.

Unit: Specify the rate unit. The allowed values are:

pps: Packets per second.
kbps: Kbits per second.

Buttons

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

Access Control List

This Access Control List Configuration page shows the Access Control List (ACL), which is made up of the ACEs defined on this switch. Each row describes the ACE that is defined. The maximum number of ACEs is 128 on each switch.

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

ACE: The ACE ID.

Ingress Port: The ingress port of the ACE. Possible values are:

All: The ACE will match all ingress port.

Port: The ACE will match a specific ingress port.

Policy/Bitmask: The policy number and bitmask of the ACE.

Frame Type: The frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.
EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.
ARP: The ACE will match ARP/RARP frames.
IPv4: The ACE will match all IPv4 frames.
IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.
IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.
IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.
IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
IPv6: The ACE will match all IPv6 standard frames.

Action: The forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.
Deny: Frames matching the ACE are dropped.
Filter: Frames matching the ACE are filtered.

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

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

Enabled: Frames received on the port are mirrored.
Disabled: Frames received on the port are not mirrored.
The default value is "Disabled".

Counter: The number of times that the ACE was hit by a frame.

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

Inserts a new ACE before the current row.

Edits the ACE row.

Moves the ACE up the list.

Moves the ACE down the list.

Deletes the ACE.

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

Buttons

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

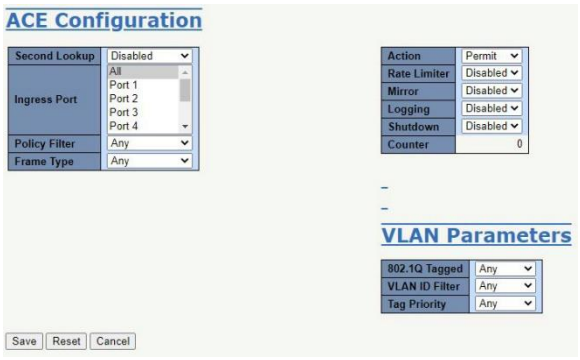
Refresh: Click to refresh the page; any changes made locally will be undone.
Clear: Click to clear the counters.
Remove All: Click to remove all ACEs.

Access Control List: ACE Configuration and VLAN Parameters

Configure an ACE (Access Control Entry) on this page.

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

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



Second Lookup: Specify the second lookup operation of the ACE.

Ingress Port: Select the ingress port for which this ACE applies.

All: The ACE applies to all port.
Port *n*: The ACE applies to this port number, where n is the number of the switch port.

Policy Filter: Specify the policy number filter for this ACE.

Any: No policy filter is specified.
Specific: If you want to filter a specific policy with this ACE, choose this value. Two fields for entering the policy value and the bitmask will appear.

Policy Value: When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is 0 to 63.

Policy Bitmask: When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is 0x0 to 0x3f. Notice the usage of bitmask. If the binary bit value is "0", it means this bit in the Policy Value can be 0 or 1. The real matched pattern is [policy_value & policy_bitmask]. For example, if the policy value is 3 and the policy bitmask is 0x10 (bit can be 0 or 1), then policy 2 and 3 are applied to this rule.

Frame Type: Select the frame type for this ACE. These frame types are mutually exclusive.

Any: Any frame can match this ACE.
Ethernet Type: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal) and the value should not be equal to 0x800(IPv4), 0x806(ARP) or 0x86DD(IPv6).
ARP: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with Ethernet type.
IPv4: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with Ethernet type.

IPv6: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.

Action: Specify the action to take with a frame that hits this ACE.

Permit: The frame that hits this ACE is granted permission for the ACE operation.
Deny: The frame that hits this ACE is dropped.
Filter: Frames matching the ACE are filtered.

Rate Limiter: Specify the rate limiter in number of base units. The allowed range is 1 to 16. Disabled indicates that the rate limiter operation is disabled.

Port Redirect: Frames that hit the ACE are redirected to the port number specified here. The rate limiter will affect these ports. The allowed range is the same as the switch port number range. Disabled indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted.

Mirror: Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port. The allowed values are:

Enabled: Frames received on the port are mirrored.
Disabled: Frames received on the port are not mirrored.
The default value is "Disabled".

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

Enabled: Frames matching the ACE are stored in the System Log.
Disabled: Frames matching the ACE are not logged.
Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.

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

Enabled: If a frame matches the ACE, the ingress port will be disabled.
Disabled: Port shut down is disabled for the ACE.
Note: The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).

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

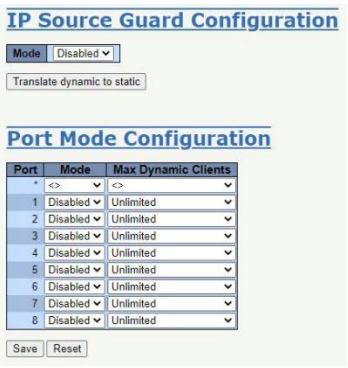
Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
Cancel: Return to the previous page.

IP Source Guard

Configuration

This page provides IP Source Guard related configuration.



Mode of IP Source Guard Configuration: Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.

Port Mode Configuration: Specify on which ports the IP Source Guard is enabled. IP Source Guard is enabled on a given port only when both Global Mode and Port Mode on the port are enabled.

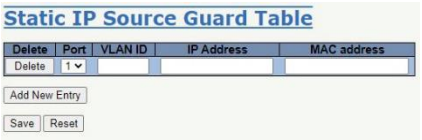
Max Dynamic Clients: Specify the maximum number of dynamic clients that can be learned on a given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, only the IP packets that are matched in static entries on the specific port are forwarded.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
Translate dynamic to static: Click to translate all dynamic entries to static entries.

Static Table

This page shows the static IP Source Guard rules. The maximum number of rules is 112 on the switch.



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

Port: The logical port for the settings.

VLAN ID: The VLAN ID for the settings.

IP Address: Allowed Source IP address.

MAC Address: Allowed Source MAC address.

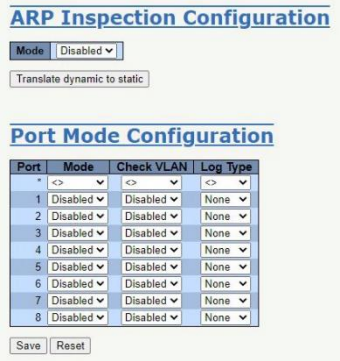
Buttons

Add New Entry: Click to add a new entry to the Static IP Source Guard table.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

ARP Inspection

Port Configuration

This page provides ARP Inspection related configuration.



Mode of ARP Inspection Configuration: Enable the Global ARP Inspection or disable the Global ARP Inspection.

Port Mode Configuration: Specify on which ports ARP Inspection is enabled. ARP Inspection is enabled on a given port only when both the global Mode and port's Mode are enabled. Possible modes are:

Enabled: Enable ARP Inspection operation.
Disabled: Disable ARP Inspection operation.
If you want to inspect the VLAN configuration, you have to enable the setting to "Check VLAN". "Check VLAN" is disabled by default. When the setting to "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. When the setting to "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. The possible settings for "Check VLAN" are:
Enabled: Enable check VLAN operation.
Disabled: Disable check VLAN operation.
If only the Global Mode and Port Mode on a given port are enabled, and the setting to "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and the possible types are:
None: Log nothing.
Deny: Log denied entries.
Permit: Log permitted entries.
ALL: Log all entries.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
Translate dynamic to static: Click to translate all dynamic entries to static entries.

VLAN Configuration

This page provides ARP Inspection related configuration.

Each page shows up to 9999 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first entry displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next VLAN Table match. The “>>” button will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the

warning message is shown in the displayed table. Use the “|<<” button to start over.

VLAN Mode Configuration: Specify on which VLANs ARP Inspection is enabled. Port mode must be enabled under port settings on the configuration web page. ARP inspection is enabled only when both Global Mode and Port Mode on the given port are enabled. A user can specify which VLAN will be inspected on the VLAN mode configuration web page. The log type can also be configured via VLAN setting. Possible types are:

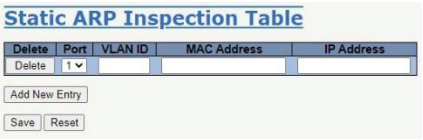
None: Log nothing.
Deny: Log denied entries.
Permit: Log permitted entries.
ALL: Log all entries.

Buttons

Add New Entry: Click to add a new VLAN to the ARP Inspection VLAN table.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

Static Table

This page shows the static ARP Inspection rules. The maximum number of rules is 256 on the switch.



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

Port: The logical port for the settings.

VLAN ID: The VLAN ID for the settings.

MAC Address: Allowed Source MAC address in ARP request packets.

IP Address: Allowed Source IP address in ARP request packets.

Buttons

Add New Entry: Click to add a new entry to the Static ARP Inspection table.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

Dynamic Table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learned by DHCP Snooping.

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

The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will assume - upon a “Refresh” button click - 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.

Port: Switch port number for which the entries are displayed.

VLAN ID: VLAN ID in which the ARP traffic is permitted.

MAC Address: User MAC address of the entry.

IP Address: User IP address of the entry.

Translate to static: Select the checkbox to translate the entry to static entry.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Refreshes the displayed table starting from the input fields.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
<<: Updates the table starting from the first entry in the Dynamic ARP Inspection Table.
>>: Updates the table, starting with the entry after the last entry currently displayed.

Aggregation

Common

This page is used to configure the Aggregation hash mode. This mode applies to the whole network element.

Source MAC Address: The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.

Destination MAC Address: The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.

IP Address: The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.

TCP/UDP Port Number: The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.

Groups

This page is used to configure the aggregation groups.

Group ID: The aggregation group ID for the settings contained in the same row. Group ID "Normal" that indicates there is no aggregation. Only one group ID is valid per port.

Port Members: Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

Mode: This parameter determines the mode for the aggregation group.

Disabled: The group is disabled.
Static: The group operates in static aggregation mode.
LACP (Active): The group operates in LACP active aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for more details.
LACP (Passive): The group operates in LACP passive aggregation mode. See IEEE 801.AX-2014, section 6.4.1 for more details.

Revertive: This parameter only applies to LACP-enabled groups. It determines if the group will perform automatic link (re-)calculation when links with higher priority becomes available.

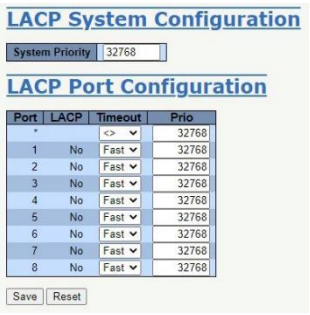
Max Bundle: This parameter only applies to LACP-enabled groups. It determines the maximum number of active bundled LACP ports allowed in an aggregation.

Buttons

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

LACP

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



System Priority: LACP uses the system priority with the MAC address to form the system ID, range 1-65535. When setting the priority, note that a higher number means a lower priority.

Port: The switch port number.

LACP: Show whether LACP is currently enabled on this switch port.

Timeout: The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.

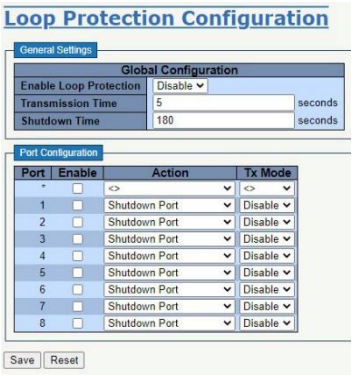
Prio: The **Prio** controls the priority of the port, range 1-65535. If the LACP partner wants to form a larger group than is supported by this device, then this parameter will control which ports will be active and which ports will be in a backup role. A lower number means greater priority.

Buttons

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

Loop Protection

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



Enable Loop Protection: Controls whether loop protections is enabled (as a whole).

Transmission Time: The interval between each loop protection PDU sent on each port. Valid values are 1 to 10 seconds. Default value is 5 seconds.

Shutdown Time: The period (in seconds) for which a port will be kept disabled in the event a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart). Default value is 180 seconds.

Port: The switch port number of the port.

Enable: Controls whether loop protection is enabled on this switch port.

Action: Configures the action performed when a loop is detected on a port. Valid values are Shutdown Port, Shutdown Port, and Log or Log Only.

Tx Mode: Controls whether the port is actively generating loop protection PDUs or whether it is just passively looking for looped PDUs.

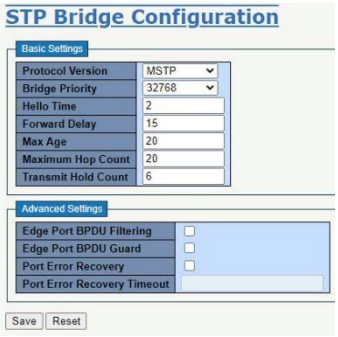
Buttons

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

Spanning Tree

Bridge Settings

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



Protocol Version: The MSTP/RSTP/STP protocol version setting. Valid values are: MSTP, RSTP and STP.

Bridge Priority: Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a Bridge Identifier. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.

Hello Time: The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds, default is 2 seconds.

> **Note:** Changing this parameter from the default value is not recommended and may have adverse effects on your network.

Forward Delay: The delay used by STP Bridges to transition the Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

Max Age: The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be <= (FwdDelay-1)*2.

Maximum Hop Count: This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.

Transmit Hold Count: The number of BPDUs a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDUs per second.

Edge Port BPDU Filtering: Control whether a port explicitly configured as Edge will transmit and receive BPDUs.

Edge Port BPDU Guard: Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled state and will be removed from the active topology.

Port Error Recovery: Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.

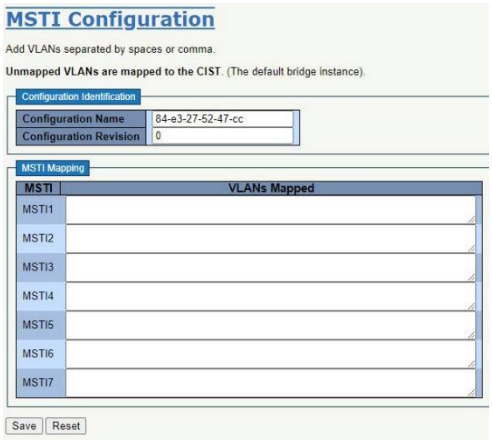
Port Error Recovery Timeout: The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Buttons

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

MSTI Mapping

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



Configuration Name: The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.

Configuration Revision: The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI: The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.

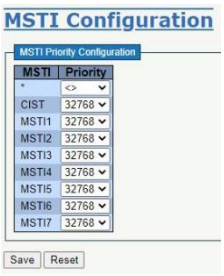
VLANs Mapped: The list of VLANs mapped to the MSTI. The VLANs can be written as single VLANs (x, where x is between 1 and 4094), or as ranges of VLANs (x-y). The VLANs are separated by a comma or a space. For example, 2,5,20-40,42. A VLAN can only be mapped to one MSTI. Leave this value empty if the MSTI is not used.

Buttons

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

MSTI Priorities

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



MSTI: The bridge instance. The CIST is the default instance, which is always active.

Priority: Controls the bridge priority. Lower numeric values have higher priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch, forms a Bridge Identifier.

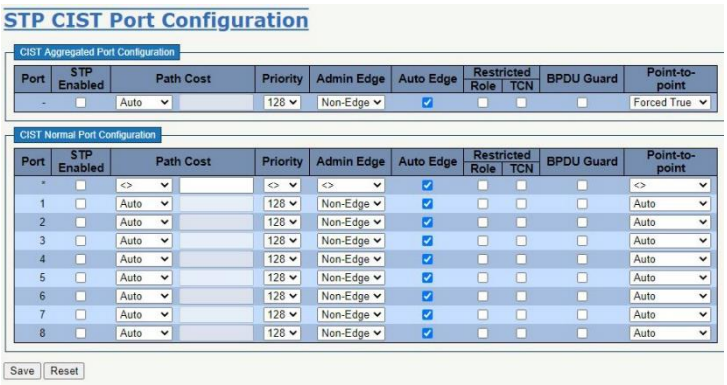
Buttons

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

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.



Port: The switch port number of the logical STP port.

STP Enabled: Controls whether STP is enabled on this switch port.

Path Cost: Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority: Controls the port priority. This can be used to control priority of ports having identical port cost (see above). Lower priority is better.

operEdge (state flag): Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor→Spanning Tree→STP Detailed Bridge Status.

AdminEdge: Controls whether the operEdge flag should start as set or cleared. (The initial operEdge state when a port is initialized).

AutoEdge: Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDUs are received on the port or not.

Restricted Role: If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

Restricted TCN: If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

BPDU Guard: If enabled, causes the port to disable itself upon receiving valid BPDUs. Contrary to the similar bridge setting, the port Edge status does not effect this setting.

A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.

Point-to-Point: Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

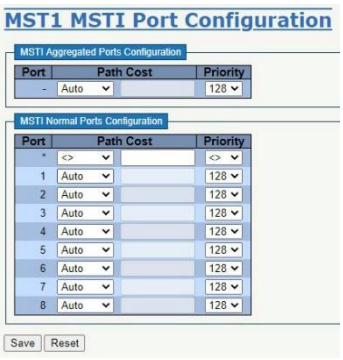
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

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.



Port: The switch port number of the corresponding STP CIST (and MSTI) port.

Path Cost: Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.

Priority: Controls the port priority. This can be used to control priority of ports having identical port cost (see above). Lower priority is better.

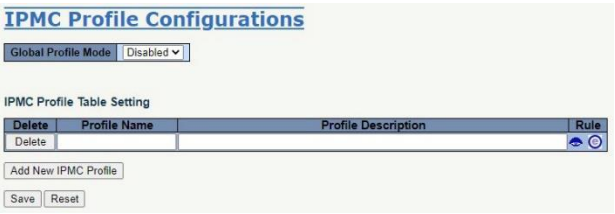
Buttons

Get: Click to retrieve settings for a specific MSTI.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

IPMC Profile

Profile Table

This page provides IPMC Profile related configurations.
The IPMC Profile Table is used to implement access control for IP multicast streams. You can add up to 64 profiles to the table. Each profile can have up to 128 rules.



Global Profile Mode: Enable/Disable the Global IPMC Profile. System filters based on profile settings only when the global profile mode is enabled.

Delete: Check to delete the entry. The designated entry will be deleted during the next save.

Profile Name: The name used for indexing the profile table. Each entry has the unique name which is composed of maximum 16 alphabetic and numeric characters. At least one alphabet must be present.

Profile Description: Additional description, which is composed of maximum 64 alphabetic character and numeric characters, about the profile. No blank or space characters are permitted as part of description. Use "_" or "-" to separate the description sentence.

Rule: When the profile is created, click the edit button to enter the rule setting page of the designated profile. Summary about the designated profile will be shown by clicking the view button. You can manage or inspect the rules of the designated profile by using the following buttons:

List the rules associated with the designated profile.

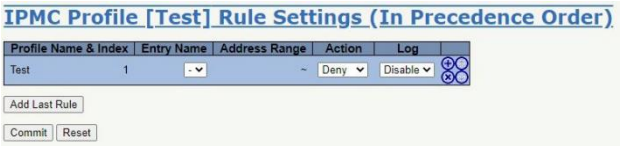
Adjust the rules associated with the designated profile.

Buttons

Add New IPMC Profile: Click to add new IPMC profile. Specify the name and configure the new entry. Click "Save".
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

IPMC Profile Rule Settings Table

This page provides the filtering rule settings for a specific IPMC profile. It displays the configured rule entries in precedence order. First rule entry has highest priority in lookup, while the last rule entry has lowest priority in lookup.



Profile Name & Index: The name of the designated profile to be associated. This field is not editable.

Entry Name: The name used in specifying the address range used for this rule. Only the existing profile address entries will be chosen in the selected box. This field is not allowed to be selected as none ("-") while the Rule Settings Table is committed.

Address Range: The corresponding address range of the selected profile entry. This field is not editable and will be adjusted automatically according to the selected profile entry.

Action: Indicates the learning action upon receiving the Join/Report frame that has the group address that matches the range specified in the rule.

Permit: The group address that matches the range specified in the rule will be learned.
Deny: The group address matches the range specified in the rule will be dropped.

Log: Indicates the logging preference upon receiving the Join/Report frame that has the group address that matches the range specified in the rule.

Enable: Corresponding information of the group address that matches the range specified in the rule will be logged.
Disable: Corresponding information of the group address that matches the range specified in the rule will not be logged.

Rule Management Buttons: You can manage rules and the corresponding precedence order by using the following buttons:

Insert a new rule before the current entry of rule.

Delete the current entry of rule.

Moves the current entry of rule up in the list.

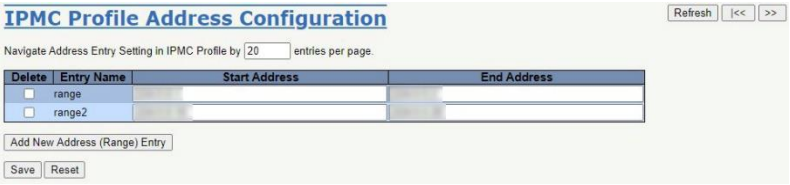
Moves the current entry of rule down in the list.

Buttons

Add Last Rule: Click to add a new rule in the end of the specific profile's rule list. Specify the address entry and configure the new entry. Click "Commit".
Commit: Click to commit rule changes for the designated profile.
Reset: Click to undo any changes made locally and revert to previously saved values.

Address Entry

This page provides address range settings used in IPMC profile.
The address entry is used to specify the address range that will be associated with IPMC Profile. It is allowed to create a maximum of 128 address entries in the system.



Delete: Check to delete the entry. The designated entry will be deleted during the next save.

Entry Name: The name used for indexing the address entry table. Each entry has the unique name which is composed of a maximum of 16 alphabetic and numeric characters. At least one alphabet character must be present.

Start Address: The starting IPv4/IPv6 Multicast Group Address that will be used as an address range.

End Address: The ending IPv4/IPv6 Multicast Group Address that will be used as an address range.

Buttons

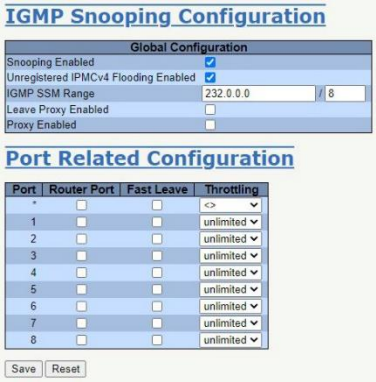
Add New Address (Range) Entry: Click to add new address range. Specify the name and configure the addresses. Click "Save".
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
Refresh: Refreshes the displayed table starting from the input fields.
|<<: Updates the table starting from the first entry in the IPMC Profile Address Configuration.
>>: Updates the table starting with the entry after the last entry currently displayed.

IPMC

IGMP Snooping

Basic Configuration

This page provides IGMP Snooping related configuration.



Snooping Enabled: Enable the Global IGMP Snooping.

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

IGMP SSM Range: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers to run the SSM service model for the groups in the address range. Assign a valid IPv4 multicast address as a prefix with a prefix length from 4 to 32 for the range.

Leave Proxy Enabled: Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled: Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port: Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave: Enable the fast leave on the port. System will remove group record and stop forwarding data upon receiving the IGMPv2 leave message without sending last member query messages. It is recommended to enable this feature only when a single IGMPv2 host is connected to the specific port.

Throttling: Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

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

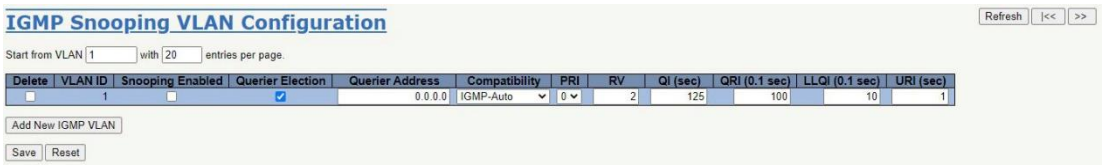
VLAN Configuration

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

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

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

For IGMP VLAN interface creation, you can create with button "Add New IGMP VLAN" or enter IP configuration page to setup IP interface. System→IP→Add Interface.



Delete: Select this option to delete an existing entry.

VLAN ID: The VLAN ID of the entry.

IGMP Snooping Enabled: Enable the per-VLAN IGMP Snooping. Up to 8 VLANs can be selected for IGMP Snooping.

Querier Election: Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.

Querier Address: Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, the system uses the IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, the system uses the first available IPv4 management address. Otherwise, the system uses a pre-defined value. By default, this value will be 192.0.2.1.

Compatibility: Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network.
The allowed selection is IGMP-Auto, Forced IGMPv1, Forced IGMPv2, Forced IGMPv3, default compatibility value is IGMP-Auto.

PRI: Priority of Interface. It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.

RV: Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255, default robustness variable value is 2.

QI: Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.

QRI: Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).

LLQI (LMQI for IGMP): Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).

URI: Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.
|<<: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
>>: Updates the table, starting with the entry after the last entry currently displayed.
Add New IGMP VLAN: Click to add a new VLAN interface for IGMP Snooping.

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

Port Filtering Profile

Port: The logical port for the settings.

Filtering Profile: Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

Profile Management Button: You can inspect the rules of the designated profile by using the following button:

: List the rules associated with the designated profile.

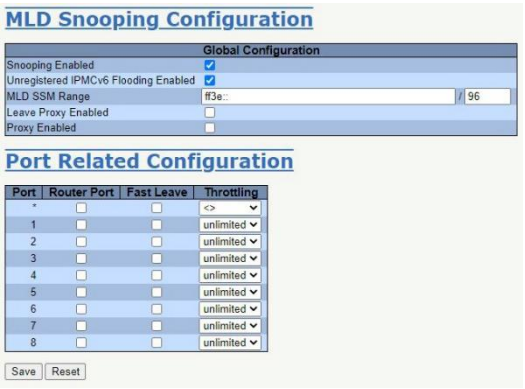
Buttons

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

MLD Snooping

Basic Configuration

This page provides MLD Snooping related configuration.



Snooping Enabled: Enable the Global MLD Snooping.

Unregistered IPMCv6 Flooding Enabled: Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.

MLD SSM Range: SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers to run the SSM service model for the groups in the address range. Assign valid IPv6 multicast address as prefix with a prefix length (from 8 to 128) for the range.

Leave Proxy Enabled: Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.

Proxy Enabled: Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.

Router Port: Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

Fast Leave: Enable the fast leave on the port. System will remove group record and stop forwarding data upon receiving the MLDv1 leave message without sending last member query messages. It is recommended to enable this feature only when a single MLDv1 host is connected to the specific port.

Throttling: Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

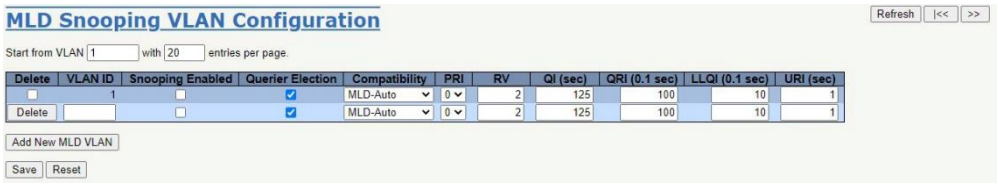
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

VLAN Configuration

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

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

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.



For MLD VLAN interface creation, you can create with button "Add New MLD VLAN" or enter IP configuration page to setup IP interface. System→IP→Add Interface.

VLAN ID: The VLAN ID of the entry.

MLD Snooping Enabled: Enable the per-VLAN MLD Snooping. Up to 8 VLANs can be selected for MLD Snooping.

Querier Election: Enable to join MLD Querier election in the VLAN. Disable to act as a MLD Non-Querier.

Compatibility: Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network.
The allowed selection is MLD-Auto, Forced MLDv1, Forced MLDv2, default compatibility value is MLD-Auto.

PRI: Priority of Interface. PRI indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.

RV: Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a link. The allowed range is 1 to 255, default robustness variable value is 2.

QI: Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.

QRI: Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).

LLQI: Last Listener Query Interval. The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The allowed range is 0 to 31744 in tenths of seconds, default last listener query interval is 10 in tenths of seconds (1 second).

URI: Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.

Buttons

Refresh: Refreshes the displayed table starting from the "VLAN" input fields.
|<<: Updates the table starting from the first entry in the VLAN Table, i.e. the entry with the lowest VLAN ID.
>>: Updates the table, starting with the entry after the last entry currently displayed.
Add New MLD VLAN: Click to add new VLAN interface for MLD Snooping.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

Port Filtering Profile

Port: The logical port for the settings.

Filtering Profile: Select the IPMC Profile as the filtering condition for the specific port. Summary about the designated profile will be shown by clicking the view button.

Profile Management Button: You can inspect the rules of the designated profile by using the following button:

: List the rules associated with the designated profile.

Buttons

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

LLDP

LLDP

This page allows the user to inspect and configure the current LLDP interface settings.

Tx Interval: The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the Tx Interval value. Valid values are restricted to 5 - 32768 seconds.

Tx Hold: Each LLDP frame contains information about how long of a time the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. Valid values are restricted to 2 - 10 times.

Tx Delay: If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than 1/4 of the Tx Interval value. Valid values are restricted to 1 - 8192 seconds.

Tx Reinit: When an interface is disabled, LLDP is disabled or the switch is rebooted, a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

Interface: The switch interface name of the logical LLDP interface.

Mode: Select LLDP mode.

- **Rx only:** The switch will not send out LLDP information, but LLDP information from neighbor units is analyzed.
- **Tx only:** The switch will drop LLDP information received from neighbors, but will send out LLDP information.
- **Disabled:** The switch will not send out LLDP information, and will drop LLDP information received from neighbors.
- **Enabled:** The switch will send out LLDP information, and will analyze LLDP information received from neighbors.

CDP Aware: Select CDP awareness.

The CDP operation is restricted to decoding incoming CDP frames (the switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the interface is enabled.

Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbors' table as shown below.

CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.

CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table.

CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.

CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.

Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.

If all interfaces have CDP awareness disabled the switch forwards CDP frames received from neighbor devices. If at least one interface has CDP awareness enabled, then all CDP frames are terminated by the switch.

Note: When CDP awareness on an interface is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.

Port Descr

Optional TLV: When checked the "port description" is included in LLDP information transmitted.

Sys Name

Optional TLV: When checked the "system name" is included in LLDP information transmitted.

Sys Descr

Optional TLV: When checked the "system description" is included in LLDP information transmitted.

Sys Capa

Optional TLV: When checked the "system capability" is included in LLDP information transmitted.

Mgmt Addr

Optional TLV: When checked the "management address" is included in LLDP information transmitted.

Buttons

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

LLDP-MED

This page allows you to configure the LLDP-MED. This function applies to VoIP devices which support LLDP-MED.

Fast start repeat count: Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems in general. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (for example only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPU space and to reduce security and system integrity issues that can come with inappropriate knowledge of the network policy.

With this in mind LLDP-MED defines an LLDP-MED Fast Start interaction between the protocol and the application layers on top of the protocol, in order to achieve these related properties. Initially, a Network Connectivity Device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED Endpoint Device is detected, will an LLDP-MED capable Network Connectivity Device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated interface. The LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second, when a new LLDP-MED neighbor has been detected in order share LLDP-MED information as fast as possible to new neighbors.

Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With Fast start repeat count it is possible to specify the number of times the fast start transmission would be repeated. The recommended value is 4 times, given that 4 LLDP frames with a 1 second interval will be transmitted, when an LLDP frame with new information is received.

It should be noted that LLDP-MED and the LLDP-MED Fast Start mechanism is only intended to run on links between LLDP-MED Network Connectivity Devices and Endpoint Devices, and as such does not apply to links between LAN infrastructure elements, including Network Connectivity Devices, or other types of links.


LLDP-MED Interface Configuration

Interface	Transmit TLVs			Device Type
	Capabilities	Policies	Location	
*	☑	☑	☑	<>
GigabitEthernet 1/1	☑	☑	☑	Connectivity
GigabitEthernet 1/2	☑	☑	☑	Connectivity
GigabitEthernet 1/3	☑	☑	☑	Connectivity
GigabitEthernet 1/4	☑	☑	☑	Connectivity
GigabitEthernet 1/5	☑	☑	☑	Connectivity
GigabitEthernet 1/6	☑	☑	☑	Connectivity
2.5GigabitEthernet 1/1	☑	☑	☑	Connectivity
2.5GigabitEthernet 1/2	☑	☑	☑	Connectivity

It is possible to select which LLDP-MED information that shall be transmitted to the neighbors. When the checkbox is checked the information is included in the frame transmitted to the neighbor.

Interface: The interface name to which the configuration applies.

Transmit TLVs – Capabilities: When checked the switch's capabilities is included in LLDP-MED information transmitted.

Transmit TLVs – Policies: When checked the configured policies for the interface is included in LLDP-MED information transmitted.

Transmit TLVs – Location: When checked the configured location information for the switch is included in LLDP-MED information transmitted.

Transmit TLVs – PoE: When checked the configured PoE (Power Over Ethernet) information for the interface is included in LLDP-MED information transmitted.

Device Type: Any LLDP-MED Device is operating as a specific type of LLDP-MED Device, which may be either a Network Connectivity Device or a specific Class of Endpoint Device, as defined below.

A Network Connectivity Device is a LLDP-MED Device that provides access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices.

An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

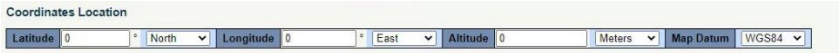
LAN Switch/Router
IEEE 802.1 Bridge

IEEE 802.3 Repeater (included for historical reasons)
IEEE 802.11 Wireless Access Point
Any device that supports the IEEE 802.1AB and MED extensions that can relay IEEE 802 frames via any method.

An Endpoint Device a LLDP-MED Device that sits at the network edge and provides some aspect of IP communications service, based on IEEE 802 LAN technology.

The main difference between a Network Connectivity Device and an Endpoint Device is that only an Endpoint Device can start the LLDP-MED information exchange.

Even though a switch always should be a Network Connectivity Device, it is possible to configure it to act as an Endpoint Device, and thereby start the LLDP-MED information exchange (In the case where two Network Connectivity Devices are connected together).



Latitude: Latitude SHOULD be normalized to within 0-90 degrees with a maximum of 4 digits. It is possible to specify the direction to either North of the equator or South of the equator.

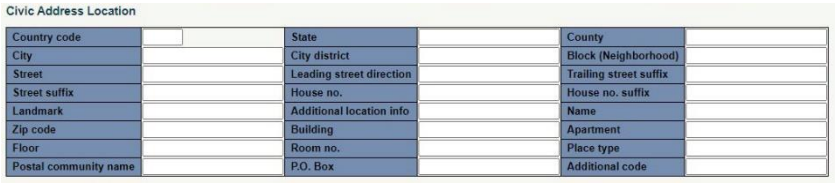
Longitude: Longitude SHOULD be normalized to within 0-180 degrees with a maximum of 4 digits. It is possible to specify the direction to either East of the prime meridian or West of the prime meridian.

Altitude: Altitude SHOULD be normalized to within -2097151.9 to 2097151.9 with a maximum of 1 digits. It is possible to select between two altitude types (floors or meters).

Meters: Representing meters of Altitude defined by the vertical datum specified.
Floors: Representing altitude in a form more relevant in buildings which have different floor-to-floor dimensions. An altitude = 0.0 is meaningful even outside a building, and represents ground level at the given latitude and longitude. Inside a building, 0.0 represents the floor level associated with ground level at the main entrance.

Map Datum: The Map Datum is used for the coordinates given in these options:

WGS84: (Geographical 3D) - World Geodesic System 1984, CRS Code 4327, Prime Meridian Name: Greenwich.
NAD83/NAVD88: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is the North American Vertical Datum of 1988 (NAVD88). This datum pair is to be used when referencing locations on land, not near tidal water (which would use Datum = NAD83/MLLW).
NAD83/MLLW: North American Datum 1983, CRS Code 4269, Prime Meridian Name: Greenwich; The associated vertical datum is Mean Lower Low Water (MLLW). This datum pair is to be used when referencing locations on water/sea/ocean.



IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). The total number of characters for the combined civic address information must not exceed 250 characters.

A couple of notes to the limitation of 250 characters.

1. If more than one civic address location is used, each of the additional civic address locations will use 2 extra characters in addition to the civic address location text.
2. The 2 letter country code is not part of the 250 characters limitation.

Country code: The two-letter ISO 3166 country code in capital ASCII letters - Example: DK, DE or US.

State: National subdivisions (state, canton, region, province, prefecture).

County: County, parish, gun (Japan), district.

City: City, township, shi (Japan) - Example: Copenhagen.

City district: City division, borough, city district, ward, chou (Japan).

Block (Neighborhood): Neighborhood, block.

Street: Street - Example: Poppelvej.

Leading street direction: Leading street direction - Example: N.

Trailing street suffix: Trailing street suffix - Example: SW.

Street suffix: Street suffix - Example: Ave, Platz.

House no.: House number - Example: 21.

House no. suffix: House number suffix - Example: A, 1/2.

Landmark: Landmark or vanity address - Example: Columbia University.

Additional location info: Additional location info - Example: South Wing.

Name: Name (residence and office occupant) - Example: Flemming Jahn.

Zip code: Postal/zip code - Example: 2791.

Building: Building (structure) - Example: Low Library.

Apartment: Unit (Apartment, suite) - Example: Apt 42.

Floor: Floor - Example: 4.

Room no.: Room number - Example: 450F.

Place type: Place type - Example: Office.

Postal community name: Postal community name - Example: Leonia.

P.O. Box: Post office box (P.O. BOX) - Example: 12345.

Additional code: Additional code - Example: 1320300003.

Emergency Call Service (e.g. E911 and others), such as defined by TIA or NENA.

Emergency Call Service: Emergency Call Service ELIN identifier data format is defined to carry the ELIN identifier as used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. This format consists of a numerical digit string, corresponding to the ELIN to be used for emergency calling.

Network Policy Discovery enables the efficient discovery and diagnosis of mismatch issues with the VLAN configuration, along with the associated Layer 2 and Layer 3 attributes, which apply for a set of specific protocol applications on that port. Improper network policy configurations are a very significant issue in VoIP environments that frequently result in voice quality degradation or loss of service.

Policies are only intended for use with applications that have specific 'real-time' network policy requirements, such as interactive voice and/or video services.

The network policy attributes advertised are:

Layer 2 VLAN ID (IEEE 802.1Q-2003)
Layer 2 priority value (IEEE 802.1D-2004)
Layer 3 Diffserv code point (DSCP) value (IETF RFC 2474)

This network policy is potentially advertised and associated with multiple sets of application types supported on a given port. The application types specifically addressed are:

Voice
Guest Voice
Softphone Voice
Video Conferencing
Streaming Video
Control / Signalling (conditionally support a separate network policy for the media types above)

A large network may support multiple VoIP policies across the entire organization, and different policies per application type. LLDP-MED allows multiple policies to be advertised per port, each corresponding to a different application type. Different ports on the same Network Connectivity Device may advertise different sets of policies, based on the authenticated user identity or port configuration.

It should be noted that LLDP-MED is not intended to run on links other than between Network Connectivity Devices and Endpoints, and therefore does not need to advertise the multitude of network policies that frequently run on an aggregated link interior to the LAN.

Delete: Check to delete the policy. It will be deleted during the next save.

Policy ID: ID for the policy. This is auto generated and shall be used when selecting the policies that shall be mapped to the specific interfaces.

Application Type: Intended use of the application types:

Voice: For use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

Voice Signalling (conditional): For use in network topologies that require a different policy for the voice signalling than for the voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Voice application policy.

Guest Voice: Support a separate 'limited feature-set' voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.

Guest Voice Signalling (conditional): For use in network topologies that require a different policy for the guest voice signalling than for the guest voice media. This application type should not be advertised if all the same network policies apply as those advertised in the Guest Voice application policy.

Softphone Voice: For use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an 'untagged' VLAN or a single 'tagged' data specific VLAN. When a network policy is defined for use with an 'untagged' VLAN (see Tagged flag below), then the L2 priority field is ignored and only the DSCP value has relevance.

Video Conferencing: For use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.

Streaming Video: For use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.

Video Signalling (conditional): For use in network topologies that require a separate policy for the video signalling than for the video media. This application type should not be advertised if all the same network policies apply as those advertised in the Video Conferencing application policy.

Tag: Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN.

Untagged indicates that the device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003. In this case, both the VLAN ID and the Layer 2 priority fields are ignored and only the DSCP value has relevance.

