



NS3553-4P-1T-2S Industrial Managed Switch User Manual

Copyright	© 2018 United Technologies Corporation. Interlogix is part of UTC Climate, Controls & Security, a unit of United Technologies Corporation. All rights reserved.
Trademarks and patents	Trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.
Manufacturer	Interlogix 2955 Red Hill Avenue, Costa Mesa, CA 92626-5923, USA Authorized EU manufacturing representative: UTC Fire & Security B.V. Kelvinstraat 7, 6003 DH Weert, The Netherlands
Version	This document applies to NS3553-4P-1T-2S.
FCC compliance	This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
FCC compliance	Class A: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
Canada	This Class A digital apparatus complies with CAN ICES-003 (A)/NMB-3 (A). Cet appareil numérique de la classe A est conforme à la norme CAN ICES-003 (A)/NMB-3 (A).
ACMA compliance	Notice! This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.
Certification	  
EU directives	This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the RoHS Directive 2011/65/EU.
 	2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info .
Product warnings and disclaimers	THESE PRODUCTS ARE INTENDED FOR SALE TO AND INSTALLATION BY QUALIFIED PROFESSIONALS. UTC FIRE & SECURITY CANNOT PROVIDE ANY ASSURANCE THAT ANY PERSON OR ENTITY BUYING ITS PRODUCTS, INCLUDING ANY "AUTHORIZED DEALER" OR "AUTHORIZED RESELLER", IS PROPERLY TRAINED OR EXPERIENCED TO CORRECTLY INSTALL FIRE AND SECURITY RELATED PRODUCTS. For more information on warranty disclaimers and product safety information, please check www.firesecurityproducts.com/policy/product-warning/ or scan the following code:
	
Contact information and manuals	For contact information go to: www.interlogix.com or www.firesecurityproducts.com. To get translations for this and other product manuals go to: www.firesecurityproducts.com.

Content

	Important information	3
Chapter 1	Introduction	4
	Package contents	4
	Product description	5
	Product features	8
	Product specifications	12
Chapter 2	Installation	17
	Hardware description	17
	Installing the industrial managed switch	26
	Cabling	29
Chapter 3	Switch management	34
	Requirements	34
	Management access overview	34
	CLI mode management	35
	Web management	37
	SNMP-based network management	38
	Smart discovery utility	38
Chapter 4	Web configuration	40
	Main web page	41
	System	43
	UDLD	70
	Simple Network Management Protocol (SNMP)	73
	Port management	85
	Link aggregation	93
	VLAN	101
	Spanning Tree Protocol (STP)	128
	Multicast	145
	Quality of Service (QoS)	169
	Access Control Lists (ACL)	192
	Authentication	205
	Security	240
	MAC address table	257
	LLDP	261
	Network diagnostics	275
	Loop protection	279
	RMON	281
	Power over Ethernet (PoE)	290
	Port identification	303

Chapter 5	Switch operation 304
	Address table 304
	Learning 304
	Forwarding and filtering 304
	Store-and-forward 304
	Auto-negotiation 305
Chapter 6	PoE overview 306
	What is PoE? 306
	PoE system architecture 306
Chapter 7	Troubleshooting 308
Appendix A	Networking connection 309
	Glossary 311

Important information

Limitation of liability

To the maximum extent permitted by applicable law, in no event will UTCFS be liable for any lost profits or business opportunities, loss of use, business interruption, loss of data, or any other indirect, special, incidental, or consequential damages under any theory of liability, whether based in contract, tort, negligence, product liability, or otherwise. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages the preceding limitation may not apply to you. In any event the total liability of UTCFS shall not exceed the purchase price of the product. The foregoing limitation will apply to the maximum extent permitted by applicable law, regardless of whether UTCFS has been advised of the possibility of such damages and regardless of whether any remedy fails of its essential purpose.

Installation in accordance with this manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory.

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, UTCFS assumes no responsibility for errors or omissions.

Advisory messages

Advisory messages alert you to conditions or practices that can cause unwanted results. The advisory messages used in this document are shown and described below.

WARNING: Warning messages advise you of hazards that could result in injury or loss of life. They tell you which actions to take or to avoid in order to prevent the injury or loss of life.

Caution: Caution messages advise you of possible equipment damage. They tell you which actions to take or to avoid in order to prevent damage.

Note: Note messages advise you of the possible loss of time or effort. They describe how to avoid the loss. Notes are also used to point out important information that you should read.

Chapter 1

Introduction

The description of the IFS NS3553-4P-1T-2S model is as follows:

- Industrial L2+ 4-port 10/100/1000T Ultra PoE
- + 1-port 10/100/1000T managed switch
- Managed switch with 2-port 100/1000T SFP

Unless specified, the term “industrial managed switch” mentioned in this user manual refers to the NS3553-4P-1T-2S.

Package contents

Open the box of the industrial managed switch and carefully unpack it. The box should contain the following items:

- The industrial managed switch × 1
- Quick installation guide × 1
- CD with user manual × 1
- RJ45 to RS232 console cable x 1
- DIN rail kit x 1
- Wall mounting kit x 1
- SFP dust-proof cap x 2
- RJ45 dust-proof cap x 6

If any of these are missing or damaged, contact your dealer immediately. If possible, retain the carton including the original packing materials for repacking the product in case there is a need to return it to us for repair.

Product description

The industrial managed switch is specially designed to build a full Gigabit backbone to transmit reliable and high-speed data in demanding heavy industrial environments and forward data to remote network through fiber optic cabling. It comes with an IP30 rugged case and redundant power system. Besides support for 60 Gbps switch fabric to handle extremely large amounts of video, voice, and important data in a secure topology, the industrial managed switch provides user-friendly, advanced IPv6/ IPv4 management interfaces and abundant L2/L4 switching functions. It is the best investment for expanding industrial business or upgrading its network infrastructure..

Redundant ring, fast recovery for critical network applications

The industrial managed switch supports redundant ring technology and features strong, rapid self-recovery capability to prevent interruptions and external intrusions. It incorporates advanced ITU-T G.8032 ERPS (Ethernet Ring Protection Switching) technology, Spanning Tree Protocol (802.1s MSTP), and redundant power input system into the customer's industrial automation network to enhance system reliability and uptime in harsh factory environments. In a certain simple ring network, the recovery time of data link can be as fast as 20 ms.

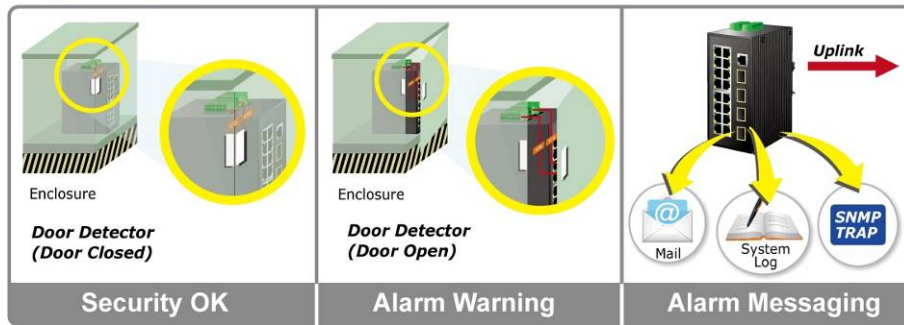
Environmentally hardened design

With its IP30 aluminum case, the industrial managed switch provides a high level of immunity against electromagnetic interference and heavy electrical surges which are usually found on plant floors or in curb-side traffic control cabinets. It also possesses an integrated power supply source with a wide range of voltages for worldwide high availability applications requiring dual or backup power inputs. Being able to operate under the temperature range from -40 to 75°C, the industrial managed switch can be placed in almost any difficult environment.

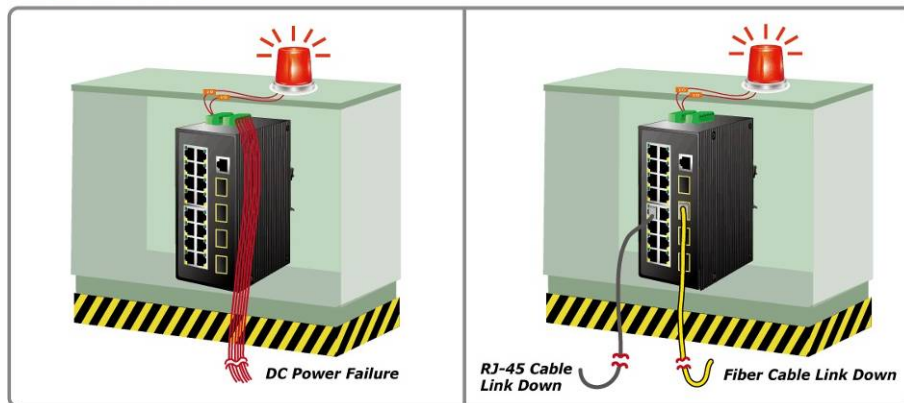
Digital input and digital output for external alarm

The industrial managed switch supports digital input and digital output on its upper panel. The external alarm allows users to use the digital input to detect an external device's status (such as door intrusion detector), and send an event alarm to the administrators. The digital output can be used to alarm the administrators if the industrial managed switch port is link-down, link-up, or power-dead.

Digital Input

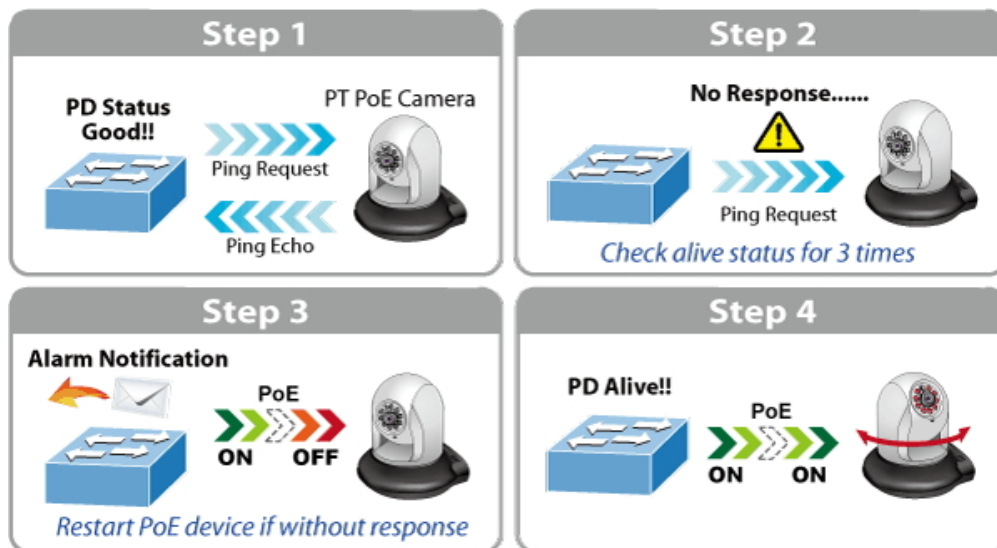


Digital Output



Intelligent powered device alive check

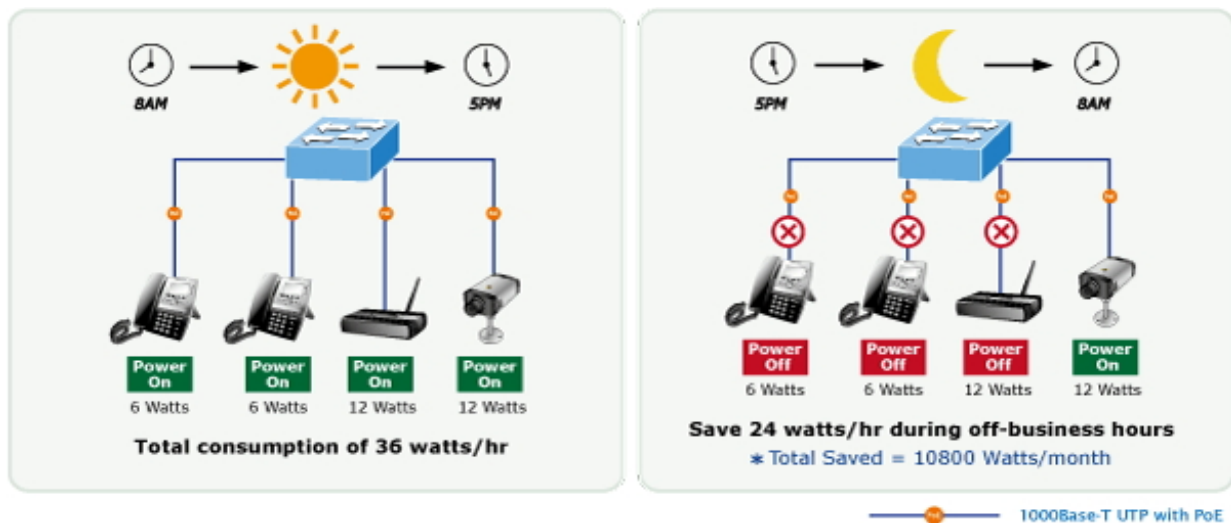
The industrial managed switch can be configured to monitor connected PD status in real time via a ping action. After the PD stops working and responding, the industrial managed switch resumes the PoE port power and puts the PD back to work. The industrial managed switch greatly enhances the network reliability through the PoE port resetting the PD's power source and reducing the administrator management burden.



PoE schedule for energy saving

Under the trend of energy saving worldwide and contributing to environmental protection, the industrial managed switch can effectively control the power supply in

addition to its capability of providing high Watt power. The “PoE schedule” function helps you to enable or disable PoE power feeding for each PoE port during specified time intervals, and is a powerful function to help SMBs or enterprises save power and money.



Robust layer 2 feature

The industrial managed switch can be programmed for advanced switch management functions such as dynamic port link aggregation, Q-in-Q VLAN, Multiple Spanning Tree Protocol (MSTP), layer 2 to layer 4 QoS, bandwidth control, and IGMP / MLD snooping. The industrial managed switch allows the operation of a high-speed trunk combining multiple ports.

IPv6/IPv4 full-function secure switch for building automation networking

The industrial managed switch is the ideal solution to fulfilling the demand of IPv6 management gigabit Ethernet switches, especially in the industrial-hardened environment. It supports both IPv4 and IPv6 protocols, advanced Layer 2 to Layer 4 data switching and redundancy, QoS traffic control, network access control and authentication, and secure management features to protect customer's industrial and building automation network connectivity with reliable switching recovery capability that is suitable for implementing fault tolerant and mesh network architectures.

IPv4/IPv6 VLAN routing for secure and flexible management

The industrial managed switch offers a IPv4/IPv6 VLAN routing feature that allows cross over of different VLANs and different IP addresses for the purpose of having a highly secured, flexible management and simpler networking application.

User-friendly management interfaces

For efficient management, the industrial managed switch is equipped with console, web, and SNMP management interfaces. With the built-in web-based management interface, the industrial managed switch offers an easy-to-use, platform-independent management and configuration facility. The industrial managed switch supports standard Simple Network Management Protocol (SNMP) and can be managed by any management software based on the standard SNMP v1 or v2 protocol. For reducing

product learning time, the industrial managed switch offers Cisco-like command via Telnet or console port, and the customer doesn't need to learn new commands from these switches. Moreover, the industrial managed switch offers secure management remotely by supporting SSH, SSL, and SNMP v3 connections where the packet content can be encrypted at each session.

Intelligent SFP diagnostic mechanism

The industrial managed switch series supports a SFP-DDM (Digital Diagnostic Monitor) function that can easily monitor real-time parameters of the SFP and SFP+ transceivers, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.

Flexible and extendable solution

The industrial managed switch features 100BASE-FX and 1000BASE-SX/LX SFP (Small Form-factor Pluggable) fiber-optic modules, meaning the administrator now can flexibly choose the suitable SFP transceiver according to the transmission distance or the transmission speed required to extend the network efficiently.

1588 precision time protocol for industrial computing networks

The industrial managed switch is intended for telecom and carrier Ethernet applications, supporting MEF service delivery and timing over packet solutions for the IEEE 1588 Precision Time Protocol and synchronous Ethernet.

Product features

Physical port

- Five 10/100/1000BASE-T gigabit RJ45 copper ports.
- Two 100/1000BASE-X mini-GBIC/SFP slots, SFP type auto detection.
- Console interface for basic switch management and setup.

Power over Ethernet

- Ultra Power over Ethernet end-span/mid-span PSE.
- Up to 60 W of power on 4-pair UTP.
- Backward compatible with IEEE 802.3af/at PD devices.
- Up to 4 ports of IEEE 802.3af/IEEE 802.3at/Ultra PoE devices powered.
- Supports PoE power up to 72 W for each PoE port.
- 240 W PoE budget
- Auto detects powered device (PD).
- Circuit protection prevents power interference between ports.
- Remote power feeding up to 100 meters.

- PoE management:
 - Total PoE power budget control
 - Per port PoE function enable/disable
 - PoE admin-mode control
 - PoE port power feeding priority
 - Per PoE port power limitation
 - PD classification detection
- Intelligent PoE features:
 - Temperature threshold control
 - PoE usage threshold control
 - PD alive check
 - PoE schedule

Industrial case and installation

- IP30 aluminum case
- DIN-rail and wall-mount design
 - Redundant power design
- Supports Ethernet ESD protection for 6000 VDC
- -40 to 75°C operating temperature

Digital input and digital output

- Two Digital Inputs (DI)
- Two Digital Outputs (DO)
- Integrates sensors into auto alarm system
- Transfers alarm to IP network via email and SNMP trap

Layer 2 features

- High performance of Store-and-Forward architecture and runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth.

Storm control support:

- Broadcast / Multicast / Unknown-Unicast

Supports VLAN

- IEEE 802.1Q tagged VLAN
- Up to 255 VLANs groups out of 4094 VLAN IDs
- Provider bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
- Private VLAN Edge (PVE)

- Protocol-based VLAN
- MAC-based VLAN
- Voice VLAN

Supports STP

- STP, IEEE 802.1D Spanning Tree Protocol
- RSTP, IEEE 802.1w Rapid Spanning Tree Protocol
- MSTP, IEEE 802.1s Multiple Spanning Tree Protocol, spanning tree by VLAN
- BPDU Guard

Supports link aggregation

- IEEE 802.3ad Link Aggregation Control Protocol (LACP)
- Cisco ether-channel (static trunk)

Provides port mirror (many-to-1)

Port mirroring to monitor the incoming or outgoing traffic on a particular port

Loop protection to avoid broadcast loops

Supports Ethernet Ring Protection Switching (ERPS)

IEEE 1588 and synchronous Ethernet network timing

Layer 3 IP routing features

- Supports static routes and route summarization.

Quality of Service

- Ingress shaper and egress rate limit per port bandwidth control
- Eight priority queues on all switch ports
- Traffic classification:
 - IEEE 802.1p CoS
 - TOS / DSCP / IP Precedence of IPv4/IPv6 packets
 - IP TCP/UDP port number
 - Typical network application
- Strict priority and Weighted Round Robin (WRR) CoS policies
- Supports QoS and In/Out bandwidth control on each port
- Traffic-policing policies on the switch port
- DSCP remarking

Multicast

- Supports IGMP snooping v1, v2, and v3
- Supports MLD snooping v1 and v2
- Querier mode support
- IGMP snooping port filtering
- MLD snooping port filtering
- Multicast VLAN Registration (MVR) support

Security

- Authentication
 - IEEE 802.1x Port-Based / MAC-Based network access authentication
 - Built-in RADIUS client to co-operate with the RADIUS servers
 - TACACS+ login users access authentication
 - RADIUS / TACACS+ users access authentication
- Access Control List (ACL)
 - IPv4 / IPv6 IP-based ACL
 - MAC-based ACL
- Source MAC / IP address binding
- DHCP snooping to filter distrusted DHCP messages
- Dynamic ARP inspection discards ARP packets with invalid MAC addresses to IP address binding.
- IP source guard prevents IP spoofing attacks.
- Auto DoS rule to defend against DoS attacks.
- IP address access management to prevent unauthorized intruders.

Management

- IPv4 and IPv6 dual stack management
- Switch management interfaces:
 - Console / Telnet Command Line Interface
 - Web switch management
 - SNMP v1 and v2c switch management
 - SSH / SSL and SNMP v3 secure access
- IPv6 IP address/NTP/DNS management
- Built-in Trivial File Transfer Protocol (TFTP) client
- System maintenance
 - Firmware upload/download via HTTP / TFTP

- Dual images
- Reset button for system reboot or reset to factory default
- Four RMON groups (history, statistics, alarms, and events)
- IPv6 IP address / NTP / DNS management and ICMPv6
- BOOTP and DHCP for IP address assignment
- DHCP relay
- DHCP Option 82
- User privilege levels control
- NTP (Network Time Protocol)
- Link Layer Discovery Protocol (LLDP) and LLDP-MED
- SFP-DDM (Digital Diagnostic Monitor)
- Smart discovery utility for deploy management
- Network diagnostic
 - ICMPv6/ICMPv4 remote ping
 - Cable diagnostic technology provides the mechanism to detect and report potential cabling issues
- SMTP/Syslog remote alarm
- SNMP trap for interface Link Up and Link Down notification
- System log

Product specifications

Hardware Specifications	
Copper Ports	Five 10/100/1000BASE-T RJ45 auto-MDI/MDI-X ports
SFP+ Slots	Two 1000BASE-SR/LX/BX SFP interfaces (Port-6 to Port-7) Compatible with 1000BASE-FX SFP
Console Port	1 x RS-232 to RJ45 serial port (115200, 8, N, 1)
Switch Architecture	Store-and-Forward
Switch Fabric	14 Gbps / non-blocking
Throughput	10.42 Mpps @ 64 bytes
Address Table	8K entries, automatic source address learning and aging
Shared Data Buffer	4 Mbits
Flow Control	IEEE 802.3x pause frame for full-duplex Back pressure for half-duplex

Jumbo Frame	9K bytes
Reset Button	< 5 seconds: System reboot > 5 seconds: Factory Default
Enclosure	IP30 aluminum case
Installation	DIN rail kit and wall-mount kit
Connector	Removable 6-pin terminal block for power input Pin 1/2 for Power 1, Pin 3/4 for fault alarm, Pin 5/6 for Power 2 Removable 6-pin terminal block for DI/DO interface Pin 1/2 for DI 1 & 2, Pin 3/4 for DO 1 & 2, Pin 5/6 for GND
Alarm	One relay output for power failure. Alarm relay current carry ability: 1A @ 24 VDC
Digital Input	Two Digital Inputs (DI) Level 0: -24~2.1 V (± 0.1 V) Level 1: 2.1~24 V (± 0.1 V) Input load to 24 VDC, 10 mA max.
Digital Output	Two Digital Outputs (DO) Open collector to 24 VDC, 100 mA max. Dual 48~56 VDC (>52 VDC for PoE+ output recommended)
LED	System: Power 1 (Green) Power 2 (Green) Fault Alarm (Red) Ring (Green) Ring Owner (Green) DIDO (Red) Per 10/100/1000T RJ45 Ports: 100 LNK/ACT (Orange) 1000 LNK/ACT (Green) Per SFP Interface: 100 LNK/ACT (Orange) 1000 LNK/ACT (Green) Per PoE Port: Ultra 60 W PoE-in-use x 1 (Green) 802.3at/af PoE-in-use x1 (Orange) PoE Usage: 60 W, 120 W, 180 W, 240 W (Green)
Power Requirement	Dual 48~56 VDC (>52 VDC for PoE+ output recommended)
ESD Protection	6K VDC
Power over Ethernet	

PoE Standard	IEEE 802.3af/802.3at/Ultra PoE PSE
PoE Power Supply Type	End-span/Mid-span/UPoE
PoE Power Output	IEEE 802.3af Standard Per port 48–52 VDC (depending on the power supply), max. 15.4 W IEEE 802.3at Standard Per port 52–56 VDC (depending on the power supply), max. 36 W Ultra PoE Per port 48–56 VDC (depending on the power supply), max. 72 W
Power Pin Assignment	End-span: 1/2(-), 3/6(+) Mid-span: 4/5(+), 7/8(-) UPoE: 1/2(-), 3/6(+), 4/5(+), 7/8(-)
PoE Power Budget	240 W maximum (depending on power input)
PoE Ability PD @ 7 watts	4 units
PoE Ability PD @ 15 watts	4 units
PoE Ability PD @ 30 watts	4 units
Layer 2 Functions	
Basic Management Interfaces	Console; Telnet; Web browser; SNMP v1, v2c
Secure Management Interfaces	SSH, SSL, SNMP v3
Port Configuration	Port disable / enable Auto-negotiation 10/100/1000Mbps full and half duplex mode selection Flow control disable/enable
Port Status	Display each port's speed duplex mode, link status, flow control status, auto-negotiation status, trunk status
Port Mirroring	TX / RX / both 1-to-1 monitor
VLAN	802.1Q tagged-based VLAN, up to 255 VLAN groups Q-in-Q tunneling Private VLAN Edge (PVE) MAC-based VLAN Protocol-based VLAN Voice VLAN MVR (Multicast VLAN Registration) Up to 255 VLAN groups, out of 4095 VLAN IDs
Link Aggregation	IEEE 802.3ad LACP/static trunk 14 groups with four ports per trunk
Spanning Tree Protocol	IEEE 802.3ad LACP static trunk
QoS	Traffic classification based, strict priority and WRR 8-level priority for switching – Port number – 802.1p priority

	– 802.1Q VLAN tag – DSCP/ToS field in IP packet
IGMP Snooping	IGMP (v1/v2/v3) snooping, up to 255 multicast groups IGMP querier mode support
MLD Snooping	MLD (v1/v2) snooping, up to 255 multicast groups MLD querier mode support
Access Control List	IP-based ACL / MAC-based ACL Up to 123 entries
Bandwidth Control	Per port bandwidth control – Ingress: 500 Kbps~1000 Mbps – Egress: 500 Kbps~1000 Mbps
Layer 3 Functions	
IP Interfaces	Maximum of eight VLAN interfaces
Routing Table	Maximum of 32 routing entries
Routing Protocols	IPv4 software static routing IPv6 software static routing
Standards Conformance	
Regulation Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/100BASE-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x flow control and back pressure IEEE 802.3ad port trunk with LACP IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1p Class of Service IEEE 802.1Q VLAN tagging IEEE 802.1X Port Authentication Network Control IEEE 802.1ab LLDP IEEE 802.3af Power over Ethernet IEEE 802.3at Power over Ethernet Plus IEEE 802.3bt Power over Ethernet ready RFC 768 UDP RFC 793 TFTP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP v1 RFC 2236 IGMP v2

SNMP MIBs	RFC 1213 MIB-II RFC 1493 Bridge MIB RFC 1643 Ethernet MIB RFC 2863 Interface MIB RFC 2665 Ether-Like MIB RFC 2819 RMON MIB (Groups 1, 2, 3 and 9) RFC 2737 Entity MIB RFC 2618 RADIUS Client MIB RFC 2933 IGMP-STD-MIB RFC 3411 SNMP-Frameworks-MIB IEEE 802.1X PAE LLDP MAU-MIB
Environment	
Operating	Temperature: -40 to 75°C Relative Humidity: 5 to 95% (non-condensing)
Storage	Temperature: -40 to 85°C Relative Humidity: 5 to 95% (non-condensing)

Chapter 2

Installation

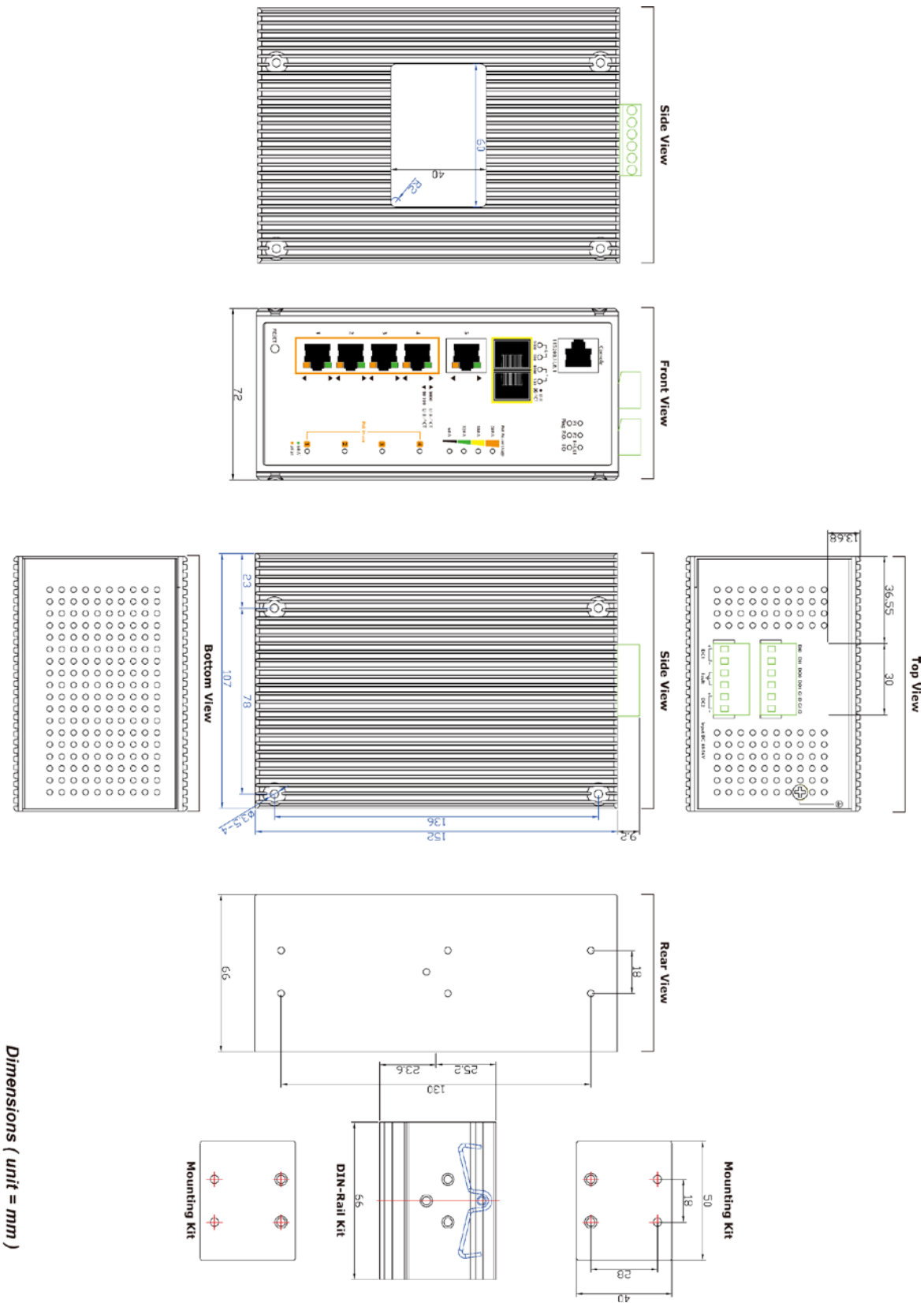
This section describes the hardware features of the industrial managed switch. For easier management and control of the industrial managed switch, familiarize yourself with its display indicators and ports. Front panel illustrations in this chapter display the unit LED indicators. Before connecting any network device to the industrial managed switch, please read this chapter completely.

Hardware description

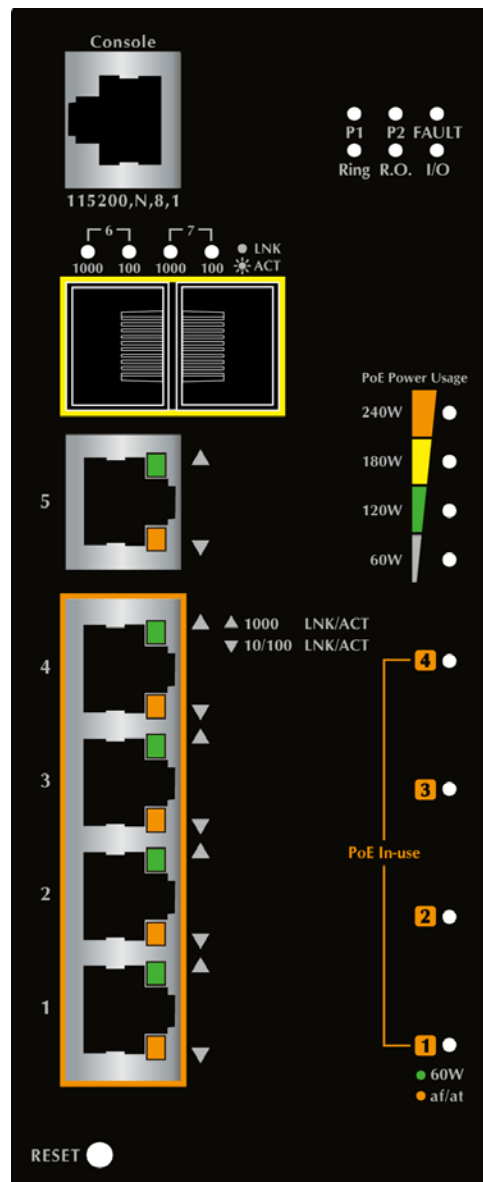
The industrial managed switch provides three different running speeds – 10Mbps, 100Mbps, and 1000Mbps, and automatically distinguishes the speed of the incoming connection.

Physical dimensions

Dimensions (W x D x H): 72 x 107 x 152 mm



Front panel



Gigabit TP interface

10/100/1000BASE-T copper, RJ45 twisted-pair: Up to 100 meters.

SFP slot

100/1000BASE-X mini-GBIC slot, SFP (Small-form Factor Pluggable) transceiver module: From 550 meters to 2 km (multi-mode fiber) and to 10/20/30/40/50/70/120 kilometers (single-mode fiber).

10 gigabit SFP+ slots

10BASE-SR/LR mini-GBIC slot, SFP+ transceiver module supports from 300 meters (multi-mode fiber) up to 10 kilometers (single-mode fiber).

Console port

The console port is a RJ45 port connector and an interface for directly connecting a terminal. Through the console port, the industrial managed switch provides diagnostic information including the IP address setting, factory reset, port management, link status, and system setting. The included DB9 to RJ45 console cable connects to the console port on the device. After making the connection, users can run any terminal emulation program (Hyper Terminal, ProComm Plus, TeliX, Winterm, and so on) to enter the startup screen of the device

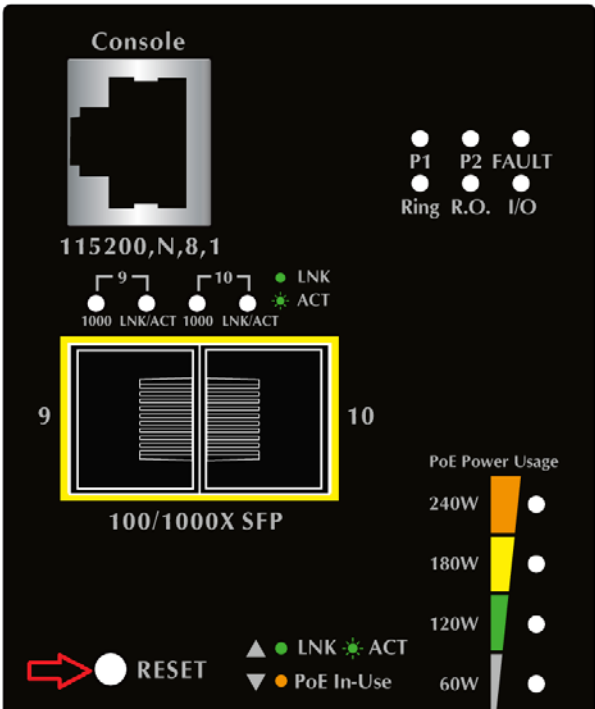
Reset button

Located on the upper left side of the front panel, the reset button is designed to reboot the industrial managed switch without turning the power off and on. The following is the summary table of the reset button functions:

Reset button pressed and released	Function
< 5 seconds: System reboot	Reboots the industrial managed switch
> 5 seconds: Factory default	Resets the industrial managed switch to factory default configuration. The switch then reboots and loads the default settings as shown below: Default Username: admin Default Password: admin Default IP address: 192.168.0.100 Subnet mask: 255.255.255.0 Default Gateway: 192.168.0.254

LED indicators

The front panel LEDs indicate port link status, data activity, and system power.



System

LED	Color	Function
DC1	Green	Lit: indicates that the DC power input 1 has power.
DC2	Green	Lit: indicates that the DC power input 2 has power.
Fault	Red	Lit: indicates that switch DC or port has failed.
Ring	Green	Lit: indicates that the ERPS ring has been successfully created.
R.O.	Green	Lit: indicates that the ring state is in idle mode. Blinking: indicates that the ring state is in protected mode.
DI/DO	Red	Blinking: indicates that switch DC or port has failed or DI has an event.

Per 10/100/1000BASE-T port

LED	Color	Function
1000 LNK/ACT	Green	Lit: indicates the port has successfully connected to the network at 1000 Mbps. Blinking: indicates that the switch is actively sending or receiving data over that port.
100 LNK/ACT	Orange	Lit: indicates the port port has successfully connected to the network at 10/100 Mbps. Blinking: indicates that the switch is actively sending or receiving data over that port.

Per SFP interface

LED	Color	Function
1000 LNK/ACT	Green	Lit: indicates the port has successfully connected to the network at 1000 Mbps. Blinking: indicates that the switch is actively sending or receiving data over that port.
100 LNK/ACT	Orange	Lit: indicates the port has successfully connected to the network at 100 Mbps. Blinking: indicates that the switch is actively sending or receiving data over that port.

PoE in-use (port 1 to port 4)

LED	Color	Function
PoE	Green	Lit: indicates the port is providing DC power with Ultra PoE mode. Off: indicates that the connected device is not a PoE powered device (PD).
	Orange	Lit: indicates the port is providing DC power with End-span/Mid-span mode. Off: indicates that the connected device is not a PoE powered device (PD).

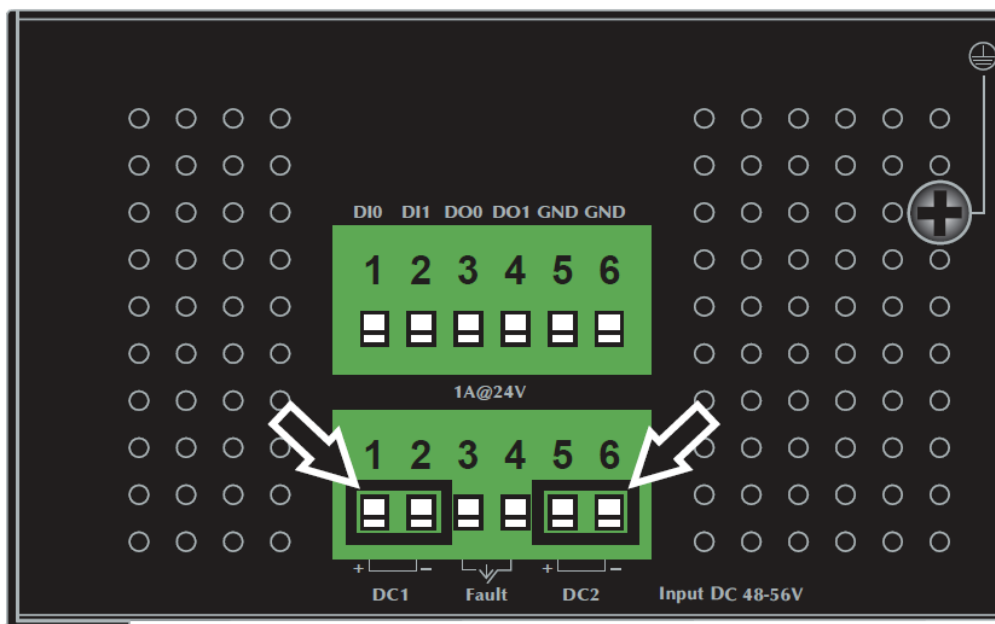
PoE power usage (unit: Watt)

LED	Color	Function
60	Orange	Lit: indicates the system consumes over 60 W PoE power budget.
120	Orange	Lit: indicates the system consumes over 120 W PoE power budget.
180	Orange	Lit: indicates the system consumes over 180 W PoE power budget.
240	Orange	Lit: indicates the system consumes over 2400 W PoE power budget.

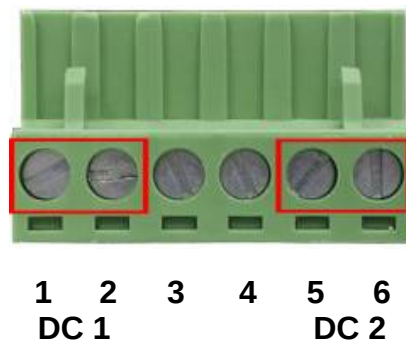
Switch upper panel

The rear panel of the industrial managed switch contains a DC inlet power socket and one terminal block connector with 6 contacts.

1. Insert positive/negative DC power wires into contacts 1 and 2 for DC Power 1, or 5 and 6 for DC Power 2.



2. Tighten the wire-clamp screws to prevent the wires from loosening.



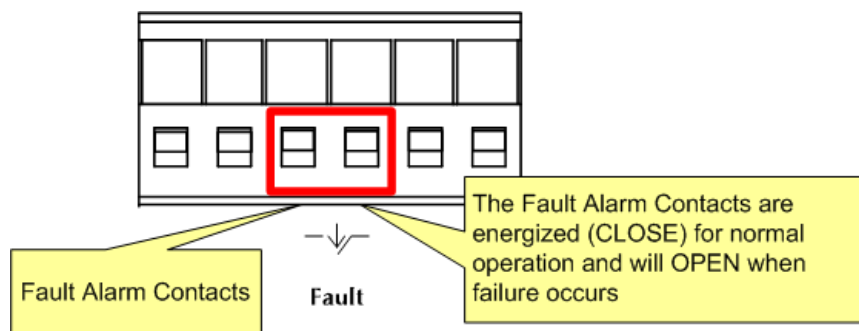
Positive (+) Pin	Negative (-) Pin	Input Voltage
Pin 1/5	Pin 2/6	DC 48~56V

Note:

1. The wire gauge for the terminal block should be in the range of 12 to 24 AWG @ 25°C.
2. When performing any of the procedures such as inserting the wires or tightening the wire-clamp screws, make sure the power is OFF to avoid electrical shock.

Wiring the fault alarm contact

The fault alarm contacts are in the middle (3 & 4) of the terminal block connector as the picture shows below. Inserting the wires, the industrial managed switch detects the fault status of the power failure, or port link failure. The following illustration shows an application example for wiring the fault alarm contacts. Wires are inserted into the fault alarm contacts.



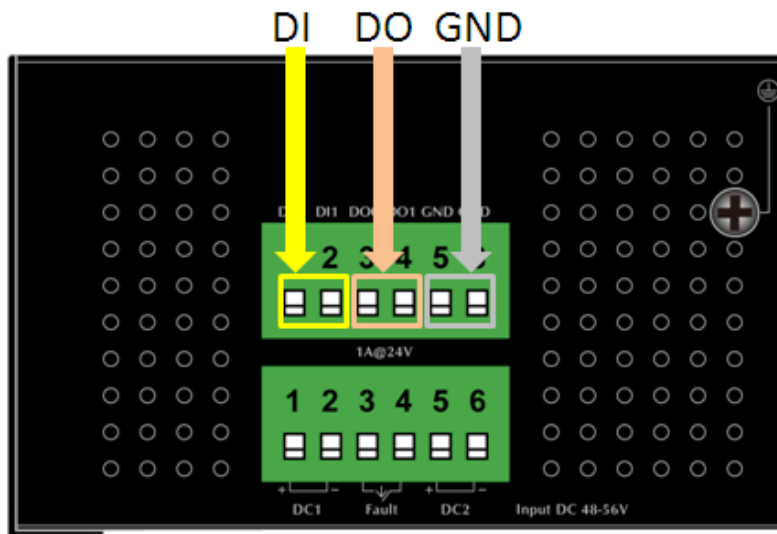
Note:

1. The wire gauge for the terminal block should be in the range of 12 to 24 AWG.
2. When performing any of the procedures such as inserting the wires or tightening the wire-clamp screws, make sure the power is OFF to avoid electrical shock.

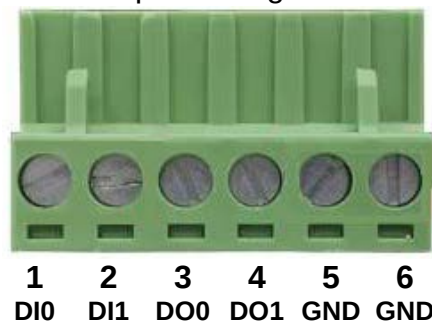
Wiring the digital input/output

The 6-contact terminal block connector on the rear panel of the industrial managed switch is used for digital input and digital output. Please follow the steps below to insert wires.

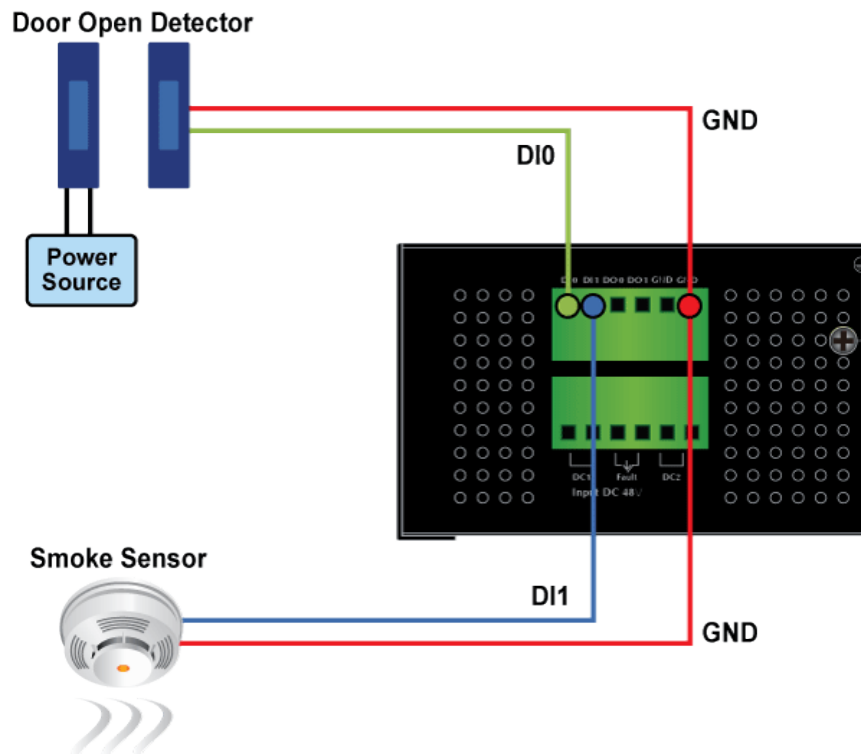
1. The industrial managed switch offers two DI and DO groups. 1 and 2 are DI groups; 3 and 4 are DO groups; and 5 and 6 are GND (ground).



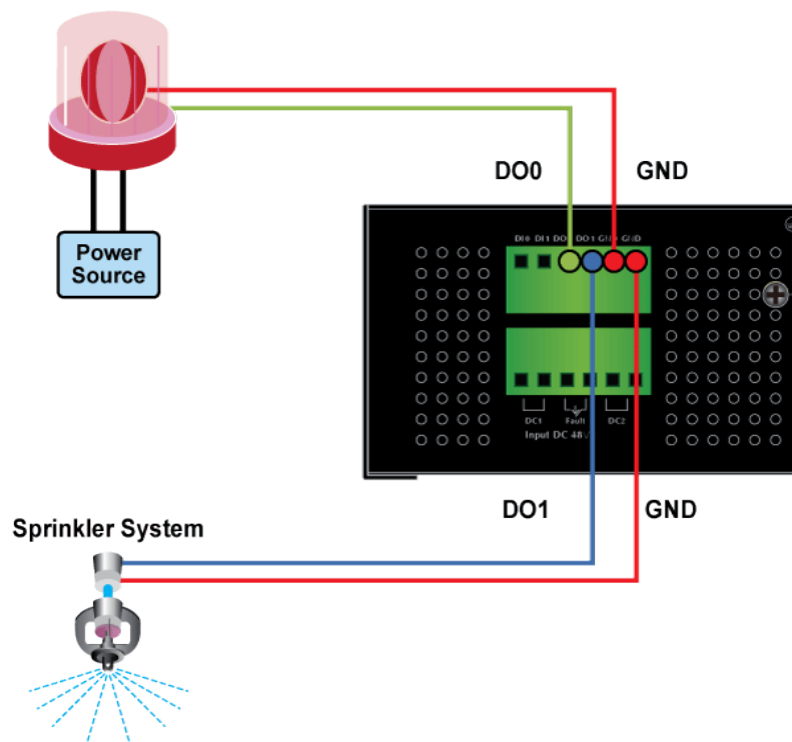
2. Tighten the wire-clamp screws for preventing the wires from loosening.



3. There are two Digital Input groups for you to monitor two different devices. The following topology shows how to wire DI0 and DI1.



4. There are two Digital Output groups for you to sense port failure or power failure and issue a high or low signal to the external device. The following topology shows how to wire DO0 and DO1.



Installing the industrial managed switch

This section describes how to install and make connections to the industrial managed switch. Read the following topics and perform the procedures in the order presented.

Installation steps

To install the industrial managed switch on a desktop or shelf:

1. Unpack the industrial managed switch
2. Ensure that the DIN-Rail is screwed onto the industrial managed switch. If the DIN-rail is not screwed on, please refer to the DIN-rail mounting section for DIN-rail installation. To wall-mount the industrial managed switch, please refer to the wall mount plate mounting section for wall-mount plate installation.
3. Power on the industrial managed switch. please refer to the wiring the power inputs section for information about how to wire the power. The power LED on the industrial managed switch illuminates. Refer to the LED Indicators section for information about LED functionality.
4. Prepare the twisted-pair, straight-through Category 5 cable for Ethernet connection.
5. Insert one side of RJ45 cable (category 5) into the industrial managed switch Ethernet port (RJ45 port) and the other side to the network device's Ethernet (RJ45) port (e.g., switch PC or server). The UTP port (RJ45) LED on the industrial managed switch illuminates when the cable is connected with the network device. Refer to the LED Indicators section for information about LED functionality.

Note: Ensure that the connected network devices support MDI/MDI-X. If they do not support this, use the crossover Category 5 cable.

6. When all connections are set and all LED lights appear normal, the installation is complete..

DIN-rail mounting

There are two methods to install the industrial managed switch: DIN-rail mounting and wall-mount plate mounting. Please read the following topics and perform the procedures in the order presented.

Note: Follow all the DIN-rail installation steps as shown in the example.

To install the DIN rails on the industrial managed switch:

1. Screw the DIN-rail onto the industrial managed switch.



2. Carefully slide the DIN-rail into the track.



3. Ensure that the DIN-rail is tightly attached to the track.

To remove the industrial managed switch from the track:

Carefully remove the DIN-rail from the track.



Wall mount plate mounting

Note: Follow all the wall mount plate installation steps as shown in the example.

To install the industrial managed switch on the wall:

1. Remove the DIN-rail from the industrial managed switch. Use the screwdriver to loosen the screws to remove the DIN-rail.
2. Place the wall-mount plate on the rear panel of the industrial managed switch.



3. Use the screwdriver to screw the wall mount plate onto the industrial managed switch.
4. Use the hook holes at the corners of the wall mount plate to hang the industrial managed switch on the wall.
5. To remove the wall mount plate, reverse the steps above.

Cabling

10/100/1000BASE-T

All 10/100/1000BASE-T ports come with auto-negotiation capability. They automatically support 1000BASE-T, 100BASE-TX, and 10BASE-T networks. Users only need to plug a working network device into one of the 10/100/1000BASE-T ports, and then turn on the industrial managed switch. The port will automatically run in 10 Mbps, 20 Mbps, 100 Mbps, or 200 Mbps, and 1000 Mbps or 2000 Mbps after negotiating with the connected device.

100BASE-FX/1000BASE-SX/LX

The industrial managed switch has four SFP interfaces that support 100/1000 Mbps dual speed mode (optional multi-mode/single-mode 100BASE-FX/1000BASE-SX/LX SFP module)

Cabling

Each 10/100/1000BASE-T port uses an RJ45 socket (similar to phone jacks) for connection of unshielded twisted-pair cable (UTP). The IEEE 802.3/802.3u 802.3ab Fast/Gigabit Ethernet standard requires Category 5 UTP for 100 Mbps 100BASE-TX. 10BASE-T networks can use Cat.3, 4, 5, or 1000BASE-T use 5/5e/6 UTP (see table below). Maximum distance is 100 meters (328 feet). The 100BASE-FX/1000BASE-SX/LX SFP slot uses an LC connector with optional SFP module. The table below provides cable specification details.

Port Type	Cable Type	Connector
10BASE-T	Cat3, 4, 5, 2-pair	RJ45
100BASE-TX	Cat5 UTP, 2-pair	RJ45
1000BASE-T	Cat5/5e/6 UTP, 2-pair	RJ45
100BASE-FX	50/125 μm or 62.5/125 μm multi-mode 9/125 μm single-mode	LC (multi/single mode)
1000BASE-SX/LX	50/125 μm or 62.5/125 μm multi-mode 9/125 μm single-mode	LC (multi/single mode)

Ethernet devices like hubs and PCs can connect to the industrial managed switch by using straight-through wires. The two 10/100/1000Mbps ports are auto-MDI/MDI-X and can be used on straight-through or crossover cable.

Installing the SFP/SFP+ transceiver

SFP transceivers are hot-pluggable and hot-swappable. They can be plugged in and removed to/from any SFP port without having to power down the industrial managed switch (see below).



Approved Interlogix SFP transceivers

The industrial managed switch supports both single mode and multi-mode SFP transceivers. The following list of approved Interlogix SFP transceivers is valid as of the time of publication:

Part #	Fiber Connector	# of Fibers	Fiber Type	Max Distance	Wave Length	Optical Budget (dBm)	Optical Power (dBm)	Receiver Sensitivity (dBm)	Operating Temperature
Twisted Pair SFP 1000Base TX									
S30-RJ	RJ 45	1	Cat5e	100M (328 ft.)					0 to +50°C (32 to 122°F)
Fast Ethernet 100Base FX									
S20-2MLC2	LC	2	Multi-mode	2 km (1.2 mi.)	1310 nm	12	-20 ~ -14	-32	0 to +50°C (32 to 122°F)
S25-2MLC2	LC	2	Multi-mode	2 km (1.2 mi.)	1310 nm	12	-20 ~ -14	-32	-40 to +75°C (-40 to 167°F)
Fast Ethernet 100Base LX									
S20-2SLC20	LC	2	Single Mode	20 km (12 mi.)	1310 nm	19	-15 ~ -8	-34	0 to +50°C (32 to 122°F)
S25-2SLC20	LC	2	Single Mode	20 km (12 mi.)	1310 nm	19	-15 ~ -8	-34	-40 to +75°C (-40 to 167°F)
Fast Ethernet 100Base BX									
S20-1SLC/A-20	LC	1	Single Mode	20 km (12 mi.)	1310 / 1550 nm	18	-14 ~ -8	-32	0 to +50°C (32 to 122°F)
S25-1SLC/B-20	LC	1	Single Mode	20 km (12 mi.)	1550 / 1310 nm	18	-14 ~ -8	-32	-40 to +75°C (-40 to 167°F)
Gigabit Ethernet 1000Base SX									
S30-2MLC	LC	2	Multi-mode	220/550 m (720 / 1800 ft.)	850 nm	7.5	-9.5 ~ -1	-17	0 to +50°C (32 to 122°F)
S35-2MLC	LC	2	Multi-mode	220/550 m (720 / 1800 ft.)	850 nm	7.5	-14 ~ -8	-17	-40 to +75°C (-40 to 167°F)
OM1 Multimode fiber @ 200/500 MHz-km									
OM2 Multimode fiber @ 500.500 MHz-km Laser Rated for GbE LANs									
S30-2MLC-2	LC	2	Multi-mode	2 km (1.2 mi.)	1310 nm	10	-9 ~ -1	-19	0 to +50°C (32 to 122°F)
OM3 Multimode fiber @ 2000/500MHz-km Optimized for 850 nm VCSELs									
Gigabit Ethernet 1000 Base LX									
S30-2SLC-10	LC	2	Single Mode	10 km (6.2 mi.)	1310 nm	18	-9.5 ~ -3	-20	0 to +50°C (32 to 122°F)
S35-2SLC-10	LC	2	Single Mode	10 km (6.2 mi.)	1310 nm	18	-9.5 ~ -3	-20	-40 to +75°C (-40 to 167°F)
S30-2SLC-30	LC	2	Single Mode	30 km (18.6 mi.)	1310 nm	18	-2 ~ +3	-23	0 to +50°C (32 to 122°F)

Part #	Fiber Connector	# of Fibers	Fiber Type	Max Distance	Wave Length	Optical Budget (dBm)	Optical Power (dBm)	Receiver Sensitivity (dBm)	Operating Temperature
S35-2SLC-30	LC	2	Single Mode	30 km (18.6 mi.)	1310 nm	18	-2 ~ +3	-23	-40 to +75°C (-40 to 167°F)
Gigabit Ethernet 1000 Base ZX									
S30-2SLC-70	LC	2	Single Mode	70 km (43 mi.)	1550 nm	19*	-15 ~ -8	-34	0 to +50°C (32 to 122°F)
S35-2SLC-70	LC	2	Single Mode	70 km (43 mi.)	1550 nm	19*	-15 ~ -8	-34	-40 to +75°C (-40 to 167°F)
Gigabit Ethernet 1000 Base BX									
S30-1SLC/A-10	LC	1	Single Mode	10 km (6.2 mi.)	1310 / 1490 nm	11	-9 ~ -3	-20	0 to +50°C (32 to 122°F)
S30-1SLC/B-10	LC	1	Single Mode	10 km (6.2 mi.)	1490 / 1310 nm	11	-9 ~ -3	-20	0 to +50°C (32 to 122°F)
S30-1SLC/A-20	LC	1	Single Mode	20 km (12 mi.)	1310 / 1490 nm	15	-8 ~ -2	-23	0 to +50°C (32 to 122°F)
S30-1SLC/B-20	LC	1	Single Mode	20 km (12 mi.)	1490 / 1310 nm	15	-8 ~ -2	-23	0 to +50°C (32 to 122°F)
Gigabit Ethernet 1000 Base BX									
S30-1SLC/A-60	LC	1	Single Mode	60 km (37 mi.)	1310 / 1490 nm	24	0 ~ +5	-24	0 to +50°C (32 to 122°F)
S30-1SLC/B-60	LC	1	Single Mode	60 km (37 mi.)	1490 / 1310 nm	24	0 ~ +5	-24	0 to +50°C (32 to 122°F)

* Note: High Power Optic. There must be a minimum of 5 dB of optical loss to the fiber for proper operation.

Note: We recommend the use of Interlogix SFPs on the industrial managed switch. If you insert an SFP transceiver that is not supported, the industrial managed switch will not recognize it.

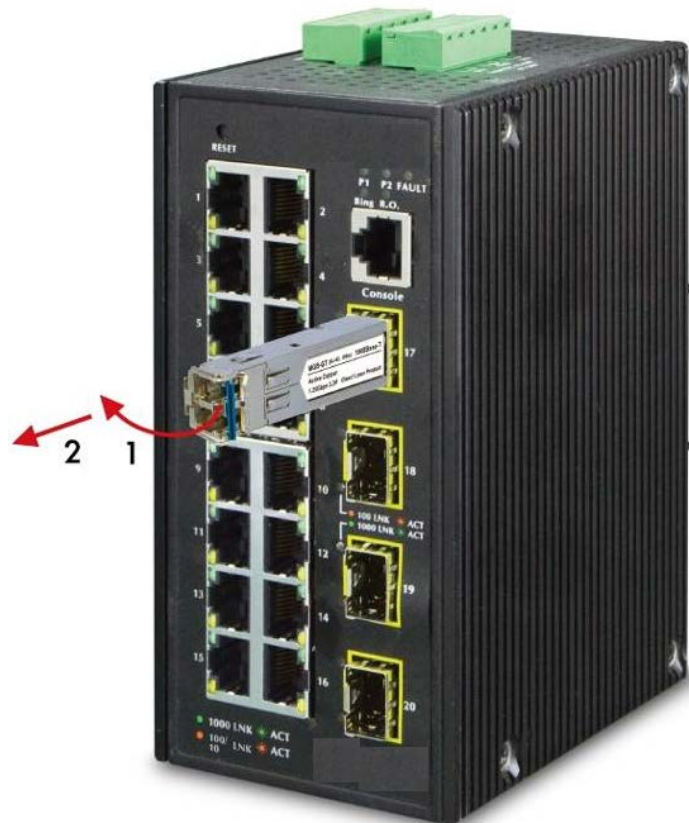
Note: Choose a SFP/SFP+ transceiver that can be operated under -40 to 75°C temperature if the industrial managed switch is working in a 0 to 50°C temperature environment.

To connect the fiber cable:

1. Attach the duplex LC connector on the network cable to the SFP/SFP+ transceiver.
2. Connect the other end of the cable to a device with the SFP/SFP+ transceiver installed.
3. Check the LNK/ACT LED of the SFP/SFP+ slot on the front of the industrial managed switch. Ensure that the SFP/SFP+ transceiver is operating correctly.

To remove the transceiver module:

1. Make sure there is no network activity by checking with the network administrator. Or, through the management interface of the switch/converter (if available), disable the port in advance.
2. Carefully remove the fiber optic cable.
3. Turn the lever of the transceiver module to a horizontal position.
4. Pull out the module gently through the lever.



Note: Never pull out the module without making use of the lever or the push bolts on the module. Removing the module with force could damage the module and the SFP/SFP+ module slot of the industrial managed switch.

Chapter 3

Switch management

This chapter explains the methods that can be used to configure management access to the industrial managed switch. It describes the types of management applications and the communication and management protocols that deliver data between the management device (workstation or personal computer) and the system. It also contains information about port connection options.

Requirements

- Workstations must have Windows XP or later, Mac OS9 or later, Linux, UNIX , or other platforms compatible with TCP/IP protocols.
- Workstations must have an Ethernet NIC (Network Interface Card) installed.
- Serial Port connection (Terminal). The workstation must have a COM Port (DB9 / RS-232) or USB-to-RS-232 converter.
- Ethernet port connection. Use standard network (UTP) cables with RJ45 connectors.
- Workstations must have a web browser and Java runtime environment plug-in installed.

Note: We recommend the use of Internet Explorer 11.0 or later to access the industrial managed switch.

Management access overview

The industrial managed switch provides the flexibility to access and manage it using any or all of the following methods:

- Remote Telnet interface
- Web browser interface
- An external SNMP-based network management application

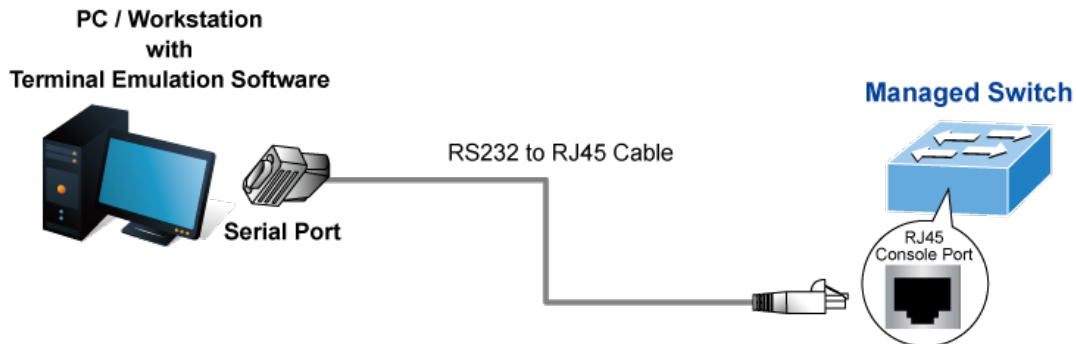
The remote Telnet and web browser interfaces support are embedded in the industrial managed switch software and are available for immediate use. The advantages of these management methods are described below:

Method	Advantages	Disadvantages
Console	- No IP address or subnet needed. - Text-based - Telnet functionality and HyperTerminal built into Windows operating systems. - ProcommPlus, putty, tera term - Secure	- Must be near the switch or use dial-up connection. - Not convenient for remote users. - Modem connection may prove to be unreliable or slow.
Remote Telnet	- Text-based - Telnet functionality and HyperTerminal built into Windows operating systems. - Can be accessed from any location.	Security can be compromised (hackers need only know the IP address and subnet mask).
Web browser	- Ideal for configuring the switch remotely. - Compatible with all popular browsers. - Can be accessed from any location. - Most visually appealing.	- Security can be compromised (hackers need only know the IP address and subnet mask). - May encounter lag times on poor connections.
SNMP agent	- Communicates with switch functions at the MIB level. - Based on open standards.	- Requires SNMP manager software - Least visually appealing of all three methods. - Some settings require calculations. - Security can be compromised (hackers need to only know the community name).

CLI mode management

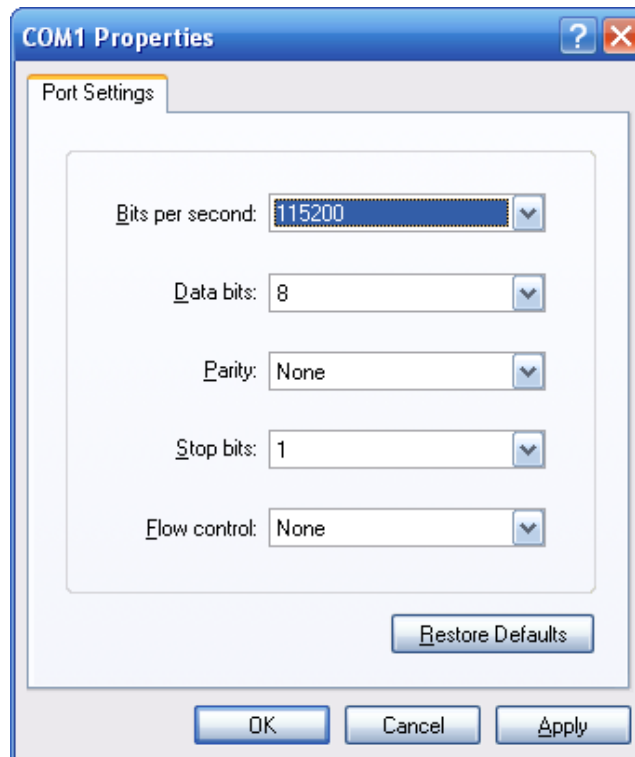
There are two methods for CLI mode management: remote telnet and operation from a console port. Remote telnet is an IP-based protocol and a console port operates the industrial managed switch locally only, but their operations are the same.

The command line user interface is for performing system administration such as displaying statistics or changing option settings. When this method is used, you can access the industrial managed switch remote telnet interface from a personal computer or workstation in the same Ethernet environment as long as you know the current IP address of the industrial managed switch.



Direct access

Direct access to the administration console is achieved by directly connecting a terminal or a computer equipped with a terminal-emulation program (such as HyperTerminal) to the industrial managed switch console (serial) port. When using this management method, a straight DB9 RS-232 cable is required to connect the switch to the computer. After making this connection, configure the terminal-emulation program to use the following parameters:

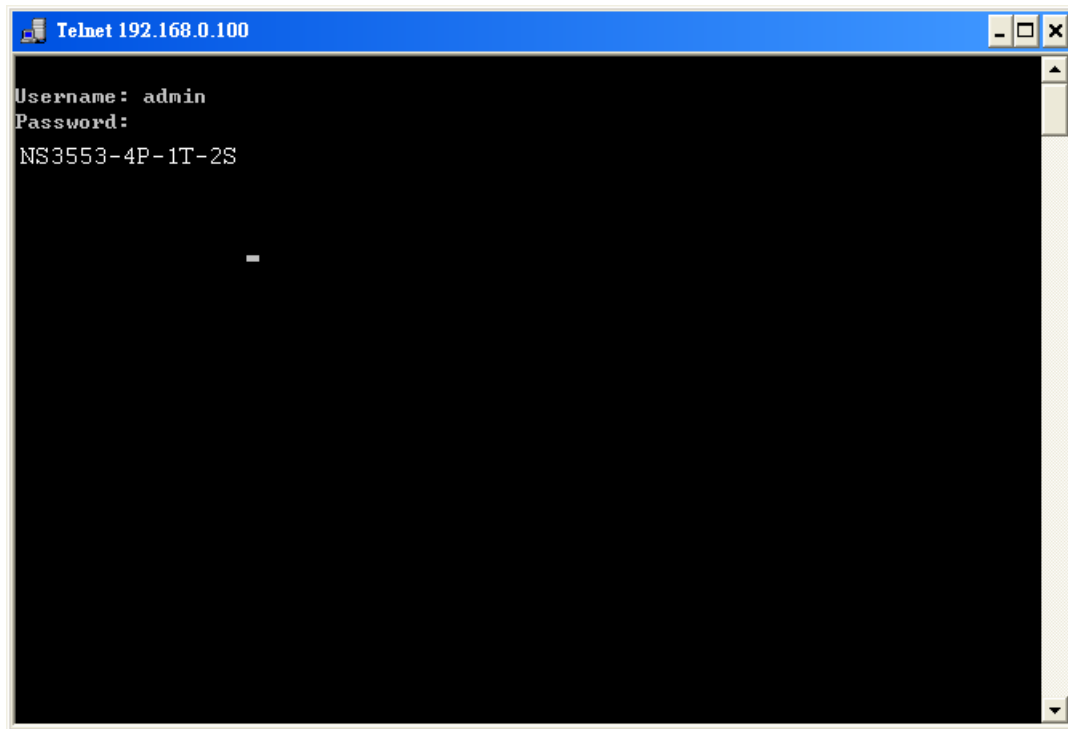


These settings can be changed after log on, if required. This management method is often preferred because the user can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A computer attachment

can use any terminal emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator.

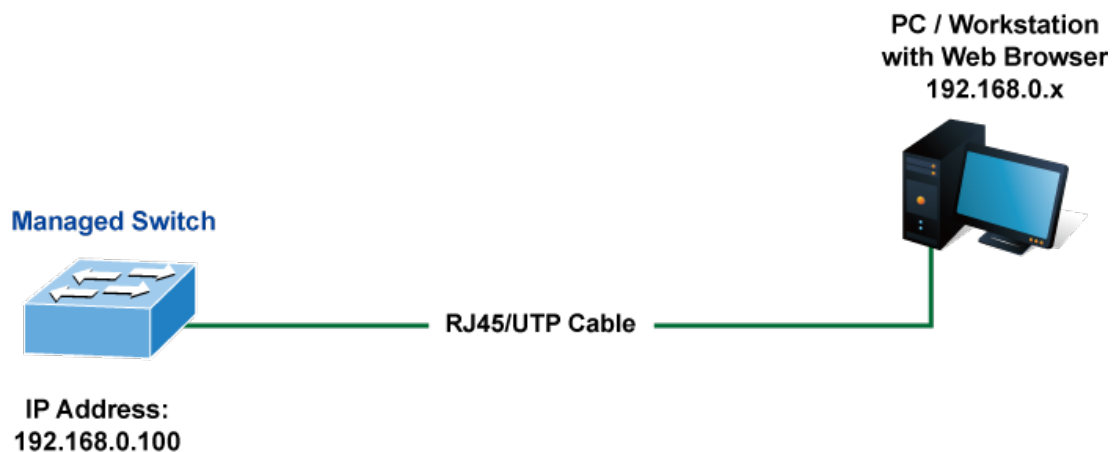
Remote Telnet

In a Windows system, open the command prompt screen, type “telnet 192.168.0.100,” and press Enter on the keyboard. The following screen appears:



Web management

The industrial managed switch provides features that allow users to manage it from anywhere on the network through a standard browser such as Microsoft Internet Explorer. After setting up the IP address for the switch, you can access the industrial managed switch's web interface applications directly in the web browser by entering the IP address of the industrial managed switch.

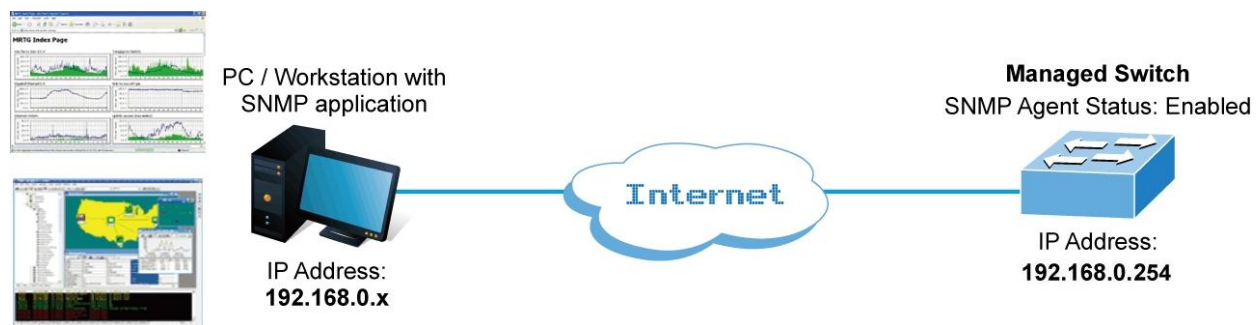


You can use a web browser to list and manage the industrial managed switch configuration parameters from one central location, just as if you were directly connected to the industrial managed switch's console port. Web management requires Microsoft Internet Explorer 11.0 or later.

SNMP-based network management

Use an external SNMP-based application to configure and manage the managed switch, such as SNMP Network Manager, HP Openview Network Node Management (NNM), or What's Up Gold. This management method requires the SNMP agent on the switch and the SNMP Network Management Station to use the same community string. This management method uses two community strings: the get community string and the set community string.

If the SNMP Network Management Station only knows the set community string, it can read and write to the MIBs. However, if it only knows the get community string, it can only read MIBs. The default get and set community strings for the industrial managed switch are public.



Smart discovery utility

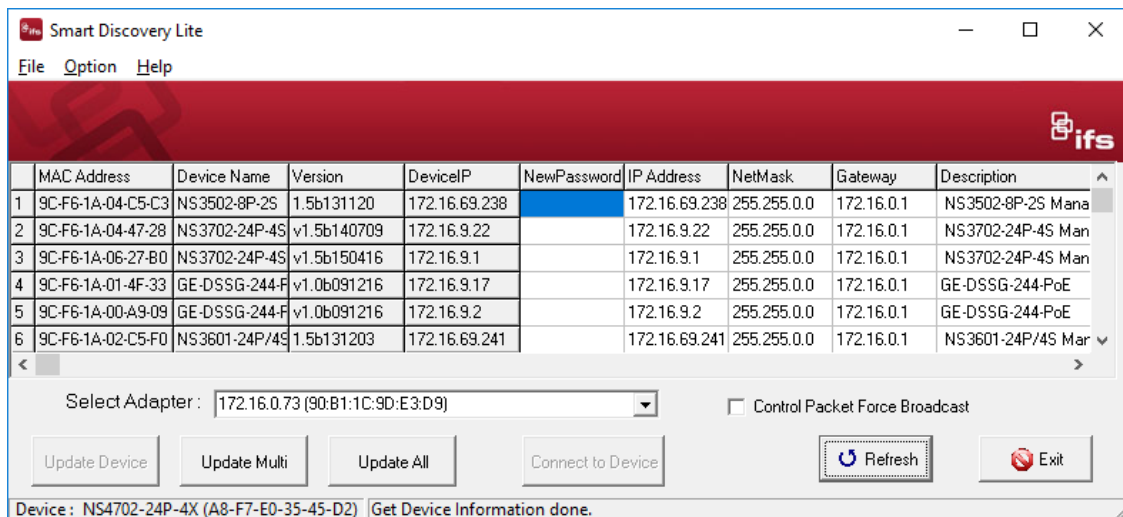
For easily listing the industrial managed switch in your Ethernet environment, the Smart Discovery utility included on the CD-ROM is an ideal solution.

To run the smart discovery utility:

1. Install the Smart Discovery Utility in the administrator PC.
2. Run the utility.

Note: If there are two or more LAN cards in the same administrator computer, choose a different LAN card by using the "Select Adapter" tool.

3. Click the **Refresh** button for the currently connected devices in the discovery list:



4. This utility shows all necessary information from the devices, such as MAC address, device name, firmware version and device IP subnet address. It can also assign new password, IP Subnet address and description for the devices. After setup is complete, click the **Update Device**, **Update Multi**, or **Update All** button:

- **Update Device:** Use the current setting on one single device.
- **Update Multi:** Use the current setting on multi-devices.
- **Update All:** Use the current setting on all devices in the list.

The same functions mentioned above also can be found in **Option** menu.

5. Selecting the **Control Packet Force Broadcast** check box allows you to assign a new setting value to the Web Smart Switch under a different IP subnet address.
6. Click the **Connect to Device** button and the web login screen appears.
7. Click the **Exit** button to shut down the Smart Discovery Utility.

Chapter 4

Web configuration

This section introduces the configuration and functions of the web-based management interface for the industrial managed switch.