Tagged indicates that the device is using the IEEE 802.1Q tagged frame format, and that both the VLAN ID and the Layer 2 priority values are being used, as well as the DSCP value. The tagged format includes an additional field, known as the tag header. The tagged frame format also includes priority tagged frames as defined by IEEE 802.1Q-2003.

VLAN ID: VLAN identifier (VID) for the interface as defined in IEEE 802.1Q-2003.

L2 Priority: L2 Priority is the Layer 2 priority to be used for the specified application type. L2 Priority may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004. A value of 0 represents use of the default priority as defined in IEEE 802.1D-2004.

DSCP: DSCP value to be used to provide Diffserv node behaviour for the specified application type as defined in IETF RFC 2474. DSCP may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

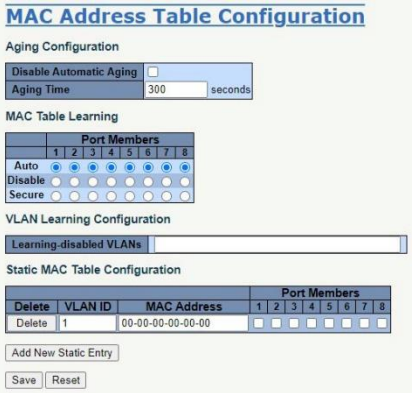
Adding a new policy: Click to add a new policy. Specify the Application type, Tag, VLAN ID, L2 Priority and DSCP for the new policy. Click "Save". The number of policies supported is 32.

Buttons

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

MAC Table

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



Aging Configuration

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

Configure aging time by entering a value here in seconds; for example, Age time seconds. The allowed range is 10 to 1000000 seconds.

Disable the automatic aging of dynamic entries by checking Disable automatic aging.

MAC Table Learning

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

Learning for ports is based on the following settings:

Auto: Learning is done automatically as soon as a frame with unknown SMAC is received.

Disable: No learning is done.

Secure: Only static MAC entries are learned, all other frames are dropped.

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

VLAN Learning Configuration

Learning-disabled VLANs: This field shows the Learning-disabled VLANs. When a NEW MAC arrives into a learning-disabled VLAN, the MAC won't be learned. By the default, the field is empty. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound.
The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters.

Static MAC Table Configuration

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The MAC table is sorted first by VLAN ID and then by MAC address.

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

VLAN ID: The VLAN ID of the entry.

MAC Address: The MAC address of the entry.

Port Members: Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.

Adding a New Static Entry: To add a new entry to the static MAC table, click “Add New Static Entry”. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save".

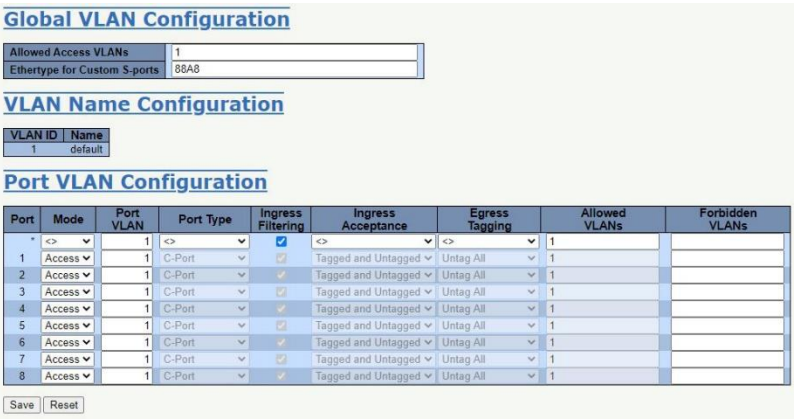
Buttons

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

VLANs

Configuration

This page allows for controlling VLAN configuration on the switch.
The page is divided into a global section and a per-port configuration section.



Global VLAN Configuration

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

Ethertype for Custom S-ports: This field specifies the Ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.

Port VLAN Configuration

Port: This is the logical port number of this row.

Mode: The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below. Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port will get when the mode is applied.

Access: Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:
Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1.
Accepts untagged and C-tagged frames.
Discards all frames not classified to the Access VLAN.
On egress all frames are transmitted untagged.

Trunk: Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics:
By default, a trunk port is member of all VLANs (1-4095).
The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs.
Frames classified to a VLAN that the port is not a member of are discarded.
By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress.

Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress.

Hybrid: Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities:
Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware.
Ingress filtering can be controlled.
Ingress acceptance of frames and configuration of egress tagging can be configured independently.

Port VLAN: Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1. On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0). On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN. The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

Port Type: Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required.

Unaware: On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress.

C-Port: On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag.

S-Port: On egress, if frames must be tagged, they will be tagged with an S-tag.
On ingress, frames with a VLAN tag with TPID = 0x88A8 get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped.
Notice: If the S-port is configured to accept Tagged and Untagged frames (see Ingress Acceptance below), frames with a C-tag are treated like frames with an S-tag. If the S-port is configured to accept Untagged Only frames, S-tagged frames will be discarded (except for priority S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID.

S-Custom-Port: On egress, if frames must be tagged, they will be tagged with the custom S-tag. On ingress, frames with a VLAN tag with a TPID equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept Tagged Only frames (see Ingress Acceptance below), frames without this TPID are dropped.
Notice: If the custom S-port is configured to accept Tagged and Untagged frames (see Ingress Acceptance below), frames with a C-tag are treated like frames with a custom S-tag. If the Custom S-port is configured to accept Untagged Only frames, custom S-tagged frames will be discarded (except for priority custom S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID.

Ingress Filtering: Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled. If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. If ingress filtering is disabled, frames classified

to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

Ingress Acceptance: Hybrid ports allow for changing the type of frames that are accepted on ingress.

Tagged and Untagged: Both, tagged and untagged frames are accepted. See Port Type for a description of when a frame is considered tagged.
Tagged Only: Only frames tagged with the corresponding Port Type tag are accepted on ingress.
Untagged Only: Only untagged frames are accepted on ingress. See Port Type for a description of when a frame is considered untagged.

Egress Tagging: Ports in Trunk and Hybrid mode may control the tagging of frames on egress.

Untag Port VLAN: Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.
Tag All: All frames, whether classified to the Port VLAN or not, are transmitted with a tag.
Untag All: All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.

Allowed VLANs: Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be a member of one VLAN, the Access VLAN.
The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become a member of all VLANs, and is therefore set to 1-4095. The field may be left empty, which means that the port will not become a member of any VLANs.

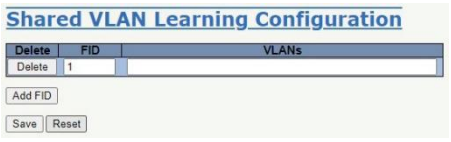
Forbidden VLANs: A port may be configured to never become a member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field. By default, the field is left blank, which means that the port may become a member of all possible VLANs.

Buttons

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

SVL

This page allows for controlling SVL configuration on the switch.
In SVL, one or more VLANs map to a Filter ID (FID). By default, there is a one-to-one mapping from VLAN to FID, in which case the switch acts as an IVL bridge, but with SVL multiple VLANs may share the same MAC address table entries.



Delete: A previously allocated FID can be deleted by the use of this button.

FID: The Filter ID (FID) is the ID that VLANs get learned on in the MAC table when SVL is in effect. No two rows in the table can have the same FID and the FID must be a number between 1 and 63.

VLANs: List of VLANs mapped into FID. The syntax is as follows: Individual VLANs are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will map VLANs 1, 10, 11, 12, 13, 200, and 300: 1,10-13,200,300. Spaces are allowed in between the delimiters. The range of valid VLANs is 1 to 4095. The same VLAN can only be a member

of one FID. A message will be displayed if one VLAN is grouped into two or more FIDs. All VLANs must map to a particular FID, and by default VLAN x maps to FID x. This implies that if FID x is defined, then VLAN x is implicitly a member of FID x unless it is specified for another FID. If FID x doesn't exist, a confirmation message will be displayed, asking whether to continue adding VLAN x implicitly to FID x.

Buttons

Add FID: Add a new row to the SVL table. The FID will be pre-filled with the first unused FID.
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

VCL

MAC-based VLAN

MAC address to VLAN ID mappings can be configured here. This page allows adding and deleting MAC-based VLAN Classification List entries and assigning the entries to different ports.

Delete: To delete a MAC to VLAN ID mapping entry, check this box and press save. The entry will be deleted in the stack.

MAC Address: The MAC address of the mapping.

VLAN ID: The VLAN ID the above MAC will be mapped to.

Port Members: A row of check boxes for each port is displayed for each MAC to VLAN ID mapping entry. To include a port in the mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.

Adding a New MAC to VLAN ID mapping entry: Click “Add New Entry” to add a new MAC to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any unicast MAC address can be used to configure the mapping. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095. The MAC to VLAN ID entry is enabled when you click on "Save". A mapping without any port members will not be added when you click "Save". The “Delete” button can be used to undo the addition of new mappings. The maximum possible MAC to VLAN ID mapping entries are limited to 256.

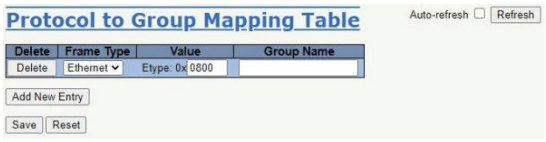
Buttons

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: Refreshes the displayed table.

Protocol-based VLAN

Protocol to Group

This page allows you to add a new Protocol to Group Name (each protocol can be part of only one Group) mapping entries as well as allow you to see and delete already mapped entries for the switch.



The displayed settings are:

Delete: To delete a Protocol to Group Name map entry, check this box. The entry will be deleted from the switch during the next Save.

Frame Type: Frame Type can have one of the following values:

Ethernet
LLC
SNAP

Note: When changing the Frame type field, the valid value of the following text field will vary depending on the new frame type you selected.

Value: Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu. Below are the criteria for the three different Frame Types:

Ethernet: Value in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype range between 0x0600 and 0xffff

LLC: Valid value in this case is comprised of two different sub-values.
DSAP: 1-byte long string (0x00-0xff)
SSAP: 1-byte long string (0x00-0xff)

SNAP: Valid value in this case is also comprised of two different sub-values.
OUI: OUI (Organizationally Unique Identifier) is a parameter in the format of xx-xx-xx where each pair (xx) in the string is a hexadecimal value ranging between 0x00 and 0xff.
PID: PID (Protocol ID). If OUI is hexadecimal 000000, then the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.
In other words, if the value of OUI field is 00-00-00 then the value of PID will be etype (0x0600-0xffff) and if the value of OUI is other than 00-00-00 then valid values of PID will be any value between 0x0000 and 0xffff.

Group Name: A valid Group Name is a 16-character long string, unique for every entry, which consists of a combination of alphabets (a-z or A-Z) and integers (0-9).

Note: Special characters and underscores (_) are not allowed.

Adding a New Group to VLAN mapping entry: Click “Add New Entry” to add a new entry in the mapping table. An empty row is added to the table, where Frame Type, Value and the Group Name can be configured as needed. The “Delete” button can be used to undo the addition of new entry. The maximum possible Protocol to Group mappings are limited to 128.

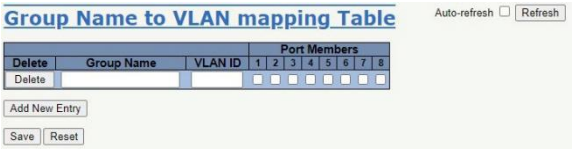
Buttons

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.

Group to VLAN

This page allows you to map a Group Name (already configured or to be configured in the future) to a VLAN for the switch.



The displayed settings are:

Delete: To delete a Group Name to VLAN mapping, check this box. The entry will be deleted from the switch during the next Save.

Group Name: A valid Group Name is a string, at the most 16 characters long, which consists of a combination of alphabets (a-z or A-Z) and integers (0-9) with no special characters allowed. You may either use a Group that already includes one or more protocols (see Protocol to Group mappings), or create a Group to VLAN ID mapping that will become active the moment you add one or more protocols inside that Group. Furthermore, the Group to VLAN ID mapping is not unique, as long as the port lists of these mappings are mutually exclusive (e.g. Group1 can be mapped to VID 1 on port#1 and to VID 2 on port#2).

VLAN ID: The VLAN ID to which the Group Name will be mapped. A valid VLAN ID ranges from 1 to 4095.

Port Members: A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in the mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members and all boxes are unchecked.

Adding a new Group to VLAN mapping entry: Click “Add New Entry” to add a new entry in the mapping table. An empty row is added to the table and the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The “Delete” button can be used to undo the addition of new entry. The maximum possible Group to VLAN mappings are limited to 256.

Buttons

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

IP Subnet-based VLAN

The IP subnet to VLAN ID mappings can be configured here. This page allows adding, updating and deleting IP subnet to VLAN ID mapping entries and assigning them to different ports.

Delete: To delete a mapping, check this box and press save. The entry will be deleted in the stack.

IP Address: Indicates the subnet's IP address (Any of the subnet's host addresses can be also provided here, the application will convert it automatically).

Mask Length: Indicates the subnet's mask length.

VLAN ID: Indicates the VLAN ID the subnet will be mapped to. IP Subnet to VLAN ID is a unique matching.

Port Members: A row of check boxes for each port is displayed for each IP subnet to VLAN ID mapping entry. To include a port in a mapping, simply check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members and all boxes are unchecked.

Adding a New IP subnet-based VLAN: Click “Add New Entry” to add a new IP subnet to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any IP address/mask can be configured for the mapping. Legal values for the VLAN ID are 1 to 4095. The IP subnet to VLAN ID mapping entry is enabled when you click on "Save". The “Delete” button can be used to undo the addition of new mappings. The maximum possible IP subnet to VLAN ID mappings are limited to 128.

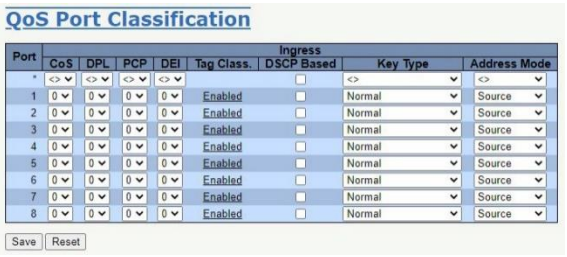
Buttons

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: Refreshes the displayed table.

QoS

Port Classification

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



The displayed settings are:

Port: The port number for which the configuration below applies.

CoS: Controls the default CoS value. All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority. If the port is VLAN aware,

the frame is tagged and Tag Class is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default CoS. The classified CoS can be overruled by a QCL entry.

Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.

DPL: Controls the default DPL value. All frames are classified to a Drop Precedence Level. If the port is VLAN aware, the frame is tagged and Tag Class is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DPL. The classified DPL can be overruled by a QCL entry.

PCP: Controls the default PCP value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.

DEI: Controls the default DEI value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.

Tag Class.: Shows the classification mode for tagged frames on this port.

Disabled: Use default CoS and DPL for tagged frames.
Enabled: Use mapped versions of PCP and DEI for tagged frames.

Click on the mode in order to configure the mode and/or mapping.

Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.

DSCP Based: Click to Enable DSCP Based QoS Ingress Port Classification.

Key Type: The key type specifying the key generated for frames received on the port. The allowed values are:

Normal: Half key, match outer tag, SIP/DIP and SMAC/DMAC.
Double Tag: Quarter key, match inner and outer tag.
IP Address: Half key, match inner and outer tag, SIP and DIP. For non-IP frames, match outer tag only.
MAC and IP Address: Full key, match inner and outer tag, SMAC, DMAC, SIP and DIP.

Filtering on DMAC type (unicast/multicast/broadcast) is supported for any key type.

Address Mode: The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. This parameter is only used when the key type is Normal. The allowed values are:

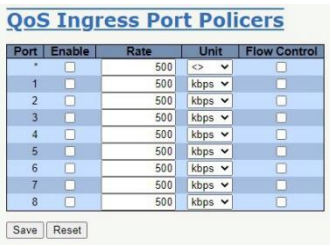
Source: Enable SMAC/SIP matching.
Destination: Enable DMAC/DIP matching.

Button

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

Port Policing

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



The displayed settings are:

Port: The port number for which the configuration below applies.

Enable: Enable or disable the port policer for this switch port.

Rate: Controls the rate for the port policer. This value is restricted to 100-3276700 when "Unit" is kbps or fps, and 1-3276 when "Unit" is Mbps or kfps. The rate is internally rounded up to the nearest value supported by the port policer.

Unit: Controls the unit of measure for the port policer rate as kbps, Mbps, fps or kfps.

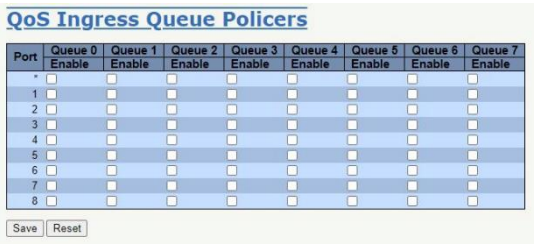
Flow Control: If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Buttons

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

Queue Policing

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



The displayed settings are:

Port: The port number for which the configuration below applies.

Enable (E): Enable or disable the queue policer for this switch port.

Rate: Controls the rate for the queue policer. This value is restricted to 100-3276700 when "Unit" is kbps, and 1-3276 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer. This field is only shown if at least one of the queue policers is enabled.

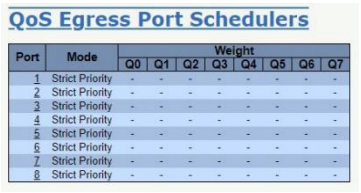
Unit: Controls the unit of measure for the queue policer rate as kbps or Mbps. This field is only shown if at least one of the queue policers is enabled.

Buttons

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

Port Scheduler

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



The displayed settings are:

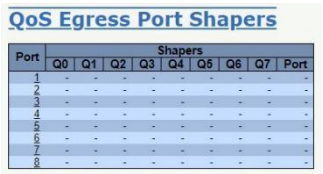
Port: The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.

Mode: Shows the scheduling mode for this port.

Qn: Shows the weight for this queue and port.

Port Shaping

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



The displayed settings are:

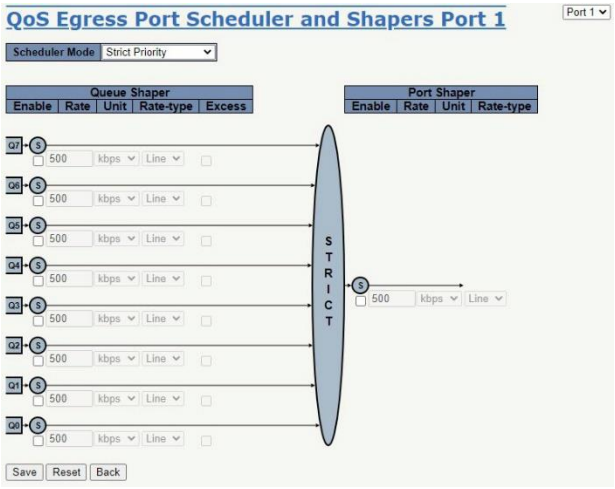
Port: The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.

Qn: Shows "-" for disabled or actual queue shaper rate - e.g. "800 Mbps".

Port: Shows "-" for disabled or actual port shaper rate - e.g. "800 Mbps".

QoS Egress Port Scheduler and Shapers

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



The displayed settings are:

Scheduler Mode: Controls how many of the queues are scheduled as strict and how many are scheduled as weighted on this switch port.

Queue Shaper Enable: Controls whether the queue shaper is enabled for this queue on this switch port.

Queue Shaper Rate: Controls the rate for the queue shaper. This value is restricted to 100-3281943 when "Unit" is kbps and 1-3281 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper.

Queue Shaper Unit: Controls the unit of measure for the queue shaper rate as kbps or Mbps.

Queue Shaper Rate-type: The rate type of the queue shaper. The allowed values are:

Line: Specify that this shaper operates on line rate.
Data: Specify that this shaper operates on data rate.

Queue Shaper Excess: Controls whether the queue is allowed to use excess bandwidth.

Queue Scheduler Weight: Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Queue Scheduler Percent: Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".

Port Shaper Enable: Controls whether the port shaper is enabled for this switch port.

Port Shaper Rate: Controls the rate for the port shaper. This value is restricted to 100-3281943 when "Unit" is kbps, and 1-3281 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the port shaper.

Port Shaper Unit: Controls the unit of measure for the port shaper rate as kbps or Mbps.

Port Shaper Rate-type: The rate type of the port shaper. The allowed values are:

Line: Specify that this shaper operates on line rate.
Data: Specify that this shaper operates on data rate.

Buttons

Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.
Back: Click to undo any changes made locally and return to the previous page.

Port Tag Remarking

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

The displayed settings are:

Port: The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking.

Mode: Shows the tag remarking mode for this port.

Classified: Use classified PCP/DEI values.
Default: Use default PCP/DEI values.
Mapped: Use mapped versions of CoS and DPL.

QoS Egress Port Tag Remarking

The QoS Egress Port Tag Remarking for a specific port are configured on this page.

Mode: Controls the tag remarking mode for this port.

Classified: Use classified PCP/DEI values.
Default: Use default PCP/DEI values.
Mapped: Use mapped versions of CoS and DPL.

PCP/DEI Configuration: Controls the default PCP and DEI values used when the mode is set to Default.

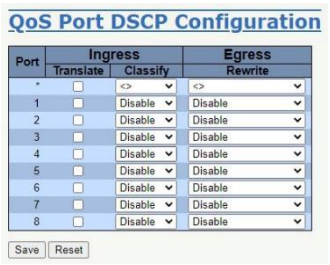
(CoS, DPL) to (PCP, DEI) Mapping: Controls the mapping of the classified (CoS, DPL) to (PCP, DEI) values when the mode is set to Mapped.

Buttons

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.

Port DSCP

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



The displayed settings are:

Port: The Port column shows the list of ports for which you can configure DSCP ingress and egress settings.

Ingress: In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress:

Translate: To Enable the Ingress Translation click the checkbox.
Classify: Classification for a port have 4 different values.
Disable: No Ingress DSCP Classification.
DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.
Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.
All: Classify all DSCP.

Egress: Port Egress Rewriting can be one of –

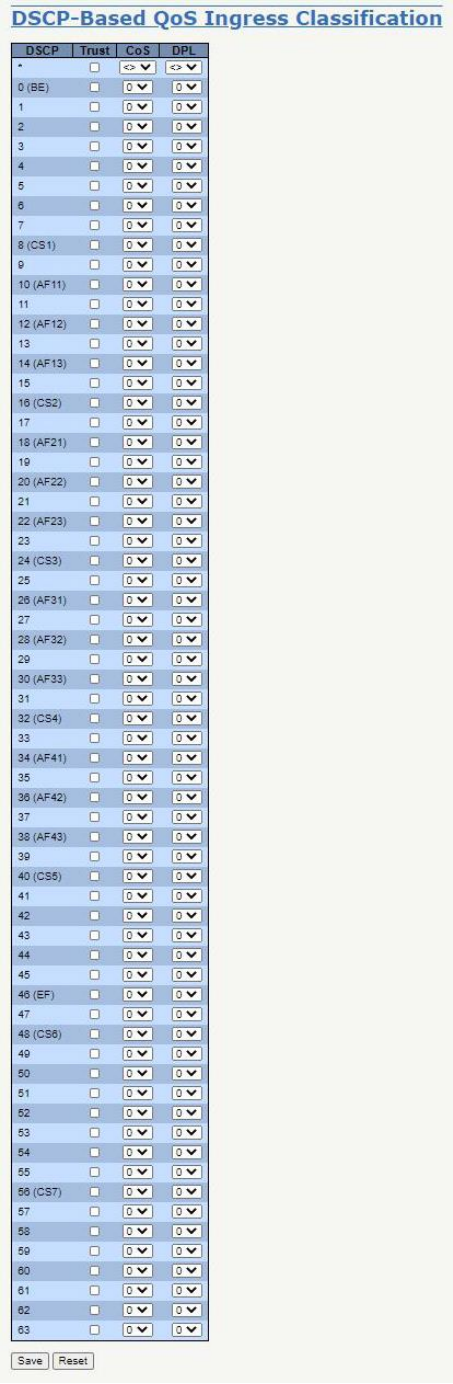
Disable: No Egress rewrite.
Enable: Rewrite enabled without remapping.
Remap DP Unaware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation→Egress Remap DP0' table.
Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation→Egress Remap DP0' table or from the 'DSCP Translation→Egress Remap DP1' table.

Buttons

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

DSCP-Based QoS

This page allows you to configure the basic QoS DSCP based QoS Ingress Classification settings for all switches.



The displayed settings are:

DSCP: Maximum number of supported DSCP values are 64.

Trust: Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific CoS and DPL. Frames with untrusted DSCP values are treated as a non-IP frame.

CoS: CoS value can be any of (0-7)

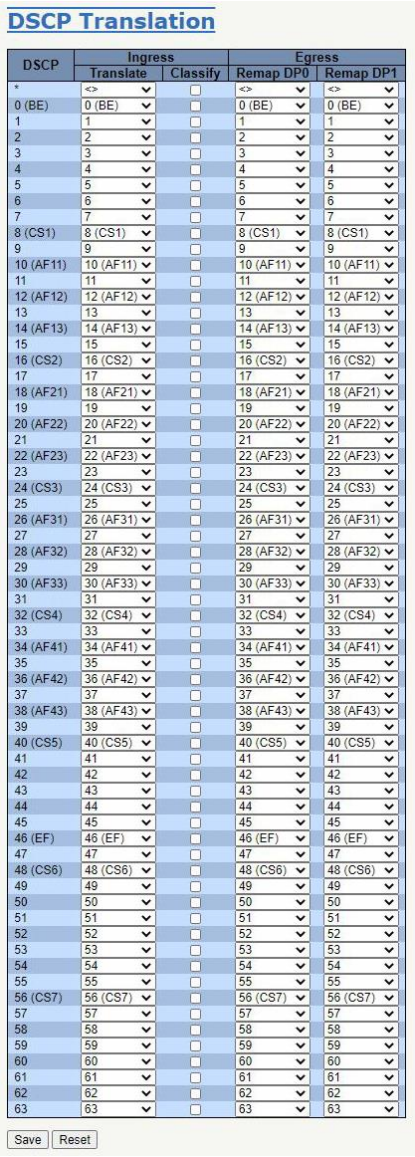
DPL: Drop Precedence Level (0-1)

Buttons

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

DSCP Translation

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



The displayed settings are:

DSCP: Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.

Ingress: Ingress side DSCP can be first translated to new DSCP before using the DSCP for CoS and DPL map.

Translate: DSCP at Ingress side can be translated to any of (0-63) DSCP values.
Classify: Click to enable Classification at Ingress side.

Egress: There are the following configurable parameters for Egress side –

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 from 0 to 63.
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 from 0 to 63.

Buttons

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

DSCP Classification

This page allows you to configure the mapping of CoS and DPL to DSCP value.

The displayed settings are:

CoS: Actual Class of Service.

DSCP DP0: Select the classified DSCP value (0-63) for Drop Precedence Level 0.

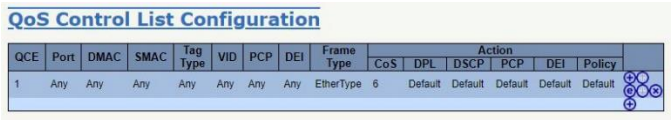
DSCP DP1: Select the classified DSCP value (0-63) for Drop Precedence Level 1.

Buttons

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

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 1024 on each switch.
Click on the lowest plus sign to add a new QCE to the list.



QCE: The QCE ID.

Port: The list of ports configured with the QCE or 'Any'.

DMAC: The destination MAC address. Possible values are:

Any: Match any DMAC.
Unicast: Match unicast DMAC.
Multicast: Match multicast DMAC.
Broadcast: Match broadcast DMAC.
<MAC>: Match specific DMAC.
The default value is 'Any'.

SMAC: Match specific source MAC address or 'Any'.

Tag Type: Tag type. Possible values are:

Any: Match tagged and untagged frames.
Untagged: Match untagged frames.
Tagged: Match tagged frames.
C-Tagged: Match C-tagged frames.
S-Tagged: Match S-tagged frames.
The default value is 'Any'.

VID: VLAN ID, either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'.

PCP: Priority Code Point: Valid values of PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.

DEI: Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.

Frame Type: The type of frame. Possible values are:

Any: Match any frame type.
Ethernet: Match EtherType frames.
LLC: Match (LLC) frames.
SNAP: Match (SNAP) frames.
IPv4: Match IPv4 frames.
IPv6: Match IPv6 frames.

Action: The classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are:

CoS: Classify Class of Service.
DPL: Classify Drop Precedence Level.
DSCP: Classify DSCP value.
PCP: Classify PCP value.
DEI: Classify DEI value.
Policy: Classify ACL Policy number.

Modification Buttons: You can modify each QCE (QoS Control Entry) in the table using the following buttons:

Inserts a new QCE before the current row.

Edits the QCE.

Moves the QCE up the list.

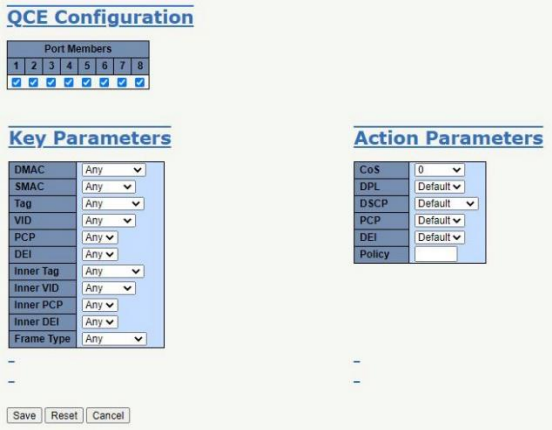
Moves the QCE down the list.

Deletes the QCE.

The lowest plus sign adds a new entry at the bottom of the QCE listings.

QoS Control List Configuration

This page allows edit/insert a single QoS Control Entry at a time. A QCE consists of several parameters. These parameters vary according to the frame type that you select.



Port Members: Check the checkbox to include the port in the QCL entry. By default, all ports are included.

Key Parameters: Key configuration is described below:

DMAC Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast', 'Specific' (xx-xx-xx-xx-xx-xx) or 'Any'.
SMAC Source MAC address: xx-xx-xx-xx-xx-xx or 'Any'.
Tag Value of Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'.
VID Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs.
PCP Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
DEI Valid value of DEI can be '0', '1' or 'Any'.
Inner Tag Value of Inner Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'. All inner tag parameters depend on the Key Type configuration in QoS Ingress Port Classification Help.
Inner VID Valid value of Inner VLAN ID can be any value in the range 1-4095 or 'Any'; the user can enter either a specific value or a range of VIDs.
Inner PCP Valid value of Inner PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.
Inner DEI Valid value of Inner DEI can be '0', '1' or 'Any'.
Frame Type Frame Type can have any of the following values:
Any: Allow all types of frames.
EtherType: Ether Type Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.
LLC: DSAP Address Valid DSAP(Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'.
SSAP Address Valid SSAP (Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'.
Control Valid Control field can vary from 0x00 to 0xFF or 'Any'.
SNAP: PID Valid PID (a.k.a Ether Type) can be 0x0000-0xFFFF or '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 x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero.

Destination IP Specific Destination IP address in value/mask format or 'Any'.
IP Fragment IPv4 frame fragmented option: 'Yes', 'No' or 'Any'.
DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'.
DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
Sport Source TCP/UDP port: (0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
Dport Destination TCP/UDP port: (0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

IPv6: Protocol IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'.
Source IP 32 LS bits of IPv6 source address in value/mask format or 'Any'.
Destination IP Specific Destination IP address in value/mask format or 'Any'.
DSCP Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.
Sport Source TCP/UDP port: (0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
Dport Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Action Parameters

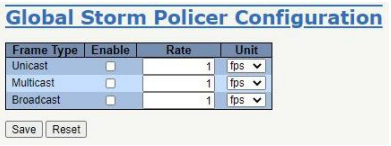
CoS Class of Service: (0-7) or 'Default'.
DP Drop Precedence Level: (0-1) or 'Default'.
DSCP DSCP: (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'.
PCP PCP: (0-7) or 'Default'. Note: PCP and DEI cannot be set individually.
DEI DEI: (0-1) or 'Default'.
Policy ACL Policy number: (0-63) or 'Default' (empty field).
'Default' means that the default classified value is not modified by this QCE.

Buttons

Save: Click to save the configuration and move to main QCL page.
Reset: Click to undo any changes made locally and revert to previously saved values.
Cancel: Return to the previous page without saving the configuration change.

Storm Policing

Global storm policers for the switch are configured on this page.
There is a unicast storm policer, multicast storm policer, and a broadcast storm policer. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.



The displayed settings are:

Frame Type: The frame type for which the configuration below applies.

Enable: Enable or disable the global storm policer for the given frame type.

Rate: Controls the rate for the global storm policer. This value is restricted to 1-1024000 when "Unit" is fps, and 1-1024 when "Unit" is kfps. The rate is internally rounded up to the nearest value

supported by the global storm policer. Supported rates are 1, 2, 4, 8, 16, 32, 64, 128, 256 and 512 fps for rates <= 512 fps and 1, 2, 4, 8, 16, 32, 64, 128, 256, 512 and 1024 kfps for rates > 512 fps.

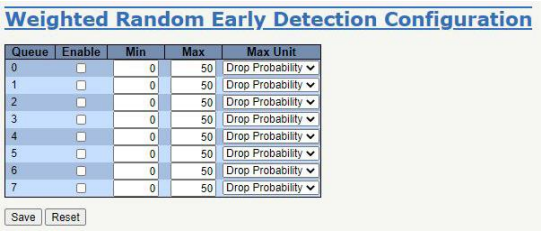
Unit: Controls the unit of measure for the global storm policer rate as fps or kfps.

Buttons

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

WRED

This page allows you to configure the Random Early Detection (RED) settings.
Through different RED configuration for the queues it is possible to obtain Weighted Random Early Detection (WRED) operation between queues.
The settings are global for all ports in the switch.



The displayed settings are:

Queue: The queue number (CoS) for which the configuration below applies.

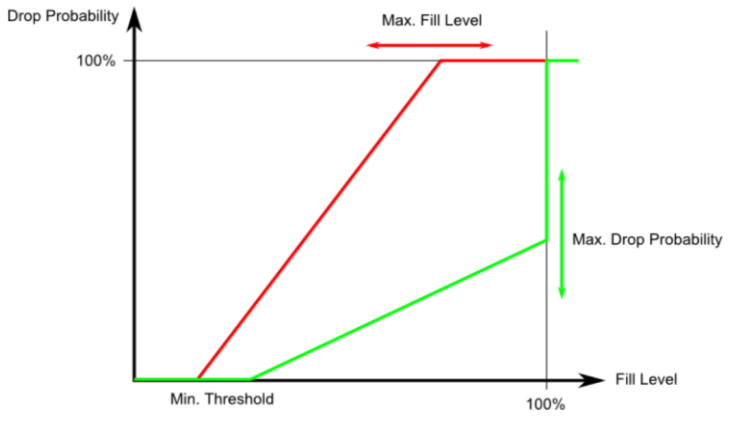
Enable: Controls whether RED is enabled for this entry.

Min: Controls the lower RED fill level threshold. If the queue filling level is below this threshold, the drop probability is zero. This value is restricted to 0-100%.

Max: Controls the upper RED drop probability or fill level threshold for frames marked with Drop Precedence Level > 0 (yellow frames). This value is restricted to 1-100%.

Max Unit: Selects the unit for Max. Possible values are:

Drop Probability: Max controls the drop probability just below 100% fill level.
Fill Level: Max controls the fill level where drop probability reaches 100%.
RED Drop Probability Function: The following illustration shows the drop probability versus fill level function with associated parameters.



Min is the fill level where the queue randomly start dropping frames marked with Drop Precedence Level > 0 (yellow frames).
If Max Unit is 'Drop Probability' (the green line), Max controls the drop probability when the fill level is just below 100%.
If Max Unit is 'Fill Level' (the red line), Max controls the fill level where drop probability reaches 100%. This configuration makes it possible to reserve a portion of the queue exclusively for frames marked with Drop Precedence Level 0 (green frames). The reserved portion is calculated as (100 - Max) %.
Frames marked with Drop Precedence Level 0 (green frames) are never dropped.
The drop probability for frames increases linearly from zero (at Min average queue filling level) to Max Drop Probability or Fill Level.

Buttons

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

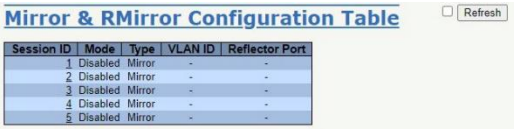
Mirroring

Mirroring is a feature that allows port analysis on the switch. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

Remote Mirroring is an extended function of Mirroring. It can mirror traffic to a destination port on another switch, allowing the remote analysis of network traffic.

If you want to get the tagged mirrored traffic, you have to set VLAN egress tagging as "Tag All" on the reflector port.

If you want to get untagged mirrored traffic, you have to set VLAN egress tagging as "Untag ALL" on the reflector port.



Session ID: Select session ID to configure.

Mode: To **Enabled/Disabled** the mirror or Remote Mirroring function.

Type: Select switch type.

Mirror: The switch is running on mirror mode. The source port(s) and destination port are located on this switch.
RMirror source: The switch is a source node for monitor flow. The source port(s), reflector port are located on this switch.
RMirror destination: The switch is an end node for monitor flow. The destination port(s) is located on this switch.

VLAN ID: The VLAN ID indicates where the monitored packets will copied. The default VLAN ID is 200.

Reflector Port: The reflector port redirects traffic to a Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until Remote Mirroring is disabled. In stacking mode, a user needs to select the switch ID in order to select the correct device. If you shut down a port, it

cannot be a reflector port. If you shut down a port that is a reflector port, the remote mirror function will not work.

Note: The reflector port needs to be selected only on a Source switch type. MAC Table learning and STP should be disabled on the reflector port. The reflector port must be a copper port.

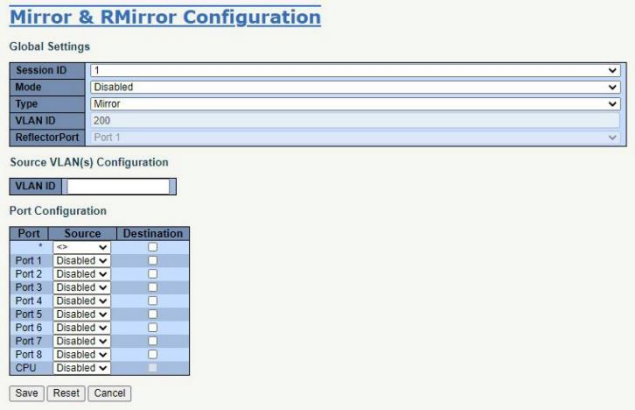
Mirror & RMirror Configuration

Mirroring is a feature that allows port analysis on the switch. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic.

Remote Mirroring is an extended function of Mirroring. It can mirror traffic to a destination port on another switch, allowing the remote analysis of network traffic.

If you want to get the tagged mirrored traffic, you have to set VLAN egress tagging as "Tag All" on the reflector port.

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



Session ID: Select session ID to configure.

Mode: To Enable/Disable mirroring or Remote Mirroring function.

Type: Select switch type.

Mirror: The switch is running on mirror mode. The source port(s) and destination port are located on this switch.

Source: The switch is a source node for monitor flow. The source port(s), reflector port are located on this switch.

RMirror destination: The switch is an end node for monitor flow. The destination port(s) is located on this switch.

VLAN ID: The VLAN ID indicates where the monitored packets will copied. The default VLAN ID is 200.

Reflector Port: The reflector port is a method to redirect the traffic to a Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until the Remote Mirroring is disabled. In the stacking mode, you need to select switch ID to select the correct device. If you shut down a port, it cannot be a reflector port. If you shut down a port that is a reflector port, the remote mirror function will not work.

Note: The reflector port needs to be selected only on a Source switch type. MAC Table learning and STP should be disabled on the reflector port. The reflector port must be a copper port.

Source VLAN(s) Configuration

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

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

Remote Mirroring Port Configuration

The following table is used for port role selecting.

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

Source: Select mirror mode.

Disabled Neither frames transmitted nor frames received are mirrored.
Both Frames received and frames transmitted are mirrored on the Destination port.
Rx only Frames received on this port are mirrored on the Destination port. Frames transmitted are not mirrored.
Tx only Frames transmitted on this port are mirrored on the Destination port. Frames received are not mirrored.