About Web-based management

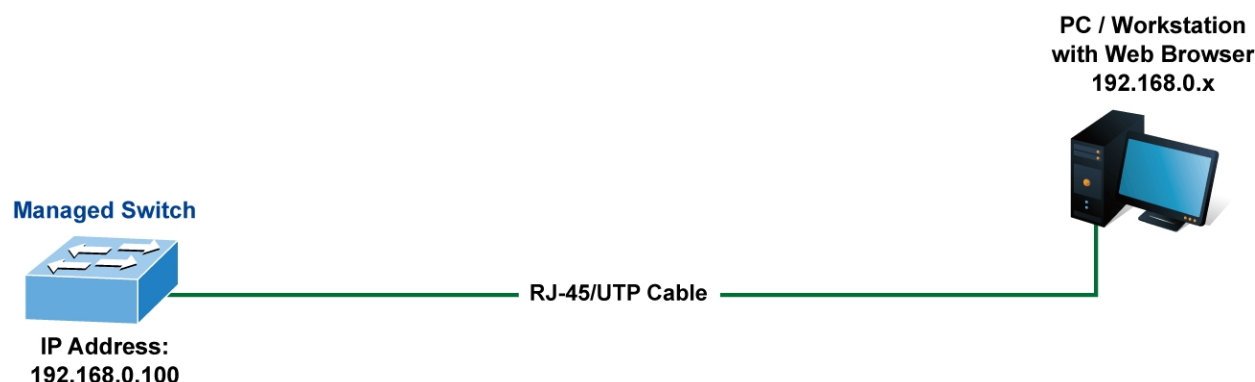
Web-based management of the industrial managed switch supports Internet Explorer 8.0 or later, and can be performed from any location on the network. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed, and present an easy viewing screen.

Note: By default, IE 7.0 and above does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

The industrial managed switch can be configured through an Ethernet connection when the manager computer is set to the same IP subnet address as the industrial managed switch.

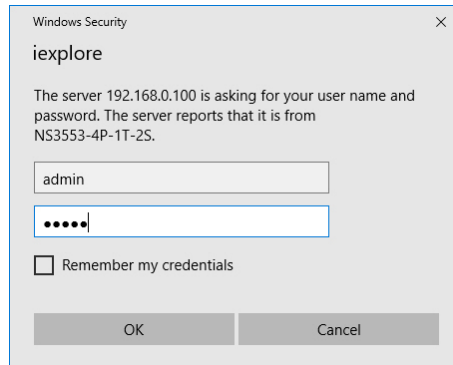
For example, if the default IP address of the industrial managed switch is 192.168.0.100, then the administrator computer should be set at 192.168.0.x (where x is a number between 1 and 254, except 100), and the default subnet mask is 255.255.255.0.

If the default IP address of the industrial managed switch has been changed to 192.168.1.1 with subnet mask 255.255.255.0 via the console, then the administrator computer should be set at 192.168.1.x (where x is a number between 2 and 254) to do the relative configuration on a manager computer.



To log into the industrial managed switch:

1. Launch the Internet Explorer 7.0 or later web browser and type the factory default IP address **http://192.168.0.100** to access the web interface.
2. When the following login screen appears, type the default username "**admin**" with password "**admin**" (or the username and password you have changed via console) to log into the main screen of the industrial managed switch.



3. After typing the username and password, the main UI screen appears. The main menu on the left side of the web page permits access to all the functions and status provided by the industrial managed switch.

Note: For security purposes, change and memorize the new password after this first setup.

Main web page

This section describes how to use the industrial managed switch's web browser interface for configuration and management.



- | | |
|----------------------------|----------------|
| 1. Main menu | 4. Help |
| 2. Copper port link status | 5. Main screen |
| 3. SFP port link status | |

Panel display

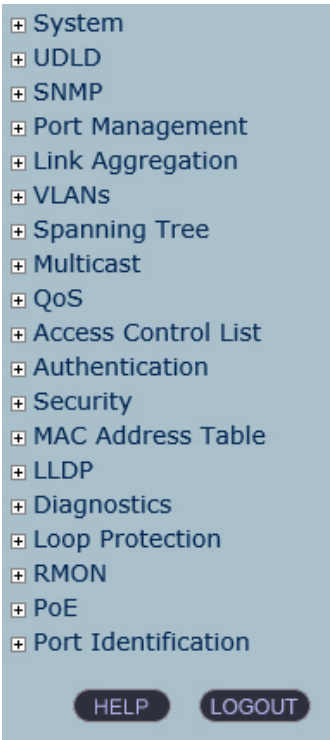
The web interface displays an image of the industrial managed switch's ports. The mode can be set to display different information for the ports, including Link up or Link down. Clicking on the image of a port opens the Port Statistics page.

Port status is indicated as follows:

State	Disabled	Down	Link
RJ45 Ports			
SFP Ports			

Main menu

Using the web interface, you can define system parameters, manage, and control the industrial managed switch and all its ports, or monitor network conditions. The administrator can set up the industrial managed switch by making selections from the main functions menu. Clicking on a main menu item opens sub menus.



System

Use the System menu items to display and configure basic administrative details of the industrial managed switch. Under the System list, the following topics are provided to configure and view the system information. This list contains the following items:

Item	Function
System Information	The industrial managed switch system information is provided here.
IP Configuration	Configures the industrial managed switch-managed IPv4/IPv6 interface and IP routes on this page.
IP Status	This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes and the neighbour cache (ARP cache) status.
Users Configuration	This page provides an overview of the current users. Currently the only way to log in as another user on the web server is to close and reopen the browser.
Privilege Levels	This page provides an overview of the privilege levels.
NTP Configuration	Configure NTP server on this page.
Time Configuration	Configure time parameter on this page.
UPnP	Configure UPnP on this page.
DHCP Relay	Configure DHCP Relay on this page.
DHCP Relay Statistics	This page provides statistics for DHCP relay.
CPU Load	This page displays the CPU load using an SVG graph.
System Log	The industrial managed switch system log information is provided here.
Detailed Log	The industrial managed switch system detailed log information is provided here.
Remote Syslog	Configure remote syslog on this page.
SMTP Configuration	Configure SMTP parameters on this page.
Digital Input/Output	Configuration digital input and output on this page.
Fault Alarm	Configuration fault alarm on this page.
Web Firmware Upgrade	This page facilitates an update of the firmware controlling the industrial managed switch.
Save Startup Config	This copies <i>running-config</i> to <i>startup-config</i> , thereby ensuring that the currently active configuration will be used at the next reboot.
Configuration Download	Download the files to the switch.
Configuration Upload	Upload files to the switch.
Configuration Activate	Activate the configuration file present on the switch.
Configuration Delete	Delete the writable files stored in flash.
Image Select	Configure active or alternate firmware on this page.
System Reboot	You can restart the industrial managed switch on this page. After restarting, the industrial managed switch will boot normally.

System information

The System Information page provides information on the current device such as the hardware MAC address, software version, and system uptime.

System Information

System	
Contact	
Name	NS3553-4P-1T-2S
Location	
Hardware	
MAC Address	a8-f7-e0-3a-a4-dc
Power Status	DC PWR1 :ON DC PWR2 :ON
Temperature	49.0 C - 120.0 F
Time	
System Date	1970-01-01 Thu 00:46:20+00:00
System Uptime	0d 00:46:20
Software	
Software Version	1.5b171213
Software Date	2017-12-13T13:48:46+08:00

Auto-refresh ☐ Refresh

The page includes the following fields:

Item	Function
Contact	The system contact configured in SNMP > System Information.
Name	The system name configured in SNMP > System Information.
Location	The system location configured in SNMP > System Information.
MAC Address	The MAC Address of this industrial managed switch.
Power Status	Indicated the type of power applied to the industrial managed switch.
Temperature	Indicates chipset temperature.
System Date	The current (GMT) system time and date. The system time is obtained through the configured NTP server, if present.
System Uptime	The period of time the device has been operational.
Software Version	The software version of the industrial managed switch.
Software Date	The date when the industrial managed switch software was produced.

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page automatically. This will undo any changes made locally.

IP configuration

This page includes the IP Configuration, IP Interface, and IP Routes. The configured column is used to view or change the IP configuration. The maximum number of interfaces supported is 128 and the maximum number of routes is 32.

IP Configuration

Domain Name	No Domain Name
Mode	Host
DNS Server	No DNS server
DNS Proxy	☐

IP Interfaces

Delete	VLAN	DHCPv4			IPv4		DHCPv6			IPv6	
		Enable	Fallback	Current Lease	Address	Mask Length	Enable	Rapid Commit	Current Lease	Address	Mask Length
☐	1	☐	0		192.168.0.100	24	☐	☐			

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
--------	---------	-------------	---------	---------------

The current column is used to show the active IP configuration.

Object	Description	
IP Configurations	Mode	Set the IP stack to act as a Host or a Router . In Host mode, IP traffic between interfaces will not be routed. In Router mode traffic is routed between all interfaces.
	Domain Name	The name string of local domain where the device belongs. Most queries for names within this domain can use short names relative to the local domain. The system then appends the domain name as a suffix to unqualified names. For example, if 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 interfaces – The first domain name offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used. From this DHCPv6 interface – Specify from which DHCPv6-enabled interface a provided domain name should be preferred.
	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 (less index has higher priority) in doing DNS name resolution. The following modes are supported:

Object			Description
			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 interfaces – 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 interfaces – 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.
IP Address	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.
	DHCPv4	Enabled	Enable the DHCP client by selecting this check box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol. The DHCPv4 client will announce the configured System Name as hostname to provide DNS lookup
		Fallback	The number of seconds for trying to obtain a DHCP lease. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol. The DHCPv4 client will announce the configured System Name as hostname to provide DNS lookup.
		Current Lease	For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.
	IPv4	Address	Provides the IP address of this industrial managed switch 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 required, or if no DHCP fallback address is required
		Mask Length	The IPv4 network mask, in number of bits (<i>prefix length</i>).

Object			Description
			Valid values are between 0 and 30 bits for a IPv4 address. If DHCP is enabled, this field configures the fallback address network mask. The field may be left blank if IPv4 operation on the interface is not required, or if no DHCP fallback address is required.
	DHCPv6	Enable	Enable the DHCPv6 client by selecting this check box. If this option is enabled, the system configures the IPv6 address of the interface using the DHCPv6 protocol.
		Rapid Commit	Enable the DHCPv6 Rapid-Commit option by selecting this check 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 manageable when the DHCPv6 client is enabled.
		Current Lease	For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.
	IPv6	Address	Provides the IP address of this industrial managed switch. A 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. The system accepts the valid IPv6 unicast address only, except the IPv4-Compatible address and IPv4-Mapped address. The field may be left blank if IPv6 operation on the interface is not required.
		Mask Length	The IPv6 network mask, in number of bits (<i>prefix length</i>). Valid values are between 1 and 128 bits for a IPv6 address. The field may be left blank if IPv6 operation on the interface is not required.
IP Routes	Delete		Select this option to delete an existing IP route.
	Network		The destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0 or IPv6 :: notation.
	Mask Length		The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 as it will match anything.
	Gateway		The IP address of the IP gateway. Valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.
	Next Hop VLAN		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

Object		Description
		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

- Click **Add Interface** to add a new IP interface. A maximum of 128 interfaces is supported.
- Click **Add Route** to add a new IP route. A maximum of 32 routes is supported.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

IP status

IP status displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IP routes, and the neighbour cache (ARP cache) status.

IP Interfaces			
Interface	Type	Address	Status
OS:lo	LINK	00-00-00-00-00-00	<UP LOOPBACK RUNNING MULTICAST>
OS:lo	IPv4	127.0.0.1/8	
OS:lo	IPv6	fe80:1::1/64	
OS:lo	IPv6	::1/128	
VLAN1	LINK	00-30-4f-11-22-33	<UP BROADCAST RUNNING MULTICAST>
VLAN1	IPv4	192.168.0.100/20	
VLAN1	IPv6	fe80:2::230:4fff:fe11:2233/64	

IP Routes		
Network	Gateway	Status
127.0.0.1/32	127.0.0.1	<UP HOST>
192.168.0.0/24	VLAN1	<UP HW_RT>
192.168.0.0/20	VLAN1	<UP HW_RT>
224.0.0.0/4	127.0.0.1	<UP>
::1/128	::1	<UP HOST>

Neighbour cache	
IP Address	Link Address
192.168.0.123	VLAN1:00-30-4f-91-e6-45
fe80:2::230:4fff:fe11:2233	VLAN1:00-30-4f-11-22-33

The page includes the following fields:

Object		Description
IP Interfaces	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).
IP Routes	Network	The destination IP network or host address of this route.
	Gateway	The gateway address of this route.
	Status	The status flags of the route.
Neighbor Cache	IP Address	The IP address of the entry.
	Link Address	The link (MAC) address for which a binding to the IP address given exists.

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page automatically. This will undo any changes made locally.

Users configuration

This page provides an overview of the current users. Close and reopen the browser to log in as another user on the web server. After setup is complete, click the **Apply** button and log in to the web interface with the new user name and password. The following appears:



User Name	Privilege Level
admin	15

Add New User

This page includes the following fields:

Object	Description
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 1 to 15. If the privilege level value is 15, it can access all groups (i.e., it is granted full control of the device). Other values need to refer to each group privilege level. User privileges should be the same or greater than the group privilege level to have access to that group. By default, most groups' privilege level 5 has read-only access and privilege level

Object	Description
	10 has read-write access. System maintenance (software upload, factory defaults, etc.) requires user 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:

- Click **Add New User** to add a new user

Add/edit user

Add, edit, or delete a user in this page.

This page includes the following fields:

Object	Description
User Name	A string identifies the user name that this entry should belong to. The allowed string length is 1 to 31 . The valid user name is a combination of letters, numbers, and underscores.
Password	The password of the user. The allowed string length is 1 to 31 .
Password (again)	Type the user password again for confirmation.
Privilege Level	The privilege level of the user. The allowed range is 1 to 15 . If the privilege level value is 15, it can access all groups (i.e., it is granted full control of the device). But other values need to refer to each group privilege level. User privileges should be the same or greater than the group privilege level to have access to that group. By default, most groups' privilege level 5 has read-only access and privilege level 10 has read-write access. System maintenance (software upload, factory defaults, etc.) requires user 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

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

- Click **Cancel** to undo changes and return to the Users Configuration page.
- Click **Delete User** to delete the current user. This function is not available for new configurations (i.e., add new user).

After a new user is added, the new user entry appears in the Users Configuration page.

User Name	Privilege Level
admin	15
quest	5
Test	1

Add New User

Note: If a password is forgotten after changing the default password, press the reset button on the front panel of the industrial managed switch for over 10 seconds and then release it. The current settings, including VLAN, will be erased and the industrial managed switch restores to default mode.

Privilege levels

This page provides an overview of the privilege levels. After setup is complete, click the **Apply** button and log in to the web interface with the new user name and password. The following appears:

Privilege Level Configuration					
Group Name	Privilege Levels				
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write	
Aggregation	5 ▾	10 ▾	5 ▾	10 ▾	
Diagnostics	5 ▾	10 ▾	5 ▾	10 ▾	
DIDO	5 ▾	10 ▾	5 ▾	10 ▾	
Firmware	5 ▾	10 ▾	5 ▾	10 ▾	
IP	5 ▾	10 ▾	5 ▾	10 ▾	
IPMC_Snooping	5 ▾	10 ▾	5 ▾	10 ▾	
LACP	5 ▾	10 ▾	5 ▾	10 ▾	
LLDP	5 ▾	10 ▾	5 ▾	10 ▾	
Loop_Protect	5 ▾	10 ▾	5 ▾	10 ▾	
MAC_Table	5 ▾	10 ▾	5 ▾	10 ▾	
Miscellaneous	15 ▾	15 ▾	15 ▾	15 ▾	
MVR	5 ▾	10 ▾	5 ▾	10 ▾	
NTP	5 ▾	10 ▾	5 ▾	10 ▾	
POE	5 ▾	10 ▾	5 ▾	10 ▾	
Ports	5 ▾	10 ▾	1 ▾	10 ▾	
Private_VLANs	5 ▾	10 ▾	5 ▾	10 ▾	
QoS	5 ▾	10 ▾	5 ▾	10 ▾	
Security (access)	10 ▾	10 ▾	5 ▾	10 ▾	
Security (network)	5 ▾	10 ▾	5 ▾	10 ▾	
Spanning_Tree	5 ▾	10 ▾	5 ▾	10 ▾	
System	5 ▾	10 ▾	1 ▾	10 ▾	
UPnP	5 ▾	10 ▾	5 ▾	10 ▾	
VLANs	5 ▾	10 ▾	5 ▾	10 ▾	
Voice_VLAN	5 ▾	10 ▾	5 ▾	10 ▾	

Apply Reset

This page includes the following fields:

Object	Description
Group name	The name identifies 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 detail: System: Contact, Name, Location, Timezone, Log. Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, and 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 Level	Every privilege level group has an authorization level for the following sub groups: Configuration read-only Configuration/execute read-write Status/statistics read-only Status/statistics read-write (e.g., for clearing of statistics)

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

NTP configuration

Configure NTP on this page. NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (data grams) as a transport layer. You can specify NTP servers in this page.

NTP Configuration

Mode	Disabled ▾	
Server 1	pool.ntp.org	
Server 2	europe.pool.ntp.org	
Server 3	north-america.pool.ntp.org	
Server 4	asia.pool.ntp.org	
Server 5	oceania.pool.ntp.org	

System Time Correction Manually

User Manually	☐ Enable	
Year	1970	(1970 ~ 2037)
Month	1	(1 ~ 12)
Day	1	(1 ~ 31)
Hour	0	(0 ~ 23)
Minute	0	(0 ~ 59)
Second	0	(0 ~ 59)

This page includes the following fields:

Object	Description
Mode	Indicates the NTP mode operation. Possible modes are: Enabled: Enable NTP mode operation. When enabling NTP mode operation, the agent forwards and transfers NTP messages between the clients and the server when they are not on the same subnet domain. Disabled: Disable NTP mode operation.
Server#	Provides the NTP IPv4 or IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). 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 only appear once. It also uses an IPv4 address (for example, '::192.1.2.34').
User Manually	Allows the user to enable set up system time manually. System time will be lost after system reboot since there is no battery to keep time running.
Year	Allows the user to input year value. (it supports from 1970 to 2037 only)
Month	Allows the user to input month value. (1 to 12 month).
Day	Allows the user to input day value. (1 to 31 days).
Hour	Allows the user to input hour value. (00 to 23 hours).
Minute	Allows the user to input minute value. (0 to 59 minutes).

Object	Description
Second	Allows the user to input second value. (0 to 59 seconds).

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Time configuration

A time zone is a region that has a uniform standard time for legal, commercial, and social purposes. It is convenient for areas in close commercial or other communication to maintain the same time, so time zones tend to follow the boundaries of countries and their subdivisions. Configure the time zone on the Time Zone Configuration page.

This page includes the following fields:

Object	Description
Time Zone	Lists various Time Zones worldwide. Select the appropriate Time Zone from the drop-down list and click Save .
Acronym	This is a user configurable acronym (up to 16 characters) used to identify the time zone.
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

Object	Description
	every year. Select Non-Recurring and configure the Daylight Saving Time duration for single time configuration. (Default: Disabled).
Start Time Settings	Week - Select the starting week number. Day - Select the starting day. Month - Select the starting month. Hours - Select the starting hour. Minutes - Select the starting minute.
End Time Settings	Week - Select the ending week number. Day - Select the ending day. Month - Select the ending month. Hours - Select the ending hour. Minutes - Select the ending minute
Offset Settings	Enter the number of minutes (1 to 1440) to add during Daylight Saving Time.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

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 home (data sharing, communications, and entertainment) and corporate environments for easy installation of computer components. Configure UPnP on the UPnP Configuration page.

UPnP Configuration	
Mode	Disabled ▾
Advertising Duration	100
IP Addressing Mode	Dynamic ▾
Static VLAN Interface ID	1

Apply Reset

This page includes the following fields:

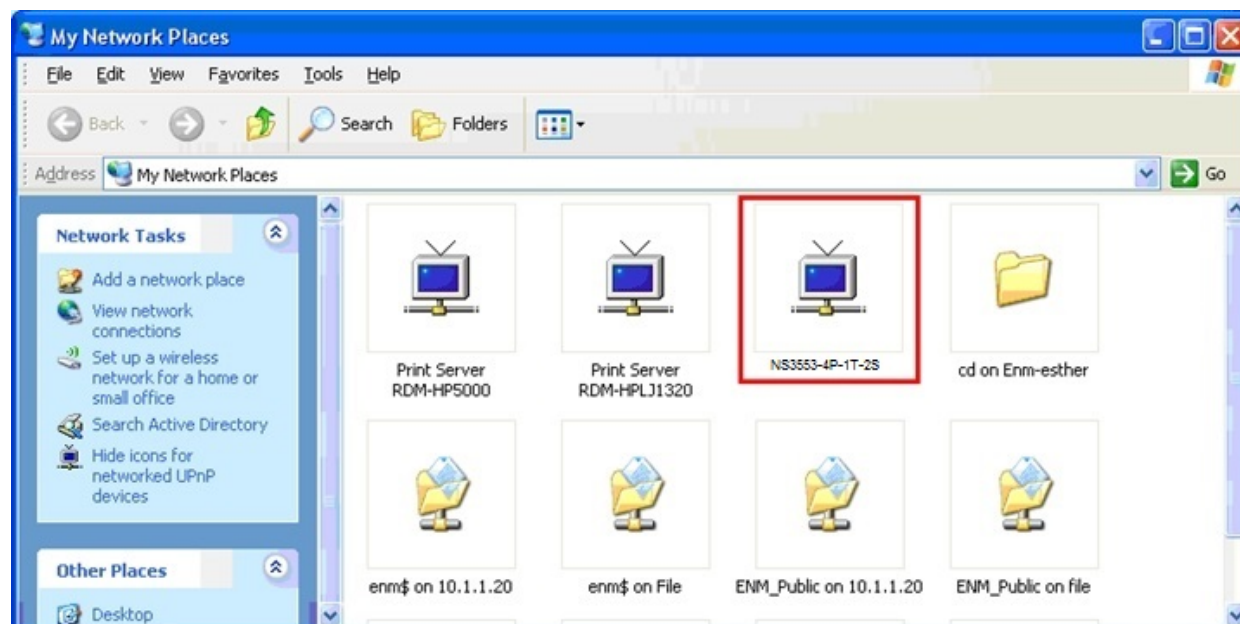
Object	Description
Mode	Indicates the UPnP operation mode. Possible modes are: Enabled : Enable UPnP mode operation. Disabled : Disable UPnP mode operation. When the mode is enabled, two ACEs are added automatically to trap UPnP related packets to the CPU. The ACEs are automatically removed when the

Object	Description
	mode is disabled.
Advertising Duration	The duration, carried in SSDP packets, is used to inform a control point or control points how often it or they should receive a SSDP advertisement message from this switch. If a control point does not receive any message within the duration, it will think that the switch no longer exists. Due to the unreliable nature of UDP, in the standard it is recommended that such refreshing of advertisements to be done at less than one-half of the advertising duration. In the implementation, the switch sends SSDP messages periodically at the interval one-half of the advertising duration minus 30 seconds. Valid values are in the range 100 to 86400.
IP Address Mode	IP addressing mode provides two ways to determine IP address assignment: Dynamic: Default selection for UPnP. UPnP module helps users choosing the IP address of the switch device. It finds the first available system IP address. Static: The user specifies the IP interface VLAN for choosing the IP address of the switch device.
Static VLAN Interface ID	The index of the specific IP VLAN interface. It will only be applied when IP Addressing Mode is static. Valid configurable values ranges from 1 to 4095. Default value is 1.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

An example of how UPnP devices appear in My Network Places:



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). This sub-option should include information specific to which circuit the request came in on.
- Remote ID (option 2). This sub-option is designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is four bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes representing the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in a standalone switch it always equals 0; in the switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The remote ID is six bytes in length, and the value equals the DHCP relay agent's MAC address. Configure DHCP relay in the DHCP Relay Configuration page.

DHCP Relay Configuration	
Relay Mode	Disabled
Relay Server	0.0.0.0
Relay Information Mode	Disabled
Relay Information Policy	Keep
Apply Reset	

This page includes the following fields:

Object	Description
Relay Mode	Indicates the DHCP relay mode operation. Possible modes are: Enabled: Enable DHCP relay mode operation. When enabling DHCP relay mode operation, the agent forwards and transfers DHCP messages between the clients and the server when they are not on the same subnet domain and the DHCP broadcast message won't flood due to security settings. Disabled: Disable DHCP relay mode operation.
Relay Server	Indicates the DHCP relay server IP address. A DHCP relay agent is used to forward and transfer DHCP messages between the clients and the server when they are not on the same subnet domain.
Relay Information Mode	Indicates the DHCP relay information mode option operation. Possible modes are: Enabled: Enable DHCP relay information mode operation. When enabling DHCP relay information mode operation, the agent inserts specific information (option82) 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.

Object	Description
Relay Information Policy	Indicates the DHCP relay information option policy. When enabling DHCP relay information mode operation, if the agent receives a DHCP message that already contains relay agent information, it will enforce the policy. This only works when DHCP relay information operation mode is enabled. Options are: Replace: Replace the original relay information when receiving a DHCP message that already contains it. Keep: Keep the original relay information when receiving a DHCP message that already contains it. Drop: Drop the package when receiving a DHCP message that already contains relay information.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

DHCP relay statistics

This page provides statistics for DHCP relay.

DHCP Relay Statistics							
Server Statistics							
Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0
Client Statistics							
Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option	
0	0	0	0	0	0	0	0
Auto Refresh ☐ Refresh Clear							

Server statistics:

Object	Description
Transmit to Server	The number of packets relayed from client to server.
Transmit Error	The number of packets erroneously sent to clients.
Receive from Server	The number of packets received from the server.
Receive Missing Agent Option	The number of packets received without agent information 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 in which the Circuit ID option does not match with the known circuit ID.
Receive Bad Remote ID	The number of packets in which the Remote ID option does not match with the known Remote ID.

Client statistics:

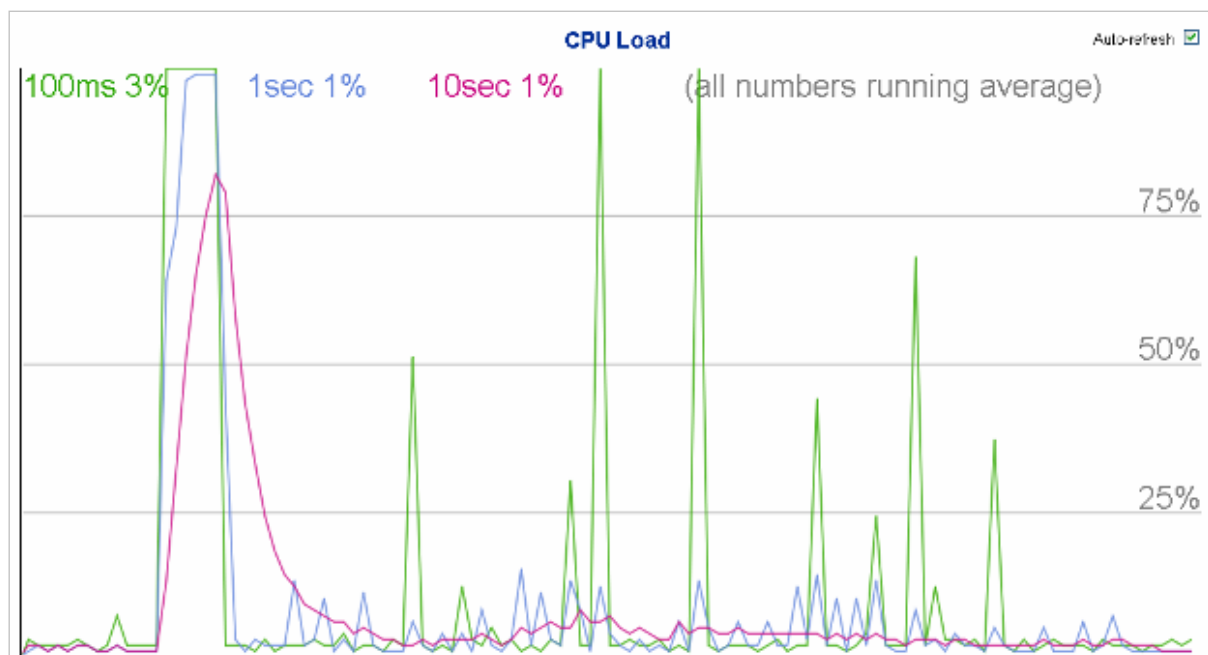
Object	Description
Transmit to Client	The number of packets relayed from server to client.
Transmit Error	The number of packets erroneously sent to servers.
Receive from Client	The number of packets received from the server.
Receive Agent Option	The number of packets received with the relay agent information option.
Replace Agent Option	The number of packets received is replaced with the relay agent information option.
Keep Agent Option	The number of packets received is kept with the relay agent information option.
Drop Agent Option	The number of packets received is dropped with the relay agent information option.

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to immediately refresh the page.
- Click **Clear** to clear all statistics.

CPU load

This page displays the CPU load using an SVG graph. The load is measured as average over the last 100 ms, 1 second, and 10 second intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well. To display the SVG graph, the browser must support the SVG format. Consult the SVG Wiki for more information on browser support as a plugin may be required.



Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.

Note: If the browser does not display anything on this page, download the Adobe SVG tool and install it in the computer.

System log

The System Log Information page shows the industrial managed switch system log information.

System Log Information

Auto-refresh ☐

Refresh

Clear

Hide

Download

|<<

<<

>>

>>|

Level

All

Clear Level

All

The total number of entries is 2 for the given level.

Start from ID with entries per page.

ID	Level	Time	Message
1	Informational	1970-01-01 Thu 00:00:45+00:00	SYS-BOOTING: Switch just made a cold boot.
2	Informational	1970-01-01 Thu 00:03:16+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/3, changed state to up.

The page includes the following fields:

Object	Description
ID	The ID (>= 1) of the system log entry.
Level	The level of the system log entry. The following level types are supported: Info: Information level of the system log. Warning: Warning level of the system log. Error: Error level of the system log. All: All levels.
Clear Level	Clears the system log entry level. The following level types are supported: Info: Information level of the system log. Warning: Warning level of the system log. Error: Error level of the system log. All: All levels.
Time	The time of the system log entry.
Message	The message of the system log entry.

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.

- Click **Refresh** to immediately refresh the page.
- Click **Clear** to clear all statistics.
- Click **Hide** to hide the selected log entries.
- Click **Download** to download the selected log entries.
- Click **I<<** to update the system log entries, starting from the first available entry ID.
- Click **<<** to update the system log entries, ending at the last entry currently displayed.
- Click **>>** to update the system log entries, starting from the last entry currently displayed.
- Click **>>I** to update the system log entries, ending at the last available entry ID.

Detailed log

The Detailed System Log Information page displays the industrial managed switch system log information details.

Detailed System Log Information

Download Refresh I<< << >> >>I Print

ID

Message

Level	Info
Time	1970-01-01 Thu 00:00:09+00:00
Message	Switch just made a cold boot.

The page includes the following fields:

Object	Description
ID	The ID (≥ 1) of the system log entry.
Message	The message of the system log entry.

Buttons

- Click **Download** to download the system log entry to the current entry ID.
- Click **Refresh** to update the system log entry to the current entry ID.
- Click **I<<** to update the system log entries, starting from the first available entry ID.
- Click **<<** to update the system log entries, ending at the last entry currently displayed.

- Click **>>** to update the system log entries, starting from the last entry currently displayed.
- Click **>>I** to update the system log entries, ending at the last available entry ID.
- Click **Print** to print the system log entry to the current entry ID.

Remote syslog

The System Log Configuration page displays the industrial managed switch remote system log information details.

The page includes the following fields:

Object	Description
Mode	Indicates the server mode operation. When the mode operation is enabled, the syslog message is sent to the 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 sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet is always sent out even if the syslog server does not exist. Selections include: Enabled: Enable remote syslog mode operation. Disabled: Disable remote syslog mode operation.
Syslog Server IP	Indicates the IPv4 host address of syslog server. If the switch provides the DNS feature, it also can be a host name.
Syslog Level	Indicates what kind of message is sent to the syslog server. Selections include: Info: Send information, warnings, and errors. Warning: Send warnings and errors. Error: Send errors.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

SMTP configuration

The SMTP Configuration page displays the industrial managed switch SMTP configuration details.

SMTP Configuration

SMTP Mode	☐ Enable	
SMTP Server	interlogix.com	(<128 Digits) test
SMTP Port	25	(1 ~ 65535)
SMTP Authentication	☐ Enable	
Authentication User Name	1234	(< 64 Digits)
Authentication Password	••••	(< 21 Digits)
E-mail From	abcd@interlogix.com	(< 128 Digits)
E-mail Subject	UTC IFS	(< 64 Digits)
E-mail 1 To	abcd@interlogix.com	(< 128 Digits)
E-mail 2 To	abcd@interlogix.com	(< 128 Digits)

Apply
Reset

The page includes the following fields:

Object	Description
SMTP Mode	Controls whether or not SMTP is enabled on the switch.
SMTP Server	Type the SMTP server name or the IP address of the SMTP server.
SMTP Port	Set the port number of SMTP service.
SMTP Authentication	SMTP authentication is enabled if selected. Authentication is required when an email is sent.
Authentication User Name	Type the user name for the SMTP server if Authentication is Enable .
Authentication Password	Type the password for the SMTP server if Authentication is Enable .
E-mail From	Type the sender's email address. This address is used for reply emails.
E-mail Subject	Type the subject/title of the email.
E-mail 1 To / E-mail 2 To	Type the receiver's email address.

Buttons

- Click **test** to send a test mail to the mail server to indicate if the account is available.
- Click **Save** to save changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Digital input/output

Digital input allows a user to log an external device (such as an industrial cooler) as dead or alive, or something else. The system will log a user customized message into system log and syslog, and issue SNMP trap or an alarm email.

Digital Output allows a user to monitor the switch port and power, and allows the system to issue a high or low signal to an external device (such as an alarm) when the monitor port or power has failed.

Digital Input/Output Control Configuration

Digital Input 0		Digital Input 1	
Enable	☐ Enable	Enable	☐ Enable
Condition	High to Low ▾	Condition	High to Low ▾
Event Description	Customize DIO Message.	Event Description	Customize DI1 Message.
Event	☐ System Log ☐ SNMP Trap	Event	☐ System Log ☐ SNMP Trap

Digital Output 0		Digital Output 1	
Enable	☐ Enable	Enable	☐ Enable
Event	☐ Power Fail ☐ Port Fail ☐ DI 0 ☐ DI 1	Event	☐ Power Fail ☐ Port Fail ☐ DI 0 ☐ DI 1
Condition	High to Low ▾	Condition	High to Low ▾
Power Alarm	☐ DC 1 ☐ DC 2	Power Alarm	☐ DC 1 ☐ DC 2
Port Fail Alarm	1 2 3 4 5 6 7 8 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ 9 10 11 12 ☐ ☐ ☐ ☐	Port Fail Alarm	1 2 3 4 5 6 7 8 ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ 9 10 11 12 ☐ ☐ ☐ ☐

The page includes the following fields:

Object	Description
Enable	Select the Enable check box to enable the digital input/output function. Deselect the Enable check bo to disable the digital input/output function.
Condition	As Digital Input: Allows the user to select High to Low or Low to High. This means a signal received by system is from High to Low or From Low to High. It will trigger an action that logs a customize message or issue the message from the switch. As Digital Output: Allows user to select High to Low or Low to High. This means that when the switch is power-failed or port-failed, then system will issue a High or Low signal to an external device such as an alarm.
Event Description	Allows user to set a customized message for Digital Input function alarming.
Event	As Digital Input: Allows the user to record alarm message to System log, syslog or issues out via SNMP Trap or SMTP. As default SNMP Trap and SMTP are disabled, please enable them first if you want to issue alarm message via them. As Digital Output: Allows the user to monitor an alarm from port failure, power failure, Digital Input 0 (DI 0), and Digital Input 1 (DI 1) which means if the Digital Output has detected these events, then Digital Output would

Object	Description
	be triggered according to the setting of Condition.
Power Alarm	Allows the user to choose the power module to be monitored.
Port Alarm	Allows the user to choose the port to be monitored.

Buttons

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

Fault alarm

The Fault Alarm Control Configuration page manages the fault alarm output.

Fault Alarm Control Configuration

Fault Alarm Output	
Enable	☐ Enable
Record	☐ System Log ☐ SNMP Trap
Action	☐ Port Fail ☐ Power Fail
Power Alarm	☐ DC 1 ☐ DC 2
Port Alarm	12345678 ☐☐☐☐☐☐☐☐ 9101112 ☐☐☐☐

The page includes the following fields:

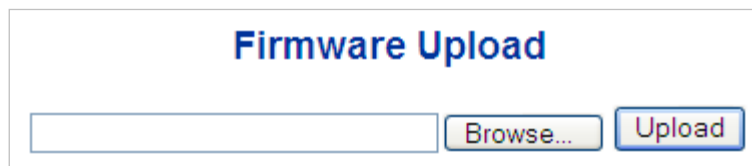
Object	Description
Enable	Controls whether or not the Fault Alarm is enabled on this switch.
Record	Controls whether or not Record is sending a System log or SNMP Trap, or both.
Action	Controls Port Fail or Power Fail, or both, for fault detection.
Power Alarm	Controls AC, DC1, or DC2, or all three, for fault detection.
Port Alarm	Controls ports for fault detection.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

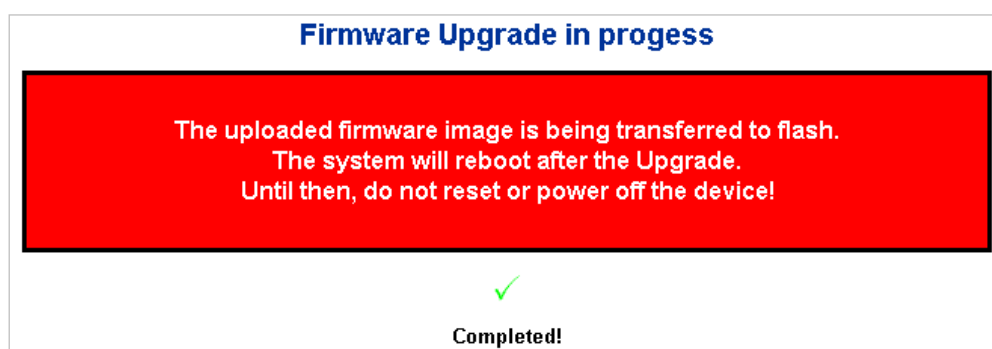
Web firmware upgrade

Update the industrial managed switch firmware using the Firmware Upload page.



To open the Firmware Upload page:

1. Click **System > Web Firmware Upgrade**. The Firmware Upload page appears.
2. Click the **Browse** button on the main page. The file selection menu to choose firmware appears.
3. Select the firmware file and then click **Upload**. The Software Upload Progress displays the file with upload status.
4. After the software is uploaded to the system successfully, the following screen appears. The system loads the new software after reboot.

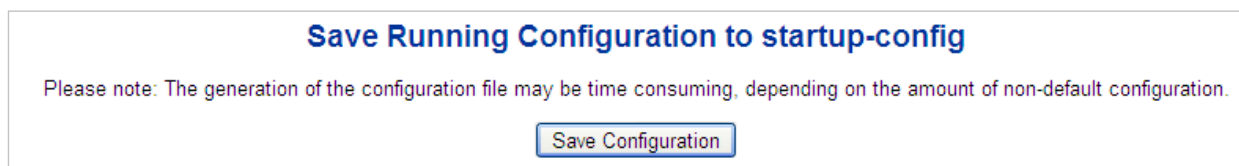


Note: DO NOT Power OFF the industrial managed switch until the update progress is completed.