Destination: Select destination port. This checkbox is designed for mirror or Remote Mirroring. The **destination port** is a switched port that will receive a copy of the traffic from the source port.

Note: On mirror mode, the device only supports one destination port. The destination port needs to disable MAC Table learning.

Configuration Guidelines for All Features

When the switch is running on Remote Mirroring mode, the administrator also needs to check whether or not other features are enabled or disabled.

For example, the administrator is not disabled the MSTP on reflector port. All monitor traffic will be blocked on reflector port.

All recommended settings are described as follows.

	IMPACT	SOURCE PORT	REFLECTOR PORT	INTERMEDIATE PORT	DESTINATION PORT	REMOTE MIRRORING VLAN
arp_inspection	High		* disabled	* disabled		
acl	Critical		* disabled	* disabled	* disabled	
dhcp_relay	High		* disabled	* disabled		
dhcp_snooping	High		* disabled	* disabled		
ip_source_guard	Critical		* disabled	* disabled	*disabled	
ipmc/igmpsnp	Critical					un-conflict
ipmc/mldsnp	Critical					un-conflict
lacp	Low				o disabled	
lldp	Low				o disabled	
mac learning	Critical		* disabled	* disabled	* disabled	
mstp	Critical		* disabled		o disabled	
mvr	Critical					un-conflict
nas	Critical		* authorized	* authorized	* authorized	

	IMPACT	SOURCE PORT	REFLECTOR PORT	INTERMEDIATE PORT	DESTINATION PORT	REMOTE MIRRORING VLAN
psec	Critical		* disabled	* disabled	* disabled	
qos	Critical		* unlimited	* unlimited	* unlimited	
upnp	Low				o disabled	
mac-based vlan	Critical		*disabled	*disabled		
protocol-based vlan	Critical		*disabled	*disabled		
vlan_translation	Critical		*disabled	*disabled	* disabled	
voice_vlan	Critical		*disabled	*disabled		
mrp	Low				o disabled	
mvrp	Low				o disabled	

Note:
* -- must
o – optional
Impact: Critical/High/Low
Critical: 5 packets -> 0 packet
High: 5 packets -> 4 packets
Low: 5 packets -> 6 packets

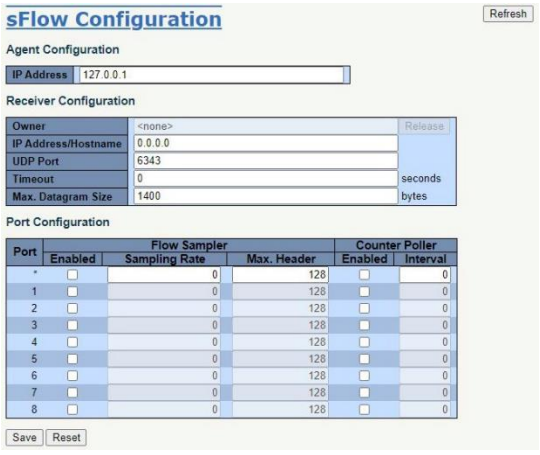
Buttons

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

sFlow

This page is for configuring sFlow. The configuration is divided into two parts: configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.

sFlow configuration is not persistent to non-volatile memory, which means that a reboot will disable sFlow sampling.



IP Address: The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time. Both IPv4 and IPv6 addresses are supported.

Owner: Basically, sFlow can be configured in two ways: through local management using the Web or CLI interface or through SNMP. This read-only field shows the owner of the current sFlow configuration and assumes values as follows:

If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.
If sFlow is configured through SNMP, all controls - except for the Release-button - are disabled to avoid unintended reconfiguration.

The Release button allows for releasing the current owner and disable sFlow sampling. The button is disabled if sFlow is currently unclaimed. If configured through SNMP, the release must be confirmed (a confirmation request will appear).

IP Address/Hostname: The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.

UDP Port: The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.

Timeout: The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated by clicking on the “Refresh” button. If locally managed, the timeout can be changed on the fly without affecting any other settings. Valid range is 0 to 2147483647 seconds.

Max. Datagram Size: The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.

Port: The port number for which the configuration below applies.

Flow Sampler Enabled: Enables/disables flow sampling on this port.

Flow Sampler Sampling Rate: The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field. Valid range is 1 to 4294967295.

Flow Sampler Max. Header: The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. To have room for any frame, the maximum datagram size should be roughly 100 bytes larger than the maximum header size. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.

Counter Poller Enabled: Enables/disables counter polling on this port.

Counter Poller Interval: With counter polling enabled, this specifies the interval - in seconds - between counter poller samples. Valid range is 1 to 3600 seconds.

Buttons

Release: See description under Owner.
Refresh: Click to refresh the page. Note that unsaved changes will be lost.
Save: Click to save changes. Note that sFlow configuration is not persisted to non-volatile memory.
Reset: Click to undo any changes made locally and revert to previously saved values.

RingV2

This page provides Ring related configuration.

Index: The group index. This parameter is used for easy identifying the ring when the user configures it.

Group 1 (Index 1): It supports configuration of ring.
Group 2 (Index 2): It supports configuration of chain and balancing-chain.

Mode: Enable Ring on the specific group.

When Group 1 is enabled, all configuration of Group 2 will be reset to default and all the configuration options for Group 2 will be locked.
To configure Group 2, both Group1 should be disabled first. When Group 2 is enabled, all configuration options for of Group1 will be reset to default and all the configuration options for Group 2 will be locked.

Role: Configure the Ring group on this switch as specific role.

Group 1: Support option of ring-master and ring-slave.
 # Ring: It could be master or slave.
Group 2: Support configuration of the chain and balancing-chain.
 # Chain: It could be head, tail or member.
 # Balancing Chain: It could be central-block, terminal-1/2 or member.
Note: Ring and Chain could be enabled either one, cannot be enabled both.

Ring Port(s): Selecting ring port(s). Each ring port must be unique, CANNOT be configured in different groups; 2 ring ports between ring/chain CANNOT be the same.

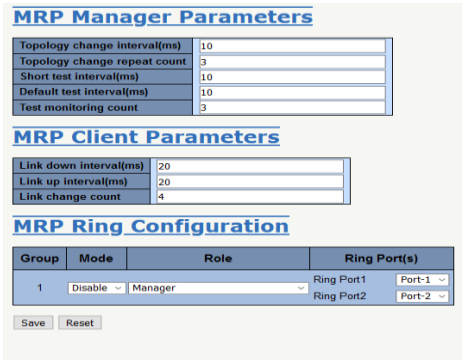
When role is ring/master, one ring port is forward port and another is block port. The block port is a redundant port; it is a blocking port in a normal state.
When role is ring/slave, both ring ports are forward ports.
When role is chain/head, one ring port is member port and another is head port. Both ring ports are forwarding ports in normal state.
When role is chain/tail, one ring port is member port and another is tail port. The tail port is a redundant port; it is a blocking port in a normal state.
When role is chain/member, both ring ports are member ports. Both ring ports are forwarding ports in normal state.
When role is balancing-chain/central-block, one ring port is member port and another is block port. The block port is a redundant port; it is a blocking port in a normal state.
When role is balancing-chain/terminal-1/2, one ring port is member port and another is terminal port. Both ring ports are forwarding ports in normal state.
When role is balancing-chain/member, both ring ports are member port. Both ring ports are forwarding port in normal state.

Buttons

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

MRP

This page provides MRP related configuration.



Topology Change Interval: Specifies the interval for sending MRP Topology Change frames.

Topology Change repeat Count: Specifies the interval count which controls repeated transmission of MRP Topology Change frames. The range is 0-1000(ms). Default is 10ms.

Short Test Interval: Specifies the short interval for sending MRP Test frames on ring ports after link changes occur in the ring. The range is 10-1000(ms). Default is 10ms.

Default Test Interval: Specifies the default interval for sending MRP Test frames on ring ports. The range is 10-1000(ms). Default is 10ms.

Test Monitoring Count: Specifies the interval count for monitoring the reception of MRP Test frames. The range is 2-10. Default is 3ms.

Link Down Interval: Specifies the interval for sending MRP Link Down frames on ring ports. The range is 10-1000(ms). Default is 20ms.

Link Up Interval: Specifies the interval for sending MRP Link Up frames on ring ports. The range is 10-1000(ms). Default is 20ms.

Link Change Count: Specifies the MRP Link Change frame count which controls the repeated transmission of MRP Link Change frames. The range is 2-10. Default is 4.

Group: Group index. Used to identify the MRP group being configured.

Mode: Enable/Disable MRP on the specific group.

Role: Configure MRP group role as Manager or Client.

Ring Port(s): Selecting ring port(s). Each ring port must be unique, CANNOT be configured in different groups; 2 ring ports CANNOT be the same.

Buttons

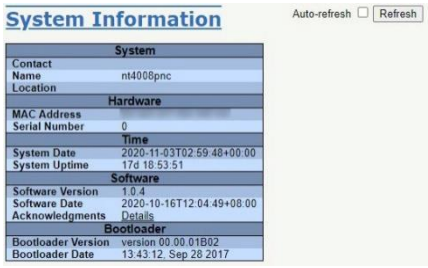
Save: Click to save changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

Chapter 6 Monitor

System

Information

The switch system information is provided here.



Contact: The system contact configured in Configuration | System | Information | System Contact.

Name: The system name configured in Configuration | System | Information | System Name.

Location: The system location configured in Configuration | System | Information | System Location.

MAC Address: The MAC Address of this switch.

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

System Uptime: The period of time the device has been operational.

Software Version: The software version of this switch.

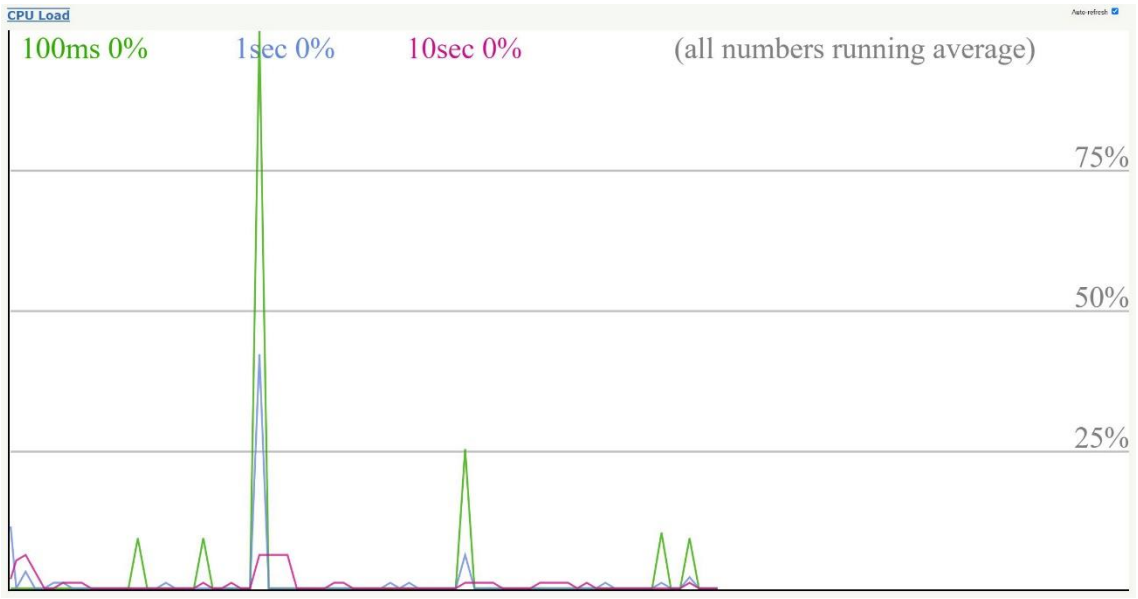
Software Date: The date when the switch software was produced.

Buttons

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

CPU Load

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

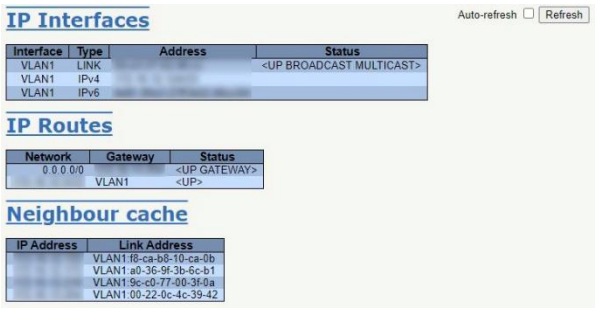


Buttons

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

IP Status

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IPv6 routes and the neighbour cache (ARP cache) status.



Interface: The name of the interface.

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

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

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

Network: The destination IPv6 network or host address of this route.

Gateway: The gateway address of this route.

Status: The status flags of the route.

IP Address: The IP address of the entry.

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

Buttons

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

Log

The switch system log information is provided here.

Each page shows up to 999 table entries, selected through the "entries per page" input field. By default each page displays 20 entries.

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

The "Clear Level" input field is used to specify which system log entries will be cleared.

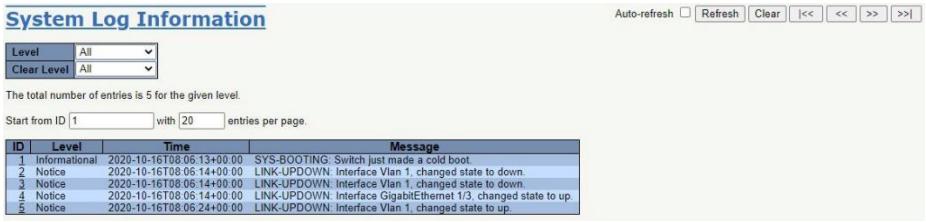
To clear specific system log entries, select the clear level first then click the “Clear” button.

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

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

The “>>” 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.



ID: The identification of the system log entry.

Level: The level of the system log entry.

All: Show all error log messages.
Informational: Show informational log messages only.
Notice: Show notice log messages only.
Warning: Show warning log messages only.
Error: Show error log messages only.

Time: The time when the system log entry occurred.

Message: The detail message of the system log entry.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Updates the table entries, starting from the current entry.
Clear: Flushes the selected entries.
|<<: Updates the table entries, starting from the first available entry.
<<: Updates the table entries, ending at the last entry currently displayed.
>>: Updates the table entries, starting from the last entry currently displayed.
>>|: Updates the table entries, ending at the last available entry.

Detailed Log

The switch system detailed log information is provided here.

Level: The severity level of the system log entry.

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

Message: The detailed message of the system log entry.

Buttons

Refresh: Updates the system log entry to the current entry ID.
|<<: Updates the system log entry to the first available entry ID.
<<: Updates the system log entry to the previous available entry ID.
>>: Updates the system log entry to the next available entry ID.
>>|: Updates the system log entry to the last available entry ID.

Alarm

Alarm Current

Current Alarms are shown on this page.

SeqNo: Alarm Sequence Number.

Description: Alarm Type Description.

Time: Alarm occurrence date time.

Buttons

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

Alarm History

Alarm history is provided on this page.

SeqNo: Alarm Sequence Number.

Description: Alarm Type Description.

State: Alarm State. Set stands for alarm occurs; Cleared stands for alarm disappear.

Time: Alarm occurrence/cleared date time.

Buttons

Auto-refresh: Click this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh data.
Clear: Click to Clear data.

Ports

State

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

RJ45 ports			
SFP ports			
State	Disabled	Down	Link

RR: RR light on when Role of Ring is configured as Ring-Master and Ring is enabled. With the following roles, RR would also light on:

Chain(Tail)
Balancing Chain(Central Block)

RS: Light on when Ring(or Chain) Signal Failure is detected.

P1: Light on when Power 1 gets power feed.

P2: Light on when Power 2 gets power feed.

ALM: Light on with Red when system has alarm happened.

PoE LED: PoE status indicator (Supported depends on HW):

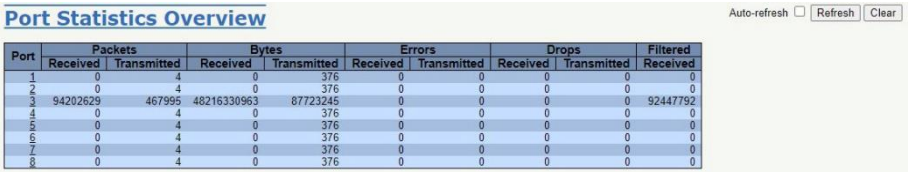
off (dark green): no power output.
Green: PoE port is connected to PoE device, using the 802.3at standard.
Amber: PoE port is connected to PoE device, using the 802.3af standard.
Red ON: PoE port is used, but no power output. (PoE detection failure, such as only Ethernet link up or short-circuit, overloading, over temperature).
Red Flash (optional): power request exceeds power budget, supported depends on HW.

Buttons

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

Traffic Overview

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



Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	4	0	376	0	0	0	0	0
2	0	4	0	376	0	0	0	0	0
3	94202629	467995	48216330963	87723245	0	0	0	0	92447792
4	0	4	0	376	0	0	0	0	0
5	0	4	0	376	0	0	0	0	0
6	0	4	0	376	0	0	0	0	0
7	0	4	0	376	0	0	0	0	0
8	0	4	0	376	0	0	0	0	0

The displayed counters are:

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

Packets: The number of received and transmitted packets per port.

Bytes: The number of received and transmitted bytes per port.

Errors: The number of frames received in error and the number of incomplete transmissions per port.

Drops: The number of frames discarded due to ingress or egress congestion.

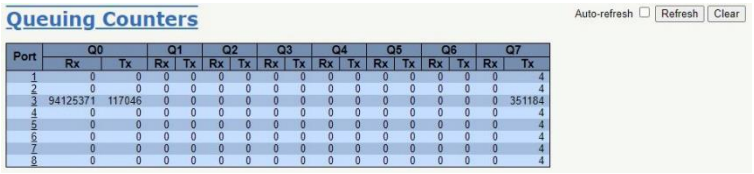
Filtered: The number of received frames filtered by the forwarding process.

Buttons

Refresh: Click to refresh the page immediately.
Clear: Clears the counters for all ports.
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 sec.

QoS Statistics

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



The displayed counters are:

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

Qn: There are 8 QoS queues per port. Q0 is the lowest priority queue.

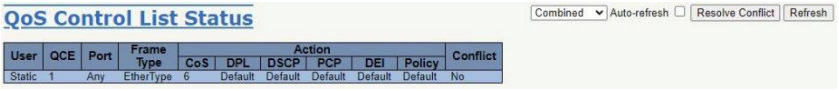
Rx/Tx: The number of received and transmitted packets per queue.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
Clear: Clears the counters for all ports.

QCL Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 1024 on each switch.



User: The QCL user.

QCE: The QCE ID.

Port: The list of ports configured with the QCE.

Frame Type: The type of frame. Possible values are:

Any: Match any frame type.
Ethernet: Match EtherType frames.
LLC: Match (LLC) frames.
SNAP: Match (SNAP) frames.
IPv4: Match IPv4 frames.
IPv6: Match IPv6 frames.

Action: The classification action taken on ingress frame if the configured parameters match the frame's contents. Possible actions are:

CoS: Classify Class of Service.
DPL: Classify Drop Precedence Level.
DSCP: Classify DSCP value.
PCP: Classify PCP value.
DEI: Classify DEI value.
Policy: Classify ACL Policy number.

Conflict: Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

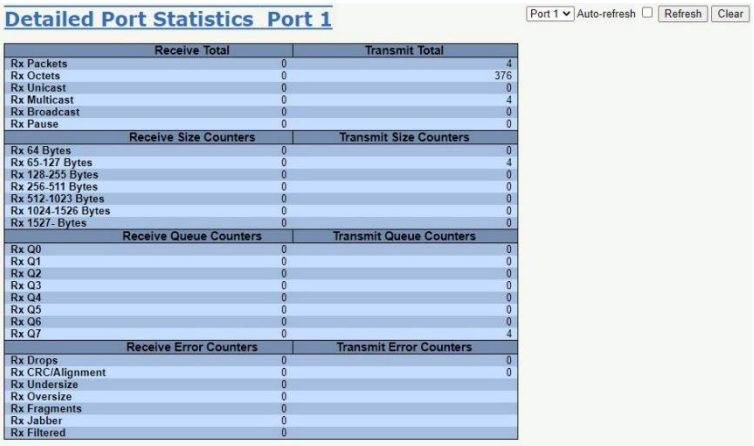
Buttons

Combined: Select the QCL status from this drop down list.
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Resolve Conflict: Click to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'.
Refresh: Click to refresh the page.

Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display.

The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit.



Rx anTx Packets: The number of received and transmitted (good and bad) packets.

Rx and Tx Octets: The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.

Rx and Tx Unicast: The number of received and transmitted (good and bad) unicast packets.

Rx and Tx Multicast: The number of received and transmitted (good and bad) multicast packets.

Rx and Tx Broadcast: The number of received and transmitted (good and bad) broadcast packets.

Rx and Tx Pause: A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.

Receive and Transmit Size Counters: The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and Transmit Queue Counters: The number of received and transmitted packets per input and output queue.

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

Rx CRC/Alignment: The number of frames received with CRC or alignment errors.

Rx Undersize: The number of short[1] frames received with valid CRC.

Rx Oversize: The number of long[2] frames received with valid CRC.

Rx Fragments: The number of short[1]frames received with invalid CRC.

Rx Jabber: The number of long[2] frames received with invalid CRC.

Rx Filtered: The number of received frames filtered by the forwarding process.

Tx Drops: The number of frames dropped due to output buffer congestion.

Tx Late/Exc. Coll.: The number of frames dropped due to excessive or late collisions.

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

Refresh: Click to refresh the page immediately.
Clear: Clears the counters for the selected port.
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

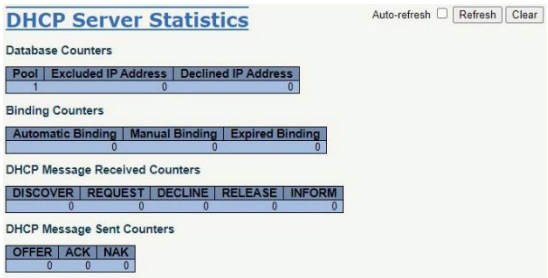
DHCP

Server

Statistics

This page displays the database counters and the number of DHCP messages sent and received by the DHCP server.

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



Pool: Number of pools.

Excluded IP Address: Number of excluded IP address ranges.

Declined IP Address: Number of declined IP addresses.

Automatic Binding: Number of bindings with network-type pools.

Manual Binding: Number of bindings that administrator assigns an IP address to a client. That is, the pool is of host type.

Expired Binding: Number of bindings that their lease time expired or they are cleared from Automatic/Manual type bindings.

DISCOVER: Number of DHCP DISCOVER messages received.

REQUEST: Number of DHCP REQUEST messages received.

DECLINE: Number of DHCP DECLINE messages received.

RELEASE: Number of DHCP RELEASE messages received.

INFORM: Number of DHCP INFORM messages received.

OFFER: Number of DHCP OFFER messages sent.

ACK: Number of DHCP ACK messages sent.

NAK: Number of DHCP NAK messages sent.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
Clear: Click to Clears DHCP Message Received Counters and DHCP Message Sent Counters.

Binding

This page displays bindings generated for DHCP clients.

IP: IP address allocated to a DHCP client.

Type: Type of binding. Possible types are Automatic, Manual, Expired.

State: State of binding. Possible states are Committed, Allocated, Expired.

Pool Name: The pool that generates the binding.

Server ID: Server IP address to service the binding.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
Clear Selected: Click to clear selected bindings. If the selected binding is Automatic or Manual, then it is changed to be Expired. If the selected binding is Expired, then it is freed.
Clear Automatic: Click to clear all Automatic bindings and Change them to Expired bindings.
Clear Manual: Click to clear all Manual bindings and Change them to Expired bindings.
Clear Expired: Click to clear all Expired bindings and free them.

Declined IP

This page displays declined IP addresses.

Declined IP: List of IP addresses declined.

Buttons

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

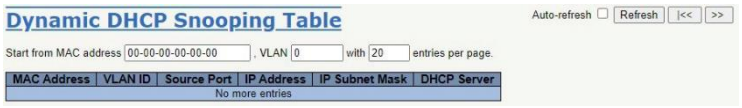
Snooping Table

This page displays the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients that obtained a dynamic IP address from the DHCP server will be listed in this table, except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

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

The "MAC address" and "VLAN" input fields allows the user to select the starting point in the Dynamic DHCP snooping Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next Dynamic DHCP snooping Table match. In addition, the two input fields will assume - upon a “Refresh” button click - 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.



MAC Address: User MAC address of the entry.

VLAN ID: VLAN-ID in which the DHCP traffic is permitted.

Source Port: Switch Port Number for which the entries are displayed.

IP Address: User IP address of the entry.

IP Subnet Mask: User IP subnet mask of the entry.

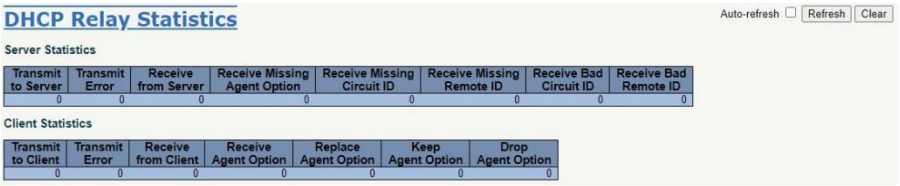
DHCP Server Address: DHCP Server address of the entry.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Refreshes the displayed table starting from the input fields.
Clear: Flushes all dynamic entries.
|<<: Updates the table starting from the first entry in the Dynamic DHCP snooping Table.
>>: Updates the table, starting with the entry after the last entry currently displayed.

Relay Statistics

This page provides statistics for DHCP relay.



Transmit to Server: The number of packets that are relayed from client to server.

Transmit to Error: The number of packets that resulted in errors while being sent to clients.

Receive from Server: The number of packets received from server.

Receive Missing Agent Option: The number of packets received without agent information options.

Receive Missing Circuit ID: The number of packets received with the Circuit ID option missing.

Receive Missing Remote ID: The number of packets received with the Remote ID option missing.

Receive Bad Circuit ID: The number of packets whose Circuit ID option did not match known circuit ID.

Receive Bad Remote ID: The number of packets whose Remote ID option did not match known Remote ID.

Transmit to Client: The number of relayed packets from server to client.

Transmit Error: The number of packets that resulted in error while being sent to servers.

Receive from Client: The number of received packets from server.

Receive Agent Option: The number of received packets with relay agent information option.

Replace Agent Option: The number of packets that were replaced with relay agent information option.

Keep Agent Option: The number of packets whose relay agent information was retained.

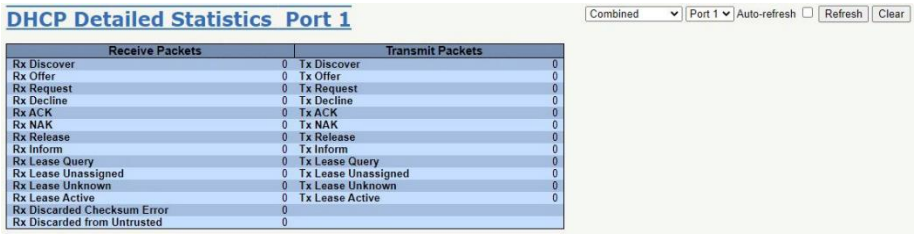
Drop Agent Option: The number of packets that were dropped and were received with relay agent information.

Buttons

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

Refresh: Click to refresh the page immediately.
Clear: Clear all statistics.

Detailed Statistics



This page provides statistics for DHCP snooping. Notice that the normal forward per-port TX statistics isn't increased if the incoming DHCP packet is done by L3 forwarding mechanism. Also clearing the statistics on a specific port may not affect global statistics since it gathers a different layer overview.

Rx and Tx Discover: The number of discover (option 53 with value 1) packets received and transmitted.

Rx and Tx Offer: The number of offer (option 53 with value 2) packets received and transmitted.

Rx and Tx Request: The number of request (option 53 with value 3) packets received and transmitted.

Rx and Tx Decline: The number of decline (option 53 with value 4) packets received and transmitted.

Rx and Tx ACK: The number of ACK (option 53 with value 5) packets received and transmitted.

Rx and Tx NAK: The number of NAK (option 53 with value 6) packets received and transmitted.

Rx and Tx Release: The number of release (option 53 with value 7) packets received and transmitted.

Rx and Tx Inform: The number of inform (option 53 with value 8) packets received and transmitted.

Rx and Tx Lease Query: The number of lease query (option 53 with value 10) packets received and transmitted.

Rx and Tx Lease Unassigned: The number of lease unassigned (option 53 with value 11) packets received and transmitted.

Rx and Tx Lease Unknown: The number of lease unknown (option 53 with value 12) packets received and transmitted.

Rx and Tx Lease Active: The number of lease active (option 53 with value 13) packets received and transmitted.

Rx Discarded checksum error: The number of discard packet that IP/UDP checksum is error.

Rx Discarded from Untrusted: The number of discarded packet that are coming from untrusted port.

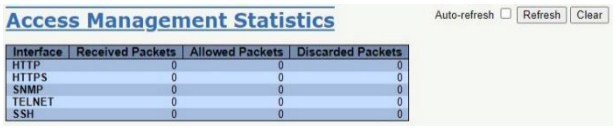
Buttons

The DHCP user select box determines which user is affected by clicking the buttons.
The port select box determines which port is affected by clicking the buttons.
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
Clear: Clears the counters for the selected port.

Security

Access Management Statistics

This page provides statistics for access management.



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

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

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

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

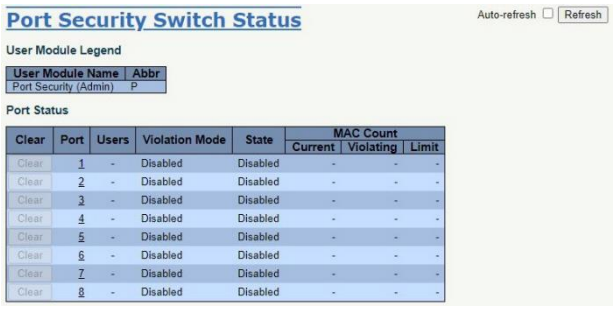
Buttons

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

Network

Port Security

Overview



This page shows the Port Security status. Port Security may be configured both administratively and indirectly through other software modules, i.e. user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to be forwarded or blocked. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree to allow the MAC address to be forwarded. If a single user module chooses to block it, it will be blocked until that user module decides otherwise.

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

User Module Legend: The legend shows all user modules that may request Port Security services.

User Module Name: The full name of a module that may request Port Security services.
Abbr: A one-letter abbreviation of the user module. This is used in the Users column in the port status table.

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

Clear: Click to remove all MAC addresses on all VLANs on this port. The button is only clickable if number of secured MAC addresses is non-zero.

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

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

Violation Mode: Shows the configured Violation Mode of the port. It can take one of four values:

Disabled: Port Security is not administratively enabled on this port.

Protect: Port Security is administratively enabled in Protect mode.

Restrict: Port Security is administratively enabled in Restrict mode.

Shutdown: Port Security is administratively enabled in Shutdown mode.

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

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

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

Limit Reached: The Port Security service is administratively enabled and the limit is reached.

Shut down: The Port Security service is administratively enabled and the port is shut down. No MAC addresses can be learned on the port until it is administratively re-opened by taking the port down and then back up on the "Configuration → Ports" page. Alternatively, the switch can be booted or the port security can be reconfigured.

MAC Count (Current, Violating, Limit): The three columns indicate the number of currently learned MAC addresses (forwarding as well as blocked), the number of violating MAC addresses (only counting in Restrict mode) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If Port Security is not administratively enabled on the port, the Violating and Limit columns will show a dash (-).

Buttons

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

Refresh: Click to refresh the page immediately.

Details

This page shows the MAC addresses secured by the Port Security module. Port Security may be configured both administratively and indirectly through other software modules, i.e. user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the Port Security module, which in turn asks all user modules whether to allow this new MAC address to be forwarded or blocked. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If single user module chooses to block it, it will be blocked until the configuration of that user module is changed.

Clear: Click to remove this particular MAC addresses from MAC table.

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

State: Indicates whether the corresponding MAC address is violating (administrative user has configured the interface in "Restrict" mode and the MAC address is blocked), blocked, or forwarding.

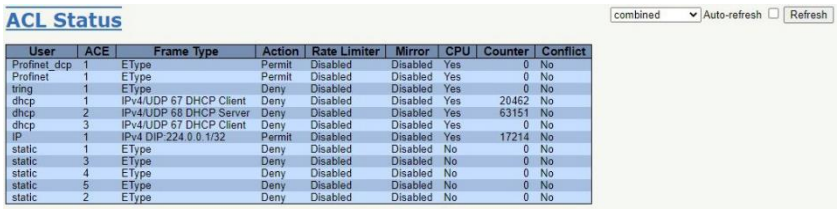
Age/Hold: If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward and aging is enabled, the Port Security module will periodically check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

Buttons

Use the port select box to select the port to show.
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.

ACL Status

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 128 on each switch.



User: The ACL user.

ACE: The ACE ID on local switch.

Frame Type: The frame type of the ACE. Possible values are:

Any: The ACE will match any frame type.
EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames.
ARP: The ACE will match ARP/RARP frames.
IPv4: The ACE will match all IPv4 frames.
IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol.
IPv4/UDP: The ACE will match IPv4 frames with UDP protocol.
IPv4/TCP: The ACE will match IPv4 frames with TCP protocol.
IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP.
IPv6: The ACE will match all IPv6 standard frames.

Action: The forwarding action of the ACE.

Permit: Frames matching the ACE may be forwarded and learned.
Deny: Frames matching the ACE are dropped.
Filter: Frames matching the ACE are filtered.

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

CPU: Forward packet that matched the specific ACE to CPU.

Counter: The number of times that the ACE was hit by a frame.

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

Buttons

The select box determines which ACL user is affected by clicking the buttons.
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page.

ARP Inspection

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learned by DHCP Snooping.

Dynamic ARP Inspection Table: Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learned by DHCP Snooping.

Navigating the ARP Inspection Table: Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table. The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will assume - upon a “Refresh” button click - 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.

Port: Switch port number for which the entries are displayed.

VLAN ID: VLAN ID in which the ARP traffic is permitted.

MAC Address: User MAC address of the entry.

IP Address: User IP address of the entry.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Refreshes the displayed table starting from the input fields.
Clear: Flushes all dynamic entries.
|<<: Updates the table starting from the first entry in the Dynamic ARP Inspection Table.
>>: Updates the table, starting with the entry after the last entry currently displayed.

IP Source Guard

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

Navigating the IP Source Guard Table: Each page shows up to 99 entries from the Dynamic IP Source Guard table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic IP Source Guard Table. The "Start from port address", "VLAN" and "IP address" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking the “Refresh” button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In addition, the two input fields will assume - upon a “Refresh” button click - 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.

Port: Switch port number for which the entries are displayed.

VLAN ID: VLAN ID in which the IP traffic is permitted.

IP Address: User IP address of the entry.

MAC Address: Source MAC address.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Refreshes the displayed table starting from the input fields.
Clear: Flushes all dynamic entries.
|<<: Updates the table starting from the first entry in the Dynamic IP Source Guard Table.
>>: Updates the table, starting with the entry after the last entry currently displayed.

Switch

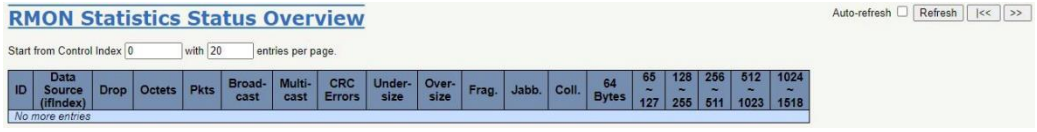
RMON

Statistics

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

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

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



The displayed counters are:

ID: The index of Statistics entry.

Data Source (ifIndex): The port ID to be monitored.

Drop: The total number of packets dropped by the probe due to lack of resources.

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

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

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

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

CRC Errors: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

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

Oversize: The total number of packets received that were longer than Max. Frame Size.

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

Jabb.: The number of frames in which size is larger than Max. Frame Size and with invalid CRC.

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

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

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

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

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

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

1024-1518: The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length.

Buttons

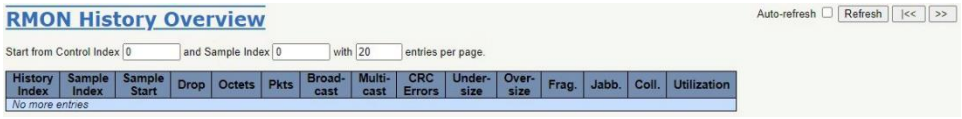
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
|<<: Updates the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID.
>>: Updates the table, starting with the entry after the last entry currently displayed.

History

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table.

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

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



The displayed fields are:

History Index: The index of History control entry.

Sample Index: The index of the data entry associated with the control entry.

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

Drop: The total number of packets dropped by the probe due to lack of resources.

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

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

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

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

CRCErrors: The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

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

Oversize: The total number of packets received that were longer than Max. Frame Size.

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

Jabb.: The number of frames in which size is larger than Max. Frame Size and with invalid CRC.

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

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

Buttons

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

Refresh: Click to refresh the page immediately.
|<<: Updates the table starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index.
>>: Updates the table, starting with the entry after the last entry currently displayed.

Alarm

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

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

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

The displayed fields are:

ID: The index of Alarm control entry.

Interval: The interval in seconds for sampling and comparing the rising and falling threshold.

Variable: The particular variable to be sampled.

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

Value: The value of the statistic during the last sampling period.

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

Rising Threshold: Rising threshold value.

Rising Index: Rising event index.

Falling Threshold: Falling threshold value.

Falling Index: Falling event index.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
|<<: Updates the table starting from the first entry in the Alarm Table, i.e. the entry with the lowest ID.
>>: Updates the table, starting with the entry after the last entry currently displayed.

Event

This page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table, default being 20, selected through the "entries per page" input field. When first visited,

the web page will show the first 20 entries from the beginning of the Event table. The first displayed will be the one with the lowest Event Index and Log Index found in the Event table.

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

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

The displayed fields are:

Event Index: The index of the event entry.

Log Index: The index of the log entry.

LogTime: Event log time.

LogDescription: The Event description.

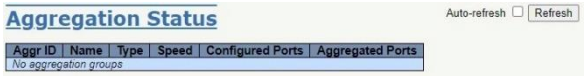
Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
|<<: Updates the table starting from the first entry in the Event Table, i.e. the entry with the lowest Event Index and Log Index.
>>: Updates the table, starting with the entry after the last entry currently displayed.

Aggregation

Status

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



Aggr ID: The Aggregation ID associated with this aggregation instance.

Name: Name of the Aggregation group ID.

Type: Type of the Aggregation group (Static or LACP).

Speed: Speed of the Aggregation group.

Configured ports: Configured member ports of the Aggregation group.

Aggregated ports: Aggregated member ports of the Aggregation group.

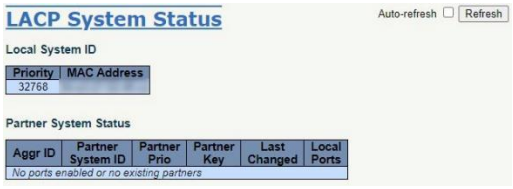
Buttons

Refresh: Click to refresh the page immediately.
Auto-refresh: Automatic refresh occurs every 3 seconds.

LACP

System Status

This page provides a status overview for the system-level LACP information.



Local System ID: This table displays both the local system priority and the local system MAC address that forms the local LACP System ID.

Partner System Status: This table display the partner system information for each LACP aggregation group.

Aggr ID: The Aggregation ID associated with this aggregation instance.
Partner System ID: The system ID (MAC address) of the aggregation partner.
Partner Prio: The priority that the partner has assigned to this aggregation ID.
Partner Key: The Key that the partner has assigned to this aggregation ID.
Last Changed: The time since this aggregation changed.
Local Ports: Shows which ports are a part of this aggregation for this switch.

Buttons

Refresh: Click to refresh the page immediately.
Auto-refresh: Automatic refresh occurs every 3 seconds.

Internal Status

This page provides a status overview for the LACP internal (i.e. local system) status for all ports.
Only ports that are part of an LACP group are shown.
For details on the shown parameters, please refer to IEEE 801.AX-2014.

Port: The switch port number.

State: The current port state:

Down: The port is not active.
Active: The port is in active state.
Standby: The port is in standby state.

Key: The key assigned to this port. Only ports with the same key can aggregate together.