Note: Do not quit the Firmware Upgrade page without clicking the **OK** button after the image is loaded. Otherwise, the system won't apply the new firmware and the user has to repeat the firmware upgrade process.

Save startup configuration

This function ensures that the current active configuration can be used after the next reboot.



After clicking **Save Configuration**, the following screen appears.

Save Running Configuration to startup-config

startup-config saved successfully.

Configuration download

The industrial managed 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.

There are three system files:

- **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.
- **default-config**: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.

It is also possible to store up to two other files and apply them to running-config, thereby switching configuration.

The Download Configuration page permits the download of the running-config, startup-config, and default-config system files to the switch.

Download Configuration

Select configuration file to save.

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

File Name
☐ running-config
☐ default-config
☐ startup-config

Configuration upload

The Upload Configuration page permits the upload of the running-config and startup-config to the switch.

Upload Configuration

File To Upload

Destination File

File Name	Parameters
☐ running-config	☒ Replace ☐ Merge
☐ startup-config	
☐ Create new file	

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 file system is full (i.e., it contains the system files mentioned above plus two other files), it is not possible to create new files unless an existing file is overwritten or another is deleted first.

Configuration activate

The Activate Configuration page permits activation of the startup-config and default-config files on the switch.

Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, potentially leading to loss of management connectivity.

Please note: The activated configuration file will not be saved to startup-config automatically.

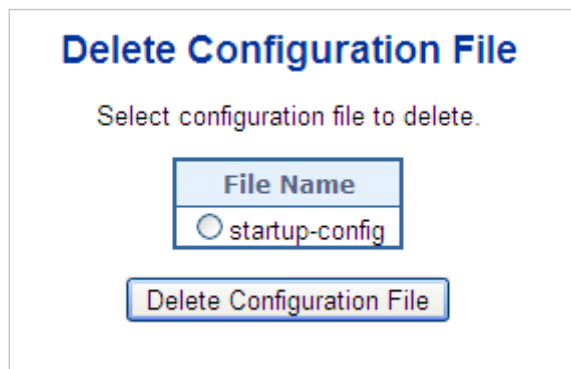
File Name
☐ default-config
☐ startup-config

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 initiates the process of completely replacing the existing configuration with that of the selected file.

Configuration delete

The Delete Configuration page permits the deletion of the startup-config and default-config files which are stored in Flash memory. If this is performed and the switch is rebooted without a prior save operation, it effectively resets the switch to default configuration.



Delete Configuration File

Select configuration file to delete.

File Name

☐ startup-config

Delete Configuration File

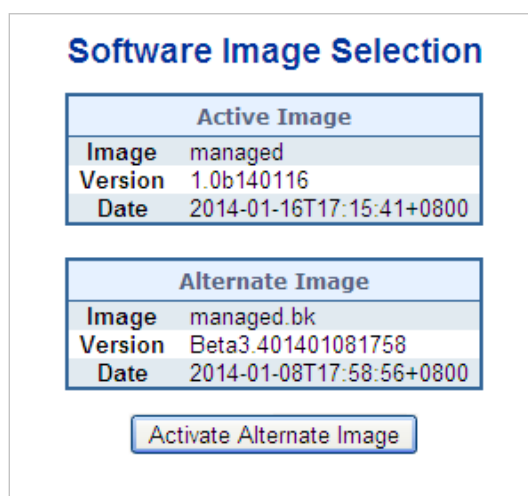
Image select

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: If 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:

1. 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 activate the primary image slot and use it instead.
2. The firmware version and date information may be empty for older firmware releases. This does not constitute an error.



Software Image Selection

Active Image	
Image	managed
Version	1.0b140116
Date	2014-01-16T17:15:41+0800

Alternate Image	
Image	managed.bk
Version	Beta3.401401081758
Date	2014-01-08T17:58:56+0800

Activate Alternate Image

The page includes the following fields:

Object	Description
Image	The flash index name of the firmware image. The name of primary (preferred) image is image, the alternate image is named image.bk.
Version	The version of the firmware image.
Date	The date when the firmware was produced.

Buttons

- Click **Activate Alternate Image** to use the alternate image. This button may be disabled depending on the system state.

System reboot

The Restart Device page permits the device to be rebooted from a remote location. After clicking the **Yes** button to restart, log in to the web interface about 60 seconds later.

Restart Device

Are you sure you want to perform a Restart?

Buttons

- Click **Yes** to reboot the system.
- Click **No** to return to the Port State page without rebooting the system.

Note: You can also check the SYS LED on the front panel to identify whether or not the system is loaded completely. If the SYS LED is blinking, then it is in the firmware load stage; if the SYS LED light is on, you can use the web browser to log in to the industrial managed switch.

UDLD

The UDLD Port Configuration page permits the user to inspect and change the current Unidirectional Link Detection (UDLD) configurations.

UDLD Port Configuration

Port	UDLD mode	Message Interval
*	<All>	7
1	Disable	7
2	Disable	7
3	Disable	7
4	Disable	7
5	Disable	7
6	Disable	7
7	Disable	7
8	Disable	7
9	Disable	7
10	Disable	7
11	Disable	7
12	Disable	7
13	Disable	7
14	Disable	7
15	Disable	7
16	Disable	7
17	Disable	7
18	Disable	7
19	Disable	7
20	Disable	7
21	Disable	7
22	Disable	7
23	Disable	7
24	Disable	7
25	Disable	7
26	Disable	7
27	Disable	7
28	Disable	7

The page includes the following fields:

Object	Description
Port	Port number of the switch.
UDLD Mode	Configures the UDLD mode on a port. Selections include Disable, Normal and Aggressive. Default mode is Disable. Disable – In disabled mode, UDLD functionality doesn't exist on the port. Normal – In normal mode, if the link state of the port was determined to be unidirectional, it will not affect the port state. Aggressive – In aggressive mode, unidirectional detected ports will get shut down. To bring back the ports up, disable UDLD on the ports.
Message Interval	Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is from 7 to 90 seconds (default value is 7 seconds). Currently, the default time interval is supported due to lack of detailed information in RFC 5171.

Buttons

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

UDLD status

The Detailed UDLD Status/Neighbor Status page displays the UDLD status of the ports.

Detailed UDLD Status for Port 1

Port 1 ▼

Auto-refresh ☐

Refresh

UDLD status	
UDLD Admin state	Disable
Device ID(local)	A8-F7-E0-35-44-59
Device Name(local)	NS3553-4P-1T-2S
Bidirectional State	Indeterminant

Neighbour Status

Port	Device Id	Link Status	Device Name
<i>No Neighbour ports enabled or no existing partners</i>			

UDLD port status

The page includes the following fields:

Object	Description
UDLD Admin State	The current port state of the logical port, Enabled if any of state(Normal,Aggressive) is Enabled.
Device ID (Local)	The ID of Device.
Device Name (Local)	Name of the Device.
Bidirectional State	The current state of the port.

Neighbor status

The page includes the following fields:

Object	Description
Port	The current port of the neighbor device.
Device ID	The current ID of the neighbor device.
Link Status	The current link status of the neighbor port.

Object	Description
Device Name	Name of the neighbor device.

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

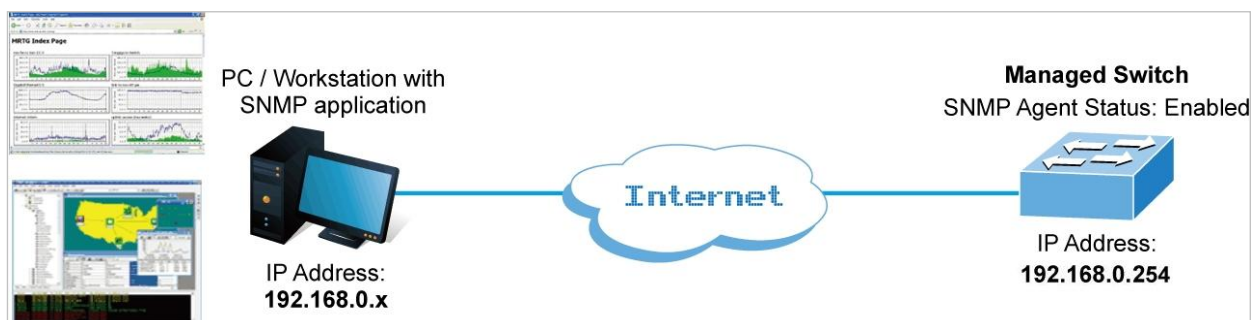
Simple Network Management Protocol (SNMP)

SNMP overview

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP permits network administrators to manage network performance, find and solve network problems, and plan for network growth.

An SNMP-managed network consists of the following:

- **Network management stations (NMSs):** Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.
- **Agents:** Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.
- **Management information base (MIB):** An MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.
- **Network-management protocol:** A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.



SNMP operations

SNMP itself is a simple request/response protocol. NMSs can send multiple requests without receiving a response.

- **Get** – Allows the NMS to retrieve an object instance from the agent.
- **Set** – Allows the NMS to set values for object instances within an agent.
- **Trap** – Used by the agent to asynchronously inform the NMS of some event. The SNMPv2 trap message is designed to replace the SNMPv1 trap message.

SNMP community

An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group. An SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. SNMP default communities are:

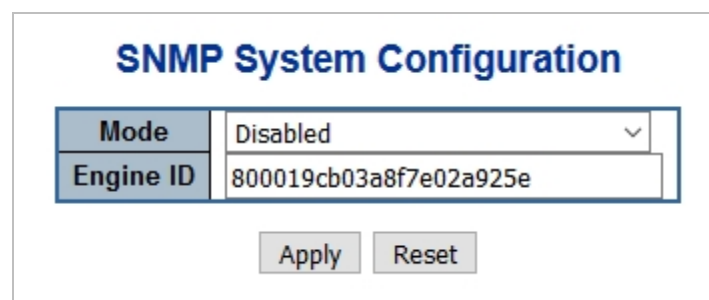
- Write (private)
- Read (public)

Use the SNMP Menu to display or configure the industrial managed switch's SNMP function. This section has the following items:

System Configuration	Configure SNMP on this page.
Trap Destination Configuration	Configure SNMP trap on this page.
Trap Source Configuration	Configure SNMP trap source on this page.
System Information	The system information is provided here.
SNMPv3 Communities	Configure SNMPv3 communities table on this page.
SNMPv3 Users	Configure SNMPv3 users table on this page.
SNMPv3 Groups	Configure SNMPv3 groups table on this page.
SNMPv3 Views	Configure SNMPv3 views table on this page.
SNMPv3 Access	Configure SNMPv3 accesses table on this page.

SNMP system configuration

Configure SNMP on the SNMP System Configuration page.



SNMP System Configuration

Mode	Disabled
Engine ID	800019cb03a8f7e02a925e

Apply Reset

The page includes the following fields:

Object	Description
Mode	Indicates the SNMP mode operation. Selections include: Enabled: Enable SNMP mode operation. Disabled: Disable SNMP mode operation.
Engine ID	Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

SNMP trap configuration

Configure the SNMP trap on the SNMP Trap Configuration page.

SNMP Trap Configuration

Trap Config Name	
Trap Mode	Disabled ▾
Trap Version	SNMP v2c ▾
Trap Community	public
Trap Destination Address	
Trap Destination Port	162
Trap Inform Mode	Disabled ▾
Trap Inform Timeout (seconds)	3
Trap Inform Retry Times	5
Trap Security Engine ID	800019cb03a8f7e02a925e
Trap Security Name	None ▾

The page includes the following fields:

Object	Description
Trap Config	Indicates the trap configuration name. The allowed string length is 0 to 255, and the allowed content is ASCII characters from 33 to 126.
Trap Mode	Indicates the SNMP trap mode operation. Selections include: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.
Trap Version	Indicates the SNMP trap supported version. Selections include: SNMP v1: Set SNMP trap supported version 1. SNMP v2c: Set SNMP trap supported version 2c. SNMP v3: Set SNMP trap supported version 3.
Write Community	Indicates the community write access string to permit access to the SNMP agent. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. The field is applicable only when the SNMP version is SNMPv1 or SNMPv2c. If the SNMP version is SNMPv3, the community string will be associated with the SNMPv3 communities table. It provides more flexibility to configure a security name than a SNMPv1 or SNMPv2c community string. In addition to the community string, a particular range of source addresses can be used to restrict the source subnet.
Trap Community	Indicates the community access string when sending the SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126.

Object	Description
Trap Destination Address	Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w') as well as a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash. Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
Trap Destination Port	Indicates the SNMP trap destination port. The SNMP agent sends an SNMP message via this port. The port range is 1~65535.
Trap Inform Mode	Indicates the SNMP trap inform mode operation. Selections include: Enabled: Enable SNMP trap authentication failure. Disabled: Disable SNMP trap authentication failure.
Trap Inform Timeout (seconds)	Indicates the SNMP trap inform timeout. The allowed range is 0 to 2147.
Trap Inform Retry Times	Indicates the SNMP trap inform retry times. The allowed range is 0 to 255.
Trap Probe Security Engine ID	Indicates the SNMPv3 trap probe security engine ID mode of operation. Selections include: Enabled: Enable SNMP trap probe security engine ID mode of operation. Disabled: Disable SNMP trap probe security engine ID mode of operation.
Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When Trap Probe Security Engine ID is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all zeros and all-F's are not allowed.
Trap Security Name	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

SNMP system information

The switch system information is provided in the System Information Configuration page.

The page includes the following fields:

Object	Description
System Contact	The textual identification of the contact person for this managed node and 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. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
System Location	The physical location of this node (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

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Trap source configuration

Configure SNMP trap source configuration on the Trap Configuration page. You don't need to configure the subset OID if you want to apply this trap to the whole SNMP OID. For example, if you want to apply a trap for any port "link down" or "link up," then configure them like as in the screen below. If you want to apply link up or link down to one of ports, input the SNMP OID to the subset OID column. For example, if you want apply a link down trap to port1, input "10000001" in the linkDown entry.

Trap Configuration

Trap Source Configurations

Delete	Name	Type	Subset OID
☐	linkUp	included ▾	
☐	newRoot	included ▾	
☐	linkDown	included ▾	
☐	coldStart	included ▾	
☐	warmStart	included ▾	
☐	topologyChange	included ▾	
☐	IldpRemTablesChange	included ▾	
☐	authenticationFailure	included ▾	

The page includes the following fields:

Object	Description
Delete	Select the check box to delete the entry. It will be deleted during the next save.
Name	Indicates the name for the entry.
Type	The filter type for the entry. Selections include: 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 depends on the trap name type. For example, the ifIndex is the subset OID of linkUp and linkDown. A valid subset OID is one or more digital numbers (0-4294967295) or asterisk(*) which are separated by dots(.). The first character must not begin with an asterisk (*) and the maximum of OID count must not exceed 128.

Buttons

- Click **Add New Entry** to add a new community entry.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

SNMPv3 configuration

SNMPv3 communities

Configure SNMPv3 communities in the SNMPv3 Community Configuration page. The entry index key is Community.

Delete	Community name	Community secret	Source IP	Source Prefix
☐	public	public	0.0.0.0	0
☐	private	private	0.0.0.0	0

The page includes the following fields:

Object	Description
Delete	Select the check box to delete the entry. It will be deleted during the next save.
Community Name	Indicates the security name to map the community to the SNMP Groups configuration. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Community Secret	Indicates the community secret (access string) to permit access using SNMPv1 and SNMPv2c to the SNMP agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Source IP	Indicates the SNMP access source address. A particular range of source addresses can be used to restrict the source subnet when combined with the source mask.
Source Mask	Indicates the SNMP access source address mask.

Buttons

- Click **Add New Entry** to add a new community entry.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

SNMPv3 users

Configure SNMPv3 users on the SNMPv3 User Configuration page. The entry index keys are Engine ID and User Name.

SNMPv3 User Configuration							
Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
☐	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None

The page includes the following fields:

Object	Description
Delete	Select Delete to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with a number of digits between 10 and 64, but all zeros and all 'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always the same as the snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is local user, otherwise it is a remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Security Level	Indicates the security model that this entry should belong to. Selections include: NoAuth, NoPriv: None authentication and none privacy. Auth, NoPriv: Authentication and none privacy. Auth, Priv: Authentication and privacy. The value of the security level cannot be modified if the entry already exists. Ensure that the value is set correctly.
Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Selections include: None: None authentication protocol. MD5: An optional flag to indicate that this user using MD5 authentication protocol. SHA: An optional flag to indicate that this user using SHA authentication protocol. The value of security level cannot be modified if the entry already exists. Ensure that the value is set correctly.
Authentication Password	A string identifying the authentication pass phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is the ASCII characters from 33 to 126.
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Selections include: None: None privacy protocol.

Object	Description
	DES: An optional flag to indicate that this user using DES authentication protocol. AES: An optional flag to indicate that this user uses AES authentication protocol.
Privacy Password	A string identifying the privacy pass phrase. The allowed string length is 8 to 32, and the allowed content is the ASCII characters from 33 to 126.

Buttons

- Click **Add New Entry** to add a new user entry.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

SNMPv3 groups

Configure SNMPv3 groups on the SMNPv3 Group Configuration page. The entry index keys are Security Model and Security Name.

SNMPv3 Group Configuration

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

The page includes the following fields:

Object	Description
Delete	Select Delete to delete the entry. It will be deleted during the next save.
Security Model	Indicates the security model that this entry should belong to. Selections include: v1: Reserved for SNMPv1. v2c: Reserved for SNMPv2c. usm: User-based Security Model (USM).
Security Name	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.

Buttons

- Click **Add New Entry** to add a new group entry.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

SNMPv3 views

Configure SNMPv3 views table in the SNMPv3 View Configuration page. The entry index keys are View Name and OID Subtree.

The image shows a web interface titled "SNMPv3 View Configuration". It contains a table with the following structure:

Delete	View Name	View Type	OID Subtree
☐	default_view	included ▼	.1

Below the table are three buttons: "Add New Entry", "Apply", and "Reset".

The page includes the following fields:

Object	Description
Delete	Select Delete to delete the entry. It will be deleted during the next save.
View Name	A string identifies the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
View Type	Indicates the view type that this entry should belong to. Selections include: included: An optional flag to indicate that this view subtree should be included. excluded: An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is excluded, it should exist in another view entry in which the view type is included and it's OID subtree overrides the excluded view entry.
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk (*).

Buttons

- Click **Add New Entry** to add a new view entry.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

SNMPv3 access

Configure SNMPv3 access on the SNMPv3 Access Configuration page. The entry index keys are Group Name, Security Model, and Security Level.

SNMPv3 Access Configuration					
Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
☐	default_ro_group	any	NoAuth, NoPriv	default_view ▼	None ▼
☐	default_rw_group	any	NoAuth, NoPriv	default_view ▼	default_view ▼

The page includes the following fields:

Object	Description
Delete	Select Delete to delete the entry. It will be deleted during the next save.
Group Name	A string identifies the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126.
Security Model	Indicates the security model that this entry should belong to. Selections include: any : Accepted any security model (v1, v2c, usm). v1 : Reserved for SNMPv1. v2c : Reserved for SNMPv2c. usm : User-based Security Model (USM)
Security Level	Indicates the security model that this entry should belong to. Selections include: NoAuth, NoPriv : None authentication and none privacy. Auth, NoPriv : Authentication and none 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 the 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 the ASCII characters from 33 to 126.

Buttons

- Click **Add New Entry** to add a new access entry.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Port management

Use the Port menu to display or configure the industrial managed switch ports. This section has the following items:

Port Configuration	Configures port connection settings
Port Statistics Overview	Lists Ethernet and RMON port statistics
Port Statistics Detail	Lists Ethernet and RMON port statistics
SFP Module Information	Displays SFP information
Port Mirror	Sets the source and target ports for mirroring

Port configuration

Ports can be configured on the Port Configuration page.

Port Configuration

Port	Port Description	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode
			Current	Configured	Current Rx	Current Tx	Configured		
*				<All>			☐	10056	<All>
1		●	Down	Auto	×	×	☐	10056	Discard
2		●	Down	Auto	×	×	☐	10056	Discard
3		●	Down	Auto	×	×	☐	10056	Discard
4		●	Down	Auto	×	×	☐	10056	Discard
5		●	Down	Auto	×	×	☐	10056	Discard
6		●	Down	Auto	×	×	☐	10056	Discard
22		●	Down	Auto	×	×	☐	10056	Discard
23		●	1Gfdx	Auto	×	×	☐	10056	Discard
24		●	1Gfdx Fiber	Auto	×	×	☐	10056	Discard
25		●	Down	Auto Fiber (10G)	×	×	☐	10056	
26		●	Down	Auto Fiber (10G)	×	×	☐	10056	
27		●	Down	Auto Fiber (10G)	×	×	☐	10056	
28		●	Down	Auto Fiber (10G)	×	×	☐	10056	

Apply

Reset

Refresh

The page includes the following fields:

Object	Description
Port	This is the logical port number for this row.
Port Description	Indicates the per port description.
Link	The current link state is displayed graphically. Green indicates the link is up and red is down.
Current Link Speed	Provides the current link speed of the port.
Configured Link Speed	Select any available link speed for the given switch port. Draw the menu bar to select the mode. Auto: Setup Auto negotiation for copper interface. 10Mbps HDX: Force sets 10Mbps/Half-Duplex mode. 10Mbps FDX: Force sets 10Mbps/Full-Duplex mode. 100Mbps HDX: Force sets 100Mbps/Half-Duplex mode. 100Mbps FDX: Force sets 100Mbps/Full-Duplex mode. 1Gbps FDX: Force sets 10000Mbps/Full-Duplex mode. Disable: Shutdown the port manually.
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 if pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto-Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed.
Maximum Frame Size	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 1518 bytes to 9600 bytes.
Excessive Collision Mode	Configure port transmit collision behavior. Discard: Discard frame after 16 collisions (default). Restart: Restart back off algorithm after 16 collisions.

Note: If setting each port to run at 100M full-, 100M half-, 10M full-, and 10M half-speed modes, the auto-MDIX function will be disabled.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Click **Refresh** to refresh the page and undo all local changes.

Port statistics overview

The Port Statistics Overview page provides an overview of general traffic statistics for all switch ports.

Port Statistics Overview										
Port	Packets		Bytes		Errors		Drops		Filtered	
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0	0
27	0	0	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0	0	0

Auto-refresh ☐ [Download](#) [Refresh](#) [Clear](#) [Print](#)

The displayed counters are:

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

Buttons

- Click **Download** to download the Port Statistics Overview result as an Excel file.
- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear the counters for all ports.
- Click **Print** to print the Port Statistics Overview result.
- Select the **Auto-refresh** check box to enable an automatic refresh of the page at regular intervals.

Port statistics detail

The Port Statistics Detail page provides detailed traffic statistics for a specific switch port. Use the port select box to select which switch port details to display. The selected port belongs to the current unit, as reflected by the page header. 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.

Detailed Port Statistics Port 1			
Port 1 Auto-refresh Refresh Clear			
Receive Total		Transmit Total	
Rx Packets	2335	Tx Packets	2066
Rx Octets	431172	Tx Octets	1531131
Rx Unicast	2039	Tx Unicast	2050
Rx Multicast	48	Tx Multicast	11
Rx Broadcast	248	Tx Broadcast	5
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	1465	Tx 64 Bytes	242
Rx 65-127 Bytes	175	Tx 65-127 Bytes	53
Rx 128-255 Bytes	66	Tx 128-255 Bytes	523
Rx 256-511 Bytes	553	Tx 256-511 Bytes	203
Rx 512-1023 Bytes	76	Tx 512-1023 Bytes	284
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	761
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	2283	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	2066
Receive Error Counters		Transmit Error Counters	
Rx Drops	52	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	52		

The page includes the following fields:

Receive total and transmit total

Object	Description
Rx and Tx Packets	The number of received and transmitted (good and bad) packets
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes, including FCS, but excluding 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 has an opcode indicating a PAUSE operation.

Receive and transmit size counters

The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.

Receive and transmit queue counters

The number of received and transmitted packets per input and output queue.

Receive error counters

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

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

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

Transmit error counters

Object	Description
Tx Drops	The number of frames dropped due to output buffer congestion.
Tx Late/Exc. Coll.	The number of frames dropped due to excessive or late collisions.

Buttons

- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear the counters for all ports.
- Select the **Auto-refresh** check box to enable an automatic refresh of the page at regular intervals.

SFP module information

The industrial managed switch supports SFP modules with the digital diagnostics monitoring (DDM) function, which is also known as digital optical monitoring (DOM). You can check the physical or operational status of an SFP module via the SFP Module Information page. This page shows the operational status such as the transceiver type, speed, wavelength, optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage in real time. You can also use the port number hyperlinks to check the statistics on a specific interface.

SFP Module Information										
Port	Type	Speed	Wave Length(nm)	Distance(m)	Temperature (C)	Voltage(V)	Current(mA)	Tx power(dBm)	Rx power(dBm)	
25	--	--	--	--	--	--	--	--	--	
26	--	--	--	--	--	--	--	--	--	
27	--	--	--	--	--	--	--	--	--	
28	--	--	--	--	--	--	--	--	--	

SFP Monitor Event Alert: ☐ Sent trap

Warning Temperature: degrees C

Auto-refresh ☐

The page includes the following fields:

Object	Description
Type	Displays the type of current SFP module. The possible types are: 1000Base-SX 1000Base-LX 100Base-FX
Speed	Displays the speed of the current SFP module. Different vendors' SFP modules might show different speed information.
Wave Length(nm)	Displays the wavelength of current SFP module. Use this column to check if the wavelength values of two nodes are matched when the fiber connection fails.
Distance(m)	Displays the supported distance of the current SFP module.
Temperature(C) – SFP DDM Module Only	Displays the temperature of the current SFP DDM module.
Voltage(V) – SFP DDM Module Only	Displays the voltage of the current SFP DDM module.
Current(mA) – SFP DDM Module Only	Displays the Ampere of the current SFP DDM module.
TX power(dBm) – SFP DDM Module Only	Displays the TX power of the current SFP DDM module.
RX power(dBm) – SFP DDM Module Only	Displays the RX power of the current SFP DDM module.

Buttons

- Select the **SFP Monitor Event Alert** check box. The switch will be in accordance with the **Warning Temperature** setting and allows users to record message out via SNMP Trap.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

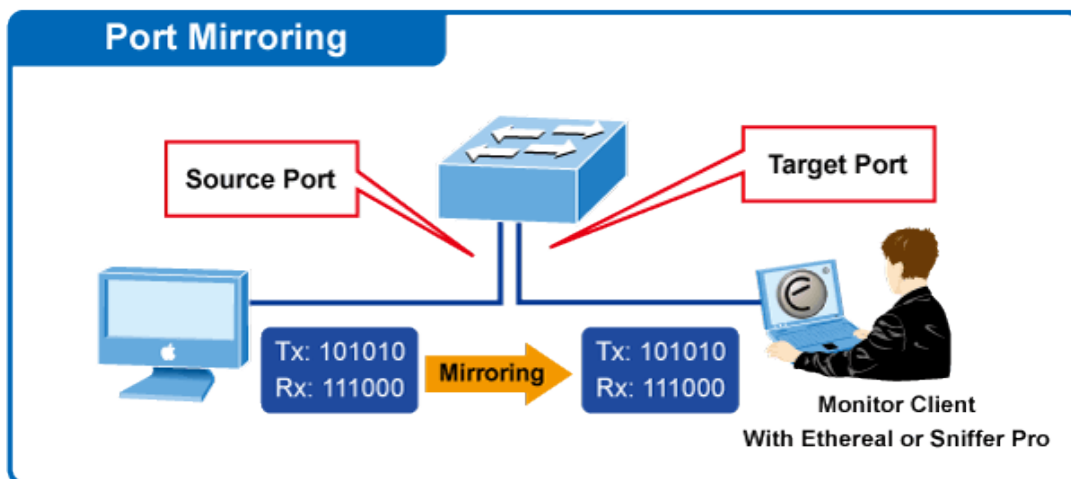
- Click **Refresh** to refresh the page immediately.
- Select the **Auto-refresh** check box to enable an automatic refresh of the page at regular intervals.

Port mirror

Configure port mirroring on the Mirror & RMirror Configuration Table page. This function provides the monitoring of network traffic that forwards a copy of each incoming or outgoing packet from one port of a network switch to another port where the packet can be studied. It enables the manager to keep close track of switch performance and alter it if necessary.

- To debug network problems, selected traffic can be copied, or mirrored, to a mirror port where a frame analyzer can be attached to analyze the frame flow.
- The industrial managed switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

Port Mirror Application



The traffic to be copied to the mirror port is selected as follows:

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

Mirror port configuration

Mirror & RMirror Configuration Table				
☐ Refresh				
Session ID	Mode	Type	VLAN ID	Reflector Port
1	Disabled	Mirror	-	-
2	Disabled	Mirror	-	-
3	Disabled	Mirror	-	-
4	Disabled	Mirror	-	-
5	Disabled	Mirror	-	-

The page includes the following fields:

Object	Description
Session ID	Select a Session ID hyperlink to configure it.
Mode	Enable/Disable the mirror or remote mirroring function.
Type	Select the switch type.
VLAN ID	The VLAN ID indicates where the monitor packet will copy to. The default VLAN ID is 200.
Reflector Port	The reflector port is a method to redirect the traffic to Remote Mirroring VLAN. Any device connected to a port set as a reflector port loses connectivity until the remote mirroring is disabled. In the stacking mode, you need to select the switch ID to select the correct device. If you shut down a port, it cannot be a candidate for a reflector port. If you shut down the port which is a reflector port, the remote mirror function will not work. Note1: The reflector port needs to select only on Source switch type. Note2: The reflector port needs to disable MAC Table learning and STP. Note3: The reflector port only supports on pure copper ports.

Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror Tx frames on the mirror port. Because of this, the mode for the selected mirror port is limited to **Disabled** or **Rx only**.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Link aggregation

Port Aggregation optimizes port usage by linking a group of ports together to form a single Link Aggregated Group (LAG). Port aggregation multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

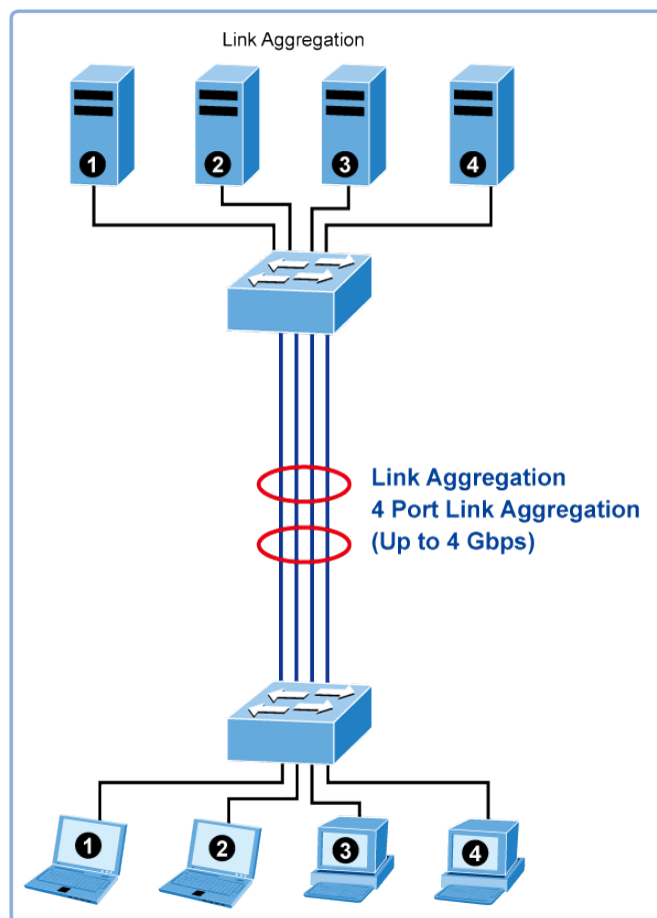
Each LAG is composed of ports of the same speed, set to full-duplex operations. Ports in a LAG can be of different media types (UTP/Fiber, or different fiber types), provided they operate at the same speed.

Aggregated links can be assigned manually (Port Trunk) or automatically by enabling Link Aggregation Control Protocol (LACP) on the relevant links.

Aggregated links are treated by the system as a single logical port. Specifically, the aggregated link has similar port attributes to a non-aggregated port, including auto-negotiation, speed, duplex setting, etc.

The industrial managed switch supports the following aggregation links :

- Static LAGs (Port Trunk) – Force aggregated selected ports to be a trunk group.
- Link Aggregation Control Protocol (LACP) LAGs – LACP LAGs negotiate aggregated port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.



The Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between partner systems that require high speed redundant links. Link aggregation permits grouping up to eight consecutive ports into a single

dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode (refer to the IEEE 802.3ad standard for further details).

Port link aggregations can be used to increase the bandwidth of a network connection or to ensure fault recovery. Link aggregation permits grouping up to four consecutive ports into a single dedicated connection between any two industrial managed switches or other Layer 2 switches. However, before making any physical connections between devices, use the link aggregation configuration menu to specify the link aggregation on the devices at both ends. When using a port link aggregation, note that:

- The ports used in a link aggregation must all be of the same media type (RJ45, 100 Mbps fiber).
- The ports that can be assigned to the same link aggregation have certain other restrictions (see below).
 - Ports can only be assigned to one link aggregation.
 - The ports at both ends of a connection must be configured as link aggregation ports.
 - None of the ports in a link aggregation can be configured as a mirror source port or a mirror target port.
 - All of the ports in a link aggregation have to be treated as a whole when moved from/to, added or deleted from a VLAN.
 - The Spanning Tree Protocol will treat all the ports in a link aggregation as a whole.
 - Enable the link aggregation prior to connecting any cable between the switches to avoid creating a data loop.
 - Disconnect all link aggregation port cables or disable the link aggregation ports before removing a port link aggregation to avoid creating a data loop.

It allows a maximum of 10 ports to be aggregated at the same time. The industrial managed switch supports Gigabit Ethernet ports (up to five groups). If the group is defined as a LACP static link aggregation group, then any extra ports selected are placed in a standby mode for redundancy if one of the other ports fails. If the group is defined as a local static link aggregation group, then the number of ports must be the same as the group member ports.

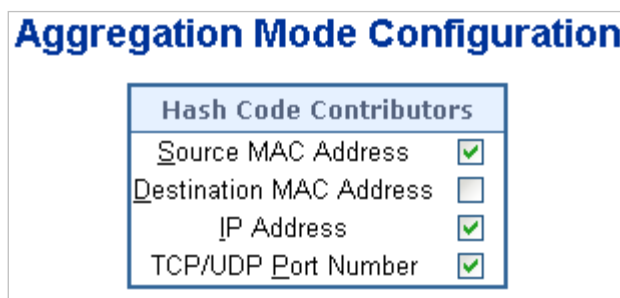
The aggregation code ensures that frames belonging to the same frame flow (for example, a TCP connection) are always forwarded on the same link aggregation member port. Reordering of frames within a flow is therefore not possible. The aggregation code is based on the following information:

- Source MAC
- Destination MAC
- Source and destination IPv4 address.
- Source and destination TCP/UDP ports for IPv4 packets

Normally, all five contributions to the aggregation code should be enabled to obtain the best traffic distribution among the link aggregation member ports. Each link aggregation may consist of up to 10 member ports. Any quantity of link aggregations may be configured for the device (they are only limited by the quantity of ports on the device). To configure a proper traffic distribution, the ports within a link aggregation must use the same link speed.

Static aggregation

The Aggregation Mode Configuration page is used to configure the aggregation hash mode and the aggregation group. The aggregation hash mode settings are global, whereas the aggregation group relate to the current device, as reflected by the page header.



The screenshot shows a web interface titled "Aggregation Mode Configuration". Inside, there is a section titled "Hash Code Contributors" with a table of four items, each with a checkbox:

Hash Code Contributors	
Source MAC Address	☒
Destination MAC Address	☐
IP Address	☒
TCP/UDP Port Number	☒

The page includes the following fields:

Object	Description
Source MAC Address	The Source MAC address can be used to calculate the destination port for the frame. Select the check box to enable the use of the Source MAC address, or uncheck it to disable. By default, the Source MAC Address is enabled.
Destination MAC Address	The Destination MAC Address can be used to calculate the destination port for the frame. Select the check box to enable the use of the Destination MAC Address, or uncheck it to disable. By default, the Destination MAC Address is disabled.
IP Address	The IP address can be used to calculate the destination port for the frame. Select the check box to enable the use of the IP Address, or uncheck it 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. Select the check box to enable the use of the TCP/UDP Port Number, or uncheck it to disable. By default, the TCP/UDP Port Number is enabled.

Static aggregation group configuration

Aggregation Group Configuration

	Port Members																											
Group ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Normal	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	
1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
4	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
5	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
9	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
10	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
11	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
12	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
13	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	
14	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

Apply

Reset

The page includes the following fields:

Object	Description
Group ID	Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.
Port Members	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Static aggregation status

The Aggregation Status page shows static aggregation status.

Aggregation Status

Auto-refresh ☐

Refresh

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

The page includes the following fields:

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

Buttons

- Click **Refresh** to refresh the page immediately.

LACP configuration

LACP LAG negotiates aggregated port links with other LACP ports located on a different device. LACP allows switches connected to each other to discover automatically whether any ports are member of the same LAG.

This page allows the user to inspect and change the current LACP port configurations. The LACP port settings relate to the current device, as reflected by the page header.

LACP Port Configuration

Port	LACP Enabled	Key		Role	Timeout	Priority
*	☐	<All> ▼		<All> ▼	<All> ▼	
1	☐	Auto ▼		Active ▼	Fast ▼	32768
2	☐	Auto ▼		Active ▼	Fast ▼	32768
3	☐	Auto ▼		Active ▼	Fast ▼	32768
4	☐	Auto ▼		Active ▼	Fast ▼	32768
5	☐	Auto ▼		Active ▼	Fast ▼	32768
6	☐	Auto ▼		Active ▼	Fast ▼	32768
7	☐	Auto ▼		Active ▼	Fast ▼	32768
8	☐	Auto ▼		Active ▼	Fast ▼	32768
9	☐	Auto ▼		Active ▼	Fast ▼	32768
10	☐	Auto ▼		Active ▼	Fast ▼	32768

Apply Reset

The page includes the following fields:

Object	Description
Port	The switch port number.
LACP Enabled	Controls whether or not LACP is enabled on this switch port. LACP will form an aggregation when two or more ports are connected to the same partner.
Key	The Key value incurred by the port, range 1-65535. Selecting Auto (default setting) sets the key as appropriate by the physical link speed: 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same key value can participate in the same aggregation group, while ports with different keys cannot.
Role	The Role shows the LACP activity status. The Active selection transmits LACP packets each second, while the Passive setting waits for a LACP packet from a partner (speak if spoken to).
Timeout	The Timeout controls the period between BPDU transmissions. Fast transmits LACP packets each second, while the Slow selection provides a wait for 30 seconds before sending a LACP packet.
Priority	The Priority controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device, then this parameter controls which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

LACP system status

The LACP System Status page provides a status overview of all LACP instances. This page displays the current LACP aggregation groups and LACP port status.