Priority: The priority assigned to this aggregation group.

Activity: The LACP mode of the group (Active or Passive).

Timeout: The timeout mode configured for the port (Fast or Slow).

Aggregation: Show whether the system considers this link to be a potential candidate for aggregation.

Synchronization: Show whether the system considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.

Collecting: Shows if collection of incoming frames on this link is enabled.

Distributing: Shows if distribution of outgoing frames on this link is enabled.

Defaulted: Shows if the Actor's Receive machine is using Defaulted operational Partner information.

Expired: Shows if that the Actor's Receive machine is in the EXPIRED state.

Buttons

Refresh: Click to refresh the page immediately.
Auto-refresh: Automatic refresh occurs every 3 seconds.

Neighbor Status

This page provides a status overview for the LACP neighbor status for all ports.
Only ports that are part of an LACP group are shown.
For details on the shown parameters, please refer to IEEE 801.AX-2014.

Port: The switch port number.

State: The current port state:

Down: The port is not active.
Active: The port is in active state.
Standby: The port is in standby state.

Aggr ID: The aggregation group ID to which the port is assigned.

Partner Key: The key assigned to this port by the partner.

Partner Port: The partner port number associated with this link.

Partner Port Priority: The priority assigned to this partner port.

Activity: The LACP mode of the group (Active or Passive).

Timeout: The timeout mode configured for the partner port (Fast or Slow).

Aggregation: Shows whether the partner considers this link to be a potential candidate for aggregation.

Synchronization: Show whether the partner considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.

Collecting: Shows if collection of incoming frames on this link is enabled.

Distributing: Shows if distribution of outgoing frames on this link is enabled.

Defaulted: Shows if the partners Receive machine is using Defaulted operational Partner information.

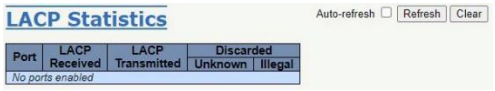
Expired: Shows if that the partners Receive machine is in the EXPIRED state.

Buttons

Refresh: Click to refresh the page immediately.
Auto-refresh: Automatic refresh occurs every 3 seconds.

Port Statistics

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



Port: The switch port number.

LACP Received: Shows how many LACP frames have been received at each port.

LACP Transmitted: Shows how many LACP frames have been sent from each port.

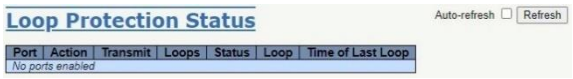
Discarded: Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
Clear: Clears the counters for all ports.

Loop Protection

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



Loop protection port status is:

Port: The switch port number of the logical port.

Action: The currently configured port action.

Transmit: The currently configured port transmit mode.

Loops: The number of loops detected on this port.

Status: The current loop protection status of the port.

Loop: Whether a loop is currently detected on the port.

Time of Last Loop: The time of the last loop event detected.

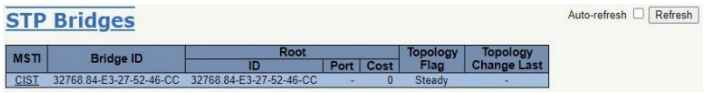
Buttons

Refresh: Click to refresh the page immediately.
Auto-refresh: Check this box to enable an automatic refresh of the page at regular intervals.

Spanning Tree

Bridge Status

This page provides a status overview of all STP bridge instances.



The displayed table contains a row for each STP bridge instance, where the column displays the following information:

MSTI: The Bridge Instance. This is also a link to the STP Detailed Bridge Status.

Bridge ID: The Bridge ID of this Bridge instance.

Root ID: The Bridge ID of the currently elected root bridge.

Root Port: The switch port currently assigned the root port role.

Root Cost: Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.

Topology Flag: The current state of the Topology Change Flag of this Bridge instance.

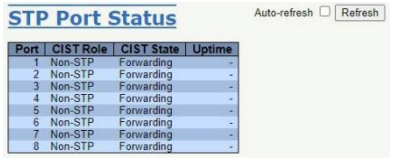
Topology Change Last: The time since last Topology Change occurred.

Buttons

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

Port Status

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



STP port status is:

Port: The switch port number of the logical STP port.

CIST Role: The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort, BackupPort, RootPort, DesignatedPort, Disabled.

CIST State: The current STP port state of the CIST port. The port state can be one of the following values: Discarding, Learning, Forwarding.

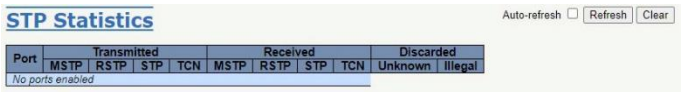
Uptime: The time since the bridge port was last initialized.

Buttons

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

Port Statistics

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



The STP port statistics counters are:

Port: The switch port number of the logical STP port.

MSTP: The number of MSTP BPDUs received/transmitted on the port.

RSTP: The number of RSTP BPDUs received/transmitted on the port.

STP: The number of legacy STP Configuration BPDUs received/transmitted on the port.

TCN: The number of (legacy) Topology Change Notification BPDUs 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 BPDUs received (and discarded) on the port.

Buttons

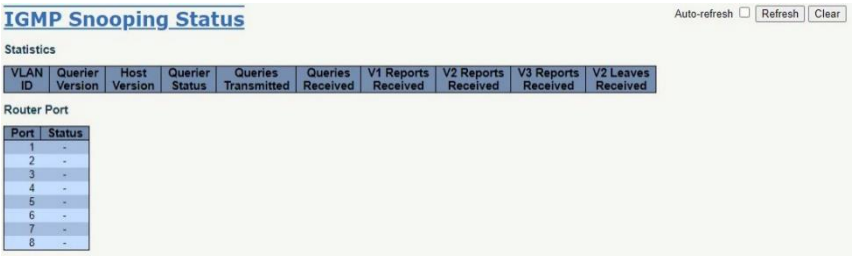
Refresh: Click to refresh the page immediately.
Clear: Click to reset the counters.
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

IPMC

IGMP Snooping

Status

This page provides IGMP Snooping status.



VLAN ID: The VLAN ID of the entry.

Querier Version: Working Querier Version currently.

Host Version: Working Host Version currently.

Querier Status: Shows if the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted: The number of Transmitted Queries.

Queries Received: The number of Received Queries.

V1 Reports Received: The number of Received V1 Reports.

V2 Reports Received: The number of Received V2 Reports.

V3 Reports Received: The number of Received V3 Reports.

V2 Leaves Received: The number of Received V2 Leaves.

Router Port: Displays the ports that act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.

Port: Switch port number.

Status: Indicate whether specific port is a router port or not.

Buttons

Auto-refresh: Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
Clear: Clears all Statistics counters.

Groups 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.

Navigating the IGMP Group Table: Each page shows up to 99 entries from the IGMP Group table, the 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 address" input fields allow the user to select the starting point in the IGMP Group Table. Clicking the “Refresh” button will update the displayed table starting from the input values or the next closest IGMP Group Table match. In addition, the two input fields will - upon a “Refresh” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The “>>” will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “|<<” button to start over.

VLAN ID: VLAN ID of the group.

Groups: Group address of the group displayed.

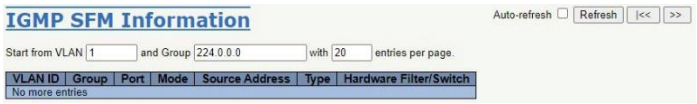
Port Members: Ports under this group.

Buttons

Auto-refresh: Check this box to refresh the page automatically. 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 displayed.

IPv4 SFM Information

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses that belong to the same group are treated as a single entry.



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

The "Start from VLAN", and "Group" input fields allow the user to select the starting point in the IGMP SFM Information Table. Clicking the “Refresh” button will update the displayed table starting from the input values or the next closest IGMP SFM Information Table match. In addition, the two input fields will - upon a “Refresh” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

VLAN ID: VLAN ID of the group.

Group: Group address of the group displayed.

Port: Switch port number.

Mode: Indicates the filtering mode maintained per VLAN ID/port number/Group Address basis. It can be either Include or Exclude.

Source Address: IP Address of the source. Currently, the maximum number of IPv4 source addresses for filtering (per group) is 8. When there are no source filtering addresses, the text "None" is shown in the Source Address field.

Type: Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch: Indicates whether the data plane destined for the specific group address from the source IPv4 address could be handled by chip or not.

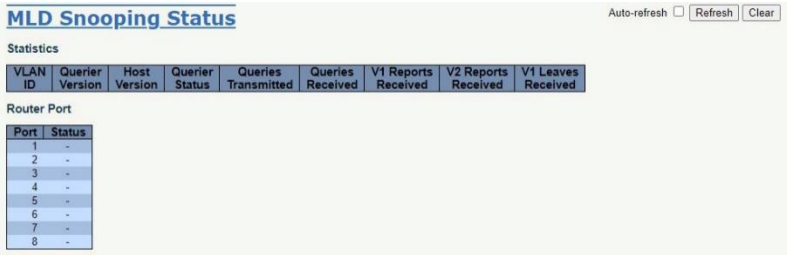
Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Refreshes the displayed table starting from the input fields.
|<<: Updates the table starting from the first entry in the IGMP SFM Information Table.
>>: Updates the table, starting with the entry after the last entry currently displayed.

MLD Snooping

Status

This page displays MLD Snooping status.



VLAN ID: The VLAN ID of the entry.

Querier Version: Working Querier Version currently.

Host Version: Working Host Version currently.

Querier Status: Shows the Querier status as "ACTIVE", "IDLE", or “DISABLE”. "DISABLE" denotes the specific interface is administratively disabled.

Queries Transmitted: The number of Transmitted Queries.

Queries Received: The number of Received Queries.

V1 Reports Received: The number of Received V1 Reports.

V2 Reports Received: The number of Received V2 Reports.

V1 Leaves Received: The number of Received V1 Leaves.

Router Port: Displays which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.

Port: Switch port number.

Status: Indicate whether specific port is a router port or not.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.
Clear: Clears all Statistics counters.

Groups Information

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

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

The "Start from VLAN", and "group address" input fields allow the user to select the starting point in the MLD Group Table. Clicking the “Refresh” button will update the displayed table starting from the input values or the next closest MLD Group Table match. In addition, the two input fields will - upon a

“Refresh” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

VLAN ID: VLAN ID of the group.

Groups: Group address of the group displayed.

Port Members: Ports under this group.

Buttons

Auto-refresh: Check this box to refresh the page automatically. 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 MLD Group Table.
>>: Updates the table, starting with the entry after the last entry currently displayed.

IPv6 SFM Information

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by port. Different source addresses that belong to the same group are treated as a single entry.

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

The "Start from VLAN", and "Group" input fields allow the user to select the starting point in the MLD SFM Information Table. Clicking the “Refresh” button will update the displayed table starting from the input values or the next closest MLD SFM Information Table match. In addition, the two input fields will - upon a “Refresh” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

VLAN ID: VLAN ID of the group.

Group: Group address of the group displayed.

Port: Switch port number.

Mode: Indicates the filtering mode maintained per VLAN ID/port number/Group Address basis. It can be either Include or Exclude.

Source Address: IP Address of the source. Currently, the maximum number of IPv6 source addresses for filtering (per group) is 8. When there are no source filtering addresses, the text "None" is shown in the Source Address field.

Type: Indicates the Type. It can be either Allow or Deny.

Hardware Filter/Switch: Indicates whether the data plane destined for the specific group address from the source IPv6 address could be handled by chip or not.

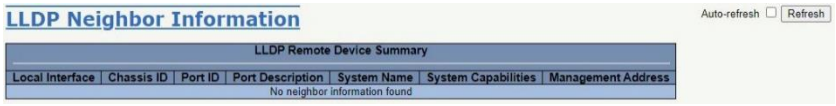
Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Refreshes the displayed table starting from the input fields.
|<<: Updates the table starting from the first entry in the MLD SFM Information Table.
>>: Updates the table, starting with the entry after the last entry currently displayed.

LLDP

Neighbors

This page provides a status overview for all LLDP neighbors. The displayed table contains a row for each interface on which an LLDP neighbor is detected.



The columns hold the following information:

Local Interface: The interface on which the LLDP frame was received.

Chassis ID: The Chassis ID is the identification of the neighbor's LLDP frames.

Port ID: The Port ID is the identification of the neighbor port.

System Name: System Name is the name advertised by the neighbor unit.

System Capabilities: System Capabilities describes the neighbor unit's capabilities. The possible capabilities are:

Other
Repeater
Bridge
WLAN Access Point
Router
Telephone
DOCSIS cable device
Station only
Reserved

When a capability is enabled, it is followed by (+). If the capability is disabled, it is followed by (-).

Management Address: Management Address is the neighbor unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbor's IP address.

Buttons

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

LLDP-MED Neighbors

This page provides a status overview of all LLDP-MED neighbors. The displayed table contains a row for each interface on which an LLDP neighbor is detected. This function applies to VoIP devices which support LLDP-MED.

The columns hold the following information:

Interface: The interface on which the LLDP frame was received.

Device Type: LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices.

LLDP-MED Network Connectivity Device Definition: LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:
LAN Switch/Router
IEEE 802.1 Bridge
IEEE 802.3 Repeater (included for historical reasons)
IEEE 802.11 Wireless Access Point
Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method.

LLDP-MED Endpoint Device Definition: LLDP-MED Endpoint Devices, as defined in TIA-1057, are located at the IEEE 802 LAN network edge, and participate in IP communication service using the LLDP-MED framework. Within the LLDP-MED Endpoint Device category, the LLDP-MED scheme is broken into further Endpoint Device Classes, as defined in the following. Each LLDP-MED Endpoint Device Class is defined to build upon the capabilities defined for the previous Endpoint Device Class. For-example any LLDP-MED Endpoint Device claiming compliance as a Media Endpoint (Class II) will also support all aspects of TIA-1057 applicable to Generic Endpoints (Class I), and any LLDP-MED Endpoint Device claiming compliance as a Communication Device (Class III) will also support all aspects of TIA-1057 applicable to both Media Endpoints (Class II) and Generic Endpoints (Class I).

LLDP-MED Generic Endpoint (Class I): The LLDP-MED Generic Endpoint (Class I) definition is applicable to all endpoint products that require the base LLDP discovery services defined in TIA-1057, however do not support IP media or act as an end-user communication appliance. Such devices may include (but are not limited to) IP Communication Controllers, other communication related servers, or any device requiring basic services as defined in TIA-1057. Discovery services defined in this class include LAN configuration, device location, network policy, power management, and inventory management.

LLDP-MED Media Endpoint (Class II): The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities however may or may not be associated with a particular end user. Capabilities include all of the capabilities defined for the previous Generic Endpoint Class (Class I), and are extended to include aspects related to media streaming. Example product categories expected to adhere to this class include (but are not limited to) Voice / Media Gateways, Conference Bridges, Media Servers, and similar. Discovery services defined in this class include media-type-specific network layer policy discovery.

LLDP-MED Communication Endpoint (Class III): The LLDP-MED Communication Endpoint (Class III) definition is applicable to all endpoint products that act as end user communication appliances supporting IP media. Capabilities include all of the capabilities defined for the

previous Generic Endpoint (Class I) and Media Endpoint (Class II) classes, and are extended to include aspects related to end user devices. Example product categories expected to adhere to this class include (but are not limited to) end user communication appliances, such as IP Phones, PC-based softphones, or other communication appliances that directly support the end user. Discovery services defined in this class include provision of location identifier (including ECS / E911 information), embedded L2 switch support, and inventory management.

LLDP-MED Capabilities: LLDP-MED Capabilities describes the neighbor unit's LLDP-MED capabilities. The possible capabilities are:
LLDP-MED capabilities
Network Policy
Location Identification
Extended Power via MDI – PSE
Extended Power vis MDI – PD
Inventory
Reserved

Application Type: Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are shown below.

Voice: For use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.
Voice Signaling: For use in network topologies that require a different policy for the voice signaling than for the voice media.
Guest Voice: To support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
Guest Voice Signaling: For use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.
Softphone Voice: For use by softphone applications on typical data centric devices, such as PCs or laptops.
Video Conferencing: For use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
Streaming Video: For use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
Video Signaling: For use in network topologies that require a separate policy for the video signaling than for the video media.

Policy: Policy indicates that an Endpoint Device wants to explicitly advertise that the policy is required by the device. Can be either Defined or Unknown.

Unknown: The network policy for the specified application type is currently unknown.
Defined: The network policy is defined (known).

TAG: TAG is indicative of whether the specified application type is using a tagged or an untagged VLAN. Can be Tagged or Untagged.

Untagged: The device is using an untagged frame format and as such does not include a tag header as defined by IEEE 802.1Q-2003.
Tagged: The device is using the IEEE 802.1Q tagged frame format.

VLAN ID: VLAN ID is the VLAN identifier (VID) for the interface as defined in IEEE 802.1Q-2003. A value of 1 through 4094 is used to define a valid VLAN ID. A value of 0 (Priority Tagged) is used if the device is using priority tagged frames as defined by IEEE 802.1Q-2003, meaning that only the IEEE 802.1D priority level is significant and the default PVID of the ingress interface is used instead.

Priority: Priority is the Layer 2 priority to be used for the specified application type. One of the eight priority levels (0 through 7).

DSCP: DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contains one of 64 code point values (0 through 63).

Auto-negotiation: Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.

Auto-negotiation status: Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined by the operational MAU type field value rather than by auto-negotiation.

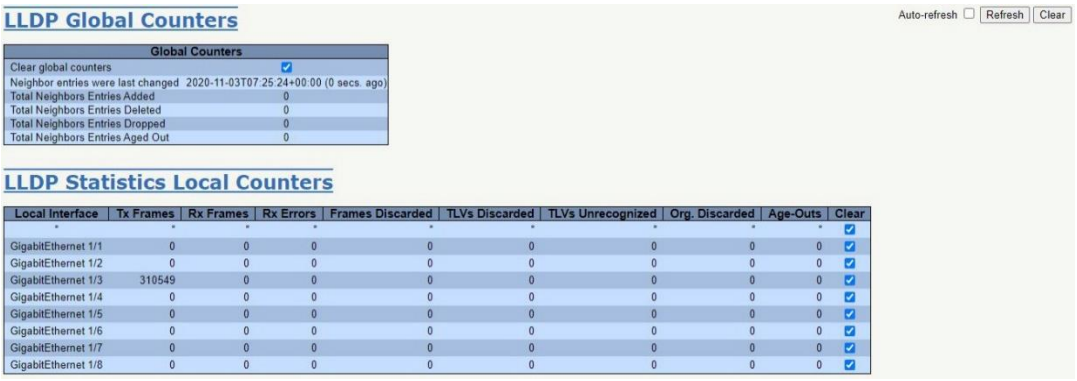
Auto-negotiation Capabilities: Auto-negotiation Capabilities shows the link partners MAC/PHY capabilities.

Buttons

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

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-interface counters.

Global Counters

Clear global counters: If checked the global counters are cleared when“Clear” is pressed.

Neighbor entries were last changed: Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.

Total Neighbors Entries Added: Shows the number of new entries added since switch reboot.

Total Neighbors Entries Deleted: Shows the number of new entries deleted since switch reboot.

Total Neighbors Entries Dropped: Shows the number of LLDP frames dropped due to the entry table being full.

Total Neighbors Entries Aged Out: Shows the number of entries deleted due to Time-To-Live expiring.

Local Counters

The displayed table contains a row for each interface. The columns hold the following information:

Local Interface: The interface on which LLDP frames are received or transmitted.

Tx Frames: The number of LLDP frames transmitted on the interface.

Rx Frames: The number of LLDP frames received on the interface.

Rx Errors: The number of received LLDP frames containing some kind of error.

Frames Discarded: If an LLDP frame is received on an interface, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbors" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given interface's link is down, an LLDP shutdown frame is received, or when the entry ages out.

TLVs Discarded: Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.

TLVs Unrecognized: The number of LLDP frames that have well-formed TLVs, but have an unknown type value.

Org. Discarded: If an LLDP frame is received with an organizationally TLV but the TLV is not supported, the TLV is discarded and counted.

Age-Outs: Each LLDP frame contains information about how long the LLDP information is valid (age-out time). If no new LLDP frame is received within the age-out time, the LLDP information is removed and the Age-Out counter is incremented.

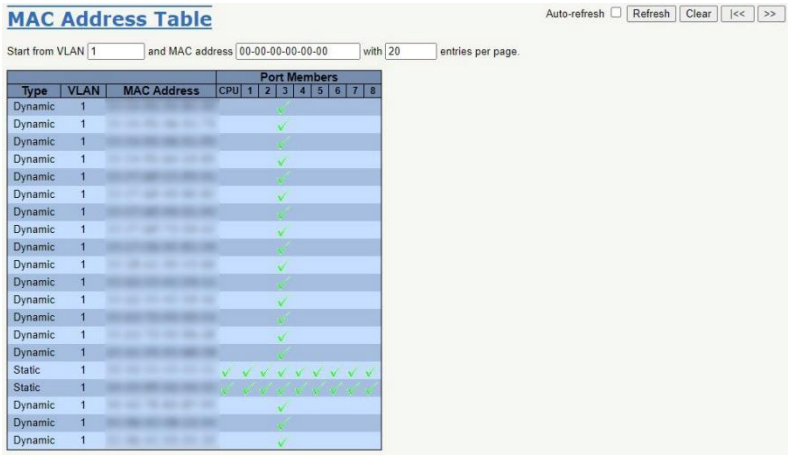
Clear: If checked the counters for the specific interface are cleared when “Clear” is pressed.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page.
Clear: Clears the counters which have the corresponding checkbox checked.

MAC Table

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



Each page shows up to 999 entries from the MAC table, the default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The "Start from VLAN " and "MAC address" input fields allow the user to select the starting point in the MAC Table. Clicking the “Refresh” button will update the displayed table starting from the input values or the next closest MAC Table match. In addition, the two input fields will - upon a “Refresh” button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

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

Type: Indicates whether the entry is a static or a dynamic entry.

VLAN: The VLAN ID of the entry.

MAC Address: The MAC address of the entry.

Port Members: The ports that are members of the entry.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Refreshes the displayed table starting from the "Start from MAC address" and "VLAN" input fields.
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.

VLANs

Membership

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

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

The "VLAN" input field allows the user to select the starting point in the VLAN Table.

Clicking the “Refresh” button will update the displayed table starting from the input value or the next closest 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 data exists for the selected user" is shown in the table. Use the “|<<” button to start over.

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

VLAN ID: VLAN ID for which the Port members are displayed.

Port Members: A row of check boxes for each port is displayed for each VLAN ID.

If a port is included in a VLAN, the following image will be displayed:  .

If a port is in the forbidden port list, the following image will be displayed:  .

If a port is in the forbidden port list while at the same time attempting to be included in the VLAN, the following image will be displayed: . 

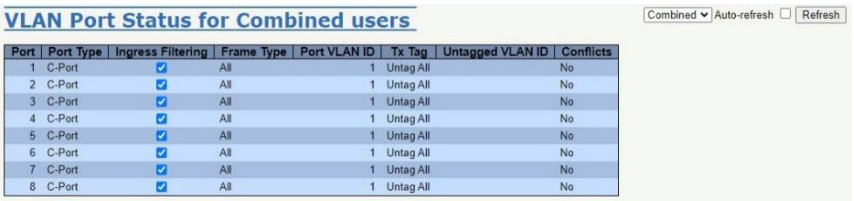
The port will not be a member of the VLAN in this case.

Buttons

Combined: Select VLAN Users from this drop down list.
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.

Ports

This page provides VLAN Port Status.



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

given software modules hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table.

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

Port Type: Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port) that a given user wants to configure on the port. The field is empty if not overridden by the selected user. Default appears to be C-Port (not empty) after reloading factory defaults.

Ingress Filtering: Shows whether a given user wants ingress filtering enabled or not. The field is empty if not overridden by the selected user. This is a checkbox and the default appears to be checked after reloading factory defaults.

Frame Type: Shows the acceptable frame types (All, Tagged, Untagged) that a given user wants to configure on the port. The field is empty if not overridden by the selected user. Default appears to be All after reloading factory defaults.

Port VLAN ID: Shows the Port VLAN ID (PVID) that a given user wants the port to have. The field is empty if not overridden by the selected user. Default appears to be 1 after reloading factory defaults.

Tx Tag: Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port. The field is empty if not overridden by the selected user. Default appears to be Untag All after reloading factory defaults.

Untagged VLAN ID: If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field will show the VLAN ID the user wants to tag or untag on egress. The field is empty if not overridden by the selected user.

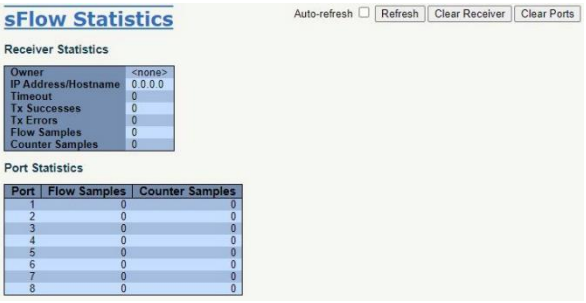
Conflicts: Two users may have conflicting requirements on a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress. Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: the higher in the list, the higher priority. If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module. The "Combined" user reflects what is actually configured in hardware.

Buttons

Combined: Select VLAN Users from this drop down list.
Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page immediately.

sFlow

This page shows receiver and per-port sFlow statistics.



Owner: This field shows the current owner of the sFlow configuration. It assumes one of three values as follows:

If sFlow is currently unconfigured/unclaimed, Owner contains <none>.
If sFlow is currently configured through Web or CLI, Owner contains <Configured through local management>.
If sFlow is currently configured through SNMP, Owner contains a string identifying the sFlow receiver.

IP Address/Hostname: The IP address or hostname of the sFlow receiver.

Timeout: The number of seconds remaining before sampling stops and the current sFlow owner is released.

Tx Successes: The number of UDP datagrams successfully sent to the sFlow receiver.

Tx Errors: The number of UDP datagrams that have failed to be transmitted. The most common source of errors is invalid sFlow receiver IP/hostname configuration. To diagnose, paste the receiver's IP address/hostname into the Ping Web page (Diagnostics→Ping/Ping6).

Flow Samples: The total number of flow samples sent to the sFlow receiver.

Counter Samples: The total number of counter samples sent to the sFlow receiver.

Port: The port number for which the following statistics applies.

Flow Samples: The number of flow samples sent to the sFlow receiver originating from this port.

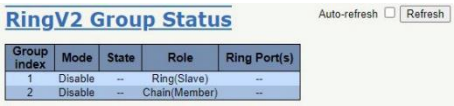
Counter Samples: The total number of counter samples sent to the sFlow receiver originating from this port.

Buttons

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh: Click to refresh the page.
Clear Receiver: Clears the sFlow receiver counters.
Clear Ports: Clears the per-port counters.

RingV2

This page provides a status overview for all of Ring status.



Group Index: The group index. This parameter is used to easy identify a ring group.

Mode: Indicates whether the group is enabled.

State: When ring is complete, it will show "Normal". When ring is incomplete (at least one link is down), it will show "Fail".

Role: Indicates to which role the group is configured.

Ring Port(s): Describes current status of ring port(s).

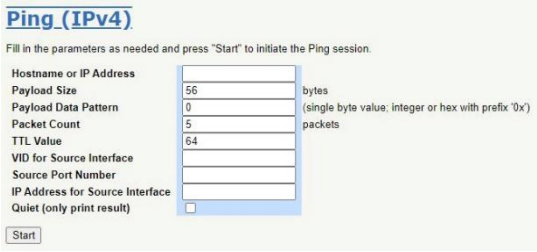
Buttons

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

Chapter 7 Diagnostics

Ping (IPv4)

This page allows you to issue ICMP (IPv4) PING packets to troubleshoot IP connectivity issues.



You can configure the following parameters for the test:

Hostname or IP Address: The address of the destination host, either as a symbolic hostname or an IP Address.

Payload Size: Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.

Payload Data Pattern: Determines the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

Packet Count: Determines the number of PING requests sent. The default value is 5. The valid range is 1-60.

TTL Value: Determines the Time-To-Live / TTL) field value in the IPv4 header. The default value is 64. The valid range is 1-255.

VID for Source Interface: This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

> **Note:** You may only specify either the VID or the IP Address for the source interface.

Source Port Number: This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration.

> **Note:** You may only specify either the Source Port Number or the IP Address for the source interface.

IP Address for Source Interface: This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.

> **Note:** You may only specify either the VID or the IP Address for the source interface.

Quiet (only print result): Checking this option will not print the result of each ping request but will only show the final result.

After you press “Start”, ICMP packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

The page refreshes automatically until responses to all packets are received or until a timeout occurs.

The output from the command will look like the following:

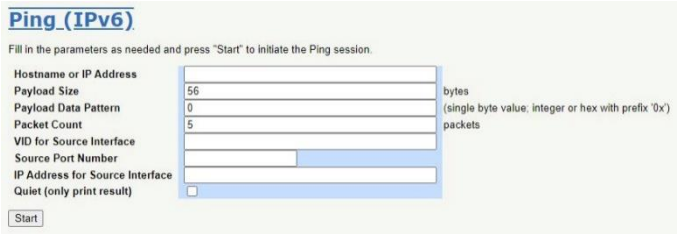
```
PING 172.16.1.1 (172.16.1.1) from 172.16.1.10: 56 data bytes

64 bytes from 172.16.1.1: seq=0 ttl=64 time=2.034 ms

64 bytes from 172.16.1.1: seq=1 ttl=64 time=1.729 ms

64 bytes from 172.16.1.1: seq=2 ttl=64 time=1.954 ms

64 bytes from 172.16.1.1: seq=3 ttl=64 time=1.699 ms

64 bytes from 172.16.1.1: seq=4 ttl=64 time=1.916 ms


--- 172.16.1.1 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 1.699/1.866/2.034 ms
```

Buttons

Start: Click to start transmitting ICMP packets.
New Ping: Click to re-start diagnostics with PING.

Ping (IPv6)

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.



You can configure the following parameters for the test:

Hostname or IP Address: The address of the destination host, either as a symbolic hostname or an IP Address.

Payload Size: Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.

Payload Data Pattern: Determines the pattern used in the ICMP data payload. The default value is 0. The valid range is 0-255.

Packet Count: Determines the number of PING requests sent. The default value is 5. The valid range is 1-60.

VID for Source Interface: This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

Source Port Number: This field can be used to force the test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the Source Port Number or the IP Address for the source interface.

IP Address for Source Interface: This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

Quiet (only print result): Checking this option will not print the result of each ping request but will only show the final result.

After you press “Start”, ICMP packets are transmitted and the sequence number and round trip time are displayed upon reception of a reply.

The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header).

The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

The output from the command will look like the following:

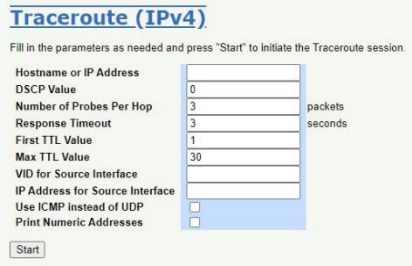
```
PING 2001::01 (2001::1) from 2001::3: 56 data bytes

64 bytes from 2001::1: seq=0 ttl=64 time=2.118 ms

64 bytes from 2001::1: seq=1 ttl=64 time=2.009 ms

64 bytes from 2001::1: seq=2 ttl=64 time=1.852 ms

64 bytes from 2001::1: seq=3 ttl=64 time=2.869 ms

64 bytes from 2001::1: seq=4 ttl=64 time=1.845 ms


--- 2001::01 ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss

round-trip min/avg/max = 1.845/2.138/2.869 ms
```

Buttons

Start: Click to start transmitting ICMP packets.
New Ping: Click to re-start diagnostics with PING.

Traceroute (IPv4)

This page allows you to perform a traceroute test over IPv4 towards a remote host. Traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv4 network.



You can configure the following parameters for the test:

Hostname or IP Address: The destination IP Address.

DSCP Value: This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-63.

Number of Probes Per Hop: Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.

Response Timeout: Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.

First TTL Value: Determines the value of the Time-To-Live (TTL) field in the IPv4 header in the first packet sent. The default number is 1. The valid range is 1-30.

Max TTL Value: Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 30. The valid range is 1-255.

VID for Source Interface: This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

IP Address for Source Interface: This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

Use ICMP instead of UDP: By default the traceroute command will use UDP datagrams. Selecting this option forces it to use ICMP ECHO packets instead.

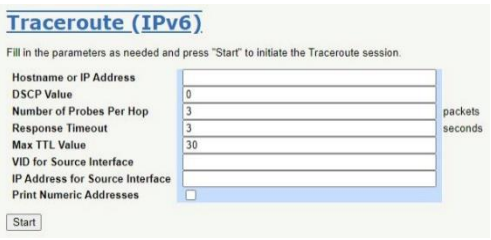
Print Numeric Addresses: By default the traceroute command will print out hop information using a reverse DNS lookup for the acquired host ip addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

Buttons

Start: Click to start traceroute test.

Traceroute (IPv6)

This page allows you to perform a traceroute test over IPv6 towards a remote host. Traceroute is a diagnostic tool for displaying the route and measuring transit delays of packets across an IPv6 network.



You can configure the following parameters for the test:

Hostname or IP Address: The destination IP Address.

DSCP Value: This value is used for the DSCP value in the IPv4 header. The default value is 0. The valid range is 0-255.

Number of Probes Per Hop: Determines the number of probes (packets) sent for each hop. The default value is 3. The valid range is 1-60.

Response Timeout: Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1-86400.

Max TTL Value: Determines the maximum value of the Time-To-Live (TTL) field in the IPv4 header. If this value is reached before the specified remote host is reached the test stops. The default number is 255. The valid range is 1-255.

VID for Source Interface: This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

IP Address for Source Interface: This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.

Note: You may only specify either the VID or the IP Address for the source interface.

Print Numeric Addresses: By default the traceroute command will print out hop information using a reverse DNS lookup for the acquired host ip addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

Buttons

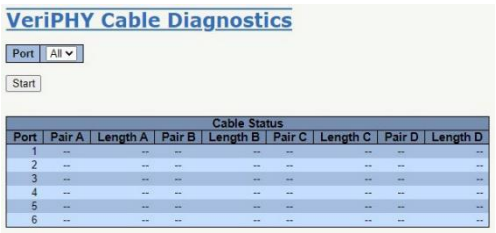
Start: Click to start traceroute test.

VeriPHY

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

Press “Start” to run the diagnostics. This will take approximately 5 seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and you can view the cable diagnostics results in the cable status table. Note that 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.



Port: The port where you are requesting VeriPHY Cable Diagnostics.

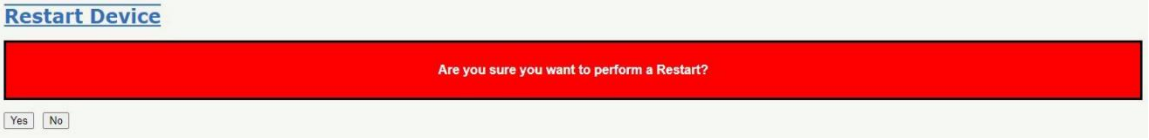
Cable Status

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. The resolution is 3 meters.

Chapter 8 Maintenance

Restart Device

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



Yes: Click to restart device.

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

Factory Defaults

You can reset the configuration of the switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary.

Yes: Click to reset the configuration to Factory Defaults.

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

Software

Upload

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

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

After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch restarts.

> **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.

Image Select

This page provides information about the active and alternate (backup) firmware images in the device, and allows you to revert to the alternate image.

The web page displays two tables with information about the active and alternate firmware images.

> **Note:** In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.

Note: If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.

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

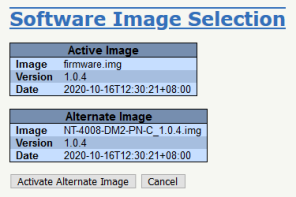


Image: The file name of the firmware image, from when the image was last updated.

Version: The version of the firmware image.

Date: The date where the firmware was produced.

Buttons

Activate Alternate Image: Click to use the alternate image. This button may be disabled depending on system state.

Cancel: Cancel activating the backup image. Navigates away from this page.

Chapter 9 Application Guides

This chapter provides procedures and examples for configuring these switch features:

- VLANs (Virtual LANs)
- Security ACLs (Access Control Lists)
- RingV2 (Ring Version 2)
- QoS (Quality of Service) Scheduling and Shaping
- IGMP (Internet Group Management Protocol)

VLAN Configuration

This section describes how to configure Virtual LANs (VLANs). The switch supports managing up to 2048 VLANs.

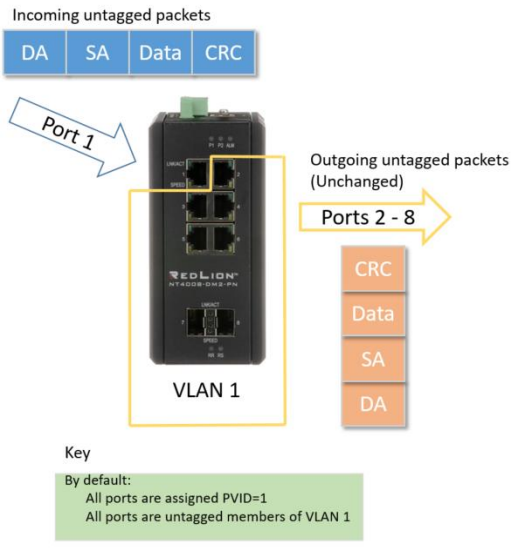
Ports are grouped into broadcast domains by assigning them to the same VLAN. Frames received on a VLAN are only forwarded within that VLAN. Similarly, broadcast, multicast, and unknown unicast frames are only flooded to ports in the same VLAN.

Every network frame may have a VLAN tag as specified by IEEE 802.1Q and IEEE 802.1p. This tag contains a number (VLAN ID) indicating which VLAN this frame belongs in.

Every port has a default Port VLAN, also known as a PVID (port VLAN ID). The PVID is configurable to any VLAN number between 1 and 4095. If an incoming frame does not have a VLAN tag, then the frame can be assigned the PVID.

Example 1: Untagged VLAN 1 Settings

In factory defaults, all port are grouped into VLAN 1 (PVID=1). All untagged incoming frames are assigned to VLAN 1 per the Port VLAN (PVID=1). All outgoing frames are untagged.



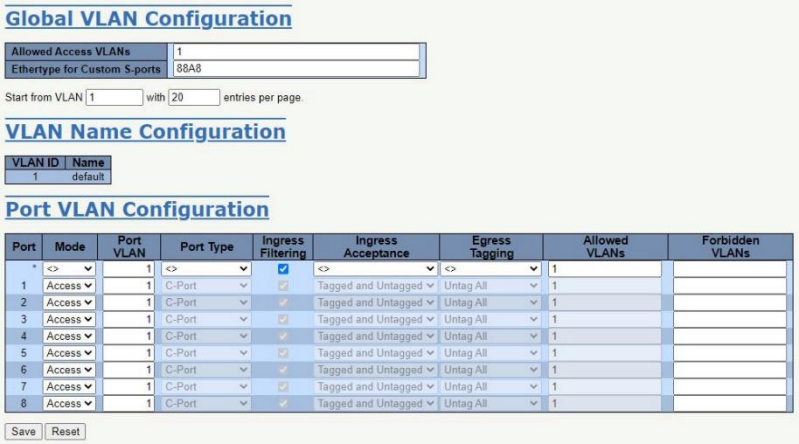
Port 1
Incoming untagged packets

Ports 2-10
Outgoing untagged packets (unchanged)

Default Configuration

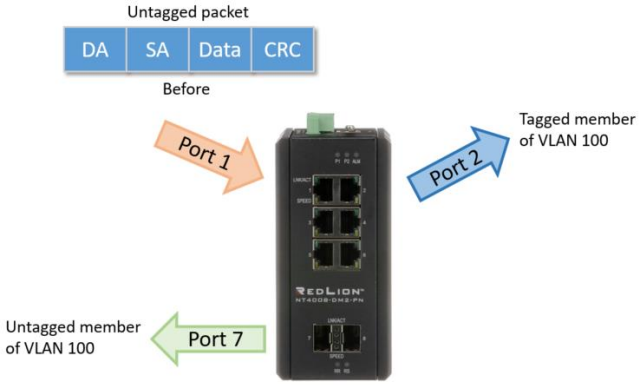
- All ports are assigned PVID=1
- All ports are members of VLAN 1
- All outgoing frames are untagged

Configuration



Example 2: Port-Based VLANs

When the switch receives an untagged VLAN packet it will add a VLAN tag to the frame according to the PVID setting on the port that received the untagged packet. As shown in the image below, the untagged packet is marked (tagged) as it leaves the switch through Port 2, which is configured as a tagged member of VLAN 100. The untagged packet remains unchanged as it leaves the switch through Port 7, which is configured as an untagged member of VLAN 100.