LACP System Status

Aggr ID	Partner System ID	Partner Key	Partner Priority	Last Changed	Local Ports
No ports enabled or no existing partners					

Auto-refresh ☐
Refresh

The page includes the following fields:

Object	Description
Aggr ID	The Aggregation ID associated with this aggregation instance. For LLAG the ID is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
Partner System ID	The system ID (MAC address) of the aggregation partner.
Partner Key	The key that the partner has assigned to this aggregation ID.
Partner Priority	The priority of the aggregation partner.
Last changed	The time since this aggregation changed.
Local Ports	Shows which ports are a part of this aggregation for this switch. The format is: "Switch ID:Port".

Buttons

- Click **Refresh** to to refresh the page immediately.
- Select the **Auto-refresh** check box to automatically refresh the page every three seconds.

LACP port status

The LACP Status page provides a LACP status overview of all ports. This page displays the current LACP aggregation groups and LACP port status.

LACP Status

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	Partner Priority
1	No	-	-	-	-	-
2	No	-	-	-	-	-
3	No	-	-	-	-	-
4	No	-	-	-	-	-
5	No	-	-	-	-	-
6	No	-	-	-	-	-
7	No	-	-	-	-	-
8	No	-	-	-	-	-
9	No	-	-	-	-	-
10	No	-	-	-	-	-

Auto-refresh ☐

The page includes the following fields:

Object	Description
Port	The switch port number.
LACP	'Yes' means that LACP is enabled and the port link is up. 'No' means that LACP is not enabled or that the port link is down. 'Backup' means that the port could not join the aggregation group but will join if other ports leave. Until that occurs, its LACP status is disabled.
Key	The key is assigned to this port. Only ports with the same key can aggregate together.
Aggregation ID	The aggregation ID assigned to this aggregation group.
Partner System ID	The partner's system ID (MAC address).
Partner Port	The partner's port number connected to this port.
Partner Priority	The partner's port priority.

Buttons

- Click **Refresh** to refresh the page immediately.
- Select the **Auto-refresh** check box to automatically refresh the page every three seconds.

LACP port statistics

The LACP Statistics page provides an overview of LACP statistics for all ports.

LACP Statistics

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0

Auto-refresh ☐

The page includes the following fields:

Object	Description
Port	The switch port number.
LACP Received	Shows how many LACP frames have been sent from each port.
LACP Transmitted	Shows how many LACP frames have been received at each port.
Discarded	Shows how many unknown or illegal LACP frames have been discarded at each port.

Buttons

- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear the counters for all ports
- Select the **Auto-refresh** check box to automatically refresh the page every three seconds.

VLAN

VLAN overview

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLAN also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily. VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded only to members of the VLAN on which the broadcast was initiated.

Note:

1. Regardless of the method used to uniquely identify end nodes and assign VLAN membership to these nodes, packets cannot cross VLAN without a network device performing a routing function between the VLANs.
2. The industrial managed switch supports IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.

Note: The industrial managed switch's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN. As a new VLAN is created, the member ports assigned to the new VLAN are removed from the DEFAULT_VLAN port member list. The DEFAULT_VLAN has a VID = 1.

This section has the following items:

VLAN Port Configuration	Enables VLAN group
VLAN Membership Status	Displays VLAN membership status
VLAN Port Status	Displays VLAN port status
Private VLAN	Creates/removes primary or community VLANs
Port Isolation	Enables/disables port isolation on port
MAC-based VLAN	Configures the MAC-based VLAN entries
MAC-based VLAN Status	Displays MAC-based VLAN entries
Protocol-based VLAN	Configures the protocol-based VLAN entries
Protocol-based VLAN Membership	Displays the protocol-based VLAN entries

IEEE 802.1Q VLAN

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This industrial managed switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by permitting relocation of devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as email), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and permit network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This industrial managed switch supports the following VLAN features:

- Up to 255 VLANs based on the IEEE 802.1Q standard.
- Port overlapping, allowing a port to participate in multiple VLANs.
- End stations can belong to multiple VLANs.
- Passing traffic between VLAN-aware and VLAN-unaware devices.
- Priority tagging

IEEE 802.1Q standard

IEEE 802.1Q (tagged) VLAN are implemented on the Switch. 802.1Q VLAN require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q compliant).

VLAN allows a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast, and unicast packets from unknown sources.

VLAN can also provide a level of security to the network. IEEE 802.1Q VLAN only delivers packets between stations that are members of the VLAN. Any port can be configured as either tagging or untagging:

- The untagging feature of IEEE 802.1Q VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in packet headers.
- The tagging feature allows VLAN to span multiple 802.1Q compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

Some relevant terms:

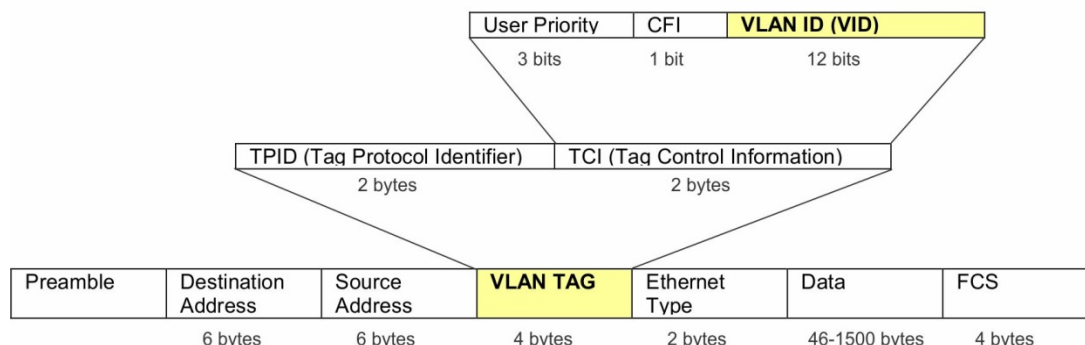
- **Tagging** – The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** – The act of stripping 802.1Q VLAN information out of the packet header.

802.1Q VLAN tags

There are four additional octets inserted after the source MAC address as shown in the following 802.1Q tag diagram. Their presence is indicated by a value of 0x8100 in the Ether Type field. When a packet's Ether Type field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of three bits of user priority: One bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of VLAN ID (VID). The three bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLAN can be identified.

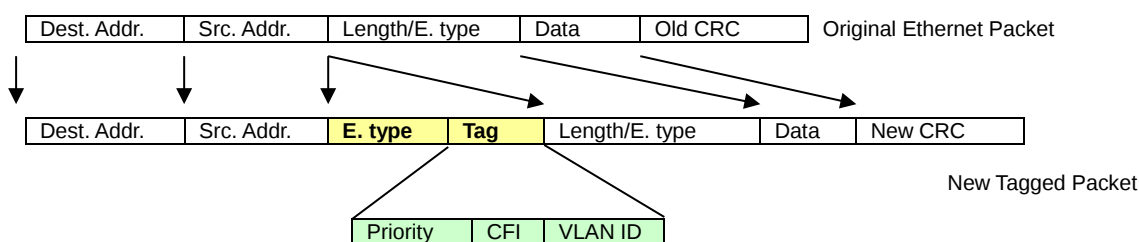
The tag is inserted into the packet header making the entire packet longer by four octets. All of the information originally contained in the packet is retained.

802.1Q tag



The Ether Type and VLAN ID are inserted after the MAC source address, but before the original Ether Type/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

Adding an IEEE802.1Q tag



Port VLAN ID

Packets that are tagged (carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLAN to span network devices as well as the entire network if all network devices are 802.1Q compliant.

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID for use within the switch. If no VLANs are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLANs are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the VID, not the PVID, is used to make packet forwarding decisions.

Tag-aware switches must keep a table to relate PVID within the switch to VID on the network. The switch compares the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VIDs are different, the switch drops the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VIDs as the switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Default VLANs

The industrial managed switch initially configures one VLAN, VID = 1, called "default." The factory default setting assigns all ports on the Switch to the "default." As new VLANs are configured in port-based mode, their respective member ports are removed from the "default."

Assigning ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default, all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port to have it carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then this port should be added to the VLAN as an untagged port.

Note: VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing them on to any end-node host that does not support VLAN tagging.

VLAN classification

When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). If the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port overlapping

Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs that do not overlap but still need to communicate, they can be connected by enabling routing on this switch.

Untagged VLANs

Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets.

VLAN port configuration

The Global VLAN Configuration page is used for configuring the industrial managed switch port VLAN. This page contains fields for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is also configured on this page. All untagged packets arriving to the device are tagged by the port's PVID.

Managed switch nomenclature:

IEEE 802.1Q tagged and untagged

Every port on an 802.1Q compliant switch can be configured as tagged or untagged.

Tagged: Ports with tagging enabled put the VID number, priority, and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.

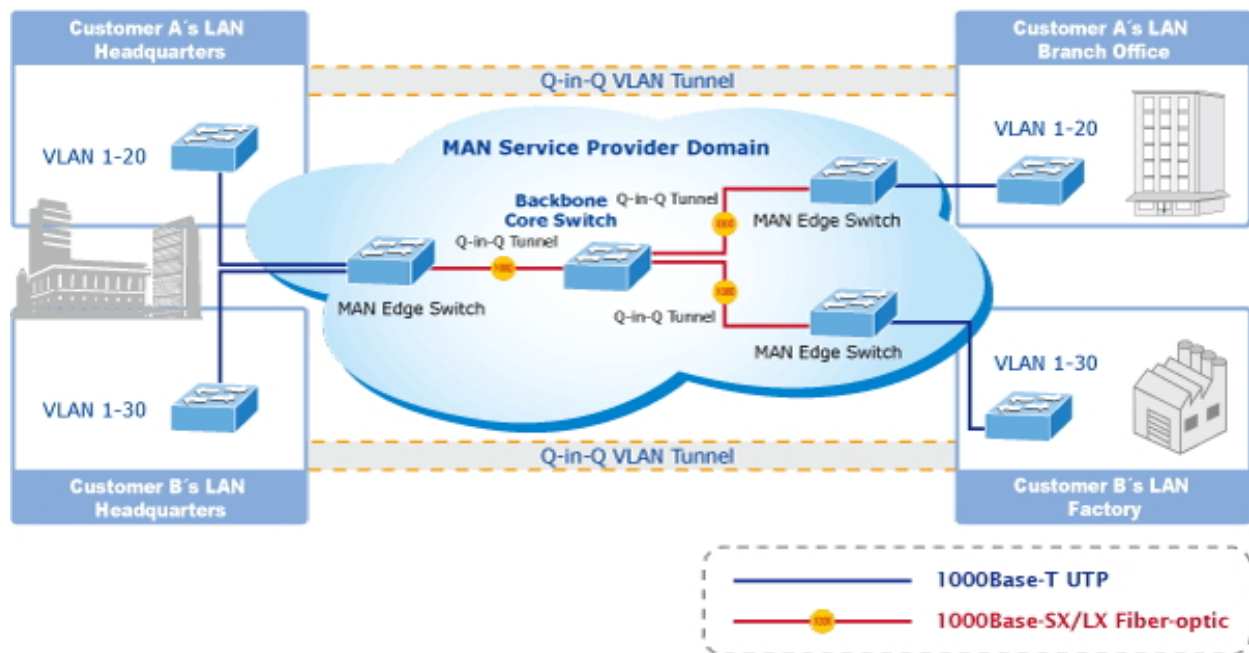
Untagged: Ports with untagging enabled strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port have no 802.1Q VLAN information (remember that the PVID is only used internally within the industrial managed switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Frame Income Frame Leave	Income Frame is tagged	Income Frame is untagged
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remains untagged

IEEE 802.1Q tunneling (Q-in-Q)

IEEE 802.1Q tunneling (Q-in-Q) is designed for service providers carrying traffic for multiple customers across their networks. Q-in-Q tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.



The industrial managed switch supports multiple VLAN tags and can therefore be used in MAN (Metro Access Network) applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the MAN space. One of the purposes of the provider bridge is to recognize and use VLAN tags so that the VLANs in the MAN space can be used independent of the customers' VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available.

This provides a tunneling mechanism to connect remote customer VLANs through a common MAN space without interfering with the VLAN tags. All tags use EtherType 0x8100 or 0x88A8, where 0x8100 is used for customer tags and 0x88A8 is used for service provider tags.

In cases where a given service VLAN only has two member ports on the switch, the learning can be disabled for the particular VLAN and can therefore rely on flooding as the forwarding mechanism between the two ports. This way, the MAC table requirements are reduced.

Global VLAN configuration

Global VLAN Configuration	
Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

The page includes the following fields:

Object	Description
Allowed Access VLANs	This field shows the allowed Access VLANs. It only affects ports configured as access ports. Ports in other modes are members of all 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 boundaries. The following example creates 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

Global VLAN Configuration

Allowed Access VLANs	1
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<All>	1	<All>	☐	<All>	<All>	1	
1	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
2	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
3	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
7	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
8	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
9	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
10	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	

Apply Reset

The page includes the following fields:

Object		Description
Port		This is the logical port number for this row.
Mode	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 (Access VLAN), which by default is 1. • Accepts untagged and C-tagged frames. • Discards all frames that are not classified to the Access VLAN. • On egress, all frames classified to the Access VLAN are transmitted untagged. Other (dynamically added VLANs) are transmitted tagged.
	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 add 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 (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.

Object	Description
	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 ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 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 an S-tag. S-Custom-port: On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports 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 the custom S-tag.
Ingress Filtering	Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled. • If ingress filtering is enabled (Ingress Filtering check box is selected), 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. Tagged Only: Only tagged frames are accepted on ingress. Untagged frames are discarded. Untagged Only: Only untagged frames are accepted on ingress. Tagged frames are discarded.
Egress Tagging	This option is only available for ports in Hybrid mode. 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.
Allowed VLANs	Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to 1-4095. The field may be left empty, which means that the port will not become member of any VLANs.
Forbidden VLANs	A port may be configured to never be a member of one or more

Object	Description
	VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. Such VLANs should be marked 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.

Note: The port must be a member of the same VLAN as the Port VLAN ID.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

VLAN membership status

The VLAN Membership Status for Combined users page provides an overview of membership status for VLAN users.

VLAN Membership Status for Combined users

Combined
Auto-refresh
Refresh

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

VLAN ID	Port Members																											
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

The page includes the following fields:

Object	Description
VLAN User	A VLAN User is a module that uses services of the VLAN management functionality to configure VLAN memberships and VLAN port configuration such as PVID and UVID. Currently, we support following VLAN : Admin : This is referred to as static. NAS : NAS provides port-based authentication, which involves communications between a Supplicant, Authenticator, and an Authentication Server. GVRP : GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network . Voice VLAN : Voice VLAN is a VLAN configured specially for voice traffic typically originating from IP phones. MVR : MVR is used to eliminate the need to duplicate multicast traffic for subscribers in each VLAN. Multicast traffic for all channels is sent only on a single (multicast) VLAN.

Object	Description
Port Members	A row of check boxes for each port appears for each VLAN ID. If a port is included in a VLAN, an image  appears. If a port is included in a Forbidden port list, an image  appears. If a port is included in a Forbidden port list and dynamic VLAN user register VLAN on same Forbidden port, then the conflict port appears as a conflict port.
VLAN Membership	The VLAN Membership Status Page shows the current VLAN port members for all VLANs configured by a selected VLAN user (selection shall be allowed by a Combo Box). When ALL VLAN users are selected, it shows this information for all the VLAN users by default. VLAN membership allows the frames classified to the VLAN ID to be forwarded on the respective VLAN member ports.

Buttons

- Select **VLAN Users** from the **Combined** drop-down list.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.
- Click **1<<** to update the table starting from the first entry in the VLAN Table (i.e., the entry with the lowest VLAN ID).
- Click **>>** to update the table, starting with the entry after the last entry currently displayed.

VLAN port status

The VLAN Port Status for Combined users page provides VLAN port status.

VLAN Port Status for Combined users

Combined v Auto-refresh ☐ Refresh							
Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☒	All	1	Untag PVID		No
2	C-Port	☒	All	1	Untag PVID		No
3	C-Port	☒	All	1	Untag PVID		No
4	C-Port	☒	All	1	Untag PVID		No
5	C-Port	☒	All	1	Untag PVID		No
6	C-Port	☒	All	1	Untag PVID		No
7	C-Port	☒	All	1	Untag PVID		No
8	C-Port	☒	All	1	Untag PVID		No
9	C-Port	☒	All	1	Untag PVID		No
10	C-Port	☒	All	1	Untag PVID		No

The page includes the following fields:

Object	Description
Port	The logical port for the settings contained in the same row.
Port Type	Shows the VLAN Awareness for the port. If VLAN awareness is enabled, the tag is removed from tagged frames received on the port. VLAN tagged frames are classified to the VLAN ID in the tag. If VLAN awareness is disabled, all frames are classified to the Port VLAN ID and tags are not removed.
Ingress Filtering	Shows the ingress filtering for a port. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame is discarded.
Frame Type	Shows if the port accepts all frames or only tagged frames. This parameter affects VLAN ingress processing. If the port only accepts tagged frames, untagged frames received on that port are discarded.
Port VLAN ID	Shows the PVID setting for the port.
Tx Tag	Shows egress filtering frame status (tagged or untagged).
Untagged VLAN ID	Shows UVID (untagged VLAN ID). The port's UVID determines the packet's behavior at the egress side.
Conflicts	Shows whether or not conflicts exist. When a Volatile VLAN user requests to set VLAN membership or VLAN port configuration, the following conflicts can occur: • Functional conflicts between features. • Conflicts due to hardware limitations. • Direct conflict between user modules.

Buttons

- Select **VLAN Users** from the **Static** drop-down list.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

Private VLAN

The Private VLAN Membership Configuration page allows you to configure private VLAN membership. The private VLAN membership configurations for the switch can be monitored and modified here; private VLANs and private VLAN port members can be added or deleted here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and private VLAN IDs can be identical. A port must be a member of both a VLAN and a private VLAN to be able to forward packets. By default, all ports are VLAN unaware and are members of VLAN 1 and private VLAN 1. A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple private VLANs.

Auto-refresh ☐ Refresh

Private VLAN Membership Configuration

		Port Members																											
Delete	PVLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
☐	1	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒

Add New Private VLAN

Apply Reset

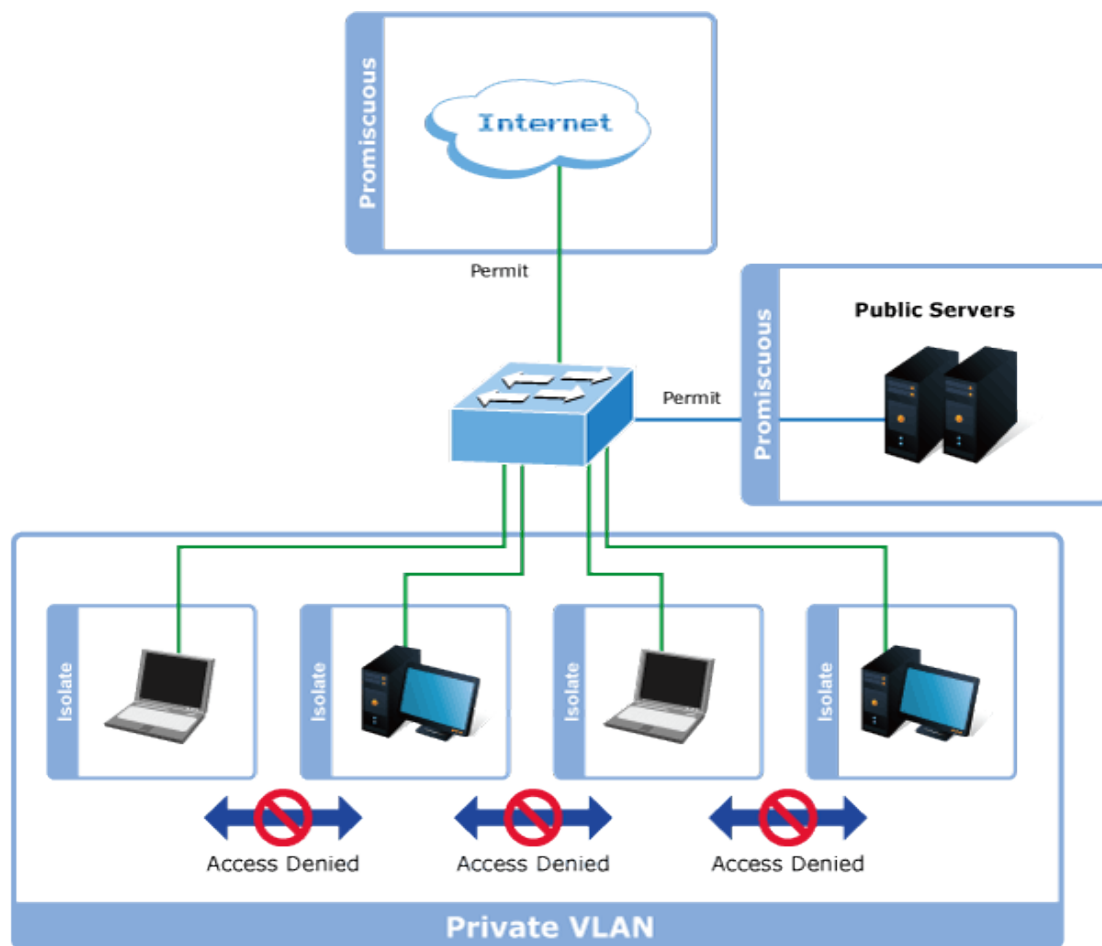
The page includes the following fields:

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

Port isolation

When a VLAN is configured to be a private VLAN, communication between ports within that VLAN can be prevented. Two application examples are provided in this section:

- Customers connected to an ISP can be members of the same VLAN, but they are not allowed to communicate with each other within that VLAN.
- Servers in a farm of web servers in a Demilitarized Zone (DMZ) are allowed to communicate with the outside world and with database servers on the inside segment, but are not allowed to communicate with each other.



For private VLANs to be applied, the switch must first be configured for standard VLAN operation. When this is in place, one or more of the configured VLANs can be configured as private VLANs. Ports in a private VLAN fall into one of these two groups:

Promiscuous ports

- Ports from which traffic can be forwarded to all ports in the private VLAN.
- Ports that can receive traffic from all ports in the private VLAN.

Isolated ports

- Ports from which traffic can only be forwarded to promiscuous ports in the private VLAN.
- Ports that can receive traffic from only promiscuous ports in the private VLAN.

The configuration of promiscuous and isolated ports applies to all private VLANs. When traffic comes in on a promiscuous port in a private VLAN, the VLAN mask from the VLAN table is applied. When traffic comes in on an isolated port, the private VLAN mask is applied in addition to the VLAN mask from the VLAN table. This reduces the ports to which forwarding can be done to just the promiscuous ports within the private VLAN.

The Port Isolation Configuration page is used for enabling or disabling port isolation on ports in a private VLAN. A port member of a VLAN can be isolated to other isolated ports on the same VLAN and private VLAN.

Auto-refresh ☐ Refresh

Port Isolation Configuration

Port Number																											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Apply Reset

The page includes the following fields:

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

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

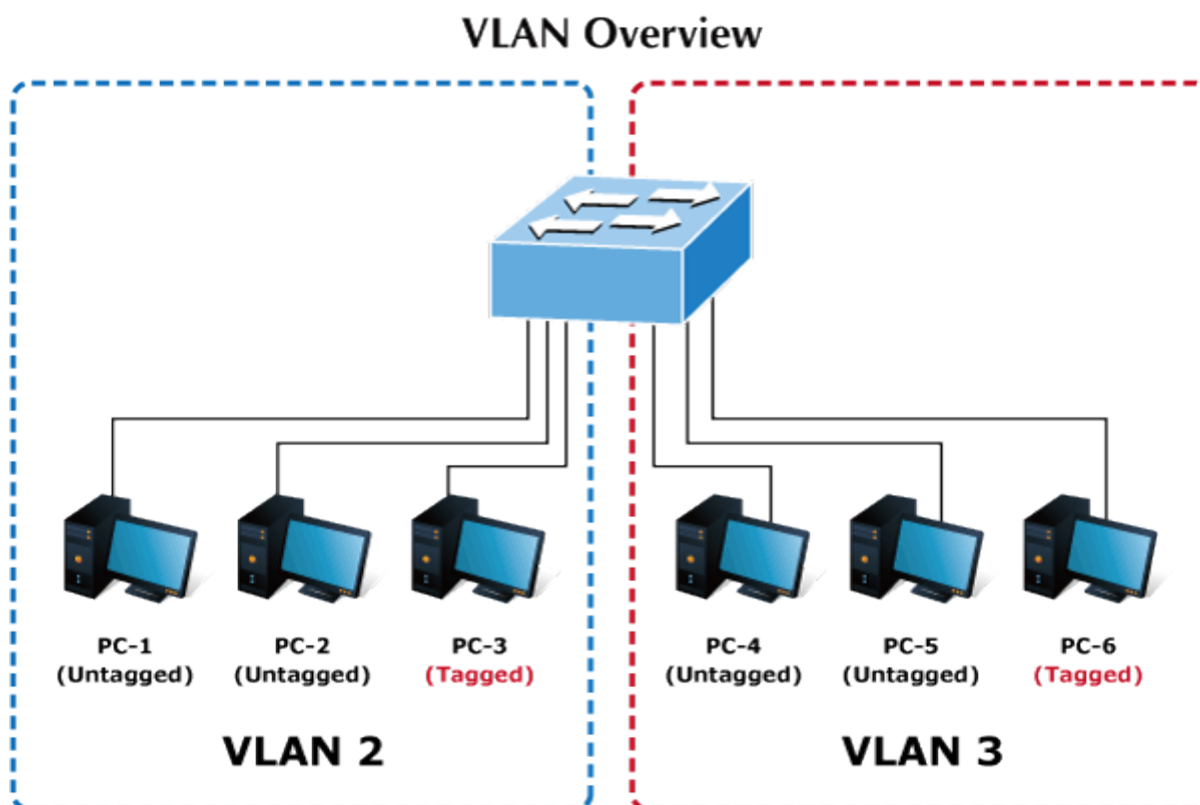
VLAN setting examples

This section covers the following setup scenarios:

- Separate VLAN
- 802.1Q VLAN Trunk
- Port Isolate

Two Separate 802.1Q VLANs

The diagram below shows how the industrial managed switch handles tagged and untagged traffic flow for two VLANs. VLAN Group 2 and VLAN Group 3 are separated VLANs. Each VLAN isolates network traffic, so only members of the VLAN receive traffic from the same VLAN members. The table below describes the port configuration of the industrial managed switches.



VLAN Group	VID	Untagged Members	Tagged Members
VLAN Group 1	1	Port-7 ~ Port-28	N/A
VLAN Group 2	2	Port-1,Port-2	Port-3
VLAN Group 3	3	Port-4,Port-5	Port-6

The scenario is described as follows:

Untagged packet entering VLAN 2

1. While [PC-1], an untagged packet, enters Port-1, the industrial managed switch will tag it with a VLAN Tag=2. [PC-2] and [PC-3] will receive the packet through Port-2 and Port-3.
2. [PC-4],[PC-5] and [PC-6] received no packet.
3. While the packet leaves Port-2, it will be stripped away, becoming an untagged packet.
4. While the packet leaves Port-3, it will remain as a tagged packet with VLAN Tag=2.

Tagged packet entering VLAN 2

1. While [PC-3], a tagged packet with VLAN Tag=2 enters Port-3, [PC-1] and [PC-2] will receive the packet through Port-1 and Port-2.
2. While the packet leaves Port-1 and Port-2, it will be stripped away, becoming an untagged packet.

Untagged packet entering VLAN 3

1. While [PC-4] an untagged packet enters Port-4, the switch will tag it with a VLAN Tag=3. [PC-5] and [PC-6] will receive the packet through Port-5 and Port-6.
2. While the packet leaves Port-5, it will be stripped away, becoming an untagged packet.
3. While the packet leaves Port-6, it will keep as a tagged packet with VLAN Tag=3.

Note: For this example, set VLAN Group 1 as the default VLAN, but only focus on VLAN 2 and VLAN 3 traffic flow.

Setup steps

1. Add VLAN group

Add two VLANs – VLAN 2 and VLAN 3

Type 1-3 in an Allowed Access VLANs column, the 1-3 includes VLAN1 and 2 and 3.

Global VLAN Configuration

Allowed Access VLANs	1-3
Ethertype for Custom S-ports	88A8

2. Assign VLAN members and PVIDs to each port:

VLAN 2 : Port-1,Port-2 and Port-3

VLAN 3 : Port-4, Port-5 and Port-6

VLAN 1 : All other ports – Port-7~Port-28

Global VLAN Configuration

Allowed Access VLANs	1-3
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<All>	2	<All>	☐	<All>	<All>	2	
1	Access	2	C-Port	☒	Tagged and Untagged	Untag Port VLAN	2	
2	Access	2	C-Port	☒	Tagged and Untagged	Untag Port VLAN	2	
3	Access	2	C-Port	☒	Tagged and Untagged	Untag Port VLAN	2	
4	Access	3	C-Port	☒	Tagged and Untagged	Untag Port VLAN	3	
5	Access	3	C-Port	☒	Tagged and Untagged	Untag Port VLAN	3	
6	Access	3	C-Port	☒	Tagged and Untagged	Untag Port VLAN	3	
7	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
8	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
9	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	
10	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	

3. Enable VLAN Tag for specific ports

Link Type: Port-3 (VLAN-2) and Port-6 (VLAN-3)

Change Port 3 Mode as Trunk and select Egress Tagging as **Tag All** and Types 2 in the Allowed VLANs column.

Change Port 6 Mode as Trunk and select Egress Tagging as **Tag All** and Types 3 in the allowed VLANs column.

Global VLAN Configuration

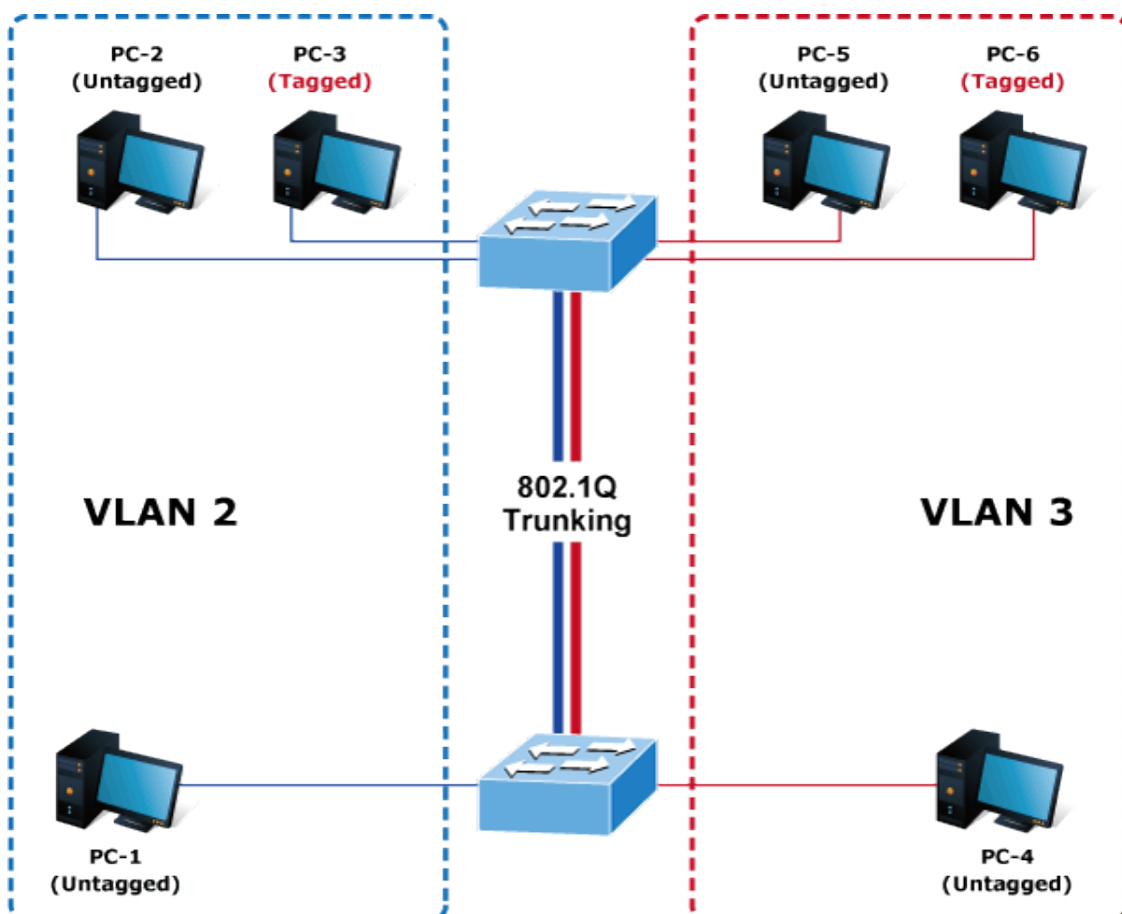
Allowed Access VLANs	1-3
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<All>	2	<All>	☐	<All>	<All>	2	
1	Access	2	C-Port	☒	Tagged and Untagged	Untag Port VLAN	2	
2	Access	2	C-Port	☒	Tagged and Untagged	Untag Port VLAN	2	
3	Trunk	2	C-Port	☒	Tagged Only	Tag All	2	
4	Access	3	C-Port	☒	Tagged and Untagged	Untag Port VLAN	3	
5	Access	3	C-Port	☒	Tagged and Untagged	Untag Port VLAN	3	
6	Trunk	3	C-Port	☒	Tagged Only	Tag All	3	
7	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	

VLAN trunking between two 802.1Q-aware switches

In most cases, they are used for “Uplink” to other switches. VLANs are separated at different switches, but they need access to other switches within the same VLAN group.



Setup steps

1. Add a VLAN group.
Add two VLANs – VLAN 2 and VLAN 3

Type 1-3 in the allowed Access VLANs column; the 1-3 includes VLAN 1 and 2 and 3.

Global VLAN Configuration	
Allowed Access VLANs	1-3
Ethertype for Custom S-ports	88A8

2. Assign VLAN members and PVIDs to each port:

VLAN 2: Port-1, Port-2 and Port-3

VLAN 3: Port-4, Port-5 and Port-6

VLAN 1: All other ports – Port-7~Port-48

Global VLAN Configuration	
Allowed Access VLANs	1-3
Ethertype for Custom S-ports	88A8

Port VLAN Configuration									
Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs	
*	<All>	2	<All>	☐	<All>	<All>	2		
1	Access	2	C-Port	☒	Tagged and Untagged	Untag Port VLAN	2		
2	Access	2	C-Port	☒	Tagged and Untagged	Untag Port VLAN	2		
3	Access	2	C-Port	☒	Tagged and Untagged	Untag Port VLAN	2		
4	Access	3	C-Port	☒	Tagged and Untagged	Untag Port VLAN	3		
5	Access	3	C-Port	☒	Tagged and Untagged	Untag Port VLAN	3		
6	Access	3	C-Port	☒	Tagged and Untagged	Untag Port VLAN	3		
7	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1		
8	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1		
9	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1		
10	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1		

For the VLAN ports connecting to the hosts, see “IP subnet-based VLAN” on page 124 for examples. The following steps focus on the VLAN trunk port configuration.

1. Specify Port-7 to be the 802.1Q VLAN Trunk port.
2. Assign Port-7 to both VLAN 2 and VLAN 3 on the VLAN Member configuration page.
3. Define a VLAN 1 as a “Public Area” that overlaps with both VLAN 2 members and VLAN 3 members.
4. Assign the VLAN Trunk Port to being the member of each VLAN to be aggregated. For example, include Port-7 to be VLAN 2 and VLAN 3 member ports.
5. Specify Port-7 to be the 802.1Q VLAN trunk port, and the trunking port must be a tagged port during egress. The Port-7 configuration is shown below.

Global VLAN Configuration

Allowed Access VLANs	1-3
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

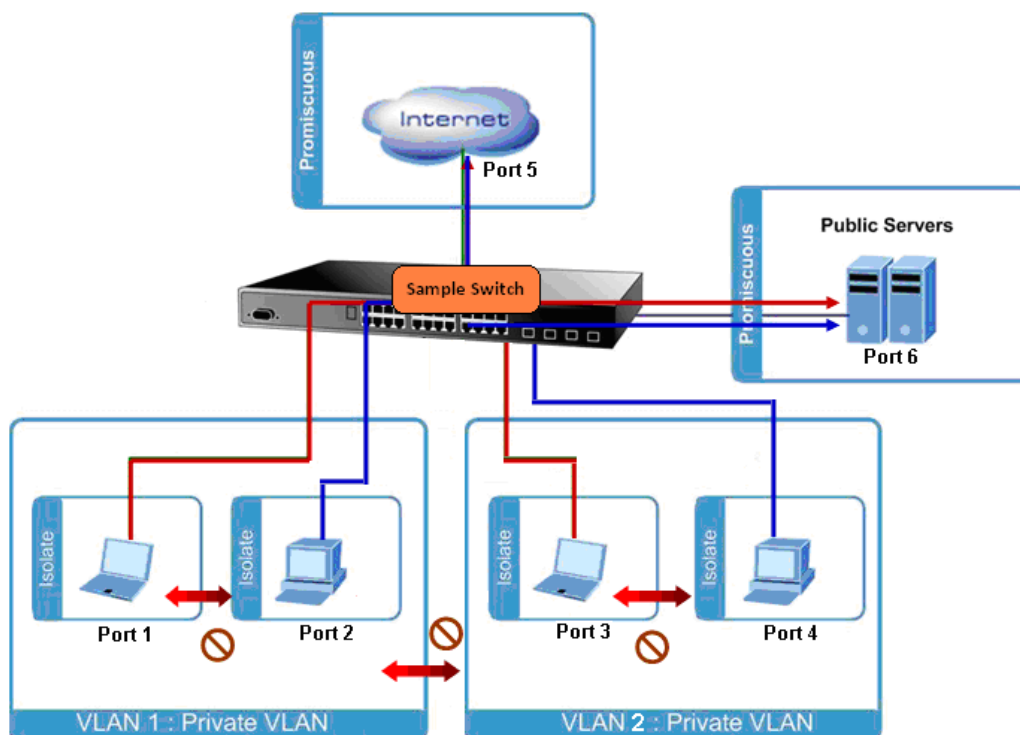
Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<All>	2	<All>	☐	<All>	<All>	2	1
1	Access	2	C-Port	☒	Tagged and Untagged	Untag Port VLAN	2	1
2	Access	2	C-Port	☒	Tagged and Untagged	Untag Port VLAN	2	1
3	Access	2	C-Port	☒	Tagged and Untagged	Untag Port VLAN	2	1
4	Access	3	C-Port	☒	Tagged and Untagged	Untag Port VLAN	3	1
5	Access	3	C-Port	☒	Tagged and Untagged	Untag Port VLAN	3	1
6	Access	3	C-Port	☒	Tagged and Untagged	Untag Port VLAN	3	1
7	Trunk	1	C-Port	☒	Tagged Only	Tag All	1-3	
8	Access	1	C-Port	☒	Tagged and Untagged	Untag Port VLAN	1	

Both the VLAN 2 members of Port-1 to Port-3 and VLAN 3 members of Port-4 to Port-6 belong to VLAN 1. But with different PVID settings, packets from VLAN 2 or VLAN 3 are not able to access the other VLAN.

- Repeat Steps 1 to 5 by setting up the VLAN trunk port at the partner switch and add more VLANs to join the VLAN trunk. Repeat Steps 1 to 3 to assign the trunk port to the VLANs.

Port isolate

The diagram below shows how the industrial managed switch handles isolated and promiscuous ports, and how computers are not able to access each other's isolated port. However, each computer requires access to the same server/AP/Printer. This section explains how to configure the port for the server so that it can be accessed by each isolated port.



1. Assign Port Mode

Set Port-1~Port-4 as isolated.

Set Port-5 and Port-6 as promiscuous. The Port Isolation Configuration page appears.

Auto-refresh ☐

Port Isolation Configuration

Port Number																																																
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	
☒	☒	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

2. Assign VLAN Member:

VLAN 1 : Port-5 and Port-6

VLAN 2 : Port-1, Port-2, Port-5 and Port-6

VLAN 3: Port-3~Port-6.

The Private VLAN Membership Configuration page appears.

Auto-refresh ☐

Private VLAN Membership Configuration

Delete	PVLAN ID	Port Members																											
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
☐	1	☐	☐	☐	☐	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
☐	2	☒	☒	☐	☐	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
☐	3	☐	☐	☒	☒	☒	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

MAC-based VLAN

The MAC-based VLAN entries can be configured on the MAC-based VLAN Membership Configuration page. This page allows for adding and deleting MAC-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

MAC-based VLAN Membership Configuration

Auto-refresh ☐

Delete	MAC Address	VLAN ID	Port Members																											
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Currently no entries present																														

The page includes the following fields:

Object	Description
Delete	To delete a MAC-based VLAN entry, select this box and click Save .
MAC Address	Indicates the MAC address.
VLAN ID	Indicates the VLAN ID.
Port Members	A row of check boxes for each port appears for each MAC-based VLAN entry. To include a port in a MAC-based VLAN, select the check box. To remove or exclude the port from the MAC-based VLAN, make sure the box is deselected. By default, no ports are members, and all boxes are deselected.
Adding a New MAC-based VLAN	Click Add New Entry to add a new MAC-based VLAN entry. An empty row is added to the table, and the MAC-based VLAN entry can be configured as needed. Any unicast MAC address can be configured for the MAC-based VLAN entry. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095. The MAC-based VLAN entry is enabled when clicking Save. A MAC-based VLAN without any port members will be deleted when clicking Save. The Delete button can be used to undo the addition of new MAC-based VLANs.

Buttons

- Click **Add New Entry** to add a new MAC-based VLAN entry
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.
- Click **1<<** to update the table starting from the first entry in the MAC-based VLAN table.
- Click **>>** to update the table, starting with the entry after the last entry currently displayed.

MAC-based VLAN status

The MAC-based VLAN Membership Status page shows MAC-based VLAN entries configured by various MAC-based VLAN users

MAC-based VLAN Membership Status for User Static

☐ Auto-refresh

MAC Address	VLAN ID	Port Members																											
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
No data exists for the user																													

The page includes the following fields:

Object	Description
MAC Address	Indicates the MAC address.
VLAN ID	Indicates the VLAN ID.
Port Members	Port members of the MAC-based VLAN entry.

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

IP subnet-based VLAN

The IP subnet-based VLAN entries can be configured on the IP Subnet-based VLAN Membership Configuration page. This page allows for adding, updating, and deleting IP subnet-based VLAN entries and assigning the entries to different ports. This page shows only static entries.

IP Subnet-based VLAN Membership Configuration

Auto-refresh ☐

					Port Members									
Delete	VCE ID	IP Address	Mask Length	VLAN ID	1	2	3	4	5	6	7	8	9	10
Currently no entries present														

The page includes the following fields:

Object	Description
Delete	Select this box to delete a Protocol to Group Name map entry. The entry will be deleted on the switch during the next save.
VCE ID	Indicates the index of the entry. It is user configurable with a value range from 0-256. If a VCE ID is 0, the application will auto-generate the VCE ID for that entry. Deletion and lookup of IP subnet-based VLAN are based on VCE ID.
IP Address	Indicates the IP address.
Mask Length	Indicates the network mask length.
VLAN ID	Indicates the VLAN ID. VLAN ID can be changed for the existing entries.
Port Members	A row of check boxes for each port displays for each IP subnet-based VLAN entry. To include a port in a IP subnet-based VLAN, select the check box. To remove or exclude the port from the IP subnet-based VLAN, make sure the box is deselected. By default, no ports are members, and all boxes are deselected.
Add New Entry	Click Add New Entry to add a new IP subnet-based VLAN entry. An empty row is added to the table, and the IP subnet-based VLAN entry can be configured as needed. Any IP address/mask can be configured for the IP subnet-based VLAN entry. Legal values for a VLAN ID are 1 through 4095. The IP subnet-based VLAN entry is enabled when clicking Save. The Delete button can be clicked to undo the addition of new IP subnet-based VLANs.

Buttons

- Click **Add New Entry** to add a new MAC-based VLAN entry
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

Protocol-based VLAN

The Protocol to Group Mapping Table page permits the addition of new protocols to the Group Name (unique for each Group) mapping entries, and allows you to see and delete entries already mapped for the switch.

Protocol to Group Mapping Table

Delete	Frame Type	Value	Group Name
No Group entry found!			

Auto-refresh ☐

The page includes the following fields:

Object	Description
Delete	Select this box to delete a Protocol to Group Name map entry. The entry will be deleted on the switch during the next save.
Frame Type	Frame Type values are as follows: Ethernet, LLC, SNAP Note: When changing the Frame Type field, the Value field changes depending on the new frame type selected.
Value	Values that can be entered in this text field depend on the option selected in the Frame Type selection menu. Below are the criteria for three different frame types: For Ethernet: Values in the text field when Ethernet is selected as a Frame Type is called etype. Values for etype ranges from 0x0600-0xffff For 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) For SNAP: A valid value in this case is comprised of two different sub-values. OUI: OUI (Organizationally Unique Identifier) is value in format of xx-xx-xx where each pair (xx) in string is a hexadecimal value ranges from 0x00-0xff. PID: If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if the OUI is 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 value of OUI field is 00-00-00 then value of PID will be etype (0x0600-0xffff) and if value of OUI is other than 00-00-00 then the valid value of PID will be any value from 0x0000 to 0xffff.
Group Name	A valid Group Name is a unique 16-character long string for every entry that consists of a combination of alphabets (a-z or A-Z) and integers (0-9). Note: Special character and underscore(_) are not allowed.
Adding a New Group to VLAN mapping entry	Click the Add New Entry to add a new entry in mapping table. An empty row is added to the table, and Frame Type, Value, and the Group Name can be configured as needed. Click the Delete button to undo the addition of a new entry.

Buttons

- Click **Add New Entry** to add a new MAC-based VLAN entry
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

Protocol-based VLAN membership

The Group Name to VLAN Mapping Table page permits mapping an already configured Group Name to a VLAN.

Group Name to VLAN Mapping Table

			Port Members																											
Delete	Group Name	VLAN ID	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
No Group entries																														

Auto-refresh ☐

The page includes the following fields:

Object	Description
Delete	Select this box to delete a Group Name to VLAN map entry. The entry will be deleted on the switch during the next save.
Group Name	A valid Group Name is a unique 16-character long string for every entry which consists of a combination of alphabets (a-z or A-Z) and integers (0-9). No special character is allowed. Whichever group name you try map to a VLAN must be present in the Protocol to Group mapping table and must not be used by any other existing mapping entry on this page.
VLAN ID	Indicates the ID to which the group name will be mapped. A valid VLAN ID ranges from 1-4095.
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 a mapping, select the box. To remove or exclude the port from the mapping, make sure the box is deselected. By default, no ports are members, and all boxes are deselected.
Adding a New Group to VLAN mapping entry	Click the Add New Entry to add a new entry in mapping table. An empty row is added to the table, and Frame Type, Value, and the Group Name can be configured as needed. Click the Delete button to undo the addition of a new entry.

Buttons

- Click **Add New Entry** to add a new entry in the mapping table.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

Spanning Tree Protocol (STP)

Theory

STP can be used to detect and disable network loops, and to provide backup links between switches, bridges, or routers. This allows the switch to interact with other bridging devices in the network to ensure that only one route exists between any two stations on the network, and provides backup links that automatically take over when a primary link goes down. The spanning tree algorithms supported by this switch include these versions:

- **STP** – Spanning Tree Protocol (IEEE 802.1D)
- **RSTP** – Rapid Spanning Tree Protocol (IEEE 802.1w)
- **MSTP** – Multiple Spanning Tree Protocol (IEEE 802.1s)

The IEEE 802.1D Spanning Tree Protocol and IEEE 802.1w Rapid Spanning Tree Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the STP is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the spanning tree algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the spanning tree is incorrectly configured. Please read the following before making any changes from the default values.

The switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.

- Creates multiple spanning trees from any combination of ports contained within a single switch, in user specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Bridge protocol data units

For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier.
- The path cost to the root associated with each switch port.
- The port identifier

STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch.
- The path cost to the root from the transmitting port.
- The port identifier of the transmitting port.

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU and, if the topology changes, initiates a BPDU transmission.

The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch.
- The shortest distance to the root switch is calculated for each switch.
- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a stable STP topology

The goal is to make the root port the fastest link. If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network becomes the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For example, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP port states

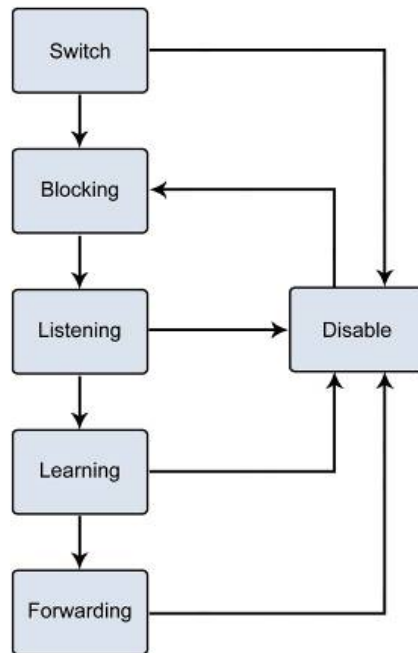
The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a blocking state to a forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists in one of the following five states:

- **Blocking** – The port is blocked from forwarding or receiving packets.
- **Listening** – The port is waiting to receive BPDU packets that may tell the port to go back to the blocking state.
- **Learning** – The port is adding addresses to its forwarding database, but not yet forwarding packets.
- **Forwarding** – The port is forwarding packets.
- **Disabled** – The port only responds to network management messages and must return to the blocking state first.

A port transitions from one state to another as follows:

- From initialization (switch boot) to blocking.
- From blocking to listening or to disabled.
- From listening to learning or to disabled.
- From learning to forwarding or to disabled.
- From forwarding to disabled.
- From disabled to blocking.



You can modify each port state by using management software. When STP is enabled, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state. No packets (except BPDUs) are forwarded from, or received by, STP-enabled ports until the forwarding state is enabled for that port.

STP parameters

STP operation levels

The industrial managed switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.

Note: On the switch level, STP calculates the bridge identifier for each switch and then sets the root bridge and the designated bridges. On the port level, STP sets the root port and the designated ports.

The following are the user-configurable STP parameters for the switch level:

Parameter	Description	Default Value
Bridge Identifier (Not user configurable except by setting priority below)	A combination of the user-set priority and the switch's MAC address. The Bridge Identifier consists of two parts: A 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC.	32768 + MAC
Priority	A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge	32768
Hello Time	The length of time between broadcasts of the hello message by the switch	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer	The amount of time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

The following are the user-configurable STP parameters for the port or port group level:

Variable	Description	Default Value
Port Priority	A relative priority for each port – lower numbers give a higher priority and a greater chance of a given port being elected as the root port	128
Port Cost	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active path	200,000-100Mbps Fast Ethernet ports 20,000-1000Mbps Gigabit Ethernet ports 0 - Auto

Default spanning-tree configuration

Feature	Default Value
Enable state	STP disabled for all ports
Port priority	128
Port cost	0
Bridge Priority	32,768

User-changeable STA parameters

The factory default settings for the switch should cover the majority of installations. It is advisable to keep the default settings as set at the factory unless it is absolutely necessary. The user changeable parameters in the switch are as follows:

- **Priority** – A priority for the switch can be set from 0 to 65535. 0 is equal to the highest priority.

- **Hello Time** – The hello time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the root bridge to tell all other switches that it is indeed the root bridge. If you set a hello time for the switch and it is not the root bridge, the set hello time will be used if and when the switch becomes the root bridge.

Note: The hello time cannot be longer than the max. age or a configuration error will occur.

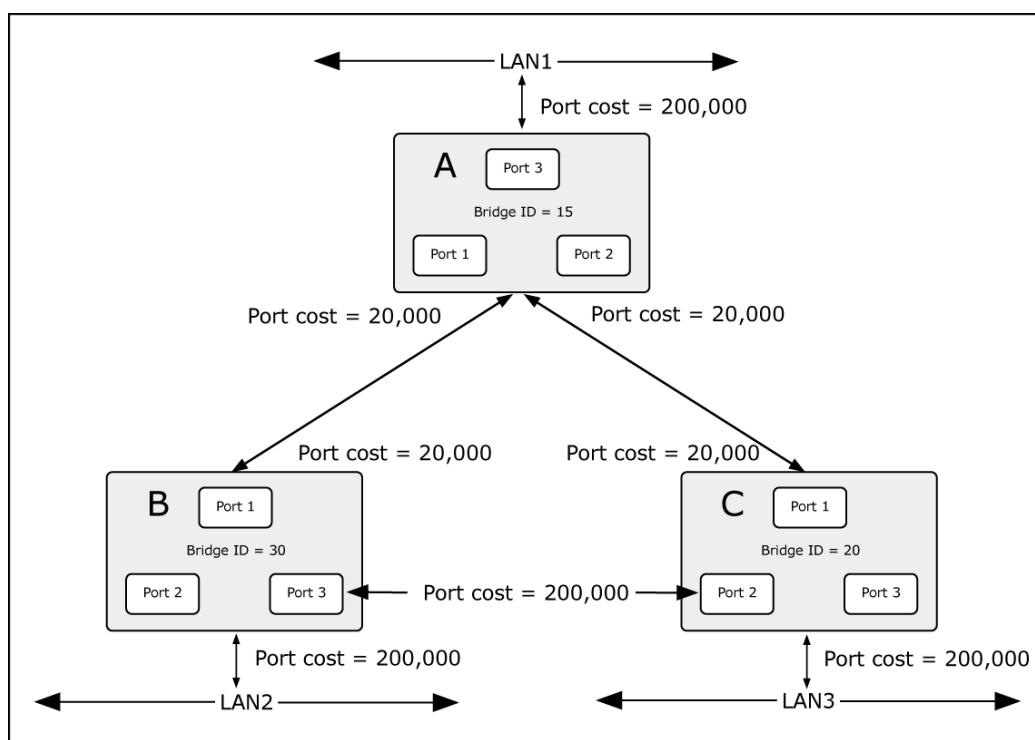
- **Max. Age** – The max. age can be from 6 to 40 seconds. At the end of the max age, if a BPDU has still not been received from the root bridge, the switch starts sending its own BPDU to all other switches for permission to become the root bridge. If the switch has the lowest bridge identifier, it will become the root bridge.
- **Forward Delay Timer** – The forward delay can be from 4 to 30 seconds. This is the time any port on the switch spends in the listening state while moving from the blocking state to the forwarding state.

Note: Observe the following formulas when setting the above parameters: **Max. Age** $\geq 2 \times (\text{Forward Delay} - 1 \text{ second})$, **Max. Age** $\geq 2 \times (\text{Hello Time} + 1 \text{ second})$.

- **Port Priority** – A port priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the root port.
- **Port Cost** – A port cost can be set from 0 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.

Illustration of STP

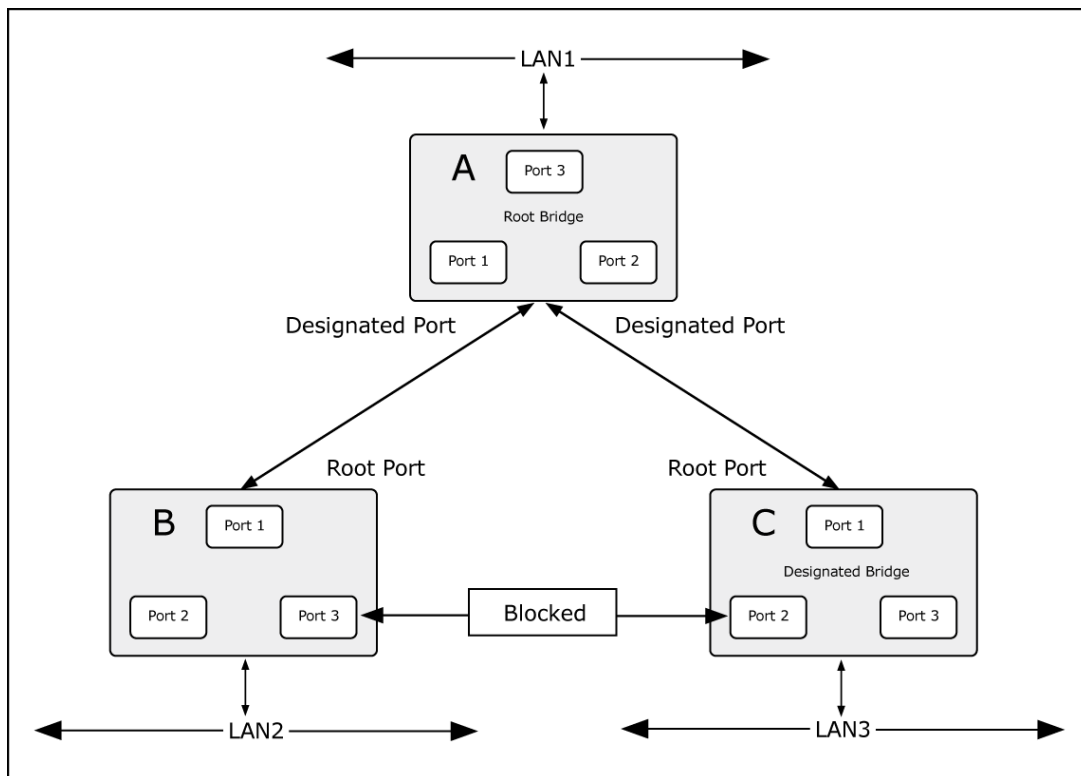
A simple illustration of three switches connected in a loop is depicted in the following diagram. In this example, you can anticipate some major network problems if the STP assistance is not applied.



If switch A broadcasts a packet to switch B, switch B broadcasts to switch C, and switch C broadcasts back to switch A and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure. In this example, STP breaks the loop by blocking the connection between switch B and C. The decision to block a particular connection is based on the STP calculation of the most current bridge and port settings.

Now, if switch A broadcasts a packet to switch C, then switch C drops the packet at port 2 and the broadcast ends there. Setting up STP using values other than the defaults, can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the priority setting, or influencing STP to choose a particular port to block using the port priority and port cost settings is, however, relatively straightforward.

In this example, only the default STP values are used:



The switch with the lowest bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 20,000) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 200,000). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between switch B and switch C is the blocked link.

STP system configuration

The STP Bridge Configuration page permits configuration of the STP system settings. The settings are used by all STP bridge instances in the switch. The industrial managed switch supports the following spanning tree protocols:

- **Compatible** – Spanning Tree Protocol (STP): Provides a single path between end stations, avoiding and eliminating loops.
- **Normal** – Rapid Spanning Tree Protocol (RSTP) : Detects and uses network topologies that provide faster spanning tree convergence, without creating forwarding loops.
- **Extension** – Multiple Spanning Tree Protocol (MSTP) : Defines an extension to RSTP to further develop the usefulness of virtual LANs (VLANs). This "Per-VLAN" MSTP configures a separate spanning tree for each VLAN group and blocks all but one of the possible alternate paths within each spanning tree.

The screenshot shows the 'STP Bridge Configuration' web page. It has a title 'STP Bridge Configuration' in blue. Below it is a section 'Basic Settings' containing a table with the following fields: Protocol Version (MSTP), Bridge Priority (32768), Forward Delay (15), Max Age (20), Maximum Hop Count (20), and Transmit Hold Count (6). Below this is an 'Advanced Settings' section with a table containing: Edge Port BPDU Filtering (checkbox), Edge Port BPDU Guard (checkbox), Port Error Recovery (checkbox), and Port Error Recovery Timeout (text input). At the bottom are 'Apply' and 'Reset' buttons.

The page includes the following fields:

Basic settings

Object	Description
Protocol Version	The STP protocol version setting. Selections are STP , RSTP and MSTP .
Bridge 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. For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
Forward Delay	The delay used by STP bridges to transition root and designated ports to forwarding (used in STP compatible mode). Valid values are in the range of 4 to 30 seconds

Object	Description
	Default: 15 Minimum: The higher of 4 or $[(\text{Max. Message Age} / 2) + 1]$ Maximum: 30
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. Default: 20 Minimum: The higher of 6 or $[2 \times (\text{Hello Time} + 1)]$. Maximum: The lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$
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. Valid values are in the range 6 to 40 hops.
Transmit Hold Count	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU is delayed. Valid values are in the range of 1 to 10 BPDU's per second.

Advanced settings

Object	Description
Edge Port BPDU Filtering	Controls whether a port explicitly configured as Edge will transmit and receive BPDUs.
Edge Port BPDU Guard	Controls whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port enters the error-disabled state, and is removed from the active topology.
Port Error Recovery	Controls 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 that has to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).

Note: The industrial managed switch implements the rapid spanning protocol as the default spanning tree protocol. When selecting “Compatibles” mode, the system uses the RSTP (802.1w) to be compatible and work with another STP (802.1D)’s BPDU control packet.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Bridge status

The STP Bridges page provides a status overview of all STP bridge instances. The table contains a row for each STP bridge instance, and the columns display the following information:

STP Bridges						
MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	80:00-00:30:4F:11:22:55	80:00-00:30:4F:11:22:55	-	0	Steady	-
Auto-refresh ☐ Refresh						

The page includes the following fields:

Object	Description
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 this is zero. For all other bridges, it is the sum of the port path costs on the least cost path to the root bridge.
Topology Flag	The current state of the topology change flag for this bridge instance.
Topology Change Last	The time since the last topology change occurred.

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

CIST port configuration

This STP CIST Port Configuration page permits the user to inspect and change the current STP CIST port configurations.

STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-Point
							Role	TCN		
-	☐	Auto		128	Non-Edge	☒	☐	☐	☐	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-Point
							Role	TCN		
*	☐	<All>		<All>	<All>	☐	☐	☐	☐	<All>
1	☐	Auto		128	Non-Edge	☒	☐	☐	☐	Auto
2	☐	Auto		128	Non-Edge	☒	☐	☐	☐	Auto
3	☐	Auto		128	Non-Edge	☒	☐	☐	☐	Auto
4	☐	Auto		128	Non-Edge	☒	☐	☐	☐	Auto
5	☐	Auto		128	Non-Edge	☒	☐	☐	☐	Auto
6	☐	Auto		128	Non-Edge	☒	☐	☐	☐	Auto
7	☐	Auto		128	Non-Edge	☒	☐	☐	☐	Auto
8	☐	Auto		128	Non-Edge	☒	☐	☐	☐	Auto
9	☐	Auto		128	Non-Edge	☒	☐	☐	☐	Auto
10	☐	Auto		128	Non-Edge	☒	☐	☐	☐	Auto

Apply Reset

The page includes the following fields:

Object	Description
Port	The switch port number of the logical STP port.
STP Enabled	Controls if RSTP is enabled on this switch port.
Path Cost	Controls the path cost incurred by the port. The Auto setting sets 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 can be chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range of 1 to 200000000 .
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). Default: 128 Range: 0-240, in steps of 16
AdminEdge	Controls whether the operEdge flag should start as set or cleared (the initial operEdge state when a port is initialized).
AutoEdge	Controls if the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from BPDUs received on the port.

Object	Description
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 a lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network and influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard .
Restricted TCN	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set, it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.
BPDU Guard	If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting. A port entering error-disabled state due to this setting is subject to the bridge port error recovery setting as well.
Point-to-point	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transitions to the forwarding state is faster for point-to-point LANs than for shared media.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the following values. Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

Recommended STP path cost range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Recommended STP path costs

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

Default STP path costs

Port Type	Link Type	IEEE 802.1w-2001
Ethernet	Half Duplex	2,000,000
	Full Duplex	1,000,000
	Trunk	500,000
Fast Ethernet	Half Duplex	200,000
	Full Duplex	100,000
	Trunk	50,000
Gigabit Ethernet	Full Duplex	10,000
	Trunk	5,000

MSTI priorities

The MSTI Configuration page permits the user to inspect and change the current STP MSTI bridge instance priority configurations.

MSTI Configuration

MSTI Priority Configuration

MSTI	Priority
*	<All> ▼
CIST	32768 ▼
MSTI1	32768 ▼
MSTI2	32768 ▼
MSTI3	32768 ▼
MSTI4	32768 ▼
MSTI5	32768 ▼
MSTI6	32768 ▼
MSTI7	32768 ▼

The page includes the following fields:

Object	Description
MSTI	The bridge instance. The CIST is the default instance, which is always active.
Priority	Controls the bridge priority. Lower numerical 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

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

MSTI configuration

The MSTI Configuration page permits the user to inspect and change the current STP MSTI bridge instance priority configurations.

MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	00-30-4f-11-22-33
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

The page includes the following fields:

Configuration identification

Object	Description
Configuration Name	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision, as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's. (Intra-region). The name is a maximum of 32 characters.
Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.

MSTI mapping

Object	Description
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 VLAN's mapped to the MSTI. The VLANs must be separated with a comma and/or space. A VLAN can only be mapped to one MSTI. A unused MSTI should be left empty (i.e., not have any VLANs mapped to it).

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

MSTI ports configuration

The MSTI Port Configuration page permits the user to inspect and change the current STP MSTI port configurations. A MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured and applicable for 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. The aggregation settings are stack global.

MSTI Port Configuration

Select MSTI

MSTI ▼

Get

The page includes the following fields:

MSTI port configuration

Object	Description
Select MSTI	Select the bridge instance and set more detail configuration.

MST1 MSTI Port Configuration

MSTI Aggregated Ports Configuration

Port	Path Cost	Priority
-	Auto ▼	128 ▼

MSTI Normal Ports Configuration

Port	Path Cost	Priority
*	<All> ▼	<All> ▼
1	Auto ▼	128 ▼
2	Auto ▼	128 ▼
3	Auto ▼	128 ▼
4	Auto ▼	128 ▼
5	Auto ▼	128 ▼
6	Auto ▼	128 ▼
7	Auto ▼	128 ▼
8	Auto ▼	128 ▼
9	Auto ▼	128 ▼
10	Auto ▼	128 ▼

Apply Reset

The page includes the following fields:

MSTx MSTI port configuration

Object	Description
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 sets 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 favor 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.

Buttons

- Click **Get** to set MSTx configuration.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Port status

The STP Port Status page displays the STP CIST port status for physical ports in the currently selected switch.

STP Port Status

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-
10	Non-STP	Forwarding	-

Auto-refresh ☐

The page includes the following fields:

Object	Description
Port	The switch port number of the logical STP port.
CIST Role	The current STP port role of the ICST port. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort Disable
CIST State	The current STP port state of the CIST port . The port state can be one of the following values: Disabled Learning Forwarding
Uptime	The time since the bridge port was last initialized.

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

Port statistics

The STP Statistics page displays the STP port statistics counters for physical ports in the currently selected switch.

STP Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
No ports enabled										

Auto-refresh ☐

The page includes the following fields:

Object	Description
Port	The switch port number of the logical RSTP port.
MSTP	The number of MSTP Configuration BPDU's received/transmitted on the port.
RSTP	The number of RSTP Configuration BPDU's received/transmitted on the port.
STP	The number of legacy STP Configuration BPDU's received/transmitted on the port.
TCN	The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
Discarded Unknown	The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
Discarded Illegal	The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear the counters for all ports.

Multicast

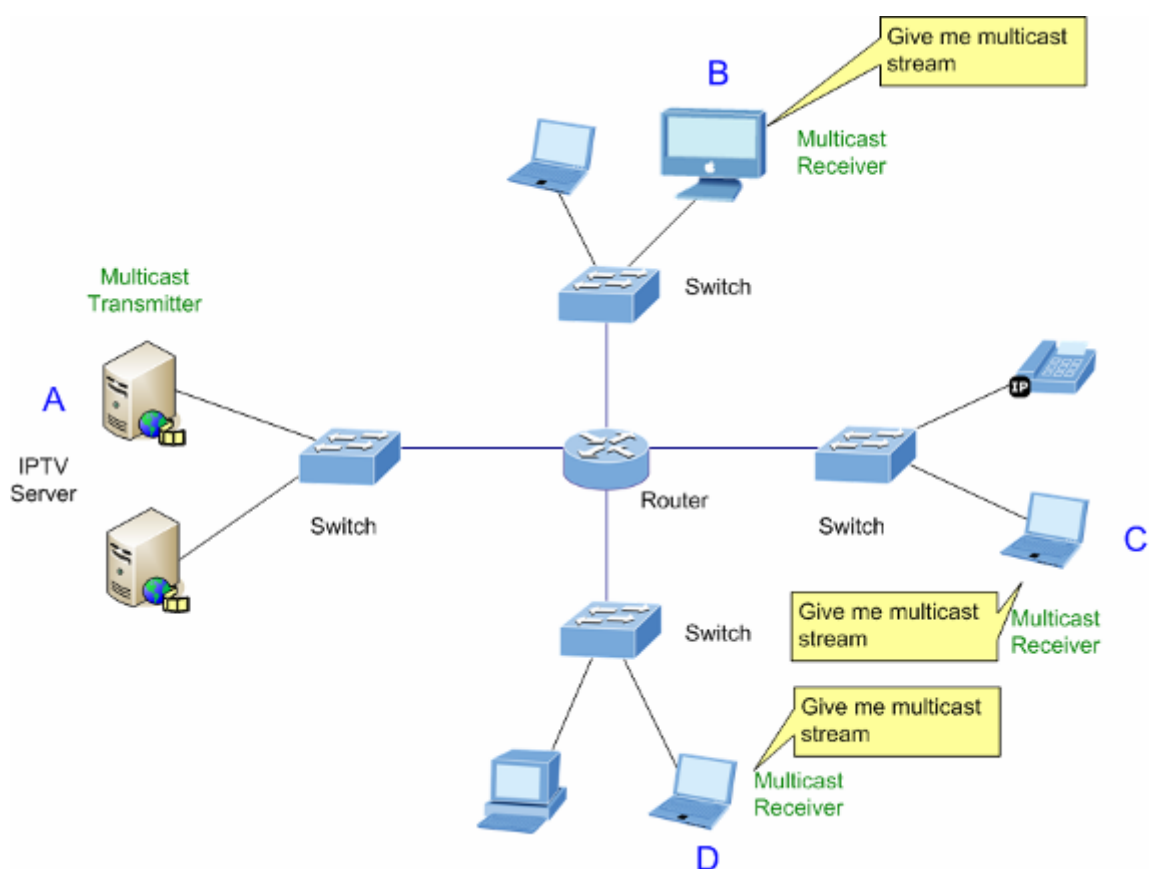
IGMP snooping

The Internet Group Management Protocol (IGMP) allows hosts and routers share information about multicast groups memberships. IGMP snooping is a switch feature that monitors the exchange of IGMP messages and copies them to the CPU for feature processing. The overall purpose of IGMP snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

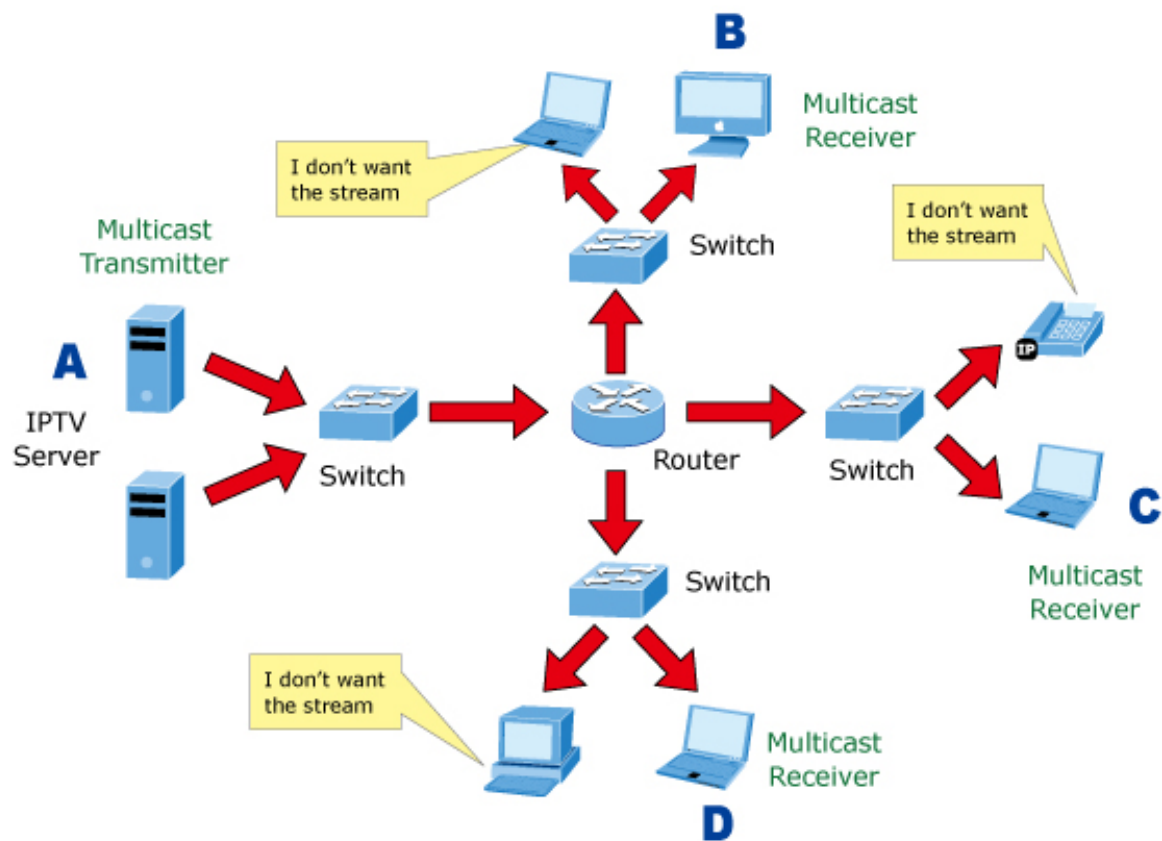
About IGMP snooping

Computers and network devices that need to receive multicast transmissions must inform nearby routers that they will become members of a multicast group. IGMP is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one multicast router on a sub network, one router is elected as 'querier.' This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine whether or not multicast packets should be forwarded to a given sub network. Using IGMP, the router can check to see if there is at least one member of a multicast group on a given sub network. If there are no members on a sub network, packets will not be forwarded to that sub network.

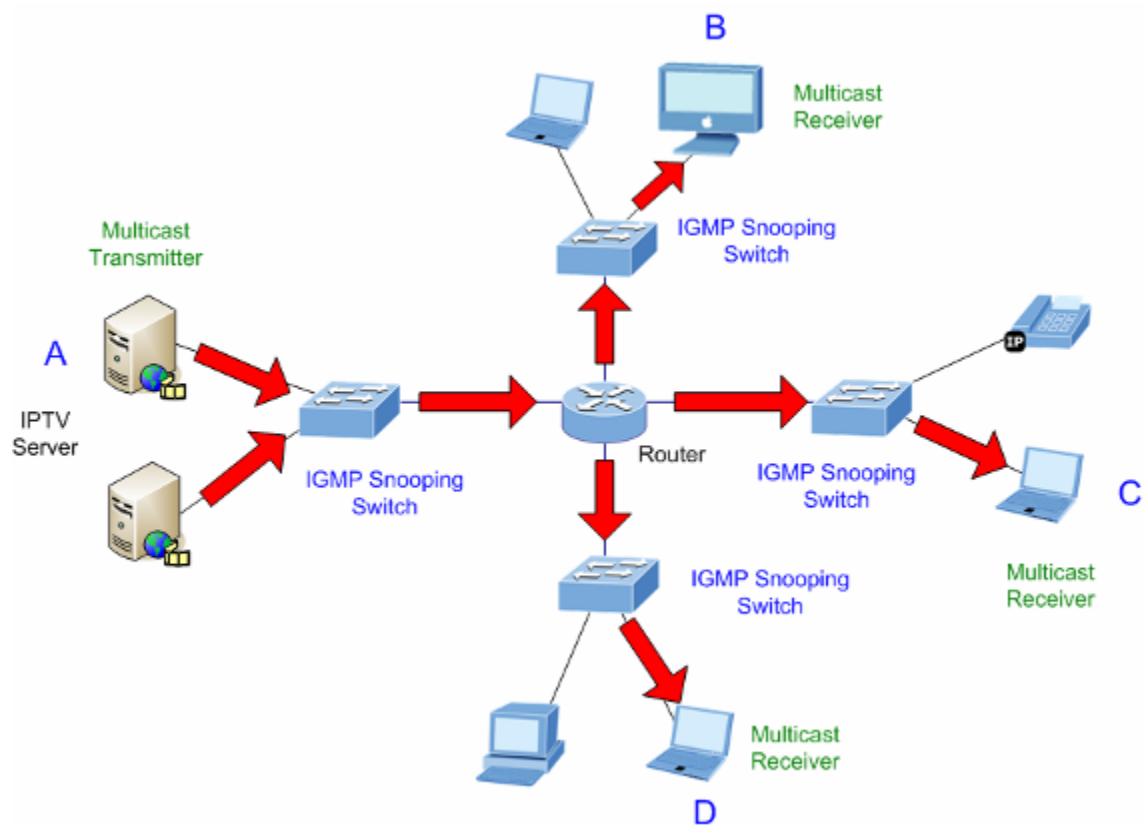
Multicast service



Multicast flooding



IGMP snooping multicast stream control

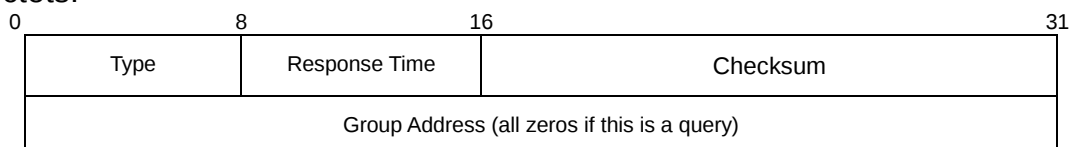


IGMP versions 1 and 2

Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group. IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data. The format of an IGMP packet is shown below:

IGMP message format

Octets:



The IGMP type codes are shown below:

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0)
0x11	Specific Group Membership Query (if Group Address is Present)
0x16	Membership Report (version 2)
0x17	Leave a Group (version 2)
0x12	Membership Report (version 1)

IGMP packets allow multicast routers to keep track of the membership of multicast groups on their respective sub networks. The following outlines what is communicated between a multicast router and a multicast group member using IGMP.