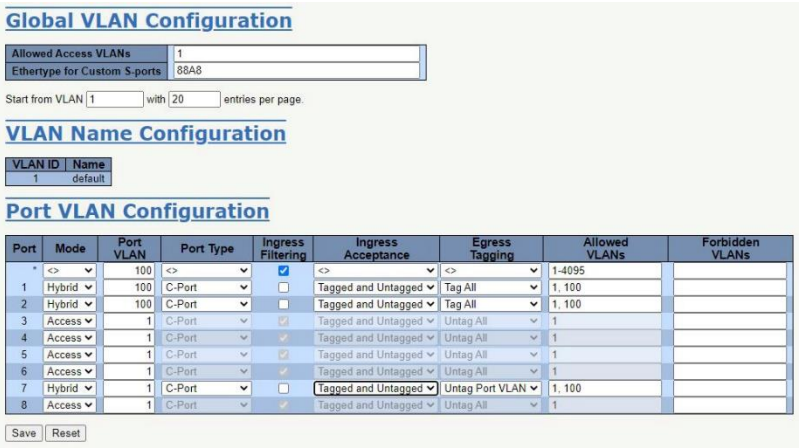


Port 1 VLAN 100
PVID=100
Outgoing tagged frames

Port 2 VLAN 100
PVID=100
Outgoing tagged frames

Port 7 VLAN 100
PVID=100
Outgoing untagged frames (unchanged)

Configuration



1. Go to Configuration→VLANs→Configuration.
   Set Port 1, Port 2, and Port 7 to be in Hybrid Mode and Ingress Acceptance must be set to Tagged and Untagged.
   Set Allow Access VLANs to 1, 100 so that the switch can be managed from either VLAN.
2. The Egress Tagging settings determine if frames that are transmitted from the port are tagged or untagged with the VLAN ID. The possible tag settings are:
   Tag All: All outgoing frames are always tagged.
   Untag Port VLAN: All outgoing frames on the same VLAN as the port's PVID are untagged. All other frames are tagged.
   Untag All: All outgoing frames are always untagged.
   Set Egress Tagging for ports 1 and 2 to Tag All. Set Egress Tagging for port 7 to Untag Port VLAN.
3. Transmit untagged unicast packets from Port 1 to Port 2 and Port 7. The switch will tag any egressing packet with VID 100. These packets have access to Port 2 and Port 7. Outgoing packets are stripped of their tags to leave Port 7 as untagged packets. For Port 2, the outgoing packets leave as a tagged packet with VID 100.
4. Transmit untagged unicast packets from Port 2 to Port 1 and Port 7. The switch should tag the packets with VID 100. The packets have access to Port 1 and Port 7. The outgoing packets are stripped of their tags to leave Port 7 as untagged packets. For Port 1, the outgoing packets leave as tagged packets with VID 100.
5. Transmit untagged unicast packets from Port 7 to Port 1 and Port 2. The switch should tag the packets with VID 100. The packets have access to Port 1 and Port 2. For Port 1 and Port 2, the outgoing packets leave as tagged packets with VID 100.
6. Repeat step 4 using broadcast and multicast packets.

CLI Commands

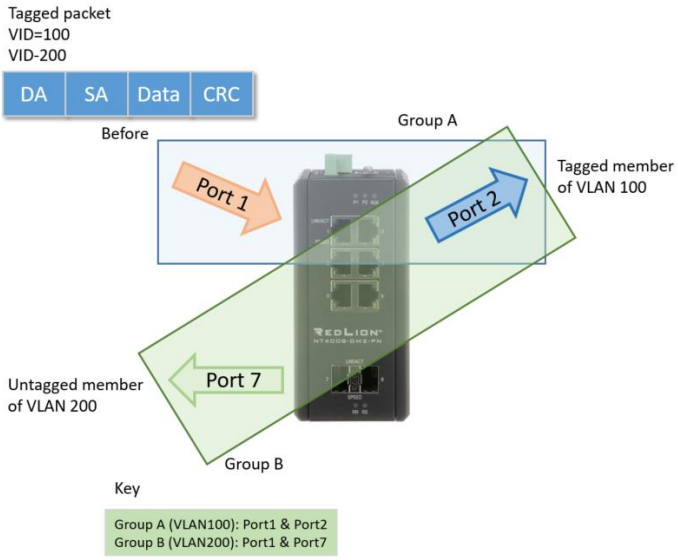
```
vlan 1, 100

interface GigabitEthernet 1/1
switchport hybrid native vlan 100
switchport hybrid allowed vlan 1,100
switchport hybrid egress-tag all
switchport mode hybrid
exit

interface GigabitEthernet 1/2
switchport hybrid native vlan 100
switchport hybrid allowed vlan 1,100
```

```
switchport hybrid egress-tag all
switchport mode hybrid
exit

interface GigabitEthernet 1/7
switchport access vlan 100
switchport hybrid native vlan 100
switchport hybrid allowed vlan 1,100
switchport mode hybrid
exit
```

Example 3: IEEE 802.1Q Tagged VLANs

In the following figure, the tagged incoming frame are assigned directly to VLAN 100 and VLAN 200 because of the tag assignment in the frame. Port 2 is configured as a tagged member of VLAN 100, and Port 7 is configured as an untagged member of VLAN 200. Port 1 is a member of both VLAN 100 and VLAN 200. Port 1 is an uplink port.

Hosts in the same VLAN communicate with each other as if in a single LAN. However, hosts in different VLANs cannot communicate with each other directly.



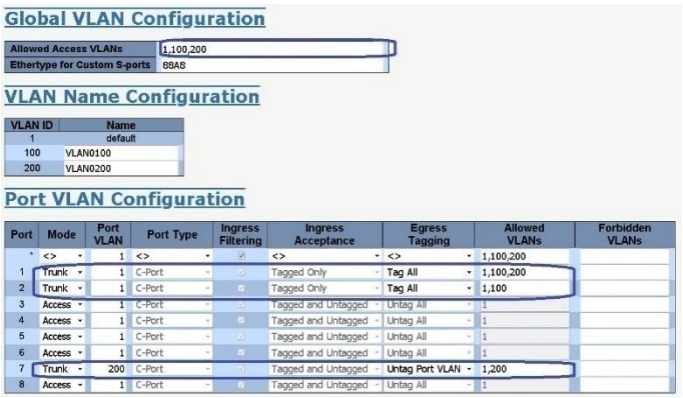
Port 1 VLAN 100 & 200	**Port 2 VLAN 100**	**Port 7 VLAN 200**
Groups A & B	Group A	Group B
PVID=1	PVID=100	PVID=200
Outgoing tagged frames	Outgoing tagged frames	Outgoing untagged frames (unchanged)

In this case:

1. The hosts from Group A can communicate with each other.
2. The hosts from Group B can communicate with each other.
3. The hosts from Group A and Group B cannot communicate with each other.
4. Both the hosts of Group A and Group B can connect to an external network through the uplink Port 1.

Configuration

1. Go to Configuration→VLANs→Configure and specify the VLAN membership as follows:



2. Transmit unicast frames with VLAN tag 100 from Port 1 to Port 2 and Port 7. The switch assigns it to VLAN 100. The frame only has access to Port 2. For Port 2, the outgoing frame leaves as a tagged frame with VLAN ID 100.
3. Transmit unicast frames with VLAN tag 200 from Port 1 to Port 2 and Port 7. The switch assigns it to VLAN 200. The frame only has access to Port 7. The outgoing frame on Port 7 is stripped of its tag as an untagged frame.
4. Transmit unicast frames with VLAN tag 100 from Port 2 to Port 1 and Port 7. The switch assigns it to VLAN 100. The frame only has access to Port 1. For Port 1, the outgoing frame leaves as a tagged frame with VLAN ID 100.
5. Transmit unicast frames with VLAN tag 200 from Port 7 to Port 1 and Port 2. The switch assigns it to VLAN 200. The frame only has access to Port 1. The outgoing frame on Port 1 will leave as a tagged frame with VLAN ID 200.
6. Repeat the above steps using broadcast and multicast packets.

CLI Commands

```
enable
configure terminal
vlan 1, 100, 200

interface GigabitEthernet 1/1
switchport trunk allowed vlan 1,100,200
switchport trunk vlan tag native
switchport mode trunk
exit

interface GigabitEthernet 1/2
switchport trunk allowed vlan 1,100
switchport trunk vlan tag native
switchport mode trunk
exit

interface GigabitEthernet 1/7
switchport trunk native vlan 200
switchport trunk allowed vlan 1,200
switchport mode trunk
exit
```

Security ACL Configuration

The ACL (Access Control List) is a list of ACEs (Access Control Entries) that control the network traffic transiting the switch by looking for matching frames, where the match can be made on MAC addresses, IP

addresses, ARPs, Layer 4 Ports, Class of Service, and other criteria. One of 3 default actions can be taken for each matching frame: Deny, Permit, and Filter (which applies the ACE only to specific egress ports). Various sub-actions can also be taken including: Rate Limit, Port Redirect, Mirror, Log, Port Shutdown, and Count Matches.

The following table summarizes some of the ACL functions.

DEFAULT ACL RULE	ACTION ON MATCH						
	PORT REDIRECT	FILTER PORTS	RATE LIMITER	MIRROR	LOGGING	SHUTDOWN	COUNTER
DENY (1)	(a)	-	-	(d)	(e)	(f)	(g)
PERMIT (2)	-	-	(c)	(d)	(e)	(f)	(g)
FILTER (3)	-	(b)	(c)	(d)	(e)	(f)	(g)

Brief descriptions of the above table:

Deny (1): Drop frames that match.

Permit (2): Forward frames that match.

Filter (3): Forward frames that match, only on the specified outgoing Filter Ports.

Port Redirect (a): Redirect denied frames to these ports.

Filter Ports (b): Apply the ACE on frames that go out these ports.

Rate Limiter (c): Rate limit the matching frames.

Mirror (d): Forward a copy of the matching frames to this port.

Logging (e): Store a copy of the matching frame in a System Log entry.

Shutdown (f): Shutdown the port when a matching frame is detected.

Counter (g): Count the number of matching frames.

ACEs are managed under the web page Configuration→Security→Network→ACL→Access Control List.

Port Polices – Groups of ACEs

A policy is a group of ACEs. Each policy is given an ID, which is a number from 0 to 63. ACEs may be assigned a Policy ID to add them to a policy.

Ports can be assigned a Policy ID so that all the ACEs in that policy apply to the port. This helps to simplify the assignment of multiple ACEs to ports. For example, there can be one policy for access ports and a different policy for trunk ports.

Port Policies are managed under the web page Configuration→Security→Network→ACL→Ports.

Access Control Based on MAC Addresses

A MAC address ACE can filter frames based on matching the source MAC address, the destination MAC address, or both.

When matching both, the frame must match the criteria for both the source **and** the destination MAC address. To match only one MAC address, the other MAC address must be set to Any or zeros.

Additional matching criteria includes VLAN tag properties and EtherType. If the VLAN or Ether type is irrelevant, the user can just set those values to Any or zeros. The following are examples related to the above table:

Example 1: Deny by Source MAC and VLAN

With the following Access Control all normal VLAN traffic is permitted to enter Port 4, however entry is denied for frames matching a particular source MAC and VLAN.

1. Set Port 4 to Permit all frames by default and assign the port to Policy ID=1.

2. Create a new ACE. (Deny MAC: 11 and VLAN: 4) assigned to Policy 1.
3. Bind ACL profile 1 to a Port 4.
4. Setup ports 3 and 4 to accept VLANs 4 and 5 and to Tag All frames on Egress.
5. Send frames into Port 3 and Port 4, and see note the dropped frames.

CLI Commands

access-list ace 6 ingress interface GigabitEthernet 1/4 policy 1 tag tagged vid 4 frame-type etype smac 00-00-00-00-00-11 action deny

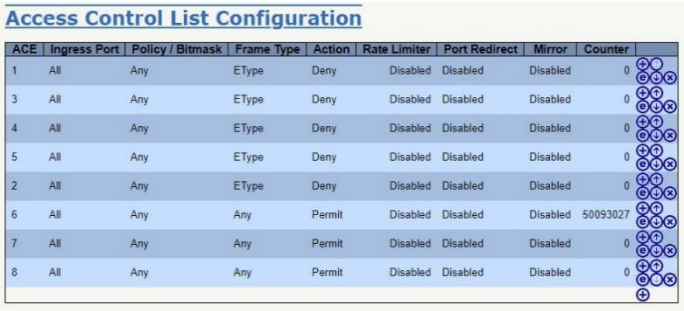
```
exit
!
interface GigabitEthernet 1/3
switchport trunk allowed vlan 4,5
switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
switchport trunk allowed vlan 4,5
switchport trunk vlan tag native
access-list policy 1

exit
```

Example 2: Deny by Source and Destination MAC

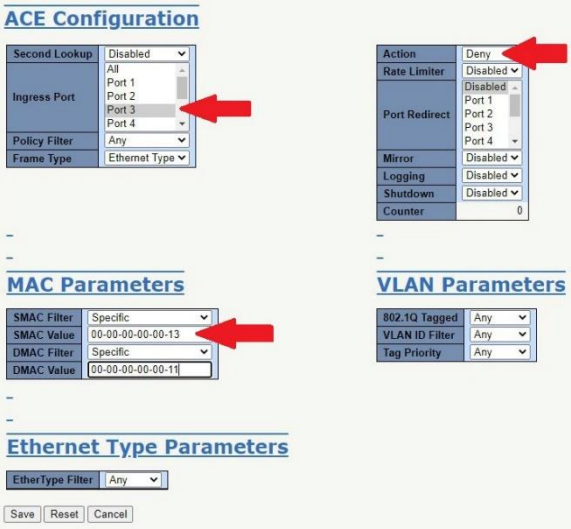
With the following Access Control all normal VLAN traffic is permitted to enter Port 3, however entry is denied for frames matching a specific combination of source and destination MAC received on any VLAN.

1. Set Port 3 to Permit all frames by default and leave the port assigned to Policy ID=0.

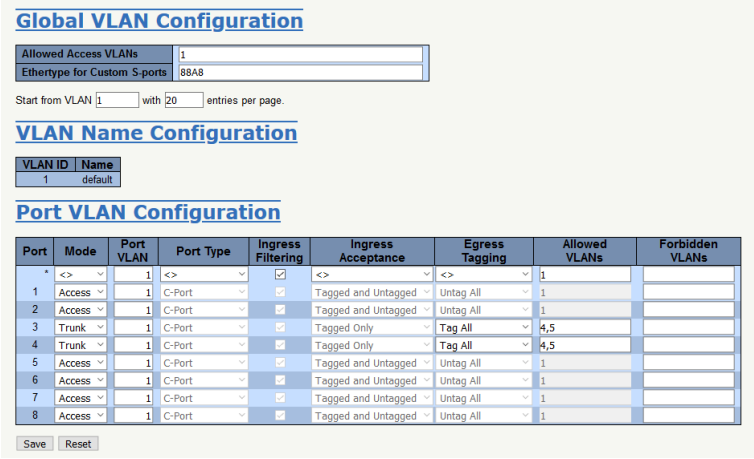
2. Create a new ACE. (Deny SrcMAC: 13 and DesMAC: 11 and any VLAN) with the default Policy ID=0.



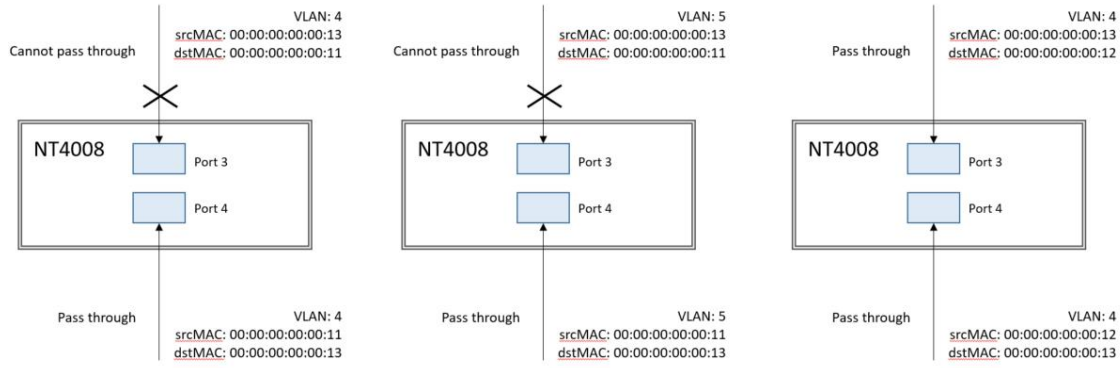
3. Bind this ACE to Port 3, leaving the Policy ID in defaults.



4. Setup ports 3 and 4 to accept VLANs 4 and 5 and to Tag All frames on Egress.



5. Send these frames between Port 3 and Port 4, and note the dropped frames.



CLI Commands

```
access-list ace 2 ingress interface GigabitEthernet 1/3 policy 0 frametype etype smac
00-00-00-00-00-13 dmac 00-00-00-00-00-11 action deny

exit
interface GigabitEthernet 1/3
switchport trunk allowed vlan 4,5
```

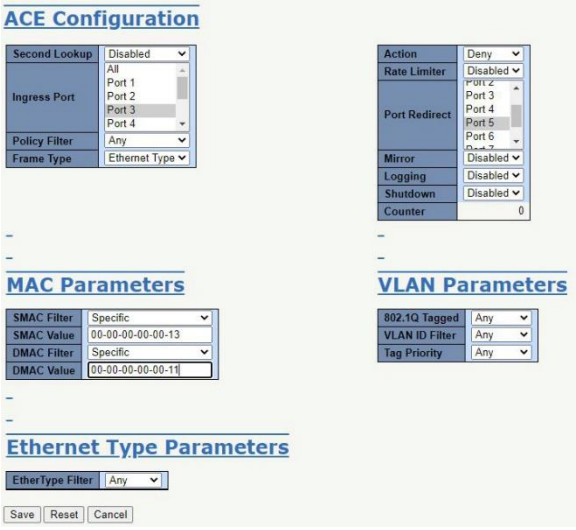
```
switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
switchport trunk allowed vlan 4,5
switchport trunk vlan tag native

exit
```

Example 3: Redirect by Source and Destination MAC

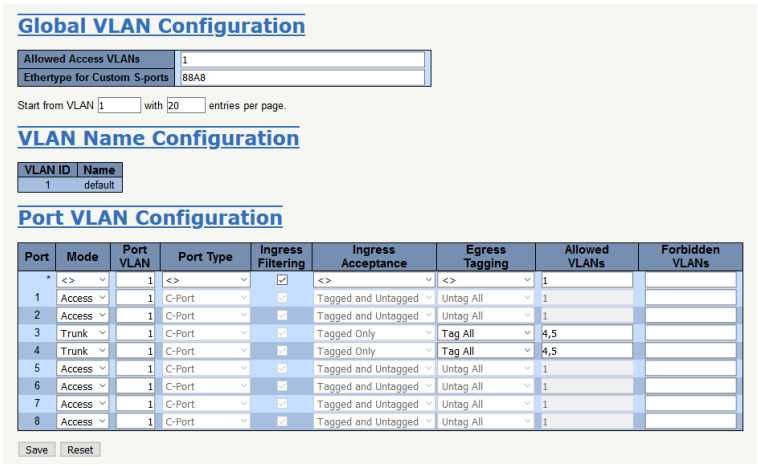
With the following Access Control all normal VLAN traffic is permitted to enter Port 3, however redirect frames with a specific combination of source and destination MAC to Port 5, instead of forwarding to their normal destination port.

1. Set Port 3 to Permit all frames by default and leave the port assigned to Policy ID=0.

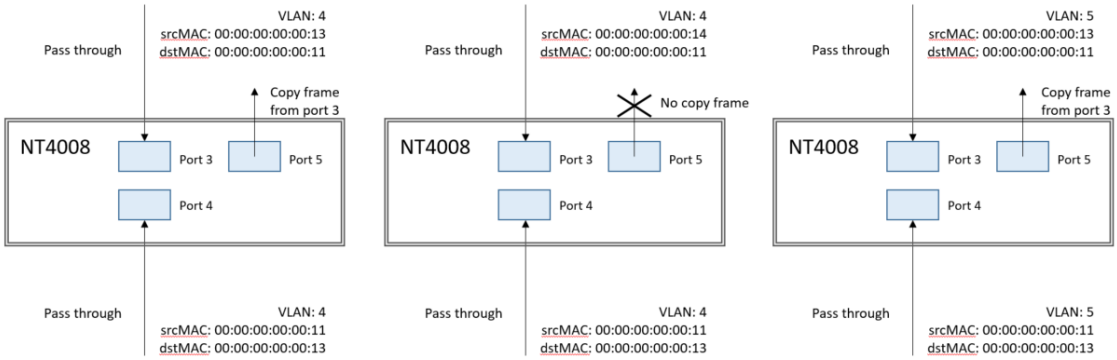
2. Create a new ACE (SrcMAC: 13 and DesMAC: 11) with the default Policy ID. Deny normal forwarding of the frame, and Enable Mirroring and Port Redirect to Port 5.



3. Setup ports 3 and 4 to accept VLANs 4 and 5 and to Tag All frames on Egress.



4. Send these frames between Port 3 and Port 4, and note the copied frames egressing Port 5.



CLI Commands

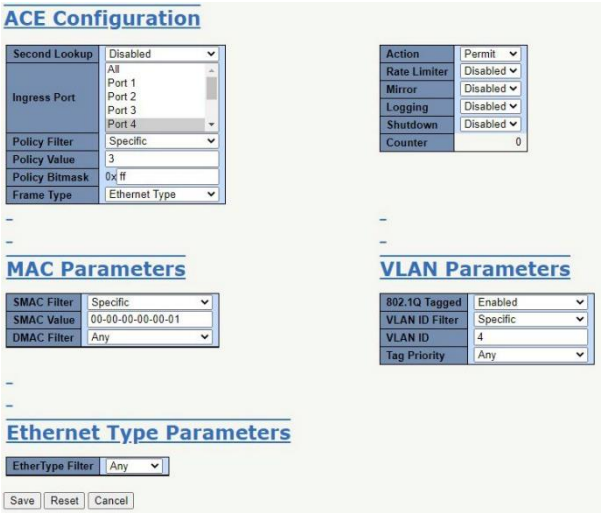
```
access-list ace 2 next 3 ingress interface GigabitEthernet 1/3 policy 0 frametype etype smac 00-00-00-00-00-13 dmac 00-00-00-00-00-11 action deny mirror redirect interface
GigabitEthernet 1/5
exit

interface GigabitEthernet 1/3
switchport trunk allowed vlan 4,5
switchport trunk vlan tag native
exit
!
interface GigabitEthernet 1/4
switchport trunk allowed vlan 4,5
switchport trunk vlan tag native
exit
```

Example 4: Permit by Source MAC and VLAN

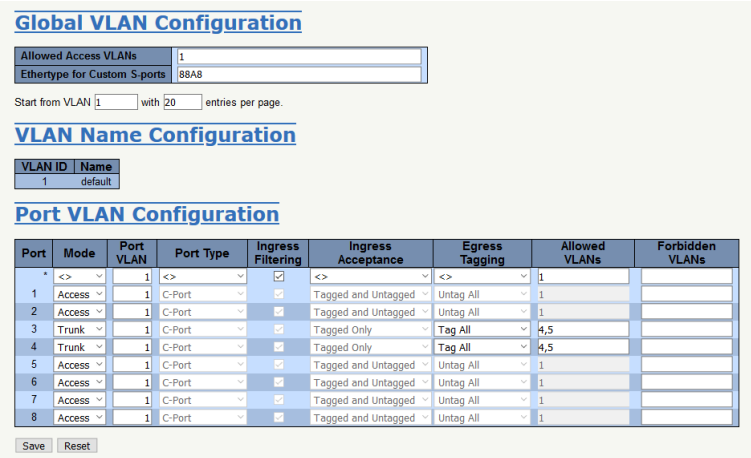
With the following Access Control all normal VLAN traffic is denied to enter Port 4 by default, except for frames allowed by the ACEs in Policy ID=3. In this case, the permitted frames match a specific source MAC on VLAN 4.

1. Set Port 4 to Deny all frames by default and set it to use Policy ID=3.

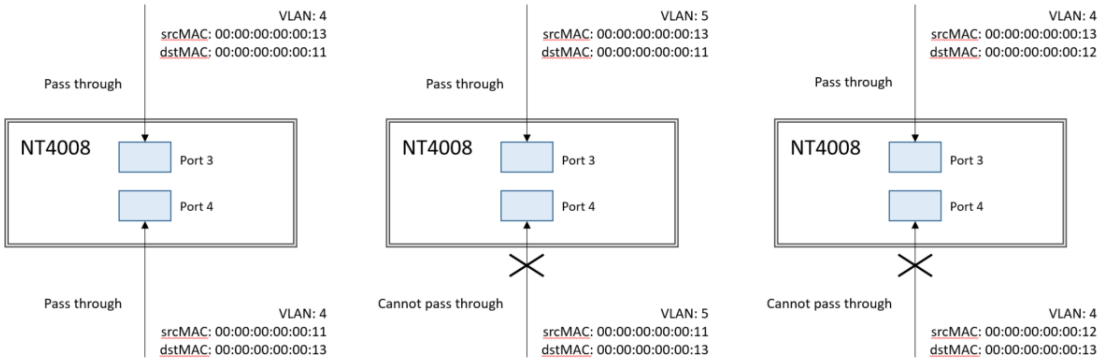
2. Create a new ACE under this ACL profile. (Permit MAC: 11 and VLAN: 4). Bind this ACE to profile 3 and to Ingress Port 4.



3. Setup Ports 3 and 4 to accept VLANs 4 and 5 and to Tag All frames on Egress.



4. Send these frames between Port 3 and Port 4, and note the frames egressing Port 4.



CLI Commands

TBD command that sets deny on port 3 by default?
!
access-list ace 4 ingress interface GigabitEthernet 1/4 policy 3 tag tagged vid 4 frametype etype smac 00-00-00-00-00-11
exit

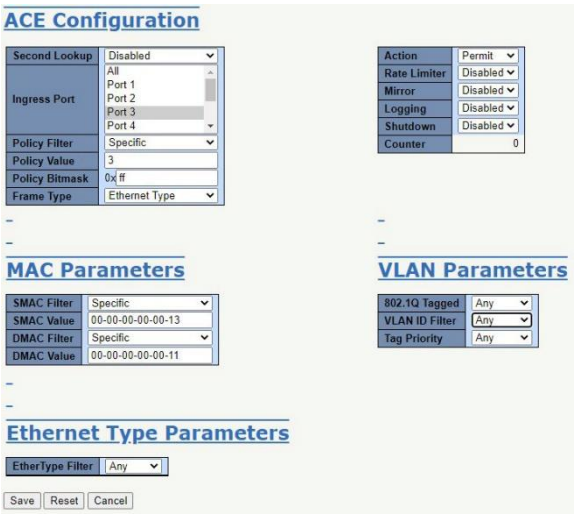
interface GigabitEthernet 1/3
switchport trunk allowed vlan 4,5
switchport trunk vlan tag native
exit
!
interface GigabitEthernet 1/4
switchport trunk allowed vlan 4,5
switchport trunk vlan tag native
exit

Example 5: Permit by Source and Destination MAC

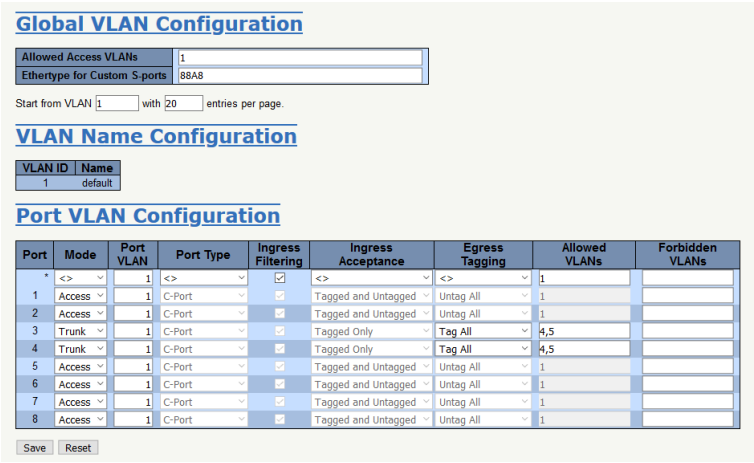
With the following Access Control all normal VLAN traffic is denied to enter Port 3 by default, except for frames allowed by the ACEs in Policy ID=5. In this case, the permitted frames match a specific pair of source and destination MACs.

1. Set Port 3 to Deny all frames by default and set it to use Policy ID=5.

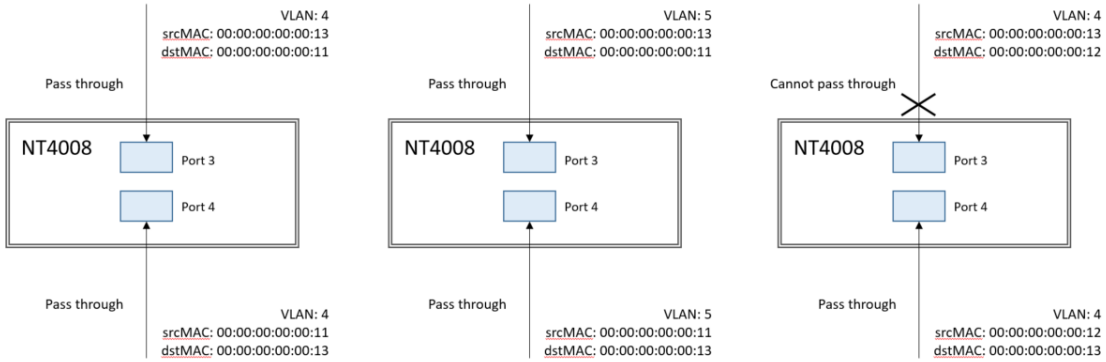
2. Create a new ACE under this ACL profile. (Permit SrcMAC: 13 and DesMAC: 11). Bind this ACE to profile 4 and to Ingress Port 3.



3. Setup Ports 3 and 4 to accept VLANs 4 and 5 and to Tag All frames on Egress.



4. Send frames between Port 3 and Port 4, see test result.



CLI Commands

TBD command that sets deny on port 3 by default?
!
access-list ace 5 ingress interface GigabitEthernet 1/3 policy 5 frametype etype smac 00-00-00-00-00-13 dmac 00-00-00-00-00-11
exit

```
interface GigabitEthernet 1/3
switchport trunk allowed vlan 4,5
switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
switchport trunk allowed vlan 4,5
switchport trunk vlan tag native
exit
```

Access Control Based on IPv4 Addresses

An IPv4 address ACE can match on source IP address, destination IP address, or both. An ACE can also match a range of IP addresses (subnets).

When the match is set for both a source and destination IP address, only packets meeting both criteria will match. Packets that meet only one criteria do not match the criteria.

If a user wants to match only the source or only the destination IP address, then set the IP of the source or destination as needed and set the other IP address to 0.0.0.0.

Additional matching criteria includes values of generic IPv4 fields and specific fields used by ICMP, TCP, and UDP packets. Every criteria must be met for the packet to match the ACE.

If a user wants to match a protocol, regardless of the IP address, then they should set both IP addresses to 0.0.0.0.

Access Control Based on IPv6 Addresses

An IPv6 address ACE can match on source IP address and Hop Limit. An ACE can also match a range of IP addresses.

Additional matching criteria includes values of specific fields used by ICMP, TCP, and UDP packets. . Every criteria must be met for the packet to match the ACE.

If a user wants to match a protocol, regardless of the IP address, then they should set the SIP and DIP Filters to Any.

Access Control Based on ARP Frames

An ACE can match specific types and fields of ARP frames including ARP/RARP frames, Request/Reply frames, Sender/Target IPs, ARP Sender MAC Match, RARP Target MAC Match, IP/Ethernet Length, IP bit, and Ethernet bit.

Access Control Based on VLAN Parameters

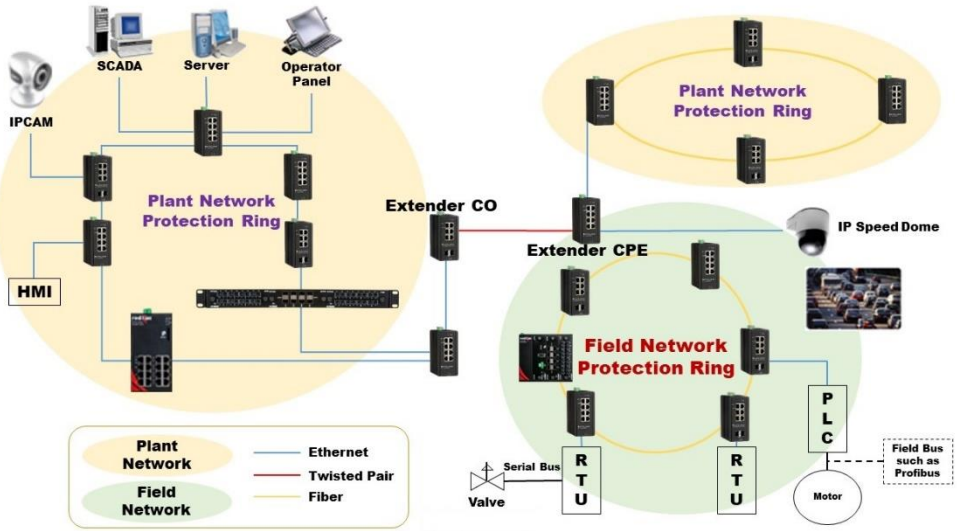
An ACE can match on just the fields of an 802.1Q VLAN tag include the presence or absence of a VLAN tag, the VLAN ID, and the priority (PCP) value.

RingV2 Configuration

Introduction

This section presents a guide to the Ring Version 2 application available for Red Lion NT4008 switch models.

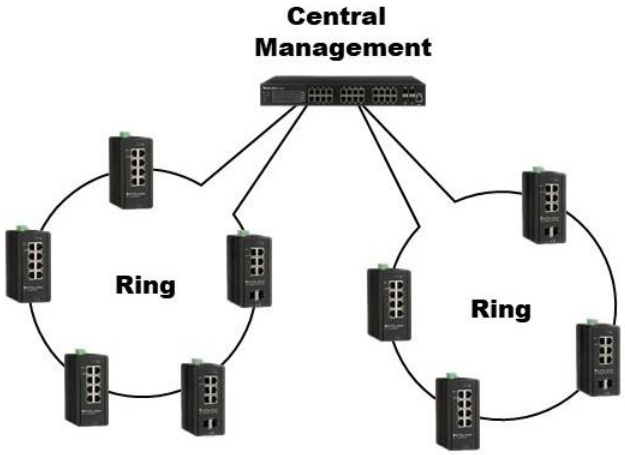
Network reliability is very important for Ethernet applications, especially in the industrial sector. The NT4008 provides approximately 20 millisecond failover ring protection and this feature offers seamless network functionality regardless of any connection issues that may arise.



Ring Version 2 Features

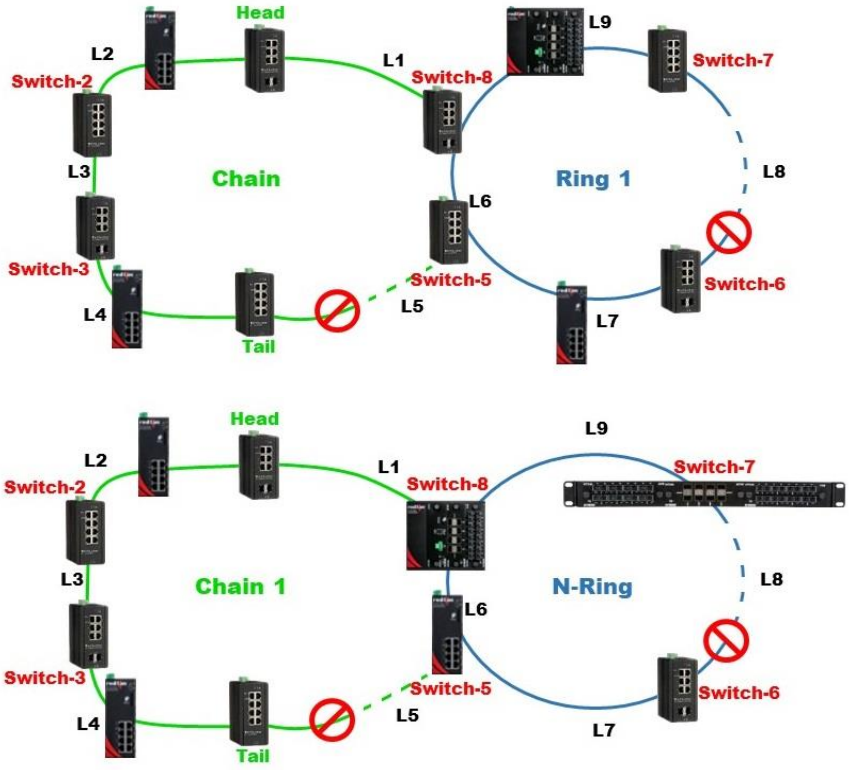
Group 1 – Ring-master and Ring-slave

- Both master and slave roles are supported for the ring.
- When the switch is set to master, one switch port is set as a forward port and another is set as a block port. The block port is not necessary. It is blocked in a normal state.
- When the switch is set to slave, both switch ports are set as forward ports.



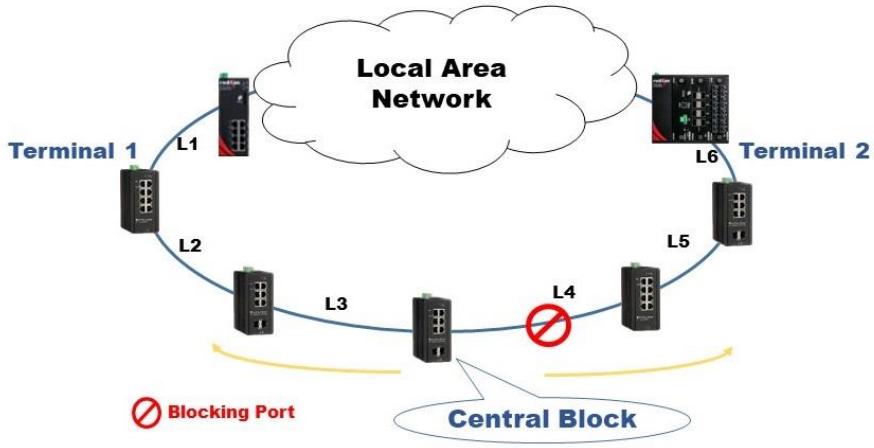
Group 2 – Chain and Balancing-Chain

- Chain - Port can be configured as head, tail or member.



- When the switch is set to chain-head, one of the switch ports is set as the head port and another is set as a member port. Both switch ports are forwarded in a normal state.
- When the switch is set to chain-tail, one of the switch ports is set as the tail port and another is set as a member port. The tail port is not necessary. It is blocked in a normal state.
- When the switch is set to chain-member, both switch ports are set as member ports. Both ring ports are forwarded in a normal state.

Group 3 – Balancing Chain



Note: The LAN network can be any type of network.

- When the switch is set to balancing-chain/central-block, one of the ring ports is a member port and another is a block port. The block port is not necessary. It is blocked in a normal state.
- When the switch is set as balancing-chain/terminal-1/2, one ring port is the terminal port and another is a member port. Both ring ports are forwarded in normal state.

- When the switch is set as balancing-chain/member, both ring ports are member ports. Both ring ports are forwarded in a normal state.

Note: Group 1 must be enabled before configuring group 2 as coupling.
Note: When Group 1 or Group 2 is enabled, the configuration of Group 3 is disabled.
Note: When Group 3 is enabled, the configuration of Group 1 and Group 2 is disabled.