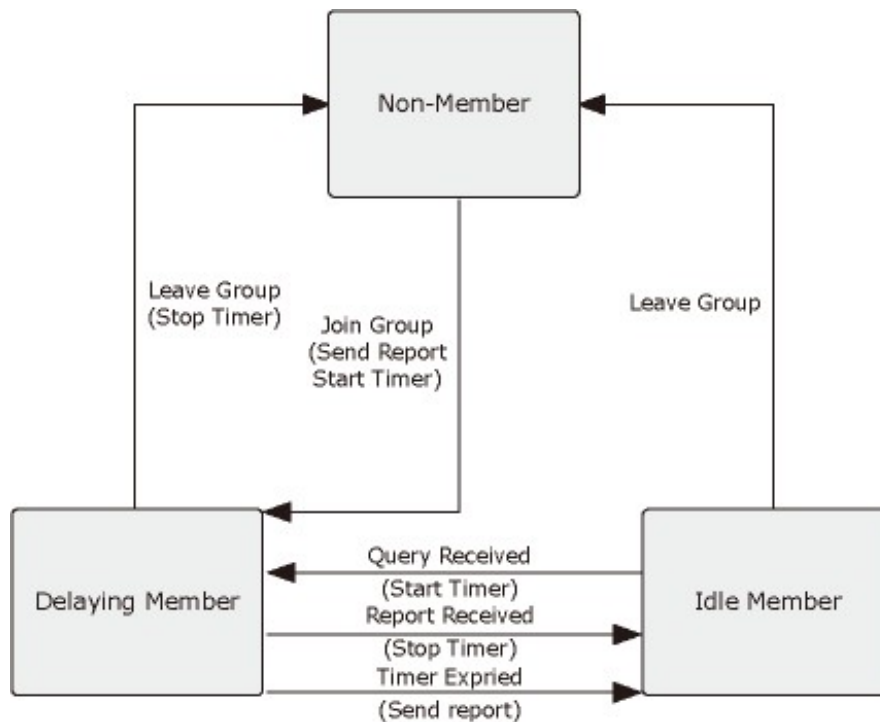
- A host sends an IGMP “report” to join a group
- A host will never send a report when it wants to leave a group (for version 1).
- A host will send a “leave” report when it wants to leave a group (for version 2).

Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their sub networks. If there is no response from a particular group, the router assumes that there are no group members on the network.

The Time-to-Live (TTL) field of query messages is set to 1 so that the queries will not be forwarded to other sub networks.

IGMP version 2 introduces some enhancements such as a method to elect a multicast queried for each LAN, an explicit leave message, and query messages that are specific to a given group.

The states a computer will go through to join or to leave a multicast group are as follows:



IGMP querier

A router or multicast-enabled switch can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the role of querying the LAN for group members. It then propagates the service requests to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Note: Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

Profile table

The IPMC Profile Configurations page provides IPMC Profile related configurations. The IPMC profile is used to deploy the access control on IP multicast streams. It is allowed to create at maximum 64 Profiles with a maximum of 128 corresponding rules for each.

IPMC Profile Configurations

Global Profile Mode
Disabled ▼

IPMC Profile Table Setting

Delete	Profile Name	Profile Description	Rule
Delete			

Add New IPMC Profile

Apply
Reset

The page includes the following fields:

Object	Description
Global Profile Mode	Enable/Disable the Global IPMC Profile. The system starts to do filtering based on profile settings only when the global profile mode is enabled.
Delete	Check to delete the entry. The designated entry is deleted during the next save.
Profile Name	The name used for indexing the profile table. Each entry has a unique name which is composed of a maximum of 16 alphabetic and numeric characters. At least one alphabet must be present.
Profile Description	Additional description, which is composed of at maximum 64 alphabetic and numeric characters, about the profile. No blank characters or spaces 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

- Click **Add New IPMC Profile** to add a new IPMC profile. Specify the name and configure the new entry, and then click **Save**.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Address entry

The IPMC Profile Address Configuration page provides address range settings used in the IPMC profile. The address entry is used to specify the address range associated with the IPMC profile. It can create a maximum of 128 address entries in the system.

IPMC Profile Address Configuration

Navigate Address Entry Setting in IPMC Profile by entries per page.

Delete	Entry Name	Start Address	End Address
Delete			

The page includes the following fields:

Object	Description
Delete	Click Delete to delete the entry. The designated entry is deleted during the next save.
Entry Name	The name used for indexing the address entry table. Each entry has a unique name with a maximum of 16 alphabetic and numeric characters. At least one alphabet 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

- Click **Add New Address (Range) Entry** to add a new address range. Specify the name and configure the addresses, and then click **Save**.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Click **1<<** to update the table starting from the first entry in the IPMC profile address configuration.
- Click **>>** to update the table starting with the entry after the last entry currently displayed.

IGMP snooping configuration

The IGMP Snooping Configuration page provides IGMP snooping-related configuration information.

IGMP Snooping Configuration

Global Configuration			
Snooping Enabled	☒		
Unregistered IPMCv4 Flooding Enabled	☐		
IGMP SSM Range	232.0.0.0	/ 8	
Leave Proxy Enabled	☐		
Proxy Enabled	☐		

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<All> ▼	☐	<All> ▼
1	Auto ▼	☐	Unlimited ▼
2	Auto ▼	☐	Unlimited ▼
3	Auto ▼	☐	Unlimited ▼
4	Auto ▼	☐	Unlimited ▼
5	Auto ▼	☐	Unlimited ▼
6	Auto ▼	☐	Unlimited ▼
7	Auto ▼	☐	Unlimited ▼
8	Auto ▼	☐	Unlimited ▼

The page includes the following fields:

Object	Description
Snooping Enabled	Enable 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.
IGMP SSM Range	SSM (Source-Specific Multicast) range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range.
Leave Proxy Enable	Enable IGMP leave proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enable	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 IGMP router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. The switch forwards IGMP join or leave packets to an IGMP router port. Selections are as follows: Auto – The industrial managed switch automatically uses the port as IGMP router port if the port receives IGMP query packets. Fix – The industrial managed switch always uses the specified port as an IGMP router port. Use this mode when connecting an IGMP multicast server or IP camera with multicast protocol to the port. None – The industrial managed switch will not use the specified port as an IGMP router port and will not keep any record of an IGMP router being connected to this port. Use this mode when connecting other IGMP multicast servers directly to the non-querier industrial managed switch, and you don't want the multicast stream to be flooded to the uplink switch through the port that connected to the IGMP querier.
Fast Leave	Enable the fast leave on the port.
Throtting	Enable to limit the number of multicast groups to which a switch port can belong.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

IGMP snooping VLAN configuration

The IGMP Snooping VLAN Configuration page shows up to 99 entries from the VLAN table (default is 20 entries per page). The range of entries per page can be typed into the **Start from VLAN** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the VLAN table. The first entry shown will be the one with the lowest VLAN ID found in the VLAN table.

IGMP Snooping VLAN Configuration

Start from VLAN with entries per page.

VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	☒	☒	192.168.0.100	IGMP-Auto	0	2	125	100	10	1

The page includes the following fields:

Object	Description
Delete	Select this check box to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enable	Enable the per-VLAN IGMP Snooping. Only up to 32 VLANs can be selected.
Querier Election	Enable the IGMP Querier election in the VLAN. Disable to act as an IGMP non-querier.
Querier Address	Define the IPv4 address as source address used in IP header for IGMP querier election. When the querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, 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. Selections include: IGMP-Auto (default selection), Forced IGMPv1 , Forced IGMPv2 , Forced IGMPv3 .
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). The default interface priority value is 0
RV	Robustness Variable. The RV permits tuning for the expected packet loss on a network. The allowed range is 1 to 255 . The default robustness variable value is 2 .
QI	Query Interval. The QI is the interval between general queries sent by the querier. The allowed range is 1 to 31744 seconds. The default query interval is 125 seconds.
QRI	Query Response Interval. This is the maximum response time used to

Object	Description
	calculate the maximum resp code inserted into the periodic general queries. The allowed range is 0 to 31744 in tenths of seconds. The 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

- Click **Refresh** to refresh the table starting from the **Start from VLAN** and **entries per page** input fields.
- Click **◀** to update the table starting from the first entry in the VLAN table (i.e., the entry with the lowest VLAN ID).
- Click **>>** to updates the table, starting with the entry after the last entry currently displayed.
- Click **Add New IGMP VLAN** to add a new IGMP VLAN. Specify the VID and configure the new entry, and then click **Save**. The specific IGMP VLAN starts working after the corresponding static VLAN is also created
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

IGMP snooping port group filtering

In certain switch applications, the administrator may want to control the multicast services that are available to end users (an IP/TV service based on a specific subscription plan, for example). The IGMP filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and IGMP throttling limits the number of simultaneous multicast groups a port can join.

The IGMP Snooping Port Group Filtering Configuration page permits assigning a profile to a switch port that specifies multicast groups that are permitted or denied on the port. An IGMP filter profile can contain one or more, or a range of, multicast addresses. However, only one profile can be assigned to a port. When enabled, IGMP join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the IGMP join report is forwarded as normal. If a requested multicast group is denied, the IGMP join report is dropped.

IGMP throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can

take one of two actions; either “deny” or “replace.” If the action is set to deny, any new IGMP join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

IGMP Snooping Port Filtering Profile Configuration

Port	Filtering Profile
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

The page includes the following fields:

Object	Description
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.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

IGMP snooping status

The IGMP Snooping Status page provides IGMP snooping status.

Auto-refresh ☐

IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-

The page includes the following fields:

Object	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	The current working querier version.
Host Version	The current working host version.
Querier Status	Shows whether the querier status is "ACTIVE" or "IDLE".
Querier Transmitted	The number of transmitted queries.
Querier Received	The number of received queries.
V1 Reports Received	The number of received V1 reports.
V2 Reports Received	The number of received V2 reports.
V3 Reports Received	The number of received V3 reports.
V2 Leave Received	The number of received V2 leave.
Router Port	Displays the ports that are acting 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 learned to be a router port. Both denote the specific port is configured or learned to be a router port.
Port	Switch port number.
Status	Indicates whether or not the specific port is a router port.

Buttons

- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear all statistics counters.
- Select **Auto-refresh** to automatically refresh the page every three seconds.

IGMP group information

Entries in the IGMP group table are shown in the IGMP Snooping Group Information page. The IGMP group table is sorted first by VLAN ID, and then by group.

Each page shows up to 99 entries from the IGMP group table (default is 20 entries per page). The range of entries per page can be typed into the **Start from VLAN** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the IGMP Group table. The **Start from VLAN** and **group Address** fields permit the user to select the starting point in the IGMP group table.

IGMP Snooping Group Information

Auto-refresh ☐

Start from VLAN and group Address with entries per page.

		Port Members																											
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
No more entries																													

The page includes the following fields:

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

Buttons

- Select **Auto-refresh** to automatically refresh the page every three seconds.
- Click **Refresh** to refresh the table starting from the input fields.
- Click **<<** to update the table starting from the first entry in the IGMP group table.
- Click **>>** to update the table, starting with the entry after the last entry currently shown.

IGMPv3 information

Entries in the IGMP SFM (Source-Filtered Multicast) information table are shown on the IGMP SFM Information page. The table also contains SSM (Source-Specific Multicast) information. The table is sorted first by VLAN ID, then by group, and then by port number. 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 range of entries per page can be typed into the **Start from VLAN** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the IGMP Group table. The **Start from VLAN** and **group Address** fields permit the user to select the starting point in the IGMP information table.

IGMP SFM Information

Auto-refresh ☐

Start from VLAN and Group with entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

The page includes the following fields:

Object	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group shown.
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, system limits the total number of IP source addresses for filtering to 128.
Type	Indicates the type. It can be either Allow or Deny .
Hardware Filter/Switch	Indicates if the data plane destined to the specific group address from the source IPv4 address can be accommodated by the chip.

Buttons

- Select **Auto-refresh** to automatically refresh the page every three seconds.
- Click **Refresh** to refresh the table starting from the input fields.
- Click **1<<** to update the table starting from the first entry in the IGMP group table.
- Click **>>** to update the table, starting with the entry after the last entry currently shown.

MLD snooping configuration

The MLD Snooping Configuration page provides MLD snooping-related configuration.

MLD Snooping Configuration

Global Configuration	
Snooping Enabled	☒
Unregistered IPMCv6 Flooding Enabled	☐
MLD SSM Range	ff3e:: / %6
Leave Proxy Enabled	☐
Proxy Enabled	☐

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<All> ▼	☐	<All> ▼
1	Auto ▼	☐	Unlimited ▼
2	Auto ▼	☐	Unlimited ▼
3	Auto ▼	☐	Unlimited ▼
4	Auto ▼	☐	Unlimited ▼
5	Auto ▼	☐	Unlimited ▼
6	Auto ▼	☐	Unlimited ▼
7	Auto ▼	☐	Unlimited ▼
8	Auto ▼	☐	Unlimited ▼

The page includes the following fields:

Object	Description
Snooping Enabled	Enable 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.
Leave Proxy Enable	Enable MLD leave proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.
Proxy Enable	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 acts as a router port. Selections are Auto , Fix , Fone , and the default compatibility value is Auto .
Fast Leave	Enable fast leave on the port.
Throtting	Enable Throtting to limit the number of multicast groups to which a switch port can belong.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

MLD snooping VLAN configuration

Each page shows up to 99 entries from the VLAN table (default is 20 entries per page). The range of entries per page can be typed into the Start from VLAN and entries per page fields. When initially accessing the page, it shows the first 20 entries from the beginning of the VLAN table. The first entry shown will be the one with the lowest VLAN ID found in the VLAN table.

MLD Snooping VLAN Configuration

Start from VLAN with entries per page.

VLAN ID	Snooping Enabled	Querier Election	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
1	☐	☐	MLD-Auto	0	2	125	100	10	1

The page includes the following fields:

Object	Description
Delete	Select this check box to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	The VLAN ID of the entry.
IGMP Snooping Enable	Enable the per-VLAN MLD snooping. Only up to 32 VLANs can be selected.
Querier Election	Enable the MLD querier election in the VLAN. Disable to act as an IGMP non-querier.
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. Selections include: MLD-Auto (default selection), Forced MLDv1 , and Forced MLDv2 .
PRI	Priority of Interface. It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest). The default interface priority value is 0
RV	Robustness Variable. The RV permits tuning for the expected packet loss on a network. The allowed range is 1 to 255 . The default robustness variable value is 2 .
QI	Query Interval. The QI is the interval between general queries sent by the querier. The allowed range is 1 to 31744 seconds. The default query interval is 125 seconds.
QRI	Query Response Interval. This is the maximum response time used to calculate the maximum resp code inserted into the periodic general queries. The allowed range is 0 to 31744 in tenths of seconds. The 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

- Click **Refresh** to refresh the table starting from the **Start from VLAN** and **entries per page** input fields.
- Click **I<<** to update the table starting from the first entry in the VLAN table (i.e., the entry with the lowest VLAN ID).
- Click **>>** to updates the table, starting with the entry after the last entry currently displayed.

- Click **Add New MLD VLAN** to add a new MLD VLAN. Specify the VID and configure the new entry, and then click **Save**. The specific MLD VLAN starts working after the corresponding static VLAN is also created.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

MLD snooping port group filtering

In certain switch applications, the administrator may want to control the multicast services available to end users (such as an IP/TV service based on a specific subscription plan, for example). The MLD filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port, and MLD throttling limits the number of simultaneous multicast groups a port can join.

The MLD Snooping Port Filtering Profile Configuration page permits assigning a profile to a switch port that specifies multicast groups that are permitted or denied on the port. A MLD filter profile can contain one or more, or a range of, multicast addresses. However, only one profile can be assigned to a port. When enabled, MLD join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the MLD join report is forwarded as normal. If a requested multicast group is denied, the MLD join report is dropped.

MLD throttling sets a maximum number of multicast groups that a port can join at the same time. When the maximum number of groups is reached on a port, the switch can take one of two actions; either “deny” or “replace.” If the action is set to deny, any new MLD join reports will be dropped. If the action is set to replace, the switch randomly removes an existing group and replaces it with the new multicast group.

MLD Snooping Port Filtering Profile Configuration		
Port	Filtering Profile	
1		- 
2		- 
3		- 
4		- 
5		- 
6		- 
7		- 
8		- 

The page includes the following fields:

Object	Description
Port	The logical port for the settings.
Filtering Group	Select the IPMC Profile as the filtering condition for the specific port. Click the View button to view a summary of the designated profile.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

MLD snooping status

The MLD Snooping Status page provides MLD snooping status.

Auto-refresh ☐ Refresh Clear

MLD Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V1 Leaves Received
---------	-----------------	--------------	----------------	---------------------	------------------	---------------------	---------------------	--------------------

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-

The page includes the following fields:

Object	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	The current working querier version.
Host Version	The current working host version.
Querier Status	Shows whether the querier status is "ACTIVE" or "IDLE".
Querier Transmitted	The number of transmitted queries.
Querier Received	The number of received queries.
V1 Reports Received	The number of received V1 reports.
V2 Reports Received	The number of received V2 reports.
V3 Reports Received	The number of received V3 reports.
V2 Leave Received	The number of received V2 leave.
Router Port	Displays the ports that are acting 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 learned to be a router port. Both denote the specific port is configured or learned to be a router port.
Port	Switch port number.
Status	Indicates whether or not the specific port is a router port.

Buttons

- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear all statistics counters.
- Select **Auto-refresh** to automatically refresh the page every three seconds.

MLD group information

Entries in the MLD group table are shown in the MLD Snooping Group Information 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 (default is 20 entries per page). The range of entries per page can be typed into the **Start from VLAN** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the MLD Group table. The **Start from VLAN** and **group Address** fields permit the user to select the starting point in the MLD group table.

MLD Snooping Group Information

Auto-refresh ☐

Start from VLAN and group Address with entries per page.

		Port Members																											
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
No more entries																													

The page includes the following fields:

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

Buttons

- Select **Auto-refresh** to automatically refresh the page every three seconds.
- Click **Refresh** to refresh the table starting from the input fields.
- Click **k<** to update the table starting from the first entry in the MLD group table.
- Click **>** to update the table, starting with the entry after the last entry currently shown.

MLDv2 information

Entries in the MLD SFM (Source-Filtered Multicast) information table are shown on the IGMP SFM Information page. The table also contains SSM (Source-Specific Multicast) information. The table is sorted first by VLAN ID, then by group, and then by port number. Different source addresses that belong to the same group are treated as single entry.

Each page shows up to 99 entries from the MLD SFM Information table. The range of entries per page can be typed into the **Start from VLAN** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the IGMP Group table. The **Start from VLAN** and **Group** fields permit the user to select the starting point in the MLD information table.

MLD SFM Information

Auto-refresh ☐

Start from VLAN and Group with entries per page.

VLAN ID	Group	Port	Mode	Source Address	Type	Hardware Filter/Switch
No more entries						

The page includes the following fields:

Object	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group shown.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per basis (VLAN ID, port number, Group Address). It can be either Include or Exclude .
Source Address	IP Address of the source. Currently, the system limits the total number of IP source addresses for filtering to 128.
Type	Indicates the type. It can be either Allow or Deny .
Hardware Filter/Switch	Indicates if the data plane destined to the specific group address from the source IPv4 address can be accommodated by the chip.

Buttons

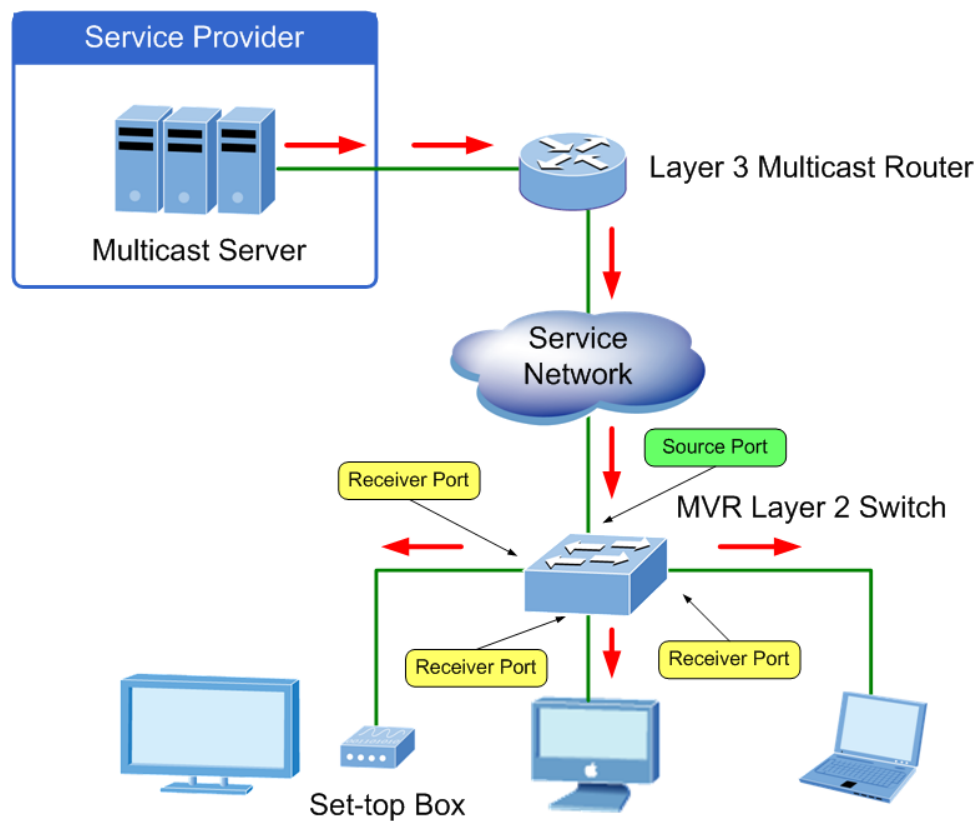
- Select **Auto-refresh** to automatically refresh the page every three seconds.
- Click **Refresh** to refresh the table starting from the input fields.
- Click **1<<** to update the table starting from the first entry in the MLD SFM information table.
- Click **>>** to update the table, starting with the entry after the last entry currently shown.

MVR (Multicast VLAN Registration)

The MVR feature enables multicast traffic forwarding on the Multicast VLANs.

- In a multicast television application, a computer or a network television or a set-top box can receive a multicast stream.
- Multiple set-top boxes or computers can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or computer sends an IGMP/MLD report message to Switch A to join the appropriate multicast group address.
- Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

A maximum of eight MVR VLANs with corresponding channel settings can be created for each multicast VLAN. A maximum of 256 group addresses are available for channel settings.



The MVR Configurations page provides MVR-related configuration information.

MVR Configurations

MVR Mode Disabled

VLAN Interface Setting (Role [I:Inactive / S:Source / R:Receiver])

Delete	MVR VID	MVR Name	IGMP Address	Mode	Tagging	Priority	LLQI	Interface Channel Profile
--------	---------	----------	--------------	------	---------	----------	------	---------------------------

Add New MVR VLAN

Immediate Leave Setting

Port	Immediate Leave
*	<All>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled

The page includes the following fields:

Object	Description
MVR Mode	Enable/Disable the Global MVR. The Unregistered Flooding control depends on the current configuration in IGMP/MLD snooping. We suggest enabling Unregistered Flooding control when the MVR group table is full.
Delete	Select Delete to delete the entry. The designated entry will be deleted during the next save.
MVR VID	Specify the Multicast VLAN ID. Caution: We do not recommend overlapping MVR source ports with management VLAN ports.
MVR Name	MVR Name is an optional attribute to indicate the name of the specific MVR VLAN. The maximum length of the MVR VLAN Name string is 16 alphanumeric characters (it must contain at least one alpha character). The MVR VLAN name can be edited for the existing MVR VLAN entries or it can be added to the new entries.
IGMP Address	Define the IPv4 address as source address used in IP header for IGMP control frames. The default IGMP address is not set (0.0.0.0). When the IGMP address is not set, 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 is 192.0.2.1.
Mode	Specify the MVR mode of operation. In Dynamic mode (default setting), MVR allows dynamic MVR membership reports on source ports. In Compatible mode, MVR membership reports are forbidden on source ports.
Tagging	Specify whether the traversed IGMP/MLD control frames will be sent as Untagged or Tagged (default setting) with the MVR VID.
Priority	Specify how the traversed IGMP/MLD control frames will be sent in a prioritized manner. The default Priority is 0.
LLQI	Define the maximum time to wait for IGMP/MLD report memberships on a receiver port before removing the port from multicast group membership. The value is in units of tenths of a seconds. The range is from 0 to 31744. The default LLQI is five-tenths or one-half second.
Interface Channel Setting	When the MVR VLAN is created, select the IPMC Profile as the channel filtering condition for the specific MVR VLAN. A summary of the Interface Channel Profiling (of the MVR VLAN) appears after clicking the View button. The profile selected for the designated interface channel cannot have an overlapped permit group address.
Port	The logical port for the settings.
Port Role	Configure an MVR port of the designated MVR VLAN as one of the following roles. Inactive: The designated port does not participate in MVR operations. Source: Configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. Receiver: Configure a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group by issuing IGMP/MLD messages. Caution: We do not recommend overlapping MVR source ports with

Object	Description
	management VLAN ports. Select the port role by clicking the Role symbol to switch the setting. I indicates Inactive; S indicates Source; R indicates Receiver. The default Role is Inactive.
Immediate Leave	Enable the fast leave on the port.

Buttons

- Click **Add New MVR VLAN** to add a new MVR VLAN. Specify the VID and configure the new entry, and then click **Save**.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

MVR status

The MVR Statistics page provides MVR status.

MVR Statistics						
VLAN ID	IGMP/MLD Queries Received	IGMP/MLD Queries Transmitted	IGMPv1 Joins Received	IGMPv2/MLDv1 Reports Received	IGMPv3/MLDv2 Reports Received	IGMPv2/MLDv1 Leaves Received
No more entries						

Auto-refresh ☐

The page includes the following fields:

Object	Description
VLAN ID	The multicast VLAN ID.
IGMP/MLD Queries Received	The number of received queries for IGMP and MLD, respectively.
IGMP/MLD Queries Transmitted	The number of transmitted queries for IGMP and MLD, respectively.
IGMPv1 Joins Received	The number of received IGMPv1 joins.
IGMPv2/MLDv1 Reports Received	The number of received IGMPv2 joins and MLDv1 reports, respectively.
IGMPv3/MLDv2 Reports Received	The number of received IGMPv1 joins and MLDv2 reports, respectively.
IGMPv2/MLDv1 Leaves Received	The number of received IGMPv2 leaves and MLDv1 done, respectively.

Buttons

- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear all statistics counters.

- Select **Auto-refresh** to automatically refresh the page every three seconds.

MVR groups information

Entries in the MVR group table are shown in the MVR Channels (Groups) Information page. The MVR group table is sorted first by VLAN ID, and then by group.

Each page shows up to 99 entries from the MLD group table (default is 20 entries per page). The range of entries per page can be typed into the **Start from VLAN** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the MVR Group table. The **Start from VLAN** and **Group Address** fields permit the user to select the starting point in the MVR group table.

MVR Channels (Groups) Information

Auto-refresh ☐

Start from VLAN and Group Address with entries per page.

		Port Members																											
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
No more entries																													

The page includes the following fields:

Object	Description
VLAN ID	VLAN ID of the group.
Groups	Group ID of the group shown.
Port Members	Ports under this group.

Buttons

- Select **Auto-refresh** to automatically refresh the page every three seconds.
- Click **Refresh** to refresh the table starting from the input fields.
- Click **k<<** to update the table starting from the first entry in the MVR group table.
- Click **>>** to update the table, starting with the entry after the last entry currently shown.

Quality of Service (QoS)

Understanding QoS

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS permits the assignment of various grades of network service to different types of traffic such as multi-media, video, protocol-specific, time critical, and file-backup traffic.

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of data and permits prioritization of certain applications across the network. You can define exactly how you want the switch to treat selected applications and types of traffic. Use QoS on the system to control a wide variety of network traffic functions by:

- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, setting higher priorities for time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Providing predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improving performance for specific types of traffic and preserving performance as the amount of traffic grows.
- Reducing the need to constantly add bandwidth to the network.
- Managing network congestion.

QoS terminology

- **Classifier** – Classifies the traffic on the network. Traffic classifications are determined by protocol, application, source, destination, and so on. You can create and modify classifications. The industrial managed switch then groups classified traffic in order to schedule them with the appropriate service level.
- **DiffServ Code Point (DSCP)** – Traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network.
- **Service Level** – Defines the priority given to a set of classified traffic. You can create and modify service levels.
- **Policy** – Comprises a set of rules that are applied to a network so that a network meets the needs of the business. That is, traffic can be prioritized across a network according to its importance to that particular business type.
- **QoS Profile** – Consists of multiple sets of rules (classifier plus service level combinations). The QoS profile is assigned to a port(s).
- **Rules** – Comprises a service level and a classifier to define how the industrial managed switch will treat certain types of traffic. Rules are associated with a QoS profile.

To implement QoS on a network, perform the following actions:

1. Define a service level to determine the priority that will be applied to traffic.
2. Apply a classifier to determine how the incoming traffic will be classified and thus treated by the industrial managed switch.
3. Create a QoS profile that associates a service level and a classifier.
4. Apply a QoS profile to a port(s).

Port policing

The QoS Ingress Port Policers page permits configuration of the policer settings for all switch ports.

QoS Ingress Port Policers				
Port	Enabled	Rate	Unit	Flow Control
*	☐	500	<All> ▼	☐
1	☐	500	kbps ▼	☐
2	☐	500	kbps ▼	☐
3	☐	500	kbps ▼	☐
4	☐	500	kbps ▼	☐
5	☐	500	kbps ▼	☐
6	☐	500	kbps ▼	☐
7	☐	500	kbps ▼	☐
8	☐	500	kbps ▼	☐

The page includes the following fields:

Object	Description
Port	The port number for which the configuration below applies.
Enable	Controls whether the policer is enabled on this switch port.
Rate	Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the Unit is kbps or fps , and it is restricted to 1-3300 when the Unit is Mbps or kfps .
Unit	Controls the unit of measure for the policer rate as kbps , Mbps , fps , or kfps . The default value is kbps .
Flow Control	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Port classification

The QoS Ingress Port Classification page permits configuration of the basic QoS ingress classification settings for all switch ports.

QoS Ingress Port Classification						
Port	CoS	DPL	PCP	DEI	Tag Class.	DSCP Based
*	<All>	<All>	<All>	<All>		☐
1	0	0	0	0	Disabled	☐
2	0	0	0	0	Disabled	☐
3	0	0	0	0	Disabled	☐
4	0	0	0	0	Disabled	☐
5	0	0	0	0	Disabled	☐
6	0	0	0	0	Disabled	☐
7	0	0	0	0	Disabled	☐
8	0	0	0	0	Disabled	☐

The page includes the following fields:

Object	Description
Port	The port number for which the configuration below applies.
CoS	Controls the default class of service. 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 and the frame is tagged, then the frame is classified to a CoS that is based on the PCP value in the tag as shown below. Otherwise, the frame is classified to the default CoS. PCP value: 0 1 2 3 4 5 6 7 CoS value: 1 0 2 3 4 5 6 7 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 drop precedence level. All frames are classified to a drop precedence level. If the port is VLAN-aware and the frame is tagged, then the frame is classified to a DPL that is equal to the 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 to configure the mode and/or mapping.

Object	Description
	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	Select DSCP Based to enable DSCP-based QoS ingress port classification.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Queue policing

Configure the queue policer settings for all switch ports in the QoS Ingress Queue Policers page.

QoS Ingress Queue Policers

Port	Queue 0	Queue 1	Queue 2	Queue 3	Queue 4	Queue 5	Queue 6	Queue 7
	Enable	Enable	Enable	Enable	Enable	Enable	Enable	Enable
*	☐	☐	☐	☐	☐	☐	☐	☐
1	☐	☐	☐	☐	☐	☐	☐	☐
2	☐	☐	☐	☐	☐	☐	☐	☐
3	☐	☐	☐	☐	☐	☐	☐	☐
4	☐	☐	☐	☐	☐	☐	☐	☐
5	☐	☐	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	☐	☐	☐	☐	☐	☐	☐
10	☐	☐	☐	☐	☐	☐	☐	☐
11	☐	☐	☐	☐	☐	☐	☐	☐
12	☐	☐	☐	☐	☐	☐	☐	☐
13	☐	☐	☐	☐	☐	☐	☐	☐
14	☐	☐	☐	☐	☐	☐	☐	☐
15	☐	☐	☐	☐	☐	☐	☐	☐
16	☐	☐	☐	☐	☐	☐	☐	☐
17	☐	☐	☐	☐	☐	☐	☐	☐
18	☐	☐	☐	☐	☐	☐	☐	☐
19	☐	☐	☐	☐	☐	☐	☐	☐
20	☐	☐	☐	☐	☐	☐	☐	☐
21	☐	☐	☐	☐	☐	☐	☐	☐
22	☐	☐	☐	☐	☐	☐	☐	☐
23	☐	☐	☐	☐	☐	☐	☐	☐
24	☐	☐	☐	☐	☐	☐	☐	☐
25	☐	☐	☐	☐	☐	☐	☐	☐
26	☐	☐	☐	☐	☐	☐	☐	☐
27	☐	☐	☐	☐	☐	☐	☐	☐
28	☐	☐	☐	☐	☐	☐	☐	☐

The page includes the following fields:

Object	Description
Port	The port number for which the configuration below applies.
Enable (E)	Enable or disable the queue policer for this switch port.
Rate	Controls the rate for the queue policer. This value is restricted to 25-13128147 when "Unit" is kbps, and 1-13128 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue policer. This field is only shown if at least one of the queue policers are enabled.
Unit	Controls the unit of measure for the queue policer rate as kbps or Mbps. This field is only shown if at least one of the queue policers are enabled.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Port scheduler

The QoS Egress Port Schedulers page provides an overview of the QoS egress port schedulers for all switch ports.

QoS Egress Port Schedulers										
Port	Mode	Weight								
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	
<u>1</u>	Strict Priority	-	-	-	-	-	-	-	-	-
<u>2</u>	Strict Priority	-	-	-	-	-	-	-	-	-
<u>3</u>	Strict Priority	-	-	-	-	-	-	-	-	-
<u>4</u>	Strict Priority	-	-	-	-	-	-	-	-	-
<u>5</u>	Strict Priority	-	-	-	-	-	-	-	-	-
<u>6</u>	Strict Priority	-	-	-	-	-	-	-	-	-
<u>7</u>	Strict Priority	-	-	-	-	-	-	-	-	-
<u>8</u>	Strict Priority	-	-	-	-	-	-	-	-	-

The page includes the following fields:

Object	Description
Port	The logical port for the settings contained in the same row. Click on the port number to configure the schedulers. For more details, refer to "Understanding QoS" on page 169.
Mode	Shows the scheduling mode for this port.
Q0 ~ Q7	Shows the weight for this queue and port.

Port shaping

The QoS Egress Port Shapers page provides an overview of the QoS egress port shapers for all switch ports.

QoS Egress Port Shapers									
Port	Shapers								Port
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	
1	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
9	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled

The page includes the following fields:

Object	Description
Port	The logical port for the settings contained in the same row. Click on the port number to configure the shapers. For more details, refer to "Understanding QoS" on page 169.
Q0 ~Q7	Shows "disabled" or actual queue shaper rate (e.g., "800 Mbps").
Port	Shows "disabled" or actual port shaper rate (e.g., "800 Mbps").

QoS egress port schedule and shapers

The port scheduler and shapers for a specific port are configured on the QoS Egress Port Schedule and Shapers page.

Port 1

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode Strict Priority

Queue Shaper			
Enable	Rate	Unit	Excess
☐	500	kbps	☐
☐	500	kbps	☐
☐	500	kbps	☐
☐	500	kbps	☐
☐	500	kbps	☐
☐	500	kbps	☐
☐	500	kbps	☐
☐	500	kbps	☐
☐	500	kbps	☐

q0

S

q1

S

q2

S

q3

S

q4

S

q5

S

q6

S

q7

S

STRICT

S

☐

500

kbps

Port Shaper		
Enable	Rate	Unit
☐	500	kbps

Apply Reset Cancel

The page includes the following fields:

Object	Description
Scheduler Mode	Controls whether the scheduler mode is Strict Priority or 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. The default value is 500 . This value is restricted to 100-1000000 when the Unit is kbps , and it is restricted to 1-13200 when the Unit is Mbps .
Queue Shaper Unit	Controls the unit of measure for the queue shaper rate as kbps or Mbps . The default value is kbps .
Queue Shaper Excess	Controls whether the queue is allowed to use excess bandwidth.
Queue Scheduler Weight	Controls the weight for this queue. The default value is 17 . This value is restricted to 1-100 . This parameter only appears if Scheduler Mode is set to Weighted .
Queue Scheduler Percent	Shows the weight in percent for this queue. This parameter only appears 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. The default value is 500 . This value is restricted to 100-1000000 when the Unit is kbps , and it is restricted to 1-13200 when the Unit is Mbps .
Port Shaper Unit	Controls the unit of measure for the port shaper rate as kbps or Mbps . The default value is kbps .

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Click **Cancel** to undo any changes made locally and return to the previous page.

Port tag remarking

The QoS Egress Port Tag Remarking page provides an overview of QoS egress port tag remarking for all switch ports.

QoS Egress Port Tag Remarking	
Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified

The page includes the following fields:

Object	Description
Port	The logical port for the settings contained in the same row. Click on the port number to configure tag remarking. For further details, refer to “QoS egress port tag remarking” below.
Mode	Shows the tag remarking mode for this port. Classified: Use classified PCP/DEI values Default: Use default PCP/DEI values. Mapped: Use mapped versions of QoS class and DP level.

QoS egress port tag remarking

The QoS Egress Port Tag Remarking page can also provide an overview of QoS egress port tag remarking for a specific port.

Port 1 ▼

QoS Egress Port Tag Remarking Port 1

Tag Remarking Mode

Classified ▼

Apply

Reset

Cancel

The page includes the following fields:

Object	Description
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 QoS class and DP level.
PCP/DEI Configuration	Controls the default PCP and DEI values used when the mode is set to Default .
(QoS class, DP level) to (PCP, DEI) Mapping	Controls the mapping of the classified (QoS class, DP level) to (PCP, DEI) values when the mode is set to Mapped .