Console and Web Configuration

Console Configuration

To configure the ring protection on the switch:

1. Login to the switch with the “admin” account using the CLI.
2. Go to configure mode through the CLI commands “cli”→“enable”→“configure terminal”.
3. Go to configure ring protection group using CLI commands "ringv2 protect group1" or "ringv2 protect group2".
4. Set all necessary parameters:
   For Node 1 and Node 1, select the ports that are connected with the other switch.
   For example, selecting Port 1 and Port 2 means that Port 1 is one of the ports connected to the other switch, as is Port 2.
   Then select one of the ring connection devices to be the “Master,” then accept the “Node 2 port” as the blocking port.
   node 1 interface GigabitEthernet 1/n (where n is a port number)
   node2 interface GigabitEthernet 1/n
   Role ring-master
   When the configuration is finished, enable ring protection by using the command “mode enable”.
   Note: Please pay attention to the status “Previous Command Result” after every action.

CLI Commands

```
Configure terminal
Ring protect group 1

node 1 interface GigabitEthernet 1/n
node2 interface GigabitEthernet 1/n
Role ring-master
Mode enable

Exit
```

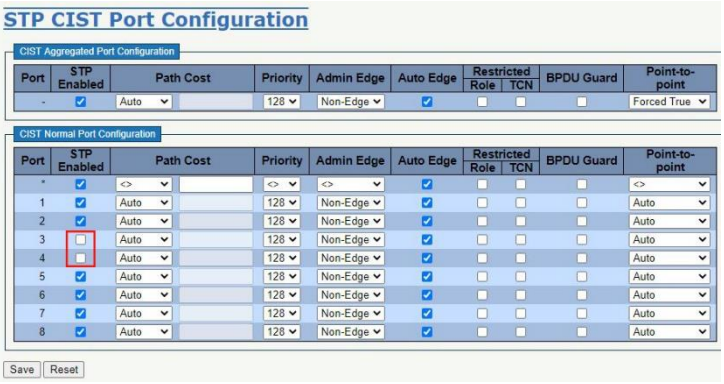
Web UI Configuration

The switch supports 2 ring groups (indices), including ring, chain, and balancing-chain.

Note: Group 1 must be enabled before configuring Group 2.
Note: When Group 1 or Group 2 is enabled, the configuration of Group 3 is unselectable.
Note: When Group 3 is enabled, the configuration of Group 1 and Group 3 is unselectable .

First Step - Disable STP on All Ring Ports

Disable STP mode on a switch that uses Ring and Chain.



1. Go to “Configuration→Spanning Tree→CIST Ports.
2. Do not enable STP global.
3. Click the "Save" button.

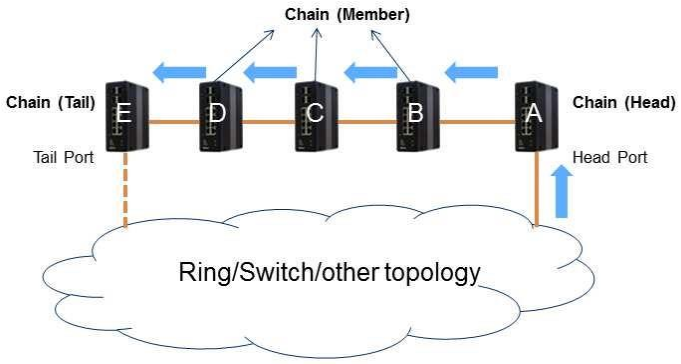
Ring Master

1. Go to “Configuration→Ringv2” Web page.
2. Enable Index 1, and Select Role as Ring(Master).
3. Select one port as "Forward Port", another as "Block Port"

Ring Slave

1. Go to “Configuration→Ringv2” Web page.
2. Enable Index 1, and Select Role as Ring(Slave).
3. Select two ports as "Forward Port".

Chain



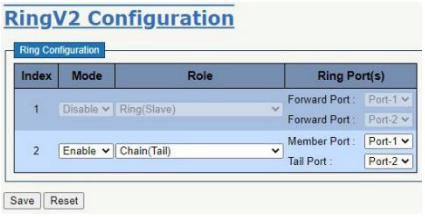
Chain (Member)

1. Go to “Configuration→RingV2” Web page.
2. Disable Index 1 and Index 2, then enable Index 3.
3. Change Role to "Chain(Member)".
4. Select two member ports for this chain member switch.

Chain (Head)

1. Go to “Configuration→Ringv2” Web page.
2. Disable Index 1 and Index 2, then enable Index 3.
3. Change Role to "Chain(Head)".
4. Select a member port and a head port for this chain head switch.

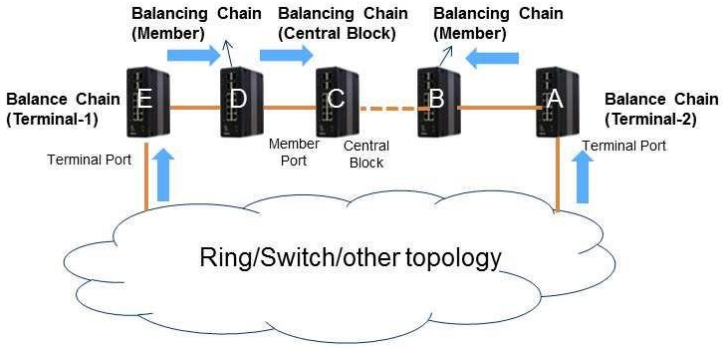
Chain(Tail)



1. Go to “Configuration→Ringv2” Web page.
2. Disable Index 1 and Index 2, then enable Index 3.

3. Change Role to "Chain(Tail)".
4. Select a member port and a tail port for this chain tail switch.

Balancing Chain



Balancing Chain(Central Block)

1. Go to “Configuration→Ringv2” Web page.
2. Disable Index 1 and Index 2, then enable Index 3.
3. Change Role to "Balancing Chain(Central Block)".
4. Select a member port and a block port for this central block switch.

Balancing Chain(Terminal-1 and -2)

1. Go to “Configuration→Ringv2” Web page.
2. Disable Index 1 and Index 2, then enable Index 3.
3. Change Role to "Balancing Chain(Terminal-1 or -2).
4. Select a member port and a terminal port for this balancing chain terminal switch.

QoS Scheduling and Shaping Configuration

This section guides users through the Quality of Service (QoS) related features.

QoS features allow you to allocate network resources to mission-critical applications at the expense of applications that are less sensitive to factors, such as time delays or network congestion. You can configure your network to prioritize specific types of traffic, ensuring that each traffic type is assigned the appropriate QoS level.

CoS Values and Prioritized Output Queues

The switch has eight output queues per port (Q0 to Q7). An egressing frame is placed into the queue corresponding to the frame's CoS (Class of Service) value. CoS=7 maps to Q7, CoS=6 maps to Q6, etc. Q7 is the highest priority queue and Q0 is the lowest.

A frame's 802.1p priority is normally found in the VLAN tag's PCP bits (Priority Code Point) and can range from PCP=0 to PCP=7. Each PCP value (PCP=0 to PCP=7) is mapped to one CoS value (CoS=0 to CoS=7). This mapping is configurable.

By default, the switch implements the IEEE 802.1Q-2005 recommendation on how to maps PCP values to priority. In particular, PCP=0 is the default "best effort" priority, while PCP=1 is the lowest "background" priority. This table shows the default relationship between PCP, CoS/Q, and priority.

PRIORITY 7 (HIGHEST)	PRIORITY 6	PRIORITY 5	PRIORITY 4	PRIORITY 3	PRIORITY 2	PRIORITY 1 (DEFAULT)	PRIORITY 0 (LOWEST)
NETWORK CONTROL	INTERWORK CONTROL	VOICE	VIDEO	CRITICAL APPLICATIONS	EXCELLENT EFFORT	BEST EFFORT	BACKGROUND
PCP=7	PCP=6	PCP=5	PCP=4	PCP=3	PCP=2	PCP=0	PCP=1
CoS=7/Q7	CoS=6/Q6	CoS=5/Q5	CoS=4/Q4	CoS=3/Q3	CoS=2/Q2	CoS=1/Q1	CoS=0/Q0

Scheduling and Shaping

The switch implements a QoS pipeline to manage traffic that egresses a port. The main components are:

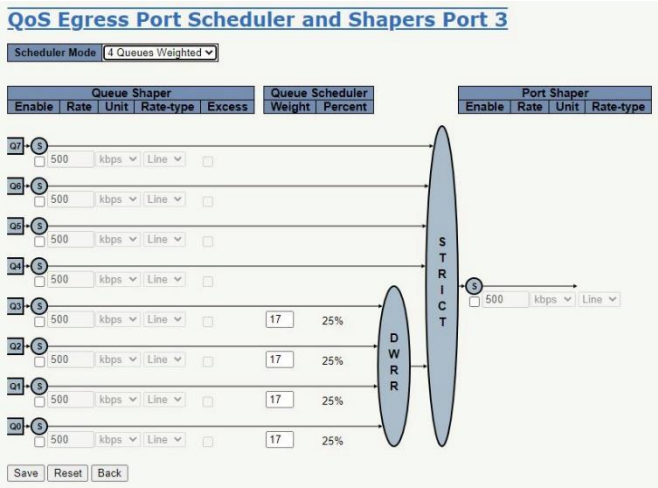
Queue Shaper: Rate limits output for each priority queue.

Use Excess Bandwidth Option: A queue may exceed its rate limit by using extra port bandwidth.

Queue Scheduling by Strict Priority: Output preference is given to the highest priority frame.

Queue Scheduling by Deficit Weighted Round Robin: 2 to 8 queues share output bandwidth.

Port Shaper: Rate limits the total output of the port.



Strict Priority (SP) Queue Scheduling

The highest priority frame will egress before any lower priority frame. If the outgoing traffic exceeds the port's bandwidth, then lower priority frames are dropped. This is the default scheduler mode.

Deficit Weighted Round Robin (DWRR) Queue Scheduling

DWRR allows the user to configure 2 to 8 of the output queues to share available bandwidth. This can allow traffic from the lowest priority queues to go out the port even when the port is congested. In other words, the lower priority traffic will not be starved out by higher priority traffic.

For DWRR, the user assigns weights to each output queue. These weights determine the percentage of the shared bandwidth that a queue can use.

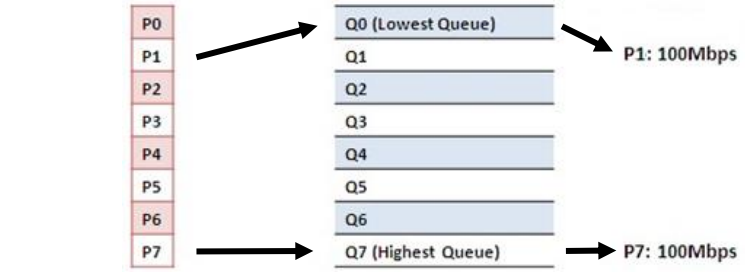
Example 1: SP Queue without Queue Shaping (Default)

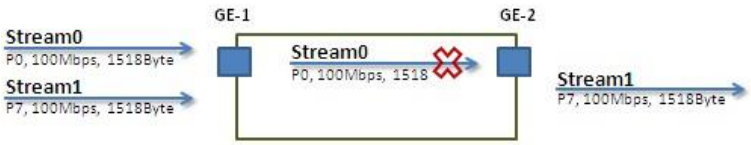
Two Streams (Stream0, Stream1) are sent from Port 1 to Port 2. Each Stream is 100 Mbps. Stream0 has PCP Priority 1, Stream1 has PCP Priority 7 in their VLAN tags. Set Port 2 link speed to 100Mbps.

Expected Result

Port 2 is expected to only output 100 Mbps of Stream1, and Stream0 will be discarded. This demonstrates how SP works.

Gigabit Port VLAN Priority & Queue Mapping





Stream0:

Dst Mac : 00:00:00:00:20:01
Src Mac : 00:00:00:00:10:01
VLAN : 100
VLAN PCP : 1
Send rate : 100Mbps
Packet length: 1518bytes

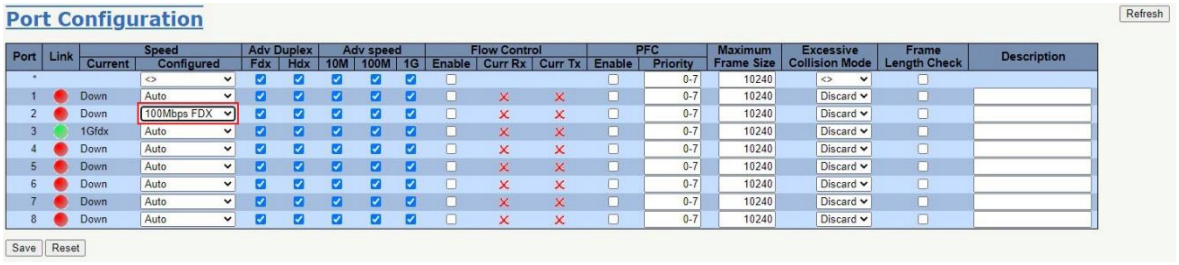
Stream1:

Dst Mac : 00:00:00:00:20:02
Src Mac : 00:00:00:00:10:02
VLAN : 100
VLAN PCP: 7
Send rate : 100Mbps

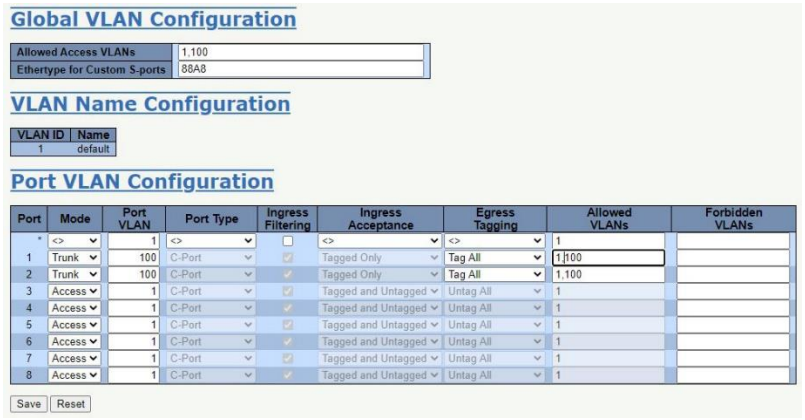
Packet length: 1518bytes

Web Management

1. Go to Configuration→Ports→set Port 2 link speed to 100Mbps full duplex.



2. Select Configuration→VLANs→Create a VLAN with VLAN ID 100. Enter a VLAN name in the Name field. Here we set tagged VLAN100 on Port 1 and Port 2.



CLI Commands

```
interface GigabitEthernet 1/1
switchport trunk native vlan 100
switchport trunk allowed vlan 1,100
switchport trunk vlan tag native
switchport mode trunk
!
interface GigabitEthernet 1/2
switchport trunk native vlan 100
switchport trunk allowed vlan 1,100
switchport trunk vlan tag native
switchport mode trunk
```

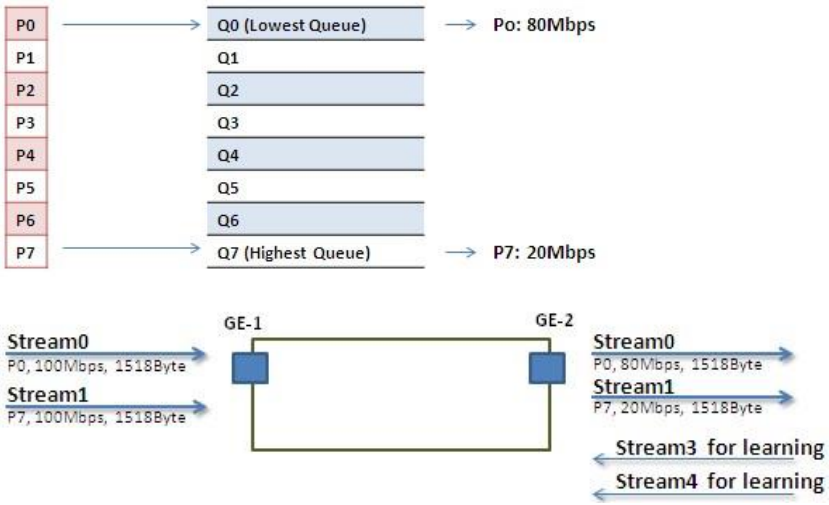
Example 2: SP Queues with Queue Shaping

Two Streams (Stream0, Stream1) are sent from Port 1 to Port 2. Each stream is 100Mbps. Stream0 includes PCP Priority 0, Stream1 includes PCP Priority 7 in their VLAN tags. Stream3 and Stream4 are for learning the MAC addresses only, which makes sure the traffic is not flooding.

Expected Result

Port 2 can receive 20Mbps of Stream1, and 80Mbps of Stream0. This case shows users how SP.

VDSL Port VLAN Priority & Queue Mapping



Stream0:

Dst Mac : 00:00:00:00:20:01
Src Mac : 00:00:00:00:10:01
VLAN : 100
VLAN PCP : 0
Send rate : 100Mbps
Packet length: 1518bytes

Stream1:

Dst Mac : 00:00:00:00:20:02
Src Mac : 00:00:00:00:10:02
VLAN : 100
VLAN PCP: 7
Send rate : 100Mbps
Packet length: 1518bytes

Stream3: (for Learning)

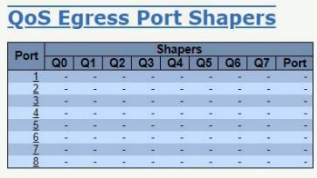
Dst Mac : 00:00:00:00:10:01
Src Mac : 00:00:00:00:20:01
VLAN : 100
VLAN PCP: 0
Send rate : 10Mbps
Packet length: 1518bytes

Stream4: (for Learning)

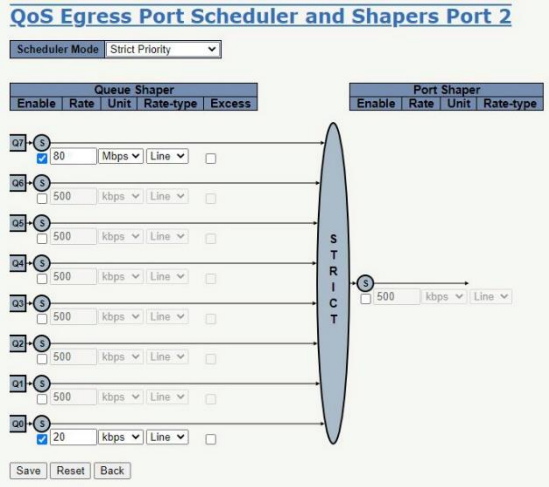
Dst Mac : 00:00:00:00:10:02
Src Mac : 00:00:00:00:20:02
VLAN : 100
VLAN PCP: 0
Send rate : 10Mbps
Packet length: 1518bytes

Web Management

1. Go to Configuration→Qos→Port Shaping, to create a Qos profile on Port 2.



2. Select schedule mode be “Strict Priority” and set shaping rate for queue 0 and queue 7 as below.



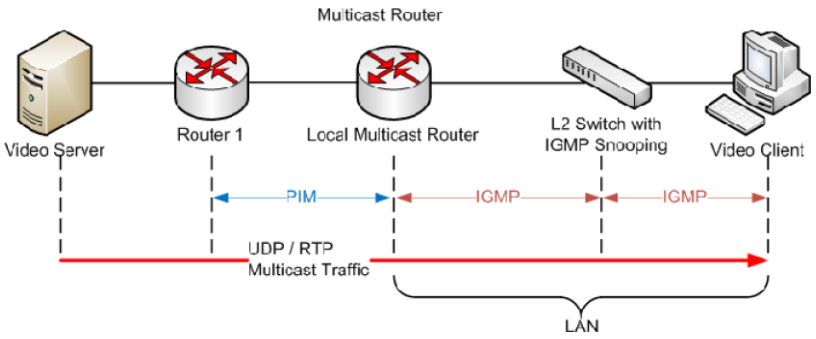
CLI Commands

```
interface GigabitEthernet 1/1
switchport trunk native vlan 100
switchport trunk allowed vlan 1,100
switchport trunk vlan tag native
switchport mode trunk

interface GigabitEthernet 1/2
switchport trunk native vlan 100
switchport trunk allowed vlan 1,100
switchport trunk vlan tag native
switchport mode trunk
qos queue-shaper queue 0 20 mbps
qos queue-shaper queue 7 80 mbps
qos tag-remark mapped
```

IGMP Configuration

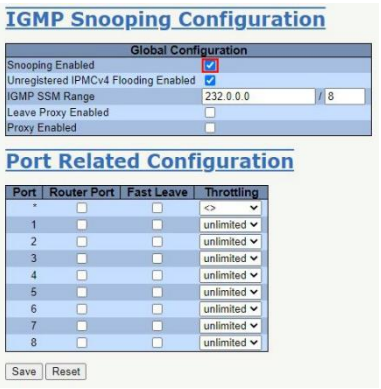
IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast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

IGMP ensures that a multicast traffic stream routes from the server to only the ports where clients have requested membership in that stream’s multicast group. It keeps multicast traffic from flooding to a port that does not need the multicast stream and creating unnecessary traffic on a network. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

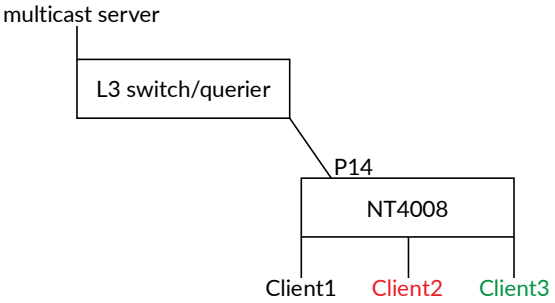


Example 1 Basic IGMP

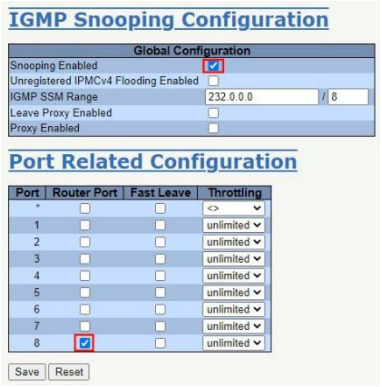
An administrator can enable IGMP-controlled streaming for every client by going to Configuration→IPMC→Basic Configuration and selecting the check box “Snooping Enable”.



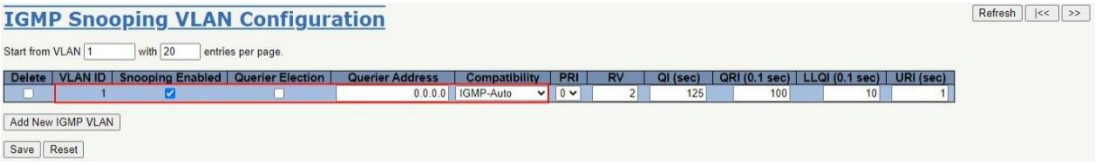
Example 2 Require Clients to Join Groups



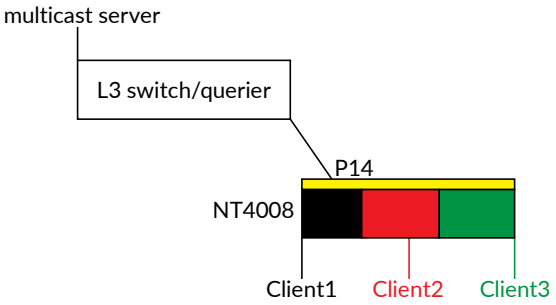
1. Go to Configuration→IPMC→Basic Configuration to select the check box “Snooping Enable”.
2. Deselect the check box of "Unregistered IPMCv4 Flooding Enabled".
3. If the Multicast stream is from an L3 switch, then the uplink port must be a “Router Port”.
   Note: If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.



4. Go to Configuration→IPMC→VLAN Configuration to select the check box of “Snooping Enable” and set VLAN ID of Port 14.

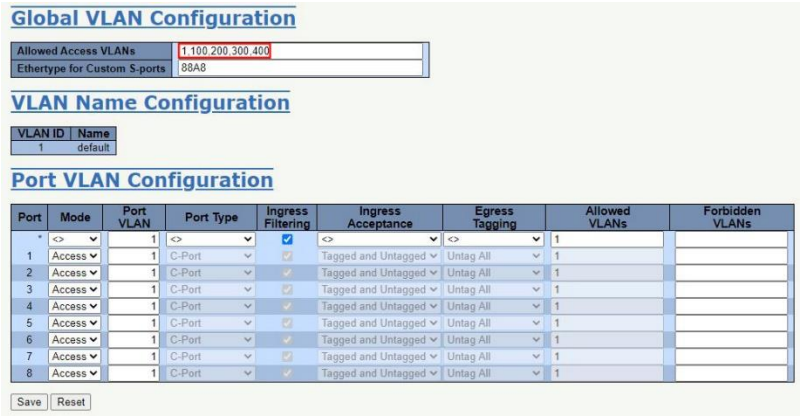


Example 3 IGMP on Multiple VLANs

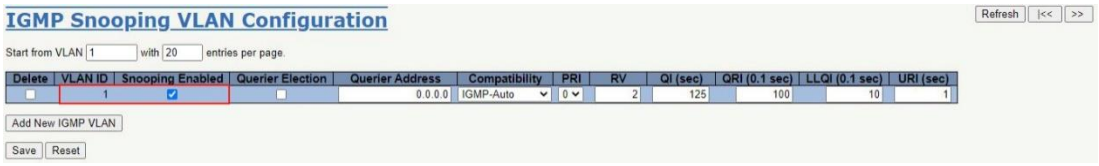


In this scenario, these clients belong to multiple VLANs; the user must create one more VLAN to be the agent for all client VLANs.

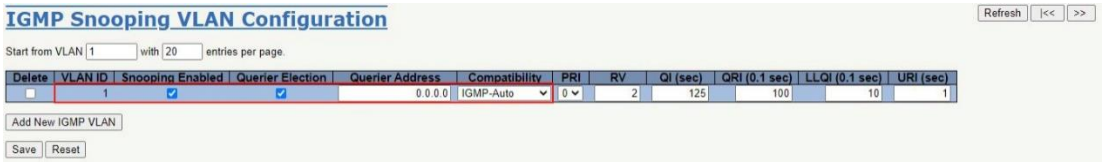
1. To create a VLAN: go to Configuration→VLANs→Allow Access VLANs, then set Port 14 be vlan200 member port.



2. Go to Configuration→IPMC→VLAN Configuration to select the check box of “Snooping Enable” and set VLAN ID of Port 14.



3. If there is no querier on the L3 switch, to the user must select “Querier Election”, and set the “Querier Address” to the same network as uplink interface.
4. Select the IGMP version as server.



Appendix A CLI Commands

Introduction

This appendix describes the CLI operator interface provided in the Red Lion Controls NT4008 switch.

The Command Line Interface (CLI) can be accessed by connecting a host device to the console port on the switch. Once connected, the switch will appear as a serial connection. A standard terminal application may be used to communicate to the switch through the serial connection. For detailed information, see the “Console Connection” section of the NT4008 Hardware Manual.

There are two additional methods for connecting to the CLI: Telnet and SSH. Using any standard Telnet client, simply enter the IP address of the switch to start a connection to the CLI. SSH, the secure alternative to Telnet, can also be used with any standard SSH client by entering the IP address of the switch to start a secure connection to the CLI.

The CLI contains some status and configuration capability. To interact with the CLI, a login is required. Both the default username and default password are 'admin'. After loggin in using the default password, the admin user will be prompted to change it. Once logged in, a listing of available commands can be obtained through the help interface. This is accessible by typing either “?” or “help” The following commands are available:

Connection Interface

To connect a host PC to the Console port, an RJ45 (male) connector-to-RS232 DB9 (female) connector cable is required. This is supplied with the switch. For details see the Hardware Guide.

INTERFACE	PARAMETER
Console	Baud rate: 115200bps Data bit: 8 Parity: None Stop bit: 1 Flow Control: None
Telnet	Port 23
SSH	Port 22 (In Windows, you can run terminal emulator such as PuTTY)

Authorization Levels

LEVEL	DESCRIPTION
Superuser	Superuser can access all management features.
Engineer	Engineer can access all management features except user account management.
Guest (default)	Read-only mode (guest can only change his own password). Users of this level can query pages like PM and FM.

Login Example

```
Username: admin

Password:

nt4008dm2pnc# show v

version  vlan

nt4008dm2pnc# show version
```

```
MAC Address       : 84-e3-27-52-48-3c
```

```
Serial Number     : 0

Previous Restart  : Cold

System Contact    :
System Name       : nt4008dm2pnc
System Location   :
System Time       : 2020-10-05T15:05:47+00:00
System Uptime     : 4d 21:54:15



Bootloader
----------
Image             : RedBoot (bootloader)
Version           : version v00.00.03B01
Date              : 00:32:52, Sep  2 2020

Active Image
------------
Image             : linux (primary)
Version           : 1.0.3
Date              : 2020-09-02T00:59:20+08:00
Upload filename   : firmware.img

Backup Image
------------
Image             : linux.bk (backup)
Version           : 1.0.3
Date              : 2020-09-02T00:59:20+08:00
Upload filename   : NT-4008-DM2-PN-C_1.0.3.img


------------------
```

```
SID : 1

------------------

Board Type        : NT-4008-DM2-PN-C

Port Count        : 8
```

```
Product           : NT-4008-DM2-PN-C

Software Version  : 1.0.3

Build Date        : 2020-09-02T00:59:20+08:00


nt4008dm2pnc#
```

Execution Modes

The CLI contains several execution modes. Users will see different sets of commands under different execution modes. When users enter an execution mode, the corresponding mode prompt will appear on the screen automatically. Table 1 lists all of the execution modes, their access levels, and mode prompts.

Table 1: List of Execution Modes

MODE	ACCESS LEVEL	TO ENTER MODE	PROMPT
Initial Mode	Guest	login, disable	>
Enable Mode	Guest	enable	#
Configure Mode	Engineer	configure terminal	(config)#
Interface Gigabit Configure Mode	Engineer	interface GigabitEthernet <portNo>	(config-if)#
Interface 2.5Gigabit Configure Mode	Engineer	interface 2.5GigabitEthernet <portNo>	(config-if)#
Interface LLAG Configure Mode	Engineer	interface llag <number>	(config-llag)#
Interface VLAN Configure Mode	Engineer	interface vlan <vlanid>	(config-if-vlan)#
IP DHCP Pool Configure Mode	Engineer	ip dhcp pool <name>	(config-dhcp-pool)#
Alarm Profile Configure Mode	Engineer	profile alarm	(alm-profile-config)#
RingV2 Group1 Configure Mode	Engineer	ringv2 protect group1	(config-ringv2-group1)#
RingV2 Group2 Configure Mode	Engineer	ringv2 protect group2	(config-ringv2-group2)#
Line Terminal Configure Mode.	Engineer	line <number> line console <number> line vty <number>	(config-line)#
Media Redundancy Protocol (MRP) Group 1 Configure Mode.	Engineer	mrp group 1	(profinet-mrp1-config)#
Media Redundancy Protocol (MRP) Group 2 Configure Mode.	Engineer	mrp group 2	(profinet-mrp2-config)#
PROFINET Configure Mode.	Engineer	profinet	(profinet-config)#
Spanning Tree Aggregation Configure Mode.	Engineer	spanning-tree aggregation	(config-stp-aggr)#
IC Profile Configure Mode	Engineer	ipmc profile <word16>	(config-ipmc-profile)#

Help

A user can get help by entering a question mark '?' at any position in the command. The displayed result depends on the execution mode and previous input. Entering a question mark again on the same command will display the command syntax.

Terminal Key Function

Following is the list of all the terminal keys and their functions.

Table 2: List of Terminal Keys

KEYS	FUNCTION
ENTER	Run a CLI config script
CTRL-M	
TAB	Tab completion If Tab is pressed after a non-whitespace character, this completes the word before the Tab. If Tab is pressed after a whitespace character, this completes the next word.
CTRL-I	
?	Display available commands If ? is pressed after a non-whitespace character, this shows possible choices for this word. If ? is pressed after a whitespace character, this shows possible choices for the next word.
<Up Arrow>	Up history
CTRL-P	
<Down Arrow>	Down history
CTRL-N	
Home	Move the cursor to the beginning of the input line
CTRL-A	
End	Move the cursor to the end of the input line
CTRL-E	
<Left Arrow>	Move the cursor backward
CTRL-B	
<Right Arrow>	Move the cursor forward
CTRL-F	
BACKSPACE	Erase the character before the cursor
CTRL-H	

Notation Conventions

The notation conventions for the parameter syntax of each CLI command are as follows:

- Parameters enclosed in [ ] are optional.
- Parameter values are separated by a vertical bar "|" only when one of the specified values can be used.
- Parameter values are enclosed in { } when you must use one of the values specified.

Initialize (Disable) Mode Commands

To enter this mode type “disable” after logging in to the switch. To return to this type end under any other mode and then “disable”.

clear

Description	Clear Address Conflict Detection.
Syntax	• clear ip acd
Example	• clear ip acd

disable

Description	Turn off privileged commands.
Syntax	• disable [<new_priv>]
Examples	• disable • disable 3

do

Description	Run exec commands in the configuration mode.
Syntax	• do <command>
Example	• do show running-config

enable

Description	Turn on privileged commands.
Syntax	• enable [<new_priv>]
Examples	• enable • enable 5

exit

Description	Logs out of the switch.
Syntax	• exit
Example	• exit

help

Description	Description of the interactive help system.
Syntax	• help
Example	• help

logout

Description	Exit from EXEC mode.
Syntax	• logout
Example	• logout

ping

Description	Send ICMP echo messages.
Syntax	• ping ip { <domain_name> | <ip_addr> } [ttl <ttl_value>] [repeat <count>] [{ saddr <src_addr> | sif { <port_type> <src_if> | vlan <vlan_id> } }] [size <size>] [data <data_value>] [{ verbose | quiet }] • ping ipv6 { <domain_name> | <ip_addr> } [repeat <count>] [saddr <src_addr>] [sif { <port_type> <src_if> | vlan <vlan_id> }] [size <size>] [data <data_value>] [{ verbose | quiet }]
Example	• ping ip 192.0.2.11

show

Description	Show various settings.
Syntax	• show alarm { history | current } • show clock • show clock detail • show history • show interface (<port_type> [<in_port_list>]) switchport [access | trunk | hybrid] • show interface (<port_type> [<v_port_type_list>]) capabilities • show interface (<port_type> [<v_port_type_list>]) statistics [{ packets | bytes | errors | discards | filtered | dot3br | { priority [<priority_v_0_to_7>] } }] [{ up | down }] • show interface (<port_type> [<v_port_type_list>]) status [err-disable] • show interface (<port_type> [<v_port_type_list>]) veriphy • show ip acd • show ip arp • show ip arp inspection [interface (<port_type> [<in_port_type_list>]) | vlan <in_vlan_list>] • show ip dhcp detailed statistics { server | client | snooping | relay | normal-forward | combined } [interface (<port_type> [<in_port_list>])] • show ip dhcp excluded-address • show ip dhcp pool [<pool_name>] • show ip dhcp relay [statistics] • show ip dhcp server • show ip dhcp server binding <ip> • show ip dhcp server binding [state { allocated | committed | expired }] [type { automatic | manual | expired }] • show ip dhcp server declined-ip • show ip dhcp server declined-ip <declined_ip> • show ip dhcp server statistics • show ip dhcp snooping [interface (<port_type> [<in_port_list>])] • show ip domain • show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail] • show ip igmp snooping mrouter [detail] • show ip interface [brief] • show ip name-server • show ip route • show ip statistics [system] • show ip verify source [interface (<port_type> [<in_port_type_list>])] • show ipv6 interface [brief] • show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail] • show ipv6 mld snooping mrouter [detail] • show ipv6 neighbor • show ipv6 route • show ipv6 statistics [system] [interface vlan <vlan_list>] • show line [alive] • show lldp med media-vlan-policy [<v_0_to_31>] • show lldp med remote-device [interface (<port_type> [<port_list>])] • show lldp neighbors [interface (<port_type> [<v_port_type_list>])] • show lldp preempt [interface (<port_type> [<v_port_type_list>])] • show lldp statistics [interface (<port_type> [<v_port_type_list>])]

	• show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>]) | vlan <v_vlan_id_2>] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])] • show port-security [interface (<port_type> [<plist>])] • show port-security address [interface (<port_type> [<plist>])] • show privilege • show profile alarm • show profinet mrp { <groupIdx> | all } • show profinet name • show ringv2 • show sflow • show sflow statistics { receiver [<rcvr_idx_list>] | samplers [interface [<samplers_list>] (<port_type> [<v_port_type_list>])] } • show svl { [fid [<fid_list>]] | [vlan [<vlan_list>]] } • show switchport forbidden [{ vlan <vlan_list> } | { name <name> }] • show system cpu status • show terminal • show users [myself] • show version [brief] • show web privilege group [<group_name>] level •
Examples	• show interface GigabitEthernet 1/1 status • show mac address-table

traceroute

Description	Send IP Traceroute messages.
Syntax	• traceroute ip { <domain_name> | <ip_addr> } [dscp <dscp>] [timeout <timeout>] [{ saddr <src_addr> | sif { <port_type> <src_if> | vlan <vlan_id> } }] [probes <probes>] [firstttl <firstttl>] [maxttl <maxttl>] [icmp] [numeric] • traceroute ipv6 { <domain_name> | <ip_addr> } [dscp <dscp>] [timeout <timeout>] [saddr <src_addr>] [sif { <port_type> <src_if> | vlan <vlan_id> }] [probes <probes>] [maxttl <maxttl>] [numeric]
Example	• traceroute ip 192.0.2.11 timeout 30 icmp dscp 12

Enable Mode Commands

This is the default mode available after logging in to the CLI.
All commands in this mode can be executed from any other mode using the “do” command.

clear

Description	Clear various settings.
Syntax	• clear access management statistics • clear access-list ace statistics • clear ip acd • clear ip arp • clear ip dhcp detailed statistics { server | client | snooping | relay | helper | all } [interface (<port_type> [<in_port_list>])] • clear ip dhcp relay statistics • clear ip dhcp server binding <ip> • clear ip dhcp server binding type { automatic | manual | expired } • clear ip dhcp server statistics • clear ip dhcp snooping statistics [interface (<port_type> [<in_port_list>])] • clear ip igmp snooping [vlan <v_vlan_list>] statistics • clear ip statistics • clear ipv6 mld snooping [vlan <v_vlan_list>] statistics • clear ipv6 neighbors • clear ipv6 statistics • clear lacp statistics • clear lldp statistics { [interface (<port_type> [<plist>])] | global } • clear logging [informational] [notice] [warning] [error] [switch <switch_list>] • clear mac address-table • clear port-security dynamic [{ address <mac> [vlan <vlan_on_mac>] } | { interface (<port_type> [<plist>]) [vlan <vlan_on_interface>] } | vlan <vlan>] • clear sflow statistics { receiver [<receiver_index_list>] | samplers [interface [<samplers_list>] (<port_type> [<v_port_type_list>])] } • clear spanning-tree { { statistics [interface (<port_type> [<v_port_type_list>])] } | { detected-protocols [interface (<port_type> [<v_port_type_list_1>])] } } • clear statistics [interface] (<port_type> [<v_port_type_list>])
Examples	• clear ip dhcp relay statistics • clear mac address-table • clear ip dhcp server binding type expired

configure

Description	Enter configuration mode.
Syntax	• configure terminal
Example	• configure terminal

copy

Description	Copy files.
Syntax	• copy { startup-config | running-config | <source_path> } { startup-config | running-config | <destination_path> } [syntax-check]
Examples	• copy running-config startup-config syntax-check • copy flash:profinet_log.dat tftp://mytftpserver/profinetlog.txt

delete

Description	Deletes a file in the "flash:" file system.
Syntax	• delete <path>
Example	• delete flash:profinet_log.dat

dir

Description	List all files in the "flash:" file system.
Syntax	• dir
Example	• dir

disable

Description	Turn off privileged commands.
Syntax	• disable [<new_priv>]
Examples	• disable • disable 3

do

Description	Run exec commands in the configuration mode.
Syntax	• do <command>
Example	• do show running-config

enable

Description	Turn on privileged commands.
Syntax	• enable [<new_priv>]
Examples	• enable • enable 5

exit

Description	Exit from EXEC mode.
Syntax	• exit
Example	• exit

firmware

Description	Firmware upgrade/swap.
Syntax	• firmware swap • firmware upgrade <url_file>
Example	• firmware swap

help

Description	Description of the interactive help system.
Syntax	• help
Example	• help

ip

Description	IPv4 commands.
Syntax	• ip dhcp retry interface vlan <vlan_id>
Example	• ip dhcp retry interface vlan 2

ipv6

Description	IPv6 configuration commands.

Syntax	• ipv6 dhcp-client restart [interface vlan <v_vlan_list>]
Examples	• ipv6 dhcp-client restart • ipv6 dhcp-client restart interface vlan 2,3-5

logout

Description	Exit from EXEC mode.
Syntax	• logout
Example	• logout

more

Description	Display file.
Syntax	• more <path>
Examples	• more tftp://server/path-and-filename • more flash:path-and-filename

no

Description	Reset settings to defaults.
Syntax	• no debug gdbserver • no debug interrupt monitor [source <intr_name>] • no debug ipv6 nd • no debug trace hunt • no terminal editing • no terminal exec-timeout • no terminal history size • no terminal length • no terminal width
Example	• no terminal history size

ping

Description	Send ICMP echo messages.
Syntax	• ping ip { <domain_name> | <ip_addr> } [ttl <ttl_value>] [repeat <count>] [{ saddr <src_addr> | sif { <port_type> <src_if> | vlan <vlan_id> } }] [size <size>] [data <data_value>] [{ verbose | quiet }] • ping ipv6 { <domain_name> | <ip_addr> } [repeat <count>] [saddr <src_addr>] [sif { <port_type> <src_if> | vlan <vlan_id> }] [size <size>] [data <data_value>] [{ verbose | quiet }]
Example	• ping ip 192.0.2.11

platform

Description	Platform configuration.
Syntax	• platform debug { allow | deny }
Example	• platform debug allow

reload

Description	Reload system and reset configuration to factory defaults.
Syntax	• reload { { { cold | warm } [sid <usid>] } | { defaults [keep-ip] } }
Examples	• reload cold • reload defaults

send

Description	Send a message to other TTY lines. The command requires a delimiter character. After pressing enter all the text typed before the delimiter character is found will be sent to the specified TTY line.
Syntax	• send { * | <session_list> | console 0 | vty <vty_list> } <message>
Example	• send * . hello.

show

Description	Show running system information.
Syntax	• show access management [statistics | <access_id_list>] • show access-list [interface [(<port_type> [<v_port_type_list>])]] [rate-limiter [<rate_limiter_list>]] [ace statistics [<ace_list>]] • show access-list ace-status [static] [link-oam] [loop-protect] [dhcp] [ptp] [upnp] [arp-inspection] [evc] [mep] [ipmc] [ip-source-guard] [ip-mgmt] [tt-loop] [y1564] [ztp] [ip] [conflicts] [switch <switch_list>] • show aggregation [mode] • show alarm { history | current } • show clock • show clock detail • show history • show interface (<port_type> [<in_port_list>]) switchport [access | trunk | hybrid] • show interface (<port_type> [<v_port_type_list>]) capabilities • show interface (<port_type> [<v_port_type_list>]) statistics [{ packets | bytes | errors | discards | filtered | dot3br | { priority [<priority_v_0_to_7>] } }] [{ up | down }] • show interface (<port_type> [<v_port_type_list>]) status [err-disable] • show interface (<port_type> [<v_port_type_list>]) veriphy • show interface vlan [<vlist>] • show ip acd • show ip arp • show ip arp inspection [interface (<port_type> [<in_port_type_list>]) | vlan <in_vlan_list>] • show ip arp inspection entry [dhcp-snooping | static] [interface (<port_type> [<in_port_type_list>])] • show ip dhcp detailed statistics { server | client | snooping | relay | normal-forward | combined } [interface (<port_type> [<in_port_list>])] • show ip dhcp excluded-address • show ip dhcp pool [<pool_name>] • show ip dhcp relay [statistics] • show ip dhcp server • show ip dhcp server binding <ip> • show ip dhcp server binding [state { allocated | committed | expired }] [type { automatic | manual | expired }] • show ip dhcp server declined-ip • show ip dhcp server declined-ip <declined_ip> • show ip dhcp server statistics • show ip dhcp snooping [interface (<port_type> [<in_port_list>])] • show ip dhcp snooping table • show ip domain • show ip http • show ip igmp snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail] • show ip igmp snooping mrouter [detail] • show ip interface [brief] • show ip name-server • show ip route • show ip source binding [dhcp-snooping | static] [interface (<port_type> [<in_port_type_list>])] • show ip ssh • show ip statistics [system] • show ip telnet • show ip verify source [interface (<port_type> [<in_port_type_list>])]

	• show ipmc profile [<profile_name>] [detail] • show ipmc range [<entry_name>] • show ipv6 dhcp-client [interface vlan <v_vlan_list>] • show ipv6 interface [brief] • show ipv6 mld snooping [vlan <v_vlan_list>] [group-database [interface (<port_type> [<v_port_type_list>])] [sfm-information]] [detail] • show ipv6 mld snooping mrouter [detail] • show ipv6 neighbor • show ipv6 route • show ipv6 statistics [system] [interface vlan <vlan_list>] • show lacp { internal | statistics | system-id | neighbor } [details] • show line [alive] • show lldp med media-vlan-policy [<v_0_to_31>] • show lldp med remote-device [interface (<port_type> [<port_list>])] • show lldp neighbors [interface (<port_type> [<v_port_type_list>])] • show lldp preempt [interface (<port_type> [<v_port_type_list>])] • show lldp statistics [interface (<port_type> [<v_port_type_list>])] • show logging <log_id> [switch <switch_list>] • show logging [informational] [notice] [warning] [error] [switch <switch_list>] • show loop-protect [interface (<port_type> [<plist>])] • show mac address-table [conf | static | aging-time | { { learning | count } [interface (<port_type> [<v_port_type_list>]) | vlan <v_vlan_id_2>] } | { address <v_mac_addr> [vlan <v_vlan_id>] } | vlan <v_vlan_id_1> | interface (<port_type> [<v_port_type_list_1>])] • show monitor [session { <session_number> | all | remote }] • show ntp status • show platform debug • show platform phy [interface (<port_type> [<v_port_type_list>])] • show platform phy id [interface (<port_type> [<v_port_type_list>])] • show platform phy instance • show port-security [interface (<port_type> [<plist>])] • show port-security address [interface (<port_type> [<plist>])] • show privilege • show process list [detail] • show process load • show profile alarm • show profinet mrp { <groupIdx> | all } • show profinet name • show qos [{ interface [(<port_type> [<port>])] } | wred | { maps [dscp-cos] [dscp-ingress-translation] [dscp-classify] [cos-dscp] [dscp-egress-translation] [{ ingress [<ing_id>] }] [{ egress [<egr_id>] }] } | storm | { qce [<qce>] }] • show ringv2 • show rmon alarm [<id_list>] • show rmon event [<id_list>] • show rmon history [<id_list>] • show rmon statistics [<id_list>] • show running-config [all-defaults] • show running-config feature <feature_name> [all-defaults] • show running-config interface (<port_type> [<list>]) [all-defaults] • show running-config interface vlan <list> [all-defaults] • show running-config line { console | vty } <list> [all-defaults] • show running-config vlan { [<vlan_list>] } [all-defaults] • show sflow • show sflow statistics { receiver [<rcvr_idx_list>] | samplers [interface [<samplers_list>] (<port_type> [<v_port_type_list>])] } • show snmp • show snmp access [<group_name> [{ v1 | v2c | v3 | any } [{ auth | noauth | priv }]]] • show snmp community [<community>] • show snmp host [<conf_name>] • show snmp mib context • show snmp mib ifmib ifIndex [port] [aggregation] [vlan] • show snmp security-to-group [{ v1 | v2c | v3 } [<security_name>]] • show snmp trap [<source_name>] • show snmp user [<username> [<engineID>]]

	• show snmp view [<view_name> [<oid_subtree>]] • show spanning-tree [summary | active | { interface (<port_type> [<v_port_type_list>]) } | { detailed [interface (<port_type> [<v_port_type_list_1>])] } | { mst [configuration | { <instance> [interface (<port_type> [<v_port_type_list_2>])] }] }] • show svl { [fid [<fid_list>]] | [vlan [<vlan_list>]] } • show switchport forbidden [{ vlan <vlan_list> } | { name <name> }] • show system cpu status • show terminal • show user-privilege • show users [myself] • show version [brief] • show vlan [id <vlan_list> | name <name> | brief] [all] • show vlan ip-subnet [<ipv4>] • show vlan mac [address <mac_addr>] • show vlan protocol [eth2 { <etype> | arp | ip | ipx | at }] [snap { <oui> | rfc-1042 | snap-8021h } <pid>] [llc <dsap> <ssap>] • show vlan status [interface (<port_type> [<plist>])] [admin | all | combined | conflicts | erps | evc | gvrp | mep | mstp | mvr | nas | rmirror | vcl | voice-vlan] • show web privilege group [<group_name>] level
Examples	• show running-config • show qos interface GigabitEthernet 1/1 • show interface vlan 1

terminal

Description	Set terminal line parameters.
Syntax	• terminal editing • terminal exec-timeout <min> [<sec>] • terminal help • terminal history size <history_size> • terminal length <lines> • terminal width <width>
Examples	• terminal exec-timeout 30 50 • terminal length 250

traceroute

Description	Send IP Traceroute messages.
Syntax	• traceroute ip { <domain_name> | <ip_addr> } [dscp <dscp>] [timeout <timeout>] [{ saddr <src_addr> | sif { <port_type> <src_if> | vlan <vlan_id> } }] [probes <probes>] [firstttl <firstttl>] [maxttl <maxttl>] [icmp] [numeric] • traceroute ipv6 { <domain_name> | <ip_addr> } [dscp <dscp>] [timeout <timeout>] [saddr <src_addr>] [sif { <port_type> <src_if> | vlan <vlan_id> }] [probes <probes>] [maxttl <maxttl>] [numeric]
Example	• traceroute ip 192.0.2.11 timeout 30 icmp dscp 12

veriphy

Description	Run veriphy cable diagnostics.
Syntax	• veriphy [{ interface (<port_type> [<v_port_type_list>]) }]
Examples	• veriphy interface GigabitEthernet 1/1 • veriphy

Configure Mode Commands

To enter this execution mode type "**configure terminal**"under any execution mode.

access

Description	Access management configuration. It is used to specify access management entries. Up to 16 entries can be added.
Syntax	• access management <access_id> <access_vid> <start_addr> [to <end_addr>] { [web] [snmp] [telnet] | all }
Examples	• access management 1 1 192.0.0.3 to 192.0.2.5 SNMP • access management 1 1 192.0.0.3 all

access-list

Description	Configure access control lists and rate limits. Up to 128 access control entries can be specified. Access control filter policies can be specified by value, bitmask, and frame type. Entries can be port specific or by VLAN. The access control actions can be monitored with mirroring and logging. VLAN filters can also be used. Additionally rate-limiting policies can be implemented. Up to 16 rate-limiting configurations can be specified, using packets per second (pps) or kilobits per second (kbps).
Syntax	• access-list rate-limiter [<rate_limiter_list>] { pps <pps_rate> | 10pps <pps10_rate> | 100pps <pps100_rate> | 25kbps <kpbs25_rate> | 100kbps <kpbs100_rate> } • access-list ace [update] <ace_id> [next { <ace_id_next> | last }] [ingress { switch <ingress_switch_id> | switchport { <ingress_switch_port_id> | <ingress_switch_port_list> } | interface { <port_type> <ingress_port_id> | (<port_type> [<ingress_port_list>]) } | any }] [policy <policy> [policy-bitmask <policy_bitmask>]] [tag { tagged | untagged | any }] [vid { <vid> | any }] [tag-priority { <tag_priority> | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7 | any }] [dmac-type { unicast | multicast | broadcast | any }] [frame-type { any | etype [etype-value { <etype_value> | any }] [smac { <etype_smac> | any }] [dmac { <etype_dmac> | any }] | arp [sip { <arp_sip> | any }] [dip { <arp_dip> | any }] [smac { <arp_smac> | any }] [arp-opcode { arp | rarp | other | any }] [arp-flag [arp-request { <arp_flag_request> | any }] [arp-smac { <arp_flag_smac> | any }] [arp-tmac { <arp_flag_tmac> | any }] [arp-len { <arp_flag_len> | any }] [arp-ip { <arp_flag_ip> | any }] [arp-ether { <arp_flag_ether> | any }]] | ipv4 [sip { <sipv4> | any }] [dip { <dipv4> | any }] [ip-protocol { <ipv4_protocol> | any }] [ip-flag [ip-ttl { <ip_flag_ttl> | any }] [ip-options { <ip_flag_options> | any }] [ip-fragment { <ip_flag_fragment> | any }]] | ipv4-icmp [sip { <sipv4_icmp> | any }] [dip { <dipv4_icmp> | any }] [icmp-type { <icmpv4_type> | any }] [icmp-code { <icmpv4_code> | any }] [ip-flag [ip-ttl { <ip_flag_icmp_ttl> | any }] [ip-options { <ip_flag_icmp_options> | any }] [ip-fragment { <ip_flag_icmp_fragment> | any }]] | ipv4-udp [sip { <sipv4_udp> | any }] [dip { <dipv4_udp> | any }] [sport { <sportv4_udp_start> [to <sportv4_udp_end>] | any }] [dport { <dportv4_udp_start> [to <dportv4_udp_end>] | any }] [ip-flag [ip-ttl { <ip_flag_udp_ttl> | any }] [ip-options { <ip_flag_udp_options> | any }] [ip-fragment { <ip_flag_udp_fragment> | any }]] | ipv4-tcp [sip { <sipv4_tcp> | any }] [dip { <dipv4_tcp> | any }] [sport { <sportv4_tcp_start> [to <sportv4_tcp_end>] | any }] [dport { <dportv4_tcp_start> [to <dportv4_tcp_end>] | any }] [ip-flag [ip-ttl { <ip_flag_tcp_ttl> | any }] [ip-options { <ip_flag_tcp_options> | any }] [ip-fragment { <ip_flag_tcp_fragment> | any }]] [tcp-flag [tcp-fin { <tcpv4_flag_fin> | any }] [tcp-syn { <tcpv4_flag_syn> | any }] [tcp-rst { <tcpv4_flag_rst> | any }] [tcp-psh { <tcpv4_flag_psh> | any }] [tcp-ack { <tcpv4_flag_ack> | any }] [tcp-urg { <tcpv4_flag_urg> | any }]] | ipv6 [next-header { <next_header> | any }] [sip { <sipv6> [sip-bitmask <sipv6_bitmask>] | any }] [hop-limit { <hop_limit> | any }] | ipv6-icmp [sip { <sipv6_icmp> [sip-bitmask <sipv6_bitmask_icmp>] | any }] [icmp-type { <icmpv6_type> | any }] [icmp-code { <icmpv6_code> | any }] [hop-limit { <hop_limit_icmp> | any }] | ipv6-udp [sip { <sipv6_udp> [sip-bitmask <sipv6_bitmask_udp>] | any }] [sport { <sportv6_udp_start> [to <sportv6_udp_end>] | any }] [dport { <dportv6_udp_start> [to <dportv6_udp_end>] | any }] [hop-limit { <hop_limit_udp> | any }] | ipv6-tcp [sip { <sipv6_tcp> [sip-bitmask <sipv6_bitmask_tcp>] | any }] [sport { <sportv6_tcp_start> [to <sportv6_tcp_end>] | any }] [dport { <dportv6_tcp_start> [to <dportv6_tcp_end>] | any }] [hop-limit { <hop_limit_tcp> | any }] [tcp-flag [tcp-fin { <tcpv6_flag_fin> | any }] [tcp-syn { <tcpv6_flag_syn> | any }] [tcp-rst { <tcpv6_flag_rst> | any }] [tcp-psh { <tcpv6_flag_psh> | any }] [tcp-ack { <tcpv6_flag_ack> | any }] [tcp-urg { <tcpv6_flag_urg> | any }]] }] [action { permit | deny | filter { switchport <filter_switch_port_list> | interface (<port_type> [<fliter_port_list>]) } }] [rate-limiter { <rate_limiter_id> | disable }] [evc-policer { <evc_policer_id> | disable }] [mirror [disable]] [

	logging [disable]] [shutdown [disable]] [lookup-second [disable]] [redirect { switchport { <redirect_switch_port_id> | <redirect_switch_port_list> } | interface { <port_type> <redirect_port_id> | (<port_type> [<redirect_port_list>]) } | disable }]
Examples	• access-list ace 6 ingress interface GigabitEthernet 1/2 • access-list ace 4 next 5 frame-type etype etype-value 0x8892 dmac 01-0e-cf-00-04-40 action deny • access-list rate-limiter 100kbps 200 • access-list rate-limiter 2 100pps 33

aggregation

Description	Configure aggregation mode.
Syntax	• aggregation mode { [smac] [dmac] [ip] [port] }*1
Example	• aggregation mode ip

alarm

Description	Configure alarms and clears alarm history.
Syntax	• alarm <alarm_name> <alarm_expression> • alarm history clear
Example	

banner

Description	Define a banner. Banners can be configured for process execution, login, or a message of the day. Multiple lines can be added by pressing enter before typing the delimiter character.
Syntax	• banner [motd | login | exec] <banner>
Examples	• banner motd ! Today's the day! • banner * This banner is delimited by asterisk*

clock

Description	Configure time-of-day clock.
Syntax	• clock datetime <input_year> <input_month> <input_date> <input_hour> <input_minute> <input_second> • clock summer-time <word16> date [<start_month_var> <start_date_var> <start_year_var> <start_hour_var> <end_month_var> <end_date_var> <end_year_var> <end_hour_var> [<offset_var>]] • clock summer-time <word16> recurring [<start_week_var> <start_day_var> <start_month_var> <start_hour_var> <end_week_var> <end_day_var> <end_month_var> <end_hour_var> [<offset_var>]] • clock timezone <word_var> <hour_var> [<minute_var> [<subtype_var>]]
Examples	• clock datetime 2020 08 12 15 45 45 • clock timezone moria 13 15 0

default

Description	• Set rate limiters for access control lists to defaults.
Syntax	• default access-list rate-limiter [<rate_limiter_list>]
Example	• default access-list rate-limiter

do

Description	Used to run exec commands in the configuration mode.
Syntax	• do <command>
Example	• do show running-config

enable

Description	Modify enable password parameters.
Syntax	• enable password [level <priv>] <password> • enable secret { 0 | 5 } [level <priv>] <password>
Examples	• enable password newpass • enable secret 5 encryptedpw

end

Description	Go back to EXEC mode
Syntax	• end
Example	• end

exit

Description	Exit from current mode.
Syntax	• exit
Example	• exit

help

Description	Show a description of the interactive help system.
Syntax	• help
Example	• help

hostname

Description	Set system's network name.
Syntax	• hostname <hostname>
Example	• hostname myswitch

interface

Description	Select an interface to configure. This sets the CLI in interface configuration mode.
Syntax	• interface (<port_type> [<plist>]) • interface llag <llag_id> • interface vlan <vlist>
Examples	• interface vlan 1 • interface GigabitEthernet 1/2 GigabitEthernet 1/5 (configure interfaces 2 and 5 together)

ip

Description	Interface Internet Protocol configuration commands.
Syntax	• ip arp inspection • ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var> • ip arp inspection translate [interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>] • ip arp inspection vlan <in_vlan_list> • ip arp inspection vlan <in_vlan_list> logging { deny | permit | all } • ip dhcp excluded-address <low_ip> [<high_ip>] • ip dhcp pool <pool_name> • ip dhcp relay • ip dhcp relay information option • ip dhcp relay information policy { drop | keep | replace }

	• ip dhcp server • ip dhcp snooping • ip dns proxy • ip domain name { <v_domain_name> | dhcp [ipv4 | ipv6] [interface vlan <v_vlan_id_dhcp>] } • ip helper-address <v_ipv4_ucast> • ip http secure-certificate { upload <url_file> [pass-phrase <pass_phrase>] | delete | generate } • ip http secure-redirect • ip http secure-server • ip igmp host-proxy [leave-proxy] • ip igmp snooping • ip igmp snooping vlan <v_vlan_list> • ip igmp ssm-range <v_ipv4_mcast> <ipv4_prefix_length> • ip igmp unknown-flooding • ip name-server [<order>] { <v_ipv4_ucast> | { <v_ipv6_ucast> [interface vlan <v_vlan_id_static>] } | dhcp [ipv4 | ipv6] [interface vlan <v_vlan_id_dhcp>] } • ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw> [<v_distance>] • ip routing • ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mac_var> • ip ssh • ip telnet • ip verify source • ip verify source translate
Examples	• ip domain name dhcp ipv4 • ip dhcp relay information option

ipmc

Description	IPv4/IPv6 multicast configuration.
Syntax	• ipmc profile • ipmc profile <profile_name> • ipmc range <entry_name> { <v_ipv4_mcast> [<v_ipv4_mcast_1>] | <v_ipv6_mcast> [<v_ipv6_mcast_1>] }
Examples	• ipmc profile testprofile • ipmc range testrange 224.0.0.1 224.0.0.4

ipv6

Description	IPv6 configuration commands.
Syntax	• ipv6 mld host-proxy [leave-proxy] • ipv6 mld snooping • ipv6 mld snooping vlan <v_vlan_list> • ipv6 mld ssm-range <v_ipv6_mcast> <ipv6_prefix_length> • ipv6 mld unknown-flooding • ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }
Example	• ipv6 mld snooping vlan 1,5-9

json

Description	JavaScript Object Notation RPC.
Syntax	• json notification host <hname> • json notification listen <notification> <host>
Examples	• json notification host jsonhost • json notification listen ip.status.interface..update jsondest

lacp

Description	LACP settings.
Syntax	• lacp system-priority <v_1_to_65535>

Example	• lacp system-priority 50

line

Description	Configure a terminal line.
Syntax	line { <0~16> | console 0 | vty <0~15> }
Examples	• line 0 • line console 0 • line vty 2

lldp

Description	Link Layer Discover Protocol configuration.
Syntax	• lldp holdtime <val> • lldp med datum { wgs84 | nad83-navd88 | nad83-mllw } • lldp med fast <v_1_to_10> • lldp med location-tlv altitude { meters | floors } <v_word11> • lldp med location-tlv civic-addr { { country <country> } | { state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code } <v_line> } • lldp med location-tlv elin-addr <v_word25> • lldp med location-tlv latitude { north | south } <v_word8> • lldp med location-tlv longitude { west | east } <v_word9> • lldp med media-vlan-policy <policy_index> { voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling } { untagged | tagged <v_vlan_id> [l2-priority <v_0_to_7>] } [dscp <v_0_to_63>] • lldp reinit <val> • lldp timer <val> • lldp transmission-delay <val>
Examples	• lldp med datum nad83-navd88 • lldp med location-tlv altitude floors 4

logging

Description	System logging configuration.
Syntax	• logging host { <ipv4_addr> | <domain_name> } • logging level { informational | notice | warning | error } • logging notification listen <name> level { informational | notice | warning | error } <node> • logging on
Examples	• logging host 192.0.3.47 • logging level warning

loop-protect

Description	Loop protection configuration.
Syntax	• loop-protect • loop-protect shutdown-time <t> • loop-protect transmit-time <t>
Example	• loop-protect shutdown-time 30

mac

Description	MAC table entries/configuration.
Syntax	• mac address-table aging-time <v_0_10_to_1000000> • mac address-table learning vlan <vlan_list> • mac address-table static <v_mac_addr> vlan <v_vlan_id> { [interface (<port_type> [<v_port_type_list>])] [sr <v_uint>] [psfp <v_uint_1>] }

Examples	• mac address-table aging-time 10 • mac address-table static 00:aa:bb:11:33:44 vlan 2

monitor

Description	Configure monitoring (port mirroring)
Syntax	• monitor session <session_number> [destination { interface (<port_type> [<di_list>]) | remote vlan <drvid> reflector-port <port_type> <rportid> } | source { interface (<port_type> [<si_list>]) [both | rx | tx] | remote vlan <srvid> | vlan <source_vlan_list> | cpu [both | rx | tx] }]
Examples	• monitor session 1 source interface GigabitEthernet 1/1 rx • monitor session 1 destination remote vlan 2 reflector-port GigabitEthernet 1/5

mrp

Description	Media Redundancy Protocol (MRP) configuration.
Syntax	• mrp group 1 • mrp group 2
Example	• mrp group 1

no

Description	Set various settings to the default value.
Syntax	• no access management • no access management <access_id_list> • no access-list ace <ace_list> • no access-list rate-limiter [<rate_limiter_list>] • no aggregation mode • no alarm [<alarm_name>] • no banner [motd | login | exec] • no clock summer-time • no clock timezone • no enable password [level <priv>] • no enable secret { [0 | 5] } [level <priv>] • no hostname • no interface llag <llag_id> • no interface vlan <vlist> • no ip arp inspection • no ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var> • no ip arp inspection vlan <in_vlan_list> • no ip arp inspection vlan <in_vlan_list> logging • no ip dhcp excluded-address <low_ip> [<high_ip>] • no ip dhcp pool <pool_name> • no ip dhcp relay • no ip dhcp relay information option • no ip dhcp relay information policy • no ip dhcp server • no ip dhcp snooping • no ip dns proxy • no ip domain name • no ip helper-address • no ip http secure-redirect • no ip http secure-server • no ip igmp host-proxy [leave-proxy] • no ip igmp snooping • no ip igmp snooping vlan [<v_vlan_list>] • no ip igmp ssm-range • no ip igmp unknown-flooding • no ip name-server [<order>] • no ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>

	• no ip routing • no ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mac_var> • no ip ssh • no ip telnet • no ip verify source • no ipmc profile • no ipmc profile <profile_name> • no ipmc range <entry_name> • no ipv6 mld host-proxy [leave-proxy] • no ipv6 mld snooping • no ipv6 mld snooping vlan [<v_vlan_list>] • no ipv6 mld ssm-range • no ipv6 mld unknown-flooding • no ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> } • no json notification host <name> • no json notification listen [<notification> [<host>]] • no lacp system-priority <v_1_to_65535> • no lldp holdtime • no lldp med datum • no lldp med fast • no lldp med location-tlv altitude • no lldp med location-tlv civic-addr { country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code } • no lldp med location-tlv elin-addr • no lldp med location-tlv latitude • no lldp med location-tlv longitude • no lldp med media-vlan-policy <policies_list> • no lldp reinit • no lldp timer • no lldp transmission-delay • no logging host • no logging notification listen [<name>] • no logging on • no loop-protect • no loop-protect shutdown-time • no loop-protect transmit-time • no mac address-table aging-time • no mac address-table aging-time <v_0_10_to_1000000> • no mac address-table learning vlan <vlan_list> • no mac address-table static <v_mac_addr> vlan <v_vlan_id> { [interface (<port_type> [<v_port_type_list>])] [sr <v_uint>] [psfp <v_uint_1>] } • no monitor session <session_number> [destination { interface (<port_type> [<di_list>]) | remote } | source { interface (<port_type> [<si_list>]) [both | rx | tx] | remote | vlan <source_vlan_list> | cpu [both | rx | tx] }] • no ntp • no ntp server <index_var> • no port-security aging • no port-security aging time • no port-security hold time • no privilege <mode_name> level <0-15> <cmd> • no prompt • no qos fmi <fmi_id> mark-red • no qos fmi <fmi_id> mark-red-enable • no qos map cos-dscp <cos> dpl <dpl> • no qos map dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } • no qos map dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } • no qos map dscp-egress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } <dpl>

	• no qos map dscp-ingress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } • no qos qce <qce_id_range> • no qos sfi <sfi_id> block-oversize • no qos sfi <sfi_id> block-oversize-enable • no qos sgi <sgi_id> close-invalid-rx • no qos sgi <sgi_id> close-invalid-rx-enable • no qos sgi <sgi_id> gate-enabled • no qos storm { unicast | multicast | broadcast } • no qos wred group <group> queue <queue> dpl <dpl> • no ringv2 protect • no ringv2 protect group1 • no ringv2 protect group2 • no rmon alarm <id> • no rmon event <id> • no sflow agent-ip • no sflow collector-address [receiver <rcvr_idx_list>] • no sflow collector-port [receiver <rcvr_idx_list>] • no sflow max-datagram-size [receiver <rcvr_idx_list>] • no sflow timeout [receiver <rcvr_idx_list>] • no snmp-server • no snmp-server access <group_name> model { v1 | v2c | v3 | any } level { auth | noauth | priv } • no snmp-server community <v3_comm> [{ ip-range <v_ipv4_addr> <v_ipv4_netmask> | ipv6-range <v_ipv6_subnet> }] • no snmp-server contact • no snmp-server engine-id local • no snmp-server host <conf_name> • no snmp-server location • no snmp-server security-to-group model { v1 | v2c | v3 } name <security_name> • no snmp-server trap <source_name> { [id <filter_id>] | [<oid_subtree> { include | exclude }] } • no snmp-server user <username> engine-id <engineID> • no snmp-server view <view_name> <oid_subtree> • no spanning-tree edge bpdu-filter • no spanning-tree edge bpdu-guard • no spanning-tree mode • no spanning-tree mst <instance> priority • no spanning-tree mst <instance> vlan • no spanning-tree mst forward-time • no spanning-tree mst hello-time • no spanning-tree mst max-age • no spanning-tree mst max-hops • no spanning-tree mst name • no spanning-tree recovery interval • no spanning-tree transmit hold-count • no svl fid { <fid_list> | all } • no username <username> • no vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } } [group <word16>] • no vlan { { ethertype s-custom-port } | <vlan_list> } • no web privilege group [<group_name>] level
Examples	• no clock timezone • no spanning-tree mst name

ntp

Description	Configure NTP.
Syntax	• ntp • ntp server <index_var> ip-address { <ipv4_var> | <ipv6_var> | <name_var> }
Example	• ntp server 1 ip-address 192.0.2.33

port-security

Description	Configure port security settings.
Syntax	• port-security • port-security aging • port-security aging time <aging_time> • port-security hold time <hold_time>
Examples	• port-security aging time 20 • port-security hold time 30

privilege

Description	Command privilege parameters.
Syntax	• privilege <mode_name> level <privilege> <cmd>
Example	• privilege dhcp-pool level 2 interface

profile

Description	Enter Alarm Profile Mode.
Syntax	• profile alarm
Example	• profile alarm

profinet

Description	Enter PROFINET Mode.
Syntax	• profinet
Example	• profinet

prompt

Description	Set prompt.
Syntax	• prompt <prompt>
Example	• prompt testprompt

qos

Description	Quality of Service configuration settings.
Syntax	• qos map cos-dscp <cos> dpl <dpl> dscp { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } • qos map dscp-classify { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } • qos map dscp-cos { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } cos <cos> dpl <dpl> • qos map dscp-egress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } <dpl> to { <dscp_num_tr> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } • qos map dscp-ingress-translation { <dscp_num> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } to { <dscp_num_tr> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } } • qos qce refresh • qos qce { [update] } <qce_id> [{ next <qce_id_next> } | last] [interface (<port_type> [<port_list>])] [smac { <smac> | <smac_24> | any }] [dmac { <dmac> | unicast | multicast | broadcast | any }] [tag { [type { untagged | tagged | c-tagged | s-tagged | any }] [vid { <ot_vid> | any }] [pcp { <ot_pcp> | any }] [dei { <ot_dei> | any }] }*1] [inner-tag { [type { untagged | tagged | c-tagged | s-tagged | any }] [vid { <it_vid> | any }] [pcp { <it_pcp> | any }] [dei {

	<it_dei> | any }] }*1] [frame-type { any | { etype [{ <etype_type> | any }] } | { llc [dsap { <llc_dsap> | any }] [ssap { <llc_ssap> | any }] [control { <llc_control> | any }] } | { snap [{ <snap_data> | any }] } | { ipv4 [proto { <pr4> | tcp | udp | any }] [sip { <sip4> | any }] [dip { <dip4> | any }] [dscp { <dscp4> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any }] [fragment { yes | no | any }] [sport { <sp4> | any }] [dport { <dp4> | any }] } | { ipv6 [proto { <pr6> | tcp | udp | any }] [sip { <sip6> | any }] [dip { <dip6> | any }] [dscp { <dscp6> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | any }] [sport { <sp6> | any }] [dport { <dp6> | any }] } }] [action { [cos { <action_cos> | default }] [dpl { <action_dpl> | default }] [pcp-dei { <action_pcp> <action_dei> | default }] [dscp { <action_dscp_dscp> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } | default }] [policy { <action_policy> | default }] [ingress-map { <action_ingress_map> | default }] }*1] • qos storm { unicast | multicast | broadcast } <rate> [fps | kfps | kbps | mbps] • qos wred group <group> queue <queue> dpl <dpl> min-fl <min_fl> max <max> [fill-level]
Examples	• qos qce 2 action cos 3 • qos storm broadcast 64 fps • qos map dscp-cos be cos 3 dpl 0

ringv2

Description	Configure ring protection v2.
Syntax	• ringv2 protect group1 • ringv2 protect group2
Examples	• ringv2 protect group1 • ringv2 protect group2

rmon

Description	Remote monitoring configuration.
Syntax	• rmon alarm <id> { ifInOctets | ifInUcastPkts | ifInNUcastPkts | ifInDiscards | ifInErrors | ifInUnknownProtos | ifOutOctets | ifOutUcastPkts | ifOutNUcastPkts | ifOutDiscards | ifOutErrors } <ifIndex> <interval> { absolute | delta } rising-threshold <rising_threshold> [<rising_event_id>] falling-threshold <falling_threshold> [<falling_event_id>] { [rising | falling | both] } • rmon event <id> [log] [trap [<community>]] { [description <description>] }
Examples	• rmon alarm 1 ifOutOctets 1 10 absolute rising-threshold 0 3 falling-threshold -12 • rmon event 1 log

sflow

Description	Statistics flow.
Syntax	• sflow agent-ip { ipv4 <v_ipv4_addr> | ipv6 <v_ipv6_addr> } • sflow collector-address [receiver <rcvr_idx_list>] [<ipv4_var> | <ipv6_var> | <domain_name>] • sflow collector-port [receiver <rcvr_idx_list>] <collector_port> • sflow max-datagram-size [receiver <rcvr_idx_list>] <datagram_size> • sflow timeout [receiver <rcvr_idx_list>] <timeout>
Examples	• sflow agent-ip ipv4 192.0.2.128 • sflow collector-port 2

snmp-server

Description	Set SNMP server configuration.
Syntax	• snmp-server • snmp-server access <group_name> model { v1 | v2c | v3 | any } level { auth | noauth | priv } [read <view_name>] [write <write_name>] • snmp-server community <v3_comm> [{ ip-range <v_ipv4_addr> <v_ipv4_netmask> | ipv6-range <v_ipv6_subnet> }] { <v3_sec> | encrypted <v3_sec_enc> } • snmp-server contact <v_line255>

	• snmp-server engine-id local <engineID> • snmp-server host <conf_name> • snmp-server location <v_line255> • snmp-server security-to-group model { v1 | v2c | v3 } name <security_name> group <group_name> • snmp-server trap <source_name> [id <filter_id>] [<oid_subtree> { include | exclude }] • snmp-server user <username> engine-id <engineID> [{ md5 { <md5_passwd> | { encrypted <md5_passwd_encrypt> } } | sha { <sha_passwd> | { encrypted <sha_passwd_encrypt> } } } [priv { des | aes } { <priv_passwd> | { encrypted <priv_passwd_encrypt> } }]] • snmp-server view <view_name> <oid_subtree> { include | exclude }
Examples	• snmp-server user testusr engine-id abcd123456 md5 md5 md5password priv aes privpass • snmp-server access testgroup model v3 level noauth

spanning-tree

Description	Spanning Tree protocol.
Syntax	• spanning-tree aggregation • spanning-tree edge bpdu-filter • spanning-tree edge bpdu-guard • spanning-tree mode { stp | rstp | mstp } • spanning-tree mst <instance> priority <prio> • spanning-tree mst <instance> vlan <v_vlan_list> • spanning-tree mst forward-time <fwdtime> • spanning-tree mst hello-time <hellotime> • spanning-tree mst max-age <maxage> [forward-time <fwdtime>] • spanning-tree mst max-hops <maxhops> • spanning-tree mst name <name> revision <v_0_to_65535> • spanning-tree recovery interval <interval> • spanning-tree transmit hold-count <holdcount>
Examples	• spanning-tree mode rstp • spanning-tree aggregation

svl

Description	Shared VLAN Learning configuration.
Syntax	• svl fid <fid> vlan <vlan_list>
Example	• svl fid 12 vlan 3-6

username

Description	Establish User Name Authentication.
Syntax	• username { default-administrator | <input_username> } privilege <priv> password { unencrypted <unencry_password> | encrypted <encry_password> | none }
Example	• username testuser privilege 3 password none

vlan

Description	VLAN commands.
Syntax	• vlan <vlist> • vlan ethertype s-custom-port <etype> • vlan protocol { { eth2 { <etype> | arp | ip | ipx | at } } | { snap { <oui> | rfc-1042 | snap-8021h } <pid> } | { llc <dsap> <ssap> } } group <grp_id>
Examples	• vlan 1,50 • vlan protocol llc 0xab 0xaf group testgroup

web

Description	Web access settings.
Syntax	• web privilege group <group_name> level { [configRoPriv <configRoPriv>] [configRwPriv <configRwPriv>] [statusRoPriv <statusRoPriv>] [statusRwPriv <statusRwPriv>] }*1
Example	• web privilege group iP level configRwPriv 15

Interface Mode Commands for Port Interfaces

access-list

Description	Configure access list for an interface.
Syntax	• access-list action { permit | deny } • access-list logging • access-list mirror • access-list policy <policy_id> • access-list port-state • access-list rate-limiter <rate_limiter_id> • access-list shutdown • access-list { redirect } interface { <port_type> <port_type_id> | (<port_type> [<port_type_list>]) }
Examples	• access-list action deny • access-list rate-limiter 2

aggregation

Description	Create an aggregation.
Syntax	• aggregation group <v_uint> mode { [active | on | passive] }
Example	• aggregation group 1 mode passive

description

Description	Specify a description of the port.
Syntax	• description <port_desc_str>
Example	• description finance

do

Description	Run exec commands in the current mode.
Syntax	• do <command>
Example	• do reload cold

duplex

Description	Configure duplex settings for the current interface.
Syntax	• duplex { half | full | auto [half | full] }
Example	• duplex auto half

end

Description	Go back to EXEC mode.
Syntax	• end
Example	• end

excessive-restart

Description	Restart backoff algorithm after 16 collisions (No excessive-restart means discard frame after 16 collisions).
Syntax	• excessive-restart
Example	• excessive-restart

exit

Description	Exit from current mode.
Syntax	• exit
Example	• exit

flowcontrol

Description	Configure traffic flow control.
Syntax	• flowcontrol { on | off }
Example	• flowcontrol on

frame-length-check

Description	Drop frames with mismatch between EtherType/Length.
Syntax	• frame-length-check
Example	• frame-length-check

help

Description	Show a description of the interactive help system.
Syntax	• help
Example	• help

ip

Description	Interface Internet Protocol configuration commands.
Syntax	• ip arp inspection check-vlan • ip arp inspection logging { deny | permit | all } • ip arp inspection trust • ip dhcp snooping trust • ip igmp snooping filter <profile_name> • ip igmp snooping immediate-leave • ip igmp snooping max-groups <throttling> • ip igmp snooping mrouter • ip verify source • ip verify source limit <cnt_var>
Examples	• ip arp inspection logging all • ip igmp snooping immediate-leave

ipv6

Description	IPv6 configuration commands.
Syntax	• ipv6 mld snooping filter <profile_name> • ipv6 mld snooping immediate-leave • ipv6 mld snooping max-groups <throttling> • ipv6 mld snooping mrouter
Examples	• ipv6 mld snooping immediate-leave • ipv6 mld snooping mrouter

lacp

Description	Enable and configure LACP on this interface.
Syntax	• lacp • lacp port-priority <v_1_to_65535> • lacp timeout { fast | slow }

Examples	• lacp • lacp port-priority 5

lldp

Description	Link Layer Discover Protocol configuration.
Syntax	• lldp cdp-aware • lldp med media-vlan policy-list <v_range_list> • lldp med transmit-tlv [capabilities] [location] [network-policy] [poe] • lldp med type { connectivity | end-point } • lldp receive • lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name } • lldp transmit • lldp trap
Examples	• lldp transmit • lldp tlv-select management-address

loop-protect

Description	Loop protection configuration on port.
Syntax	• loop-protect • loop-protect action { [shutdown] [log] }*1 • loop-protect tx-mode
Examples	• loop-protect • loop-protect action log shutdown

mac

Description	MAC address table learning configuration.
Syntax	• mac address-table learning [secure]
Example	• mac address-table learning

media-type

Description	Media type configuration for the current interface.
Syntax	• media-type { rj45 | sfp | dual }
Example	• media-type rj45

mtu

Description	Maximum transmission unit. The size should be between 1518 and 10240.
Syntax	• mtu <max_length>
Example	• mtu 1518

no

Description	Set various settings to the default value.
Syntax	• no access-list logging • no access-list mirror • no access-list policy • no access-list port-state • no access-list rate-limiter • no access-list redirect • no access-list shutdown • no aggregation group <v_uint>

	• no debug phy loopback [near | far | connector | mac-serdes-input | mac-serdes-facility | mac-serdes-equipment | media-serdes-input | media-serdes-facility | media-serdes-equipment] • no description • no duplex • no excessive-restart • no flowcontrol • no frame-length-check • no ip arp inspection check-vlan • no ip arp inspection logging • no ip arp inspection trust • no ip dhcp snooping trust • no ip igmp snooping filter • no ip igmp snooping immediate-leave • no ip igmp snooping max-groups • no ip igmp snooping mrouter • no ip verify source • no ip verify source limit • no ipv6 mld snooping filter • no ipv6 mld snooping immediate-leave • no ipv6 mld snooping max-groups • no ipv6 mld snooping mrouter • no lacp • no lacp port-priority <v_1_to_65535> • no lacp timeout { fast | slow } • no lldp cdp-aware • no lldp med media-vlan policy-list [<v_range_list>] • no lldp med transmit-tlv [capabilities] [location] [network-policy] [poe] • no lldp med type • no lldp receive • no lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name } • no lldp transmit • no lldp trap • no loop-protect • no loop-protect action • no loop-protect tx-mode • no mac address-table learning [secure] • no media-type • no mtu • no port-security • no port-security maximum • no port-security maximum-violation • no port-security violation • no priority-flowcontrol prio [<prio>] • no qos cos • no qos dei • no qos dpl • no qos dscp-classify • no qos dscp-remark • no qos dscp-translate • no qos map cos-tag cos <cos> dpl <dpl> • no qos map tag-cos pcp <pcp> dei <dei> • no qos pcp • no qos policer • no qos qce { [addr] [key] }*1 • no qos queue-policer queue <queue> • no qos queue-shaper queue <queue> • no qos shaper • no qos tag-remark • no qos tas gate-enabled • no qos trust dscp • no qos trust tag • no qos wrr

	• no rmon collection history <id> • no rmon collection stats <id> • no sflow [<sampler_idx_list>] • no sflow counter-poll-interval [<sampler_idx_list>] • no sflow max-sampling-size [sampler <sampler_idx_list>] • no shutdown • no spanning-tree • no spanning •
Examples	• no duplex • no qos policer • no port-security maximum-violation

port-security

Description	Enable/disable port security per interface.
Syntax	• port-security • port-security maximum <limit> • port-security maximum-violation <violate_limit> • port-security violation { protect | restrict | shutdown }
Example	• port-security maximum 10

priority-flowcontrol

Description	Configure Priority Flow Control (802.1Qbb) on this interface. Priority values should be between 0 and 7.
Syntax	• priority-flowcontrol prio <prio>
Example	• priority-flowcontrol prio 3

qos

Description	Quality of Service configuration.
Syntax	• qos cos <cos> • qos dei <dei> • qos dpl <dpl> • qos dscp-classify { zero | selected | any } • qos dscp-remark { rewrite | remap | remap-dp } • qos dscp-translate • qos map cos-tag cos <cos> dpl <dpl> pcp <pcp> dei <dei> • qos map tag-cos pcp <pcp> dei <dei> cos <cos> dpl <dpl> • qos pcp <pcp> • qos policer <rate> [kbps | mbps | fps | kfps] [flowcontrol] • qos qce { [addr { source | destination }] [key { double-tag | normal | ip-addr | mac-ip-addr }] }*1 • qos queue-policer queue <queue> <rate> [kbps | mbps] • qos queue-shaper queue <queue> <rate> [kbps | mbps] [excess | credit] [rate-type { line | data }] • qos shaper <rate> [kbps | mbps] [rate-type { line | data }] • qos tag-remark { pcp <pcp> dei <dei> | mapped } • qos trust dscp • qos trust tag • qos wrr <w0> <w1> [<w2> [<w3> [<w4> [<w5> [<w6> [<w7>]]]]]]
Examples	• qos dscp-classify any • qos policer 500 fps flowcontrol

rmon

Description	Configure Remote Monitoring on an interface.
Syntax	• rmon collection history <id> [buckets <buckets>] [interval <interval>] • rmon collection stats <id>

Examples	• rmon collection history 1 • rmon collection stats 4

sflow

Description	Statistics flow configuration on an interface.
Syntax	• sflow [<sampler_idx_list>] • sflow counter-poll-interval [sampler <sampler_idx_list>] [<poll_interval>] • sflow max-sampling-size [sampler <sampler_idx_list>] [<max_sampling_size>] • sflow sampling-rate [sampler <sampler_idx_list>] [<sampling_rate>]
Examples	• sflow max-sampling-size 120 • sflow sampling-rate 20000

shutdown

Description	Shutdown of the interface.
Syntax	• shutdown
Example	• shutdown

spanning-tree

Description	Spanning Tree protocol configuration on an interface.
Syntax	• spanning-tree • spanning-tree auto-edge • spanning-tree bpdu-guard • spanning-tree edge • spanning-tree link-type { point-to-point | shared | auto } • spanning-tree mst <instance> cost { <cost> | auto } • spanning-tree mst <instance> port-priority <prio> • spanning-tree restricted-role • spanning-tree restricted-tcn
Examples	• spanning-tree edge • spanning-tree mst 2 cost 1

speed

Description	Configures interface speed. If you use 10, 100, or 1000 keywords with the auto keyword the port will only advertise the specified speeds.
Syntax	• speed { 10g | 2500 | 1000 | 100 | 10 | auto { [10] [100] [1000] [2500] [5g] [10g] } }
Example	• speed 100

switchport

Description	Set VLAN switching mode characteristics on a port.
Syntax	• switchport access vlan <pvid> • switchport forbidden vlan { add | remove } <vlan_list> • switchport hybrid acceptable-frame-type { all | tagged | untagged } • switchport hybrid allowed vlan { all | none | [add | remove | except] <vlan_list> } • switchport hybrid egress-tag { none | all [except-native] } • switchport hybrid ingress-filtering • switchport hybrid native vlan <pvid> • switchport hybrid port-type { unaware | c-port | s-port | s-custom-port } • switchport mode { access | trunk | hybrid } • switchport trunk allowed vlan { all | none | [add | remove | except] <vlan_list> } • switchport trunk native vlan <pvid> • switchport trunk vlan tag native • switchport vlan ip-subnet [id <1-128>] <ipv4> vlan <vid> • switchport vlan mac <mac_addr> vlan <vid>

	• switchport vlan protocol group <grp_id> vlan <vid>
Examples	• switchport access vlan 2 • switchport hybrid native vlan 4 • switchport trunk native vlan 6

Interface Mode Commands for VLAN Interfaces

do

Description	Run exec commands in the current mode.
Syntax	• do <command>
Example	• do reload cold

end

Description	Go back to EXEC mode.
Syntax	• end
Example	• end

exit

Description	Exit from current mode.
Syntax	• exit
Example	• exit

help

Description	Show a description of the interactive help system.
Syntax	• help
Example	• help

ip

Description	Interface Internet Protocol configuration commands.
Syntax	• ip address { { <address> <netmask> } | { dhcp [fallback <fallback_address> <fallback_netmask> [timeout <fallback_timeout>]] [client-id { <port_type> <client_id_interface> | ascii <ascii_str> | hex <hex_str> }] [hostname <hostname>] } } • ip dhcp server • ip igmp snooping • ip igmp snooping compatibility { auto | v1 | v2 | v3 } • ip igmp snooping last-member-query-interval <ipmc_lmqi> • ip igmp snooping priority <cos_priority> • ip igmp snooping querier { election | address <v_ipv4_ucast> } • ip igmp snooping query-interval <ipmc_qi> • ip igmp snooping query-max-response-time <ipmc_qri> • ip igmp snooping robustness-variable <ipmc_rv> • ip igmp snooping unsolicited-report-interval <ipmc_uri>
Examples	• ip address 192.0.2.1 255.255.255.0 • ip igmp snooping

ipv6

Description	IPv6 configuration commands.
Syntax	• ipv6 address <subnet> • ipv6 address { autoconfig | dhcp [rapid-commit] } • ipv6 mld snooping • ipv6 mld snooping compatibility { auto | v1 | v2 } • ipv6 mld snooping last-member-query-interval <ipmc_lmqi> • ipv6 mld snooping priority <cos_priority> • ipv6 mld snooping querier election • ipv6 mld snooping query-interval <ipmc_qi> • ipv6 mld snooping query-max-response-time <ipmc_qri>

	• ipv6 mld snooping robustness-variable <ipmc_rv> • ipv6 mld snooping unsolicited-report-interval <ipmc_uri>
Example	• ipv6 address dhcp

no

Description	Set various settings to the default value.
Syntax	• no access-list logging • no access-list mirror • no access-list policy • no access-list port-state • no access-list rate-limiter • no access-list redirect • no access-list shutdown • no aggregation group <v_uint> • no debug phy loopback [near | far | connector | mac-serdes-input | mac-serdes-facility | mac-serdes-equipment | media-serdes-input | media-serdes-facility | media-serdes-equipment] • no description • no duplex • no excessive-restart • no flowcontrol • no frame-length-check • no ip arp inspection check-vlan • no ip arp inspection logging • no ip arp inspection trust • no ip dhcp snooping trust • no ip igmp snooping filter • no ip igmp snooping immediate-leave • no ip igmp snooping max-groups • no ip igmp snooping mrouter • no ip verify source • no ip verify source limit • no ipv6 mld snooping filter • no ipv6 mld snooping immediate-leave • no ipv6 mld snooping max-groups • no ipv6 mld snooping mrouter • no lacp • no lacp port-priority <v_1_to_65535> • no lacp timeout { fast | slow } • no lldp cdp-aware • no lldp med media-vlan policy-list [<v_range_list>] • no lldp med transmit-tlv [capabilities] [location] [network-policy] [poe] • no lldp med type • no lldp receive • no lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name } • no lldp transmit • no lldp trap • no loop-protect • no loop-protect action • no loop-protect tx-mode • no mac address-table learning [secure] • no media-type • no mtu • no port-security • no port-security maximum • no port-security maximum-violation • no port-security violation • no priority-flowcontrol prio [<prio>] • no qos cos • no qos dei

	• no qos dpl • no qos dscp-classify • no qos dscp-remark • no qos dscp-translate • no qos map cos-tag cos <cos> dpl <dpl> • no qos map tag-cos pcp <pcp> dei <dei> • no qos pcp • no qos policer • no qos qce { [addr] [key] }*1 • no qos queue-policer queue <queue> • no qos queue-shaper queue <queue> • no qos shaper • no qos tag-remark • no qos tas gate-enabled • no qos trust dscp • no qos trust tag • no qos wrr • no rmon collection history <id> • no rmon collection stats <id> • no sflow [<sampler_idx_list>] • no sflow counter-poll-interval [<sampler_idx_list>] • no sflow max-sampling-size [sampler <sampler_idx_list>] • no shutdown • no spanning-tree • no spanning
Examples	• no duplex • no qos policer • no port-security maximum-violation

Interface Mode Commands for Local Link Aggregation Interfaces

do

Description	Run exec commands in the current mode.
Syntax	• do <command>
Example	• do reload cold

end

Description	Go back to EXEC mode.
Syntax	• end
Example	• end

exit

Description	Exit from current mode.
Syntax	• exit
Example	• exit

help

Description	Show a description of the interactive help system.
Syntax	• help
Example	• help

lacp

Description	Configure LACP interface.
Syntax	• lacp failover { revertive | non-revertive } • lacp max-bundle <v_uint>
Examples	• lacp failover revertive • lacp max-bundle 2

no

Description	Set various settings to the default value.
Syntax	• no access-list logging • no access-list mirror • no access-list policy • no access-list port-state • no access-list rate-limiter • no access-list redirect • no access-list shutdown • no aggregation group <v_uint> • no debug phy loopback [near | far | connector | mac-serdes-input | mac-serdes-facility | mac-serdes-equipment | media-serdes-input | media-serdes-facility | media-serdes-equipment] • no description • no duplex • no excessive-restart • no flowcontrol • no frame-length-check • no ip arp inspection check-vlan • no ip arp inspection logging • no ip arp inspection trust • no ip dhcp snooping trust • no ip igmp snooping filter

	• no ip igmp snooping immediate-leave • no ip igmp snooping max-groups • no ip igmp snooping mrouter • no ip verify source • no ip verify source limit • no ipv6 mld snooping filter • no ipv6 mld snooping immediate-leave • no ipv6 mld snooping max-groups • no ipv6 mld snooping mrouter • no lacp • no lacp port-priority <v_1_to_65535> • no lacp timeout { fast | slow } • no lldp cdp-aware • no lldp med media-vlan policy-list [<v_range_list>] • no lldp med transmit-tlv [capabilities] [location] [network-policy] [poe] • no lldp med type • no lldp receive • no lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name } • no lldp transmit • no lldp trap • no loop-protect • no loop-protect action • no loop-protect tx-mode • no mac address-table learning [secure] • no media-type • no mtu • no port-security • no port-security maximum • no port-security maximum-violation • no port-security violation • no priority-flowcontrol prio [<prio>] • no qos cos • no qos dei • no qos dpl • no qos dscp-classify • no qos dscp-remark • no qos dscp-translate • no qos map cos-tag cos <cos> dpl <dpl> • no qos map tag-cos pcp <pcp> dei <dei> • no qos pcp • no qos policer • no qos qce { [addr] [key] }*1 • no qos queue-policer queue <queue> • no qos queue-shaper queue <queue> • no qos shaper • no qos tag-remark • no qos tas gate-enabled • no qos trust dscp • no qos trust tag • no qos wrr • no rmon collection history <id> • no rmon collection stats <id> • no sflow [<sampler_idx_list>] • no sflow counter-poll-interval [<sampler_idx_list>] • no sflow max-sampling-size [sampler <sampler_idx_list>] • no shutdown • no spanning-tree • no spanning
Examples	• no duplex • no qos policer • no port-security maximum-violation

Line Terminal Configuration Mode Commands

do

Description	Run exec commands in the current mode.
Syntax	• do <command>
Example	• do reload cold

editing

Description	Enable command line editing.
Syntax	• editing
Example	• editing

end

Description	Go back to EXEC mode.
Syntax	• end
Example	• end

exec-banner

Description	Enable the display of the EXEC banner.
Syntax	• exec-banner
Example	• exec-banner

exec-timeout

Description	Set the EXEC timeout.
Syntax	• exec-timeout <min> [<sec>]
Example	• exec-timeout 10 45

exit

Description	Exit from current mode.
Syntax	• exit
Example	• exit

help

Description	Show a description of the interactive help system.
Syntax	• help
Example	• help

history

Description	Control the command history function.
Syntax	• history size <history_size>
Example	• history size 32

length

Description	Set number of lines on a screen. The number of lines can be zero (for no pausing) or a number between 3 and 512.

Syntax	• length <length>
Example	• length 20

location

Description	Enter terminal location description. The location text should not be more than 32 characters.
Syntax	• location <location>
Example	• location mycli

motd-banner

Description	Enable the display of the MOTD banner.
Syntax	• motd-banner
Example	• motd-banner

no

Description	Set various settings to the default value.
Syntax	• no access-list logging • no access-list mirror • no access-list policy • no access-list port-state • no access-list rate-limiter • no access-list redirect • no access-list shutdown • no aggregation group <v_uint> • no debug phy loopback [near | far | connector | mac-serdes-input | mac-serdes-facility | mac-serdes-equipment | media-serdes-input | media-serdes-facility | media-serdes-equipment] • no description • no duplex • no excessive-restart • no flowcontrol • no frame-length-check • no ip arp inspection check-vlan • no ip arp inspection logging • no ip arp inspection trust • no ip dhcp snooping trust • no ip igmp snooping filter • no ip igmp snooping immediate-leave • no ip igmp snooping max-groups • no ip igmp snooping mrouter • no ip verify source • no ip verify source limit • no ipv6 mld snooping filter • no ipv6 mld snooping immediate-leave • no ipv6 mld snooping max-groups • no ipv6 mld snooping mrouter • no lacp • no lacp port-priority <v_1_to_65535> • no lacp timeout { fast | slow } • no lldp cdp-aware • no lldp med media-vlan policy-list [<v_range_list>] • no lldp med transmit-tlv [capabilities] [location] [network-policy] [poe] • no lldp med type • no lldp receive • no lldp tlv-select { management-address | port-description | system-capabilities | system-description | system-name } • no lldp transmit • no lldp trap • no loop-protect

	• no loop-protect action • no loop-protect tx-mode • no mac address-table learning [secure] • no media-type • no mtu • no port-security • no port-security maximum • no port-security maximum-violation • no port-security violation • no priority-flowcontrol prio [<prio>] • no qos cos • no qos dei • no qos dpl • no qos dscp-classify • no qos dscp-remark • no qos dscp-translate • no qos map cos-tag cos <cos> dpl <dpl> • no qos map tag-cos pcp <pcp> dei <dei> • no qos pcp • no qos policer • no qos qce { [addr] [key] }*1 • no qos queue-policer queue <queue> • no qos queue-shaper queue <queue> • no qos shaper • no qos tag-remark • no qos tas gate-enabled • no qos trust dscp • no qos trust tag • no qos wrr • no rmon collection history <id> • no rmon collection stats <id> • no sflow [<sampler_idx_list>] • no sflow counter-poll-interval [<sampler_idx_list>] • no sflow max-sampling-size [sampler <sampler_idx_list>] • no shutdown • no spanning-tree • no spanning •
Examples	• no duplex • no qos policer • no port-security maximum-violation

privilege

Description	Change privilege level for line. Levels can range from 0 to 15.
Syntax	• privilege level <privileged_level>
Example	• privilege level 15.

width

Description	Set width of the display terminal. Width can be zero (unlimited) or a value between 40 and 512.
Syntax	• width <width>
Example	• width 50

Media Redundancy Protocol (MRP) Configuration Mode Commands

exit

Description	Exit from current mode.
Syntax	• exit
Example	• exit

mode

Description	Set mode of MRP group.
Syntax	• mode { disable | enable }
Example	• mode disable

node1

Description	Set node1 of RMP group.
Syntax	• node1 { interface (<port_type> [<port_list>]) }
Example	• node1 interface GigabitEthernet 1/2

node2

Description	Set node2 of RMP group.
Syntax	• node2 { interface (<port_type> [<port_list>]) }
Example	• node2 interface 2.5GigabitEthernet 1/ 1 2.5GigabitEthernet 1/2

role

Description	Set role of MRP group.
Syntax	• role { manage | client }
Example	• role client

Alarm Profile Mode Commands

alarm

Description	Set alarm mask.
Syntax	• alarm <typeId> { mask | unmask } • alarm all { mask | unmask }
Example	• alarm 102 mask

do

Description	Run exec commands in the current mode.
Syntax	• do <command>
Example	• do reload cold

end

Description	Go back to EXEC mode.
Syntax	• end
Example	• end

exit

Description	Exit from current mode.
Syntax	• exit
Example	• exit

help

Description	Show a description of the interactive help system.
Syntax	• help
Example	• help

PROFINET Mode Commands

devname

Description	Set PROFINET device name.
Syntax	• devname { <name> | default }
Example	• devname testname

exit

Description	Exit from current mode.
Syntax	• exit
Example	• exit

mode

Description	Enable/Disable PROFINET.
Syntax	• mode { disable | enable }
Example	• mode enable

Ring Protection V2 Configuration Mode Commands

exit

Description	Exit from current mode.
Syntax	• exit
Example	• exit

guard-time

Description	Set guard time.
Syntax	• guard-time { <ringGuardTimerDef> }
Example	• guard-time 33

mode

Description	Enable/Disable ring group.
Syntax	• mode { disable | enable }
Example	• mode disable

node1

Description	Set Ring Node 1.
Syntax	• node1 { interface (<port_type> [<port_list>]) }
Example	• node1 interface GigabitEthernet 1/2

node2

Description	Set Ring Node 2.
Syntax	• node2 { interface (<port_type> [<port_list>]) }
Example	• node2 interface 2.5GigabitEthernet 1/ 1 2.5GigabitEthernet 1/2

role

Description	Set role for group.
Syntax	• role { chain-head | chain-tail | chain-member | b-chain-terminal-1 | b-chain-terminal-2 | b-chain-central-block | b-chain-member }
Example	• role chain-head

Spanning Tree Aggregation Mode Commands

do

Description	Run exec commands in the current mode.
Syntax	• do <command>
Example	• do reload cold

end

Description	Go back to EXEC mode.
Syntax	• end
Example	• end

exit

Description	Exit from current mode.
Syntax	• exit
Example	• exit

help

Description	Show a description of the interactive help system.
Syntax	• help
Example	• help

no

Description	Set settings to factory defaults.
Syntax	• no spanning-tree • no spanning-tree auto-edge • no spanning-tree bpdu-guard • no spanning-tree edge • no spanning-tree link-type • no spanning-tree mst <instance> cost • no spanning-tree mst <instance> port-priority • no spanning-tree restricted-role • no spanning-tree restricted-tcn
Examples	• no spanning-tree edge • no spanning-tree restricted-role

spanning-tree

Description	Spanning Tree protocol settings.
Syntax	• spanning-tree • spanning-tree auto-edge • spanning-tree bpdu-guard • spanning-tree edge • spanning-tree link-type { point-to-point | shared | auto } • spanning-tree mst <instance> cost { <cost> | auto } • spanning-tree mst <instance> port-priority <prio> • spanning-tree restricted-role • spanning-tree restricted-tcn
Examples	• spanning-tree link-type point-to-point • spanning-tree restricted-role

DHCP Pool Mode Commands

broadcast

Description	Broadcast address in use on the client's subnet.
Syntax	• broadcast <ip>
Example	• broadcast 192.0.2.253

client-identifier

Description	Client identifier configuration.
Syntax	• client-identifier { { fqdn | name } <identifier> | mac-address <mac> }
Example	• client-identifier name mytestclient

client-name

Description	Client name configuration.
Syntax	• client-name <host_name>
Example	• client-name testclientname

default-router

Description	Default routers configuration.
Syntax	• default-router <ip> [<ip1> [<ip2> [<ip3>]]]
Example	• Default routers 192.0.3.1 192.0.3.2

dns-server

Description	DNS servers configuration.
Syntax	• dns-server <ip> [<ip1> [<ip2> [<ip3>]]]
Example	• dns-server 192.0.3.1 192.0.3.2 192.0.3.3 192.0.3.4

do

Description	Run exec commands in the current mode.
Syntax	• do <command>
Example	• do reload cold

domain-name

Description	Domain name configuration.
Syntax	• domain-name <domain_name>
Example	• domain-name mycompany.net

end

Description	Go back to EXEC mode.
Syntax	• end
Example	• end

exit

Description	Exit from current mode.
Syntax	• exit

Example	• exit

hardware-address

Description	Client hardware address.
Syntax	• hardware-address <mac>
Example	• hardware-address FA:00:25:11:22:33

help

Description	Description of the interactive help system.
Syntax	• help
Example	• help

host

Description	Client IP address and mask.
Syntax	• host <ip> <subnet_mask>
Example	• host 192.0.2.33 255.255.255.0

lease

Description	Address lease time.
Syntax	• lease { <day> [<hour> [<min>]] | infinite }
Examples	• lease 30 12 45 • lease infinite

netbios-name-server

Description	NetBIOS (WINS) name servers.
Syntax	• netbios-name-server <ip> [<ip1> [<ip2> [<ip3>]]]
Example	• netbios-name-server 192.168.0.254 192.168.1. 254 192.168.2.254 192.168.3.254

netbios-node-type

Description	NetBIOS node type.
Syntax	• netbios-node-type { b-node | h-node | m-node | p-node }
Example	• netbios-node-type h-node

netbios-scope

Description	NetBIOS scope.
Syntax	• netbios-scope <netbios_scope>
Example	• netbios-scope testscope

network

Description	Network number and mask.
Syntax	• network <ip> <subnet_mask>
Example	• network 192.168.3.0 255.255.255.0

nis-domain-name

Description	NIS domain name.
Syntax	• nis-domain-name <domain_name>
Example	• nis-domain-name testdomain

nis-servers

Description	Network information servers.
Syntax	• nis-server <ip> [<ip1> [<ip2> [<ip3>]]]
Example	• nis-server 192.168.0.254 192.168.1. 254 192.168.2.254 192.168.3.254

no

Description	Set settings to defaults.
Syntax	• no broadcast • no client-identifier • no client-name • no default-router • no dns-server • no domain-name • no hardware-address • no host • no lease • no netbios-name-server • no netbios-node-type • no netbios-scope • no network • no nis-domain-name • no nis-server • no ntp-server • no vendor class-identifier <class_id>
Examples	• no network • no vendor class-identifier "testclass1"

ntp-server

Description	NTP servers.
Syntax	• ntp-server <ip> [<ip1> [<ip2> [<ip3>]]]
Example	• ntp-server 192.168.0.254 192.168.1. 254 192.168.2.254 192.168.3.254

vendor

Description	Vendor configuration.
Syntax	• vendor class-identifier <class_id> specific-info <hexval>
Example	• vendor class-identifier "testclass1" specific-info 0x01

IPMC Profile Configuration Mode Commands

default

Description	Set access list rate limiter to defaults.
Syntax	• default range <entry_name>
Example	• default range TestRange

description

Description	Set additional description about the profile in 64 characters.
Syntax	• description <profile_desc>
Example	• description <profile_desc>

do

Description	Run exec commands in the current mode.
Syntax	• do <command>
Example	• do reload cold

end

Description	Go back to EXEC mode.
Syntax	• end
Example	• end

exit

Description	Exit from current mode.
Syntax	• exit
Example	• exit

help

Description	Description of the interactive help system.
Syntax	• help
Example	• help

no

Description	Set settings to defaults.
Syntax	• no description • no range <entry_name>
Example	• no description • no range TestRange

range

Description	
Syntax	• range <entry_name> { permit | deny } [log] [next <next_entry>]
Example	• range TestRange permit log

Glossary

A

ACE: ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL: ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for different situations. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACLs can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are 3 web-pages associated with the manual ACL configuration:

ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). By default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" webpage. There are a number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports that obey the same traffic rules. A Traffic Policy is created under the "Access Control List" page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc.) for each ingress port. They will only apply if the frame gets past the ACE matching without being matched. In that case, a counter associated with that port is incremented. See the Web page help text for each specific port property.

ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES: AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

AMS: AMS is an acronym for Auto Media Select. AMS is used for dual media ports (ports supporting both copper (cu) and fiber (SFP) cables. AMS automatically determines if a SFP or a CU cable is inserted and switches to the corresponding media. If both SFP and CU cables are inserted, the port will select the prefered media.

APS: APS is an acronym for Automatic Protection Switching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

Aggregation: Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.
(Also Port Aggregation, Link Aggregation).

ARP: ARP is an acronym for Address Resolution Protocol. It is a protocol that is used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet addresses of its neighbors are known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection: ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation: Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CC: CC is an acronym for Continuity Check. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM: CCM is an acronym for Continuity Check Message. It is a OAM frame transmitted from a MEP to it's peer MEP and used to implement CC functionality.

CDP: CDP is an acronym for Cisco Discovery Protocol.

CoS: CoS is an acronym for Class of Service and it is also known as QoS class.
Every incoming frame is classified to a CoS, which is used throughout the device for providing queuing, scheduling, and congestion control guarantees to the frame according to what was configured for that specific CoS.
There is a one to one mapping between CoS, queue and priority.
A CoS of 0 (zero) has the lowest priority.

CoS ID: CoS ID is an acronym for Class of Service ID.
Every incoming frame is classified to a CoS ID, which later can be used as basis for rewriting of different parts of the frame.

D

DEI: DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

DES: DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP: DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay: DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Server: DHCP Server is used to allocate network addresses and deliver configuration parameters to dynamically configured hosts called DHCP client.

DHCP Snooping: DHCP Snooping is used to block intruders on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS: DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS: DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

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.

DPL: DPL is an acronym for Drop Precedence Level.
Every incoming frame is classified to a DPL, which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DPL.
A DPL of 0 (zero) corresponds to 'Committed' (Green) frames and a DPL greater than 0 (zero) corresponds to 'Discard Eligible' (Yellow) frames.

DSA: The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993. Four revisions to the initial specification have been released: FIPS 186-1 in 1996, FIPS 186-2 in 2000, FIPS 186-3 in 2009, and FIPS 186-4 in 2013.

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

E

ECE: ECE is EVC Control Entry. These rules are ordered in a list to control the preferred classification.

EEE: EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS: EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

ERPS: ERPS is an abbreviation for Ethernet Ring Protection Switching defined in ITU/T G.8032. It provides fast protection and recovery switching for Ethernet traffic in a ring topology while also ensuring that the Ethernet layer remains loop-free.

Ethernet Type: Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

EVC: EVC is an acronym for Ethernet Virtual Connection. MEF standards describe services provided to customers at User Network Interfaces (UNIs). Inside provider networks, nodes are connected using Internal Network-to-Network Interfaces (I-NNIs). Connections between service providers are done using External Network-to-Network Interfaces (E-NNIs). An Ethernet Virtual Connection is an association of two or more UNIs.

F

FTP: FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and allows file writing and reading. It also provides directory service and security features.

Fast Leave: Multicast snooping Fast Leave processing allows the switch to remove the specific member interface, which receives the leave message, from the multicast forwarding-table without sending last member query messages. The specific member interface is also pruned from the multicast tree for the multicast group specified in the original leave message. Fast Leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMPv2 and MLDv1, and it is recommended to enable this feature only when a single IGMPv2/MLDv1 host is connected to the specific interface.

G

GARP: GARP is an acronym for Generic Attribute Registration Protocol. It is a generic protocol for registering attribute with other participants, and it is specified in IEEE 802.1D-2004, clause 12.

GVRP: GVRP is an acronym for GARP VLAN Registration Protocol. It is a protocol for dynamically registering VLANs on ports, and is specified in IEEE 802.1Q-2005, clause 11. GVRP is an example of the use of GARP, hence the G in GVRP.

H

HQoS: HQoS is an acronym for Hierarchical Quality of Service. It is a method of QoS that can be configured on a service level.

HTTP: HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that is used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed.

Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS: HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

|

ICMP: ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X: IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP: IGMP is an acronym for Internet Group Management Protocol. It 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 IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier: A router sends IGMP Query messages onto a particular link. This router is called the Querier. There will be only one IGMP Querier that wins Querier election on a particular link.

IMAP: IMAP is an acronym for Internet Message Access Protocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP: IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC: IPMC is an acronym for IP MultiCast.

IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

IPMC Profile: IPMC Profile is an acronym for IP MultiCast Profile.

IPMC Profile is used to deploy the access control on IP multicast streams.

IP Source Guard: IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

IVL: In Independent VLAN Learning, every VLAN uses its own logical source address table as opposed to SVL where two or more VLANs share the same part of the MAC address table.

J

JSON: JSON (JavaScript Object Notation) is a lightweight data-interchange format. As an alternative to XML, it can be used to transmit dynamic data between web server and application. It uses human-readable text and consist with one or more attribute–value pairs.

L

LACP: LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.

LLC: The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

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

LLDP-MED: LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LLQI: LLQI (Last Listener Query Interval) is the maximun response time used to calculate the Maximun Response Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).

LOC: LOC is an acronym for Loss Of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS.

M

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

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

MEP: MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5: MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm that uses a cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring: For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port (in this context, mirroring a frame is the same as copying the frame).

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD: MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MLD Querier: A router sends MLD Query messages onto a particular link. This router is called the Querier. There will be only one MLD Querier that wins Querier election on a particular link.

MPLS: Multiprotocol Label Switching (MPLS) is a mechanism for speeding up the network traffic transmission. The protocol uses the Layer 2 (Switching) label to forward packets instead of the Layer 3 (Routing) level, so it can avoid the complex destination lookups in the routing table. MPLS uses a variety of protocols to establish the network path, which are called Label Switched Paths (LSPs), and then forwards the packet via the network paths. The packet will be labeled at the edge of the service provider's network and service providers can use the label information to decide the best way for traffic flow forwarding.

The MPLS-TP (Multiprotocol Label Switching Transport Profile) extends MPLS and is being designed by the IETF based on requirements provided by service providers. It will be designed for use as a network layer technology in transport networks. MPLS-TP will provide service providers with a reliable packet-based technology that is based upon circuit-based transport networking, and thus is expected to align with current organizational processes and large-scale work procedures similar to other packet transport technologies. MPLS-TP is expected to be a low cost L2 technology (if the limited profile to be specified is implemented in isolation) that will provide QoS, end-to-end OAM and protection switching.

MSTP: In 2002, the IEEE introduced an evolution of RSTP: the Multiple Spanning Tree Protocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.

MRP: Multiple Registration Protocol is a generic registration framework that defines the dynamic registration and de-registration of attributes across a Bridged Local Area Network. Such attributes could be, for example, VLAN identifiers or multicast group MAC addresses. The standard was originally defined by IEEE 802.1ak, and its latest incorporation is in IEEE 802.1Q-2014.

MVR: Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP) networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.
The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them(Wikipedia).

MVRP: Multiple Vlan Registration Protocol is a protocol that defines the dynamic registration and de-registration of VLAN identifiers across a Bridged Local Area Network. It uses the MRP framework to define its operation and therefore it is also called a MRP Application. The standard was originally defined by IEEE 802.1ak, and its latest incorporation is in IEEE 802.1Q-2014.

N

NAS: NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS: NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS gives each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, and provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS: NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP: NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) at the transport layer.

O

OAM: OAM is an acronym for Operation Administration and Maintenance.
It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionalities like CC and RDI are based on this.

Optional TLVs: A LLDP frame contains multiple TLVs.
Some TLVs are configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLV is disabled, the corresponding information is not included in the LLDP frame.

OUI: OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

P

PCP: 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.

PHY: PHY is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING: ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

Policer: A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3: POP3 is an acronym for Post Office Protocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

PPPoE: PPPoE is an acronym for Point-to-Point Protocol over Ethernet.

It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

POST: POST is an acronym for Post On Self Test.

It is run automatically on various components at power on. The power on self test (POST) is used to test the basic hardware. It includes ready-made tests (e.g. BIST) embedded in hardware or ASICs such as memory tests, server tests, internal loopback test etc.

Private VLAN: In a private VLAN, PVLANs provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

PSFP: PSFP is an acronym for Per Stream Filtering and Policing.

PSFP functions allow filtering and policing decisions, and subsequent frame queuing decisions on a per-stream basis. PSFP is supported by a table of stream filters that determine the filtering and policing actions that are to be applied to frames received on ingress ports.

PTP: PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

Q

QCE: QCE is an acronym for QoS Control Entry.
A QCE is a combination of keys and actions.
The keys can be configured to match specific parts of a frame and the actions can be configured to override the default classified values of e.g. CoS.

QCL: QCL is an acronym for QoS Control List and is a list of QCEs.
Each and every frame is compared against the QCEs in the list. The comparison starts with the first entry in the list and continues until there is a match between the frame and the key parameters or the end of the list is reached.
If there is a match between the frame and the keys, the frame will be reclassified according to the action parameters.

QL: QL In SyncE - this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS: QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.
A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.
Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

QoS Class: See Class of Service (CoS).

Querier Election: Querier election is used to dedicate the Querier, the only router that sends Query messages on a particular link. The Querier election rule defines that the IGMP Querier or MLD Querier with the lowest IPv4/IPv6 address wins the election.

R

RARP: 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.

RADIUS: RADIUS is an acronym for Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI: RDI is an acronym for Remote Defect Indication. It is a OAM functionality that is used by a MEP to indicate a detected defect to the remote peer MEP.

RFC2544: RFC2544 describes a number of tests that may be run to assess the performance characteristics of a network interconnecting devices. In this context, it is specialized towards determining whether a network section conforms to a service level agreement (SLA) and is usually run during service activation.

Router Port: A router port is a port on the Ethernet switch that leads the switch towards the Layer 3 multicast device.

RSA: RSA is one of the first practicable public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician, had developed an equivalent system in 1973, but it wasn't declassified until 1997.

RSTP: In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SAMBA: Samba is a program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.
Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2.

sFLOW: sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector.
Additional information can be found at http://sflow.org.

SHA: SHA is an acronym for Secure Hash Algorithm. It was designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper: A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP: SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP: The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing on networks using IEEE 802.2 LLC for more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values. It also supports vendor-private protocol identifiers.

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 allows diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP: SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) at the transport layer.

SR: Seamless Redundancy is used to provide the high fault tolerance to link failure with zero failover time. This is done by generating the duplicate streams from the talker (stream source) to listener(s) across statically configured redundant paths, and merging the streams at listener(s).

SSID: Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH: SSH is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM: SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP: Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by RSTP.

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

Switch ID: Switch IDs (1-1) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.

SyncE: SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACAS+: 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.

TAS: TAS is an acronym for Time Aware Shaper. 802.1Qbv: This amendment specifies time-aware queue-draining procedures, managed objects and extensions to existing protocols that enable bridges and end stations to schedule the transmission of frames based on timing derived from IEEE Std 802.1AS.

Tag Priority: Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP: TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET: TELNET is an acronym for TELetype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP: TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

ToS: ToS is an acronym for Type of Service. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0-63).

TLV: TLV is an acronym for Type Length Value. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

TKIP: TKIP is an acronym for Temporal Key Integrity Protocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

TT-LOOP: TT-LOOP is an acronym for Traffic Test Loop, a firmware module that provides methods to perform tests that are defined in RFC 2544 (Benchmarking Methodology for Network Interconnect Devices) and Y.1564 (remote end).

U

UDLD: UDLD is an acronym for Uni Directional Link Detection. UDLD protocol monitors the physical configuration of the links between devices and ports that support UDLD. It detects the existence of unidirectional links. Its functionality is to provide mechanisms useful for detecting one-way connections before they create a loop or other protocol malfunction. RFC 5171 specifies a way at data link layer to detect Uni directional link.

UDP: UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP does not provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP: UPnP is an acronym for Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components.

User Priority: User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

\V

VLAN: Virtual LAN. A method to restrict communication between switch ports. At layer 2, the network is partitioned into multiple, distinct, mutually isolated broadcast domains.

VLAN ID: VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN: Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

W

WEP: WEP is an acronym for Wired Equivalent Privacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio, so are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network (Wikipedia).

WiFi: WiFi is an acronym for Wireless Fidelity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA: WPA is an acronym for Wi-Fi Protected Access. It was created in response to several serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

WPA-PSK: WPA-PSK is an acronym for Wi-Fi Protected Access - Pre Shared Key. WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia).

WPA-Radius: WPA-Radius is an acronym for Wi-Fi Protected Access - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia).

WPS: WPS is an acronym for Wi-Fi Protected Setup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

WRED: WRED is an acronym for Weighted Random Early Detection. It is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DPL is used as input to WRED. A higher DPL assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

WTR: WTR is an acronym for Wait To Restore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.

Y

Y.1564: Y.1564 is an Ethernet service activation test methodology (SAM), which is an ITU-T standard for turning up, installing and troubleshooting Ethernet-based services.
It is the only standard test methodology that allows for complete validation of Ethernet service-level agreements (SLAs) in a single test. ITU-T Y.1564 is designed around three key objectives:
To serve as a network service level agreement (SLA) validation tool, ensuring that a service meets its guaranteed performance settings in a controlled test time.
To ensure that all services carried by the network meet their SLA objectives at their maximum committed rate, proving that under maximum load network devices and paths can support all the traffic as designed.
To perform medium- and long-term service testing, confirming that network elements can properly carry all services while under stress during a soaking period.

ITU-T Y.1564: ITU-T Y.1564 defines an out-of-service test methodology to assess the proper configuration and performance of an Ethernet service prior to customer notification and delivery. (Wikipedia).