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Port DSCP

The QoS Port DSCP Configuration page permits configuration of the basic QoS port DSCP settings for all switch ports.

QoS Port DSCP Configuration				
Port	Ingress		Egress	
	Translate	Classify	Rewrite	
*	☐	<All> ▼	<All>	▼
1	☐	Disable ▼	Disable	▼
2	☐	Disable ▼	Disable	▼
3	☐	Disable ▼	Disable	▼
4	☐	Disable ▼	Disable	▼
5	☐	Disable ▼	Disable	▼
6	☐	Disable ▼	Disable	▼
7	☐	Disable ▼	Disable	▼
8	☐	Disable ▼	Disable	▼

The page includes the following fields:

Object	Description
Port	The Port column shows the list of ports for which DSCP ingress and egress settings can be configured.
Ingress	Change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: Translate Classify
Translate	Select the Translate check box to enable the Ingress translation.
Classify	Selections are as follows: Disable : No Ingress DSCP Classification. DSCP=0 : Classify if incoming (or translated if enabled) DSCP is 0. Selected : Classify only the selected DSCP for which classification is enabled as specified in the DSCP Translation window for the specific DSCP. All : Classify all DSCP.
Egress	Selections for Rewrite are as follows: Disable : No egress rewrite. Enable : Rewrite enabled without remapping. Remap DP Unaware : DSCP from the analyzer is remapped and the frame is remarked with the remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table. Remap DP Aware : DSCP from the analyzer is remapped and the frame is remarked with the 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

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

DSCP-based QoS

The QoS DSCP-Based QoS Ingress Classification page permits configuration of the basic QoS DSCP-based QoS ingress classification settings for all switches.

DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*	☐	<All>	<All>
0 (BE)	☐	0	0
1	☐	0	0
2	☐	0	0
3	☐	0	0
4	☐	0	0
5	☐	0	0
6	☐	0	0
7	☐	0	0
8 (CS1)	☐	0	0
9	☐	0	0
...			
57			
58	☐	0	0
59	☐	0	0
60	☐	0	0
61	☐	0	0
62	☐	0	0
63	☐	0	0

Apply

Reset

The page includes the following fields:

Object	Description
DSCP	Maximum number of supported DSCP values is 64.
Trust	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level. Frames with untrusted DSCP values are treated as a non-IP frame.
QoS Class	QoS Class values can be between 0-7.
DPL	Drop Precedence Level (0-1)

DSCP translation

The DSCP Translation page permits configuration of the basic QoS DSCP translation settings for all switches. DSCP translation can be done in Ingress or Egress.

DSCP Translation

DSCP	Ingress		Egress
	Translate	Classify	Remap
*	<All> v	☐	<All> v
0 (BE)	0 (BE) v	☐	0 (BE) v
1	1 v	☐	1 v
2	2 v	☐	2 v
3	3 v	☐	3 v
4	4 v	☐	4 v
5	5 v	☐	5 v
6	6 v	☐	6 v
7	7 v	☐	7 v
8 (CS1)	8 (CS1) v	☐	8 (CS1) v
	v	☐	9 v
55	55 v	☐	55 v
56 (CS7)	56 (CS7) v	☐	56 (CS7) v
57	57 v	☐	57 v
58	58 v	☐	58 v
59	59 v	☐	59 v
60	60 v	☐	60 v
61	61 v	☐	61 v
62	62 v	☐	62 v
63	63 v	☐	63 v

The page includes the following fields:

Object	Description
DSCP	The maximum number of supported DSCP values is 64 and valid DSCP values range from 0 to 63.
Ingress	The Ingress side of DSCP can be first translated to new DSCP before using the DSCP for the QoS class and DPL map. There are two configuration parameters for DSCP Translation: Translate Classify
Translate	DSCP at the Ingress side can be translated to any of 0-63 DSCP values.
Classify	Click Classify to enable classification at the Ingress side.

Object	Description
Egress	Contains a configurable parameter for Remap.
Remap DP	Select a DSCP value to which you want to remap from the Remap drop-down list. DSCP values range from 0 to 63.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

DSCP classification

The DSCP Classification page permits mapping a DSCP value to a QoS Class and DPL value.

QoS Class	DSCP
*	<All>
0	0 (BE)
1	0 (BE)
2	0 (BE)
3	0 (BE)
4	0 (BE)
5	0 (BE)
6	0 (BE)
7	0 (BE)

Apply Reset

The page includes the following fields:

Object	Description
QoS Class	Available QoS Class values range from 0 to 7. QoS Class (0-7) can be mapped to followed parameters.
DPL	Actual Drop Precedence Level.
DSCP	Select DSCP value (0-63) from DSCP menu to map DSCP to corresponding QoS Class and DPL value

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

QoS control list

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

QoS Control List Configuration

QCE	Port	DMAC	SMAC	Tag Type	VID	PCP	DEI	Frame Type	Action		
									CoS	DPL	DSCP

+

The page includes the following fields:

Object	Description
QCE#	Indicates the index of QCE.
Port	Indicates the list of ports configured with the QCE.
DMAC	Specify the type of Destination MAC addresses for incoming frames. Selections include: Any : All types of Destination MAC addresses are allowed. Default value. Unicast : Only Unicast MAC addresses are allowed. Multicast : Only Multicast MAC addresses are allowed. Broadcast : Only Broadcast MAC addresses are allowed.
SMAC	Displays the OUI field of Source MAC address (i.e., the first three octets (in bytes) of the MAC address).
Tag Type	Indicates tag type. Selections include: Any : Match tagged and untagged frames. Default value. Untagged : Match untagged frames. Tagged : Match tagged frames.
VID	Indicates VLAN ID (either a specific VID or range of VIDs). VID can be in the range of 1-4095 or Any .
PCP	Priority Code Point: Valid PCP values are specific (0, 1, 2, 3, 4, 5, 6, 7), a range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7), or Any .
DEI	Drop Eligible Indicator: Selections include 0 , 1 , or Any .
Frame Type	Indicates the type of frame to look for incoming frames. Selections include: Any : The QCE will match all frame types. Ethernet : Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. LLC : Only (LLC) frames are allowed. SNAP : Only (SNAP) frames are allowed. IPv4 : The QCE only matches IPV4 frames. IPv6 : The QCE only matches IPV6 frames.
Action	Indicates the classification action taken on the ingress frame if the parameters configured match with the frame's content. Action fields include:

Object	Description
	Class: Classified QoS class. DPL: Classified Drop Precedence Level. DSCP: Classified DSCP value.
Modification Buttons	Modify each QCE 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 list of QCL.

QoS control entry configuration

The QCE Configuration page appears as follows:

QCE Configuration

Port Members																											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Key Parameters

DMAC	Any
SMAC	Any
Tag	Any
VID	Any
PCP	Any
DEI	Any
Frame Type	Any

Action Parameters

CoS	0
DPL	Default
DSCP	Default

Apply
Reset
Cancel

The page includes the following fields:

Object	Description
Port Members	Select the Port Members check boxes to make any port a member of the QCL entry. All ports are selected by default.
Key Parameters	Key configuration selections are as follows: DMAC Type – Destination MAC type: possible values are unicast (UC), multicast (MC), broadcast (BC) or Any. SMAC – Source MAC address: 24 MS bits (OUI) or Any. Tag – Value of Tag field can be Any, Untag, or Tag. VID – Valid value of 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 PCP – Priority Code Point: Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or a range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or Any. DEI – Drop Eligible Indicator: Selections include 0, 1, or Any. Frame Type – Frame Type can have any of the following values: Any, Ethernet, LLC, SNAP, IPv4, or IPv6. Note: These frame types are described below.
Any	Allow all types of frames.
EtherType	Ethernet Type –Ethernet types can have values of 0x600-0xFFFF or Any . Excluding 0x800(IPv4) and 0x86DD(IPv6), the default value is Any .
LLC	SSAP Address – SSAP (Source Service Access Point) selections are 0x00 to 0xFF or Any (default value). DSAP Address – DSAP (Destination Service Access Point) selections are 0x00 to 0xFF or Any (default value). Control Address – Control Address selections are 0x00 to 0xFF or Any (default value).
SNAP	PID – PID(a.k.a., Ethernet type) elections are 0x00 to 0xFFFF or Any (default value).
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 the Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero. DSCP – Diffserv Code Point value (DSCP): It can be a specific value, range of values, or Any. DSCP values are in the range of 0-63 including BE, CS1-CS7, EF or AF11-AF43. IP Fragment – IPv4 frame fragmented option: yes, no, any. 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 – IPv6 source address: (a.b.c.d) or Any, 32 LS bits. 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.

Object	Description
	Dport – Destination TCP/UDP port:(0-65535) or Any , specific or port range applicable for IP protocol UDP/TCP.
Action Parameters	Class – QoS class: (0-7) or Default . DPL – Drop Precedence Level selections include (0-3) or Default . DSCP – DSCP selections include (0-63, BE, CS1-CS7, EF or AF11-AF43) or Default . Default indicates that the default classified value is not modified by this QCE.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Click **Cancel** to return to the previous page without saving the configuration change.

QCL status

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

Combined ▼
Auto-refresh ☐
Resolve Conflict
Refresh

QoS Control List Status

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

The page includes the following fields:

Object	Description
User	Indicates the QCL user.
QCE#	Indicates the index of QCE.
Port	Indicates the list of ports configured with the QCE.
Frame Type	Indicates the type of frame to look for incoming frames. Possible frame types are: Any : The QCE will match all frame types. Ethernet : Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. LLC : Only (LLC) frames are allowed. SNAP : Only (SNAP) frames are allowed. IPv4 : The QCE will match only IPV4 frames.

Object	Description
	IPv6: The QCE will match only IPV6 frames.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Action fields are as follows: Class: Classified QoS class. If a frame matches the QCE it will be put in the queue. DPL: Drop Precedence Level. If a frame matches the QCE then the DP level will be set to the value shown under the DPL column. DSCP: If a frame matches the QCE then DSCP will be classified with the value shown under DSCP column.
Conflict	Displays the conflict status of QCL entries when hardware resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in which case it shows conflict status as Yes, otherwise it is always No. Conflict can be resolved by releasing the hardware resources required to add the QCL entry by clicking the Resolve Conflict button.

Buttons

- Select the QCL status from the **Combined** drop-down list.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Resolve Conflict** to release the resources required to add the QCL entry when the conflict status for any QCL entry is **Yes**.
- Click **Refresh** to refresh the page.

Storm control configuration

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

The configuration indicates the permitted packet rate for unicast, multicast, or broadcast traffic across the switch.

QoS Port Storm Control

Port	Unicast Frames			Broadcast Frames			Unknown Frames		
	Enabled	Rate	Unit	Enabled	Rate	Unit	Enabled	Rate	Unit
*	☐	500	<All> ▾	☐	500	<All> ▾	☐	500	<All> ▾
1	☐	500	kbps ▾	☐	500	kbps ▾	☐	500	kbps ▾
2	☐	500	kbps ▾	☐	500	kbps ▾	☐	500	kbps ▾
3	☐	500	kbps ▾	☐	500	kbps ▾	☐	500	kbps ▾
4	☐	500	kbps ▾	☐	500	kbps ▾	☐	500	kbps ▾
5	☐	500	kbps ▾	☐	500	kbps ▾	☐	500	kbps ▾
6	☐	500	kbps ▾	☐	500	kbps ▾	☐	500	kbps ▾
7	☐	500	kbps ▾	☐	500	kbps ▾	☐	500	kbps ▾
8	☐	500	kbps ▾	☐	500	kbps ▾	☐	500	kbps ▾

The page includes the following fields:

Object	Description
Port	The port number for which the configuration below applies.
Enable	Enable storm control on this switch port.
Rate	Controls the rate for the storm control. The default value is 500 . This value is restricted to 100-1000000 when the Unit is kbps or fps , and it is restricted to 1-13200 when the Unit is Mbps or kfps .
Unit	Controls the unit of measure for the storm control rate as kbps , Mbps , fps or kfps . The default value is kbps .

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

QoS statistics

The Queuing Counters page provides statistics for the different queues for all switch ports.

Queuing Counters																
Auto-refresh ☐ Refresh Clear																
Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

The page includes the following fields:

Object	Description
Port	The logical port for the settings contained in the same row.
Q0 ~ Q7	There are eight QoS queues per port. Q0 is the lowest priority queue.
Rx/Tx	The number of received and transmitted packets per queue.

Buttons

- Click **Refresh** to refresh the page.
- Click **Clear** to clear the counters for all ports.
- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.

Voice VLAN configuration

The Voice VLAN Configuration page contains the Voice VLAN feature. This enables voice traffic forwarding on the Voice VLAN, permitting the switch to classify and schedule network traffic. We recommended that there be two VLANs on a port – one for voice and one for data.

Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

Voice VLAN Configuration

Mode	Disabled ▾	
VLAN ID	1000	
Aging Time	86400	seconds
Traffic Class	7 (High) ▾	

Port Configuration

Port	Mode	Security	Discovery Protocol
*	<All> ▾	<All> ▾	<All> ▾
1	Disabled ▾	Disabled ▾	OUI ▾
2	Disabled ▾	Disabled ▾	OUI ▾
3	Disabled ▾	Disabled ▾	OUI ▾
4	Disabled ▾	Disabled ▾	OUI ▾
5	Disabled ▾	Disabled ▾	OUI ▾
6	Disabled ▾	Disabled ▾	OUI ▾
7	Disabled ▾	Disabled ▾	OUI ▾
8	Disabled ▾	Disabled ▾	OUI ▾

The page includes the following fields:

Object	Description
Mode	Indicates the Voice VLAN mode operation. The MSTP feature must be disabled before enabling Voice VLAN. This helps avoid an ingress filter conflict. Selections include: Enabled: Enable Voice VLAN mode operation. Disabled: Disable Voice VLAN mode operation.
VLAN ID	Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. A configuration conflict occurs if the value equals management VID, MVR VID, PVID, etc. The permitted range is 1 to 4095.
Aging Time	Indicates the Voice VLAN secure learning age time. The permitted range is 10 to 10000000 seconds. It is used when the security mode or auto detect mode is enabled. In other cases, it is based on hardware age time. The actual age time is situated in the [age_time; 2 * age_time] interval.
Traffic Class	Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN applies to this class.
Mode	Indicates the Voice VLAN port mode. Selections include: Disabled: Disjoin from Voice VLAN. Auto: Enable auto detect mode. It detects if there is a VoIP phone attached to the specific port and configures the Voice VLAN members automatically. Forced: Force join to Voice VLAN.
Port Security	Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephone MAC address in Voice VLAN are blocked 10 seconds.

Object	Description
	Selections include: Enabled: Enable Voice VLAN security mode operation. Disabled: Disable Voice VLAN security mode operation.
Port Discovery Protocol	Indicates the Voice VLAN port discovery protocol. It only works when auto detect mode is enabled. Enable the LLDP feature before configuring the discovery protocol to LLDP or Both. Changing the discovery protocol to OUI or LLDP restarts the auto detect process. Selections include: OUI: Detect telephony device by OUI address. LLDP: Detect telephony device by LLDP. Both: Both OUI and LLDP.

Voice VLAN OUI table

Configure Voice VLAN OUI table on the Voice VLAN OUI Table page. The maximum entry number is 16. Modifying the OUI table restarts auto detection of the OUI process.

Voice VLAN OUI Table

Delete	Telephony OUI	Description
☐	00-30-4f	PLANET phones
☐	00-03-6b	Cisco phones
☐	00-0f-e2	H3C phones
☐	00-60-b9	Philips and NEC AG phones
☐	00-d0-1e	Pingtel phones
☐	00-e0-75	Polycom phones
☐	00-e0-bb	3Com phones
☐	00-01-e3	Siemens AG phones

The page includes the following fields:

Object	Description
Delete	Select the check boxes to delete the entry. Entries are deleted during the next save.
Telephony OUI	An telephony OUI address is a globally unique identifier assigned to a vendor by IEEE. It must be six characters long and the input format is "xx-xx-xx" (x is a hexadecimal digit).
Description	The description of the OUI address. Normally, it describes the vendor telephony device it belongs to. The allowed string length is 0 to 32.

Buttons

- Click **Add New Entry** to add a new access management entry.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Access Control Lists (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 if there are specific traffic object access rights.

ACL implementations can be quite complex (as when the ACEs are prioritized for various 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.

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 applications.

ACL status

The Voice VLAN OUI Table page shows the ACL status by different ACL users. Each row describes the ACE that is defined. A conflict occurs if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 on each switch.

ACL Status									
User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	CPU	CPU Once	Counter	Conflict
DHCP	All	IPv4/UDP 67 DHCP Client	Deny	Disabled	Disabled	Yes	No	0	No
DHCP	All	IPv4/UDP 68 DHCP Server	Deny	Disabled	Disabled	Yes	No	0	No
Combined ▼ Auto-refresh ☐ Refresh									

The page includes the following fields:

Object	Description
User	Indicates the ACL user.
Ingress Port	Indicates the ingress port of the ACE. Values include:

Object	Description
	All: The ACE matches all ingress ports. Port: The ACE matches a specific ingress port.
Frame Type	Indicates the frame type of the ACE. Values are: Any: The ACE matches any frame type. EType: The ACE matches Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ARP: The ACE matches ARP/RARP frames. IPv4: The ACE matches all IPv4 frames. IPv4/ICMP: The ACE matches IPv4 frames with ICMP protocol. IPv4/UDP: The ACE matches IPv4 frames with UDP protocol. IPv4/TCP: The ACE matches IPv4 frames with TCP protocol. IPv4/Other: The ACE matches IPv4 frames, which are not ICMP/UDP/TCP. IPv6: The ACE matches all IPv6 standard frames.
Action	Indicates the forwarding action of the ACE. Permit: Frames matching the ACE may be forwarded and learned. Deny: Frames matching the ACE are dropped.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is shown, the rate limiter operation is disabled.
Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is shown, the port redirect operation is disabled.
Mirror	Specify the mirror operation of this port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is Disabled .
CPU	Forward packet that matched the specific ACE to CPU.
CPU Once	Forward first packet that matched the specific ACE to CPU.
Counter	The counter indicates the number of times the ACE was hit by a frame.
Conflict	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page.

ACL configuration

The 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 512 on each switch.

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

Access Control List Configuration

Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Counter	+

Auto-refresh ☐
Refresh
Clear
Remove All

The page includes the following fields:

Object	Description
Ingress Port	Indicates the ingress port of the ACE. Possible values are: All : The ACE matches all ingress port. Port : The ACE matches a specific ingress port.
Policy / Bitmask	Indicates the policy number and bitmask of the ACE.
Frame Type	Indicates the frame type of the ACE. Possible values are: Any : The ACE matches any frame type. EType : The ACE matches Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ARP : The ACE matches ARP/RARP frames. IPv4 : The ACE matches all IPv4 frames. IPv4/ICMP : The ACE matches IPv4 frames with ICMP protocol. IPv4/UDP : The ACE matches IPv4 frames with UDP protocol. IPv4/TCP : The ACE matches IPv4 frames with TCP protocol. IPv4/Other : The ACE matches IPv4 frames, which are not ICMP/UDP/TCP. IPv6 : The ACE matches all IPv6 standard frames.
Action	Indicates the forwarding action of the ACE. Permit : Frames matching the ACE may be forwarded and learned. Deny : Frames matching the ACE are dropped.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is shown, the rate limiter operation is disabled.
Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is shown, the port redirect operation is disabled.
Counter	The counter indicates the number of times the ACE was hit by a frame.
Modification Buttons	Modify each ACE (Access Control Entry) in the table using the following buttons: +: Inserts a new ACE before the current row. e: Edits the ACE row. ↑: Moves the ACE up the list. ↓: Moves the ACE down the list. x: Deletes the ACE. +: The lowest plus sign adds a new entry at the bottom of the ACE listings.

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page.
- Click **Clear** to clear the counters.
- Click **Remove All** to remove all ACEs.

ACE configuration

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

ACE Configuration

Ingress Port	All
Policy Filter	Any
Frame Type	Any

Action	Permit
Rate Limiter	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

MAC Parameters

DMAC Filter	Any
-------------	-----

VLAN Parameters

VLAN ID Filter	Any
Tag Priority	Any

Apply Reset Cancel

The page includes the following fields:

Object	Description
Ingress Port	Select the ingress port for which this ACE applies. Any: The ACE applies to any port. Port n: The ACE applies to this port number, where n is the number of the switch port.
Policy Filter	Specify the policy number filter for this ACE. Any: No policy filter is specified (policy filter status is "don't-care"). Specific: If you want to filter a specific policy with this ACE, choose this value. Two fields for entering a policy value and bitmask appear.
Policy Value	When Specific is selected for the policy filter, you can enter a specific policy

Object	Description
	value. The permitted range is 0 to 255 .
Policy Bitmask	When Specific is selected for the policy filter, you can enter a specific policy bitmask. The permitted range is 0x0 to 0xff .
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). ARP : Only ARP frames can match this ACE. Note that the ARP frames won't match the ACE with Ethernet type. IPv4 : Only IPv4 frames can match this ACE. Note that the IPv4 frames won't match the ACE with Ethernet type. IPv6 : Only IPv6 frames can match this ACE. Note that 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.
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 allowed range is the same as the switch port number range. Disabled indicates that the port redirect operation is disabled.
Logging	Specify the logging operation of the ACE. The allowed values are: Enabled : Frames matching the ACE are stored in the System Log. Disabled : Frames matching the ACE are not logged. Note : The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.
Shutdown	Specify the port shut down operation of the ACE. The allowed values are: Enabled : If a frame matches the ACE, the ingress port will be disabled. Disabled : Port shut down is disabled for the ACE. Note : The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).
Counter	The counter indicates the number of times the ACE was hit by a frame.

MAC parameters

Object	Description
SMAC Filter	<i>This is only shown when the frame type is Ethernet Type or ARP.</i> Specify the source MAC filter for this ACE. Any : No SMAC filter is specified (SMAC filter status is "don't-care"). Specific : If you want to filter a specific source MAC address with this ACE,

Object	Description
	choose this value. A field for entering an SMAC value appears.
SMAC Value	When Specific is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.
DMAC Filter	Specify the destination MAC filter for this ACE. Any: No DMAC filter is specified. (DMAC filter status is "don't-care"). MC: Frame must be multicast. BC: Frame must be broadcast. UC: Frame must be unicast. Specific: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.
DMAC Value	When Specific is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.

VLAN parameters

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

ARP parameters

Object	Description
ARP/RARP	Specify the available ARP/RARP opcode (OP) flag for this ACE. Any: No ARP/RARP OP flag is specified. (OP is "don't-care"). ARP: Frame must have ARP/RARP opcode set to ARP. RARP: Frame must have ARP/RARP opcode set to RARP. Other: Frame has unknown ARP/RARP Opcode flag.
Request/Reply	Specify the available ARP/RARP opcode (OP) flag for this ACE. Any: No ARP/RARP OP flag is specified. (OP is "don't-care"). Request: Frame must have the ARP Request or RARP Request OP flag set. Reply: Frame must have ARP Reply or RARP Reply OP flag.
Sender IP Filter	Specify the sender IP filter for this ACE. Any: No sender IP filter is specified. (Sender IP filter is "don't-care"). Host: Sender IP filter is set to Host. Specify the sender IP address in the SIP

Object	Description
	Address field that appears. Network: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.
Sender IP Address	When Host or Network is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation.
Sender IP Mask	When Network is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.
Target IP Filter	Specify the target IP filter for this specific ACE. Any: No target IP filter is specified. (Target IP filter is "don't-care"). Host: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears. Network: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.
Target IP Address	When Host or Network is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation.
Target IP Mask	When Network is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.
ARP Sender MAC Match	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. 0: ARP frames where SHA is not equal to the SMAC address. 1: ARP frames where SHA is equal to the SMAC address. Any: Any value is allowed ("don't-care").
RARP Target MAC Match	Specify whether frames can hit the action according to their target hardware address field (THA) settings. 0: RARP frames where THA is not equal to the SMAC address. 1: RARP frames where THA is equal to the SMAC address. Any: Any value is allowed ("don't-care").
IP/Ethernet Length	Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings. 0: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04). 1: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04). Any: Any value is allowed ("don't-care").
IP	Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings. 0: ARP/RARP frames where the HLD is equal to Ethernet (1). 1: ARP/RARP frames where the HLD is equal to Ethernet (1). Any: Any value is allowed ("don't-care").
Ethernet	Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings. 0: ARP/RARP frames where the PRO is equal to IP (0x800). 1: ARP/RARP frames where the PRO is equal to IP (0x800). Any: Any value is allowed ("don't-care").

IP parameters

The IP parameters can be configured when **IPv4** is selected as the Frame Type.

Object	Description
IP Protocol Filter	Specify the IP protocol filter for this ACE. Any: No IP protocol filter is specified ("don't-care"). Specific: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears. ICMP: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters appear. UDP: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. TCP: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear.
IP Protocol Value	When Specific is selected for the IP protocol value, you can enter a specific value. The allowed range is 0 to 255. A frame that hits this ACE matches this IP protocol value.
IP TTL	Specify the Time-to-Live settings for this ACE. zero: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry. non-zero: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry. Any: Any value is allowed ("don't-care").
IP Fragment	Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. No: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry. Yes: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry. Any: Any value is allowed ("don't-care").
IP Option	Specify the options flag setting for this ACE. No: IPv4 frames where the options flag is set must not be able to match this entry. Yes: IPv4 frames where the options flag is set must be able to match this entry. Any: Any value is allowed ("don't-care").
SIP Filter	Specify the source IP filter for this ACE. Any: No source IP filter is specified. (Source IP filter is "don't-care"). Host: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears. Network: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.
SIP Address	When Host or Network is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation.
SIP Mask	When Network is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
DIP Filter	Specify the destination IP filter for this ACE.

Object	Description
	Any: No destination IP filter is specified. (Destination IP filter is "don't-care"). Host: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears. Network: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.
DIP Address	When Host or Network is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation.
DIP Mask	When Network is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.

IPv6 parameters

Object	Description
Next Header Filter	Specify the IPv6 next header filter for this ACE. Any: No IPv6 next header filter is specified ("don't-care"). Specific: If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears. ICMP: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters appear. UDP: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters appear. TCP: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters appear.
Next Header Value	When Specific is selected for the IPv6 next header value, you can enter a specific value. The allowed range is 0 to 255 . A frame that hits this ACE matches this IPv6 protocol value.
SIP Filter	Specify the source IPv6 filter for this ACE. Any: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care"). Specific: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.
SIP Address	When Specific is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supports the last 32 bits for the IPv6 address.
SIP BitMask	When Specific is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supports the last 32 bits for the IPv6 address. Notice the usage of bitmask – if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFF (bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.
Hop Limit	Specify the hop limit settings for this ACE. zero: IPv6 frames with a hop limit field greater than zero must not be able to match this entry. non-zero: IPv6 frames with a hop limit field greater than zero must be able to match this entry. Any: Any value is allowed ("don't-care").

ICMP parameters

Object	Description
ICMP Type Filter	Specify the ICMP filter for this ACE. Any: No ICMP filter is specified (ICMP filter status is "don't-care"). Specific: To filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.
ICMP Type Value	When Specific is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is 0 to 255 . A frame that hits this ACE matches this ICMP value.
ICMP Code Filter	Specify the ICMP code filter for this ACE. Any: No ICMP code filter is specified (ICMP code filter status is "don't-care"). Specific: To filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.
ICMP Code Value	When Specific is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is 0 to 255 . A frame that hits this ACE matches this ICMP code value.

TCP/UDP parameters

Object	Description
TCP/UDP Source Filter	Specify the TCP/UDP source filter for this ACE. Any: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care"). Specific: To filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears. Range: To filter a specific TCP/UDP source range filter with this ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.
TCP/UDP Source No.	When Specific is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is 0 to 65535 . A frame that hits this ACE matches this TCP/UDP source value.
TCP/UDP Source Range	When Range is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is 0 to 65535 . A frame that hits this ACE matches this TCP/UDP source value.
TCP/UDP Destination Filter	Specify the TCP/UDP destination filter for this ACE. Any: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care"). Specific: To filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears. Range: To filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.
TCP/UDP Destination Number	When Specific is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is 0 to 65535 . A

Object	Description
	frame that hits this ACE matches this TCP/UDP destination value.
TCP/UDP Destination Range	When Range is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is 0 to 65535 . A frame that hits this ACE matches this TCP/UDP destination value.
TCP FIN	Specify the TCP "No more data from sender" (FIN) value for this ACE. 0: TCP frames where the FIN field is set must not be able to match this entry. 1: TCP frames where the FIN field is set must be able to match this entry. Any: Any value is allowed ("don't-care").
TCP SYN	Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. 0: TCP frames where the SYN field is set must not be able to match this entry. 1: TCP frames where the SYN field is set must be able to match this entry. Any: Any value is allowed ("don't-care").
TCP RST	Specify the TCP "Reset the connection" (RST) value for this ACE. 0: TCP frames where the RST field is set must not be able to match this entry. 1: TCP frames where the RST field is set must be able to match this entry. Any: Any value is allowed ("don't-care").
TCP PSH	Specify the TCP "Push Function" (PSH) value for this ACE. 0: TCP frames where the PSH field is set must not be able to match this entry. 1: TCP frames where the PSH field is set must be able to match this entry. Any: Any value is allowed ("don't-care").
TCP ACK	Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE. 0: TCP frames where the ACK field is set must not be able to match this entry. 1: TCP frames where the ACK field is set must be able to match this entry. Any: Any value is allowed ("don't-care").
TCP URG	Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE. 0: TCP frames where the URG field is set must not be able to match this entry. 1: TCP frames where the URG field is set must be able to match this entry. Any: Any value is allowed ("don't-care").

Ethernet type parameters

Ethernet Type parameters can be configured when **Ethernet Type** is selected as the Frame Type.

Object	Description
EtherType Filter	Specify the Ethernet type filter for this ACE. Any: No EtherType filter is specified (EtherType filter status is "don't-care"). Specific: If you want to filter a specific EtherType filter with this ACE, you

Object	Description
	can enter a specific EtherType value. A field for entering a EtherType value appears.
Ethernet Type Value	When Specific is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is 0x600 to 0xFFFF but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Click **Cancel** to return to the previous page.

ACL ports configuration

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

ACL Ports Configuration								
Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Logging	Shutdown	State	Counter
*	0	<All> ▼	<All> ▼	<All> ▼	<All> ▼	<All> ▼	<All> ▼	*
1	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
2	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
3	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
4	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
5	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
6	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
7	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0
8	0	Permit ▼	Disabled ▼	Disabled ▼	Disabled ▼	Disabled ▼	Enabled ▼	0

The page includes the following fields:

Object	Description
Port	The logical port for the settings contained in the same row.
Policy ID	Select the policy to apply to this port. The allowed values are 0 through 255 . The default value is 0 .
Action	Select 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. Selections include Disabled (default value) or the values 1 through 16 .
Port Redirect	Select which port frames are redirected on. Selections include Disabled (default value) or a specific port number and it can't be set when action is permitted.
Logging	Specify the logging operation of this port. Selections include: 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 System Log memory size and logging rate are limited.
Shutdown	Specify the port shut down operation of this port. Selections include: Enabled : If a frame is received on the port, the port will be disabled. Disabled : Port shut down is disabled. The default value is Disabled .
State	Specify the port state of this port. Selections include: 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

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Click **Refresh** to refresh the page. Any changes made locally are undone.
- Click **Clear** to clear the counters.

ACL rate limiter configuration

Configure the rate limiter for the ACL of the industrial managed switch on the ACL Rate Limiter Configuration page.

ACL Rate Limiter Configuration

Rate Limiter ID	Rate (pps)
*	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1
16	1

The page includes the following fields:

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

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Authentication

This section describes user access and management control for the industrial managed switch, including user access and management control. The following main topics are covered:

- IEEE 802.1X port-based network access control
- MAC-based authentication

- User authentication

Overview of 802.1X (port-based) authentication

In 802.1X, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible in that it allows for different authentication methods like MD5-Challenge, PEAP, and TLS. The authenticator (switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

Overview of MAC-based authentication

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

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client using static entries into the MAC table. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, therefore MAC-based authentication has nothing to do with the 802.1X standard.

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

The 802.1X and MAC-based authentication configuration consists of two sections, a system- and a port-wide.

Overview of user authentication

The industrial managed switch may be configured to authenticate users logging into the system for management access using local or remote authentication methods, such as telnet and web browser. The industrial managed switch provides secure network management access using the following options:

- Remote Authentication Dial-in User Service (RADIUS)
- Terminal Access Controller Access Control System Plus (TACACS+)
- Local user name and privilege level control

RADIUS and TACACS+ are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS-aware devices on the network. An authentication server contains a database of multiple user name / password pairs with associated privilege levels for each user that requires management access to the industrial managed switch.

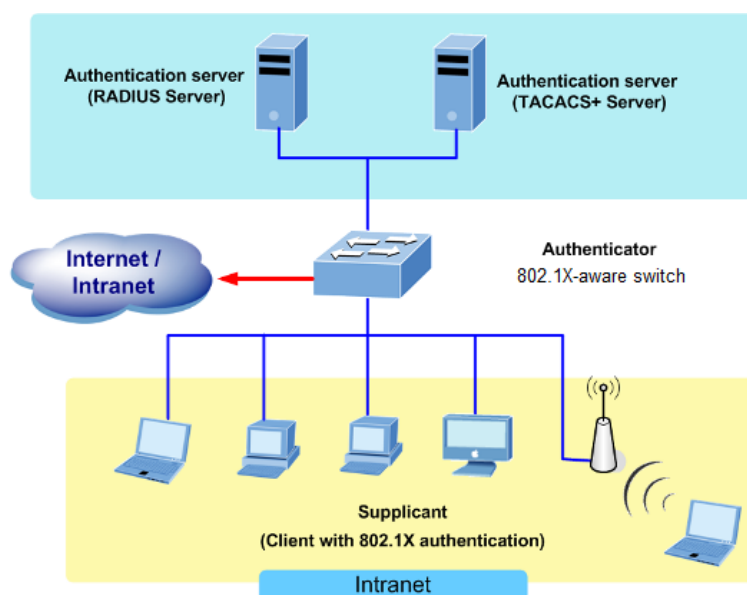
Understanding IEEE 802.1X port-based authentication

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making any services offered by the switch or the LAN available.

Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

Device roles

With 802.1X port-based authentication, the devices in the network have specific roles as shown below.



- **Client** – The device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1X-compliant client software such as that offered in the Microsoft operating systems (the client is the supplicant in the IEEE 802.1X specification).
- **Authentication server** – Performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch if the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server, which is available in the Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.
- **Switch (802.1X device)** – Controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame which is then encapsulated for Ethernet and sent to the client.

Authentication initiation and message exchange

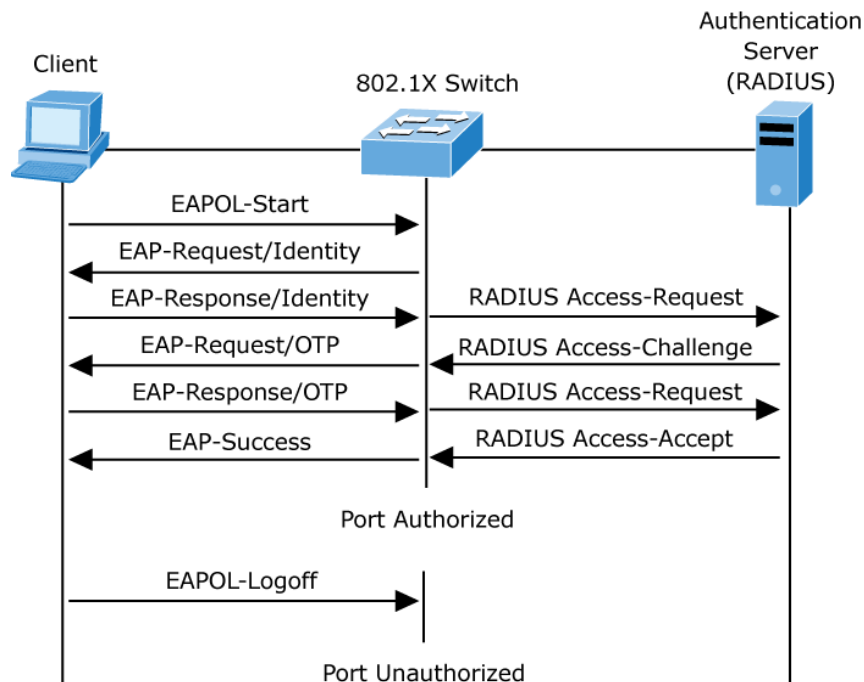
The switch or the client can initiate authentication. If you enable authentication on a port by using the `dot1x port-control auto` interface configuration command, the switch must initiate authentication when it determines that the port link state transitions from down to up. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

However, if the client does not receive an EAP-request/identity frame from the switch during bootup, the client can initiate authentication by sending an EAPOL-start frame which prompts the switch to request the client's identity.

Note: If 802.1X is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used. The diagram below shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.



Ports in authorized and unauthorized states

The switch port state determines if the client is granted access to the network. The port starts in the unauthorized state. While in this state, the port disallows all ingress and egress traffic except for 802.1X protocol packets. When a client is successfully authenticated, the port transitions to the authorized state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1X is connected to an unauthorized 802.1X port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1X-enabled client connects to a port that is not running the 802.1X protocol, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state.

If the client is successfully authenticated (receives an accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no

response is received from the server after the specified number of attempts, authentication fails and network access is not granted.

When a client logs off, it sends an EAPOL-logoff message that causes the switch port to transition to the unauthorized state.

If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

Authentication configuration

The Authentication Method Configuration page allows you to configure how a user is authenticated when logging into the switch via one of the management client interfaces.

Client	Methods		
console	local	no	no
telnet	local	no	no
ssh	local	no	no
http	local	no	no

Apply Reset

The page includes the following fields:

Object	Description
Client	The management client for which the configuration below applies.
Authentication Method	Authentication method can be set to one of the following values: None: Authentication is disabled and login is not possible. Local: Use the local user database on the switch for authentication. RADIUS: Use a remote RADIUS server for authentication. TACACS+: Use a remote TACACS+ server for authentication. Methods that involve remote servers are timed out if the remote servers are offline. In this case, the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication, we recommend configuring secondary authentication as local. This permits the management client to log in via the local user database if none of the configured authentication servers are valid.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Network access server configuration

Configure the IEEE 802.1X and MAC-based authentication system and port settings on the Network Access Server Configuration page. The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, or the back end servers, determine if the user is allowed access to the network. These back end (RADIUS) servers are configured on the "Configuration > Security > AAA" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations.

MAC-based authentication permits authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on the system. The switch uses the MAC address to authenticate against the back end server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication. The NAS configuration consists of two sections, a system- and a port-wide.

Network Access Server Configuration

System Configuration

Mode	Disabled ▼
Reauthentication Enabled	☐
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	☐
RADIUS-Assigned VLAN Enabled	☐
Guest VLAN Enabled	☐
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	☐

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
*	<All> ▼	☐	☐	☐			
1	Force Authorized ▼	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized ▼	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized ▼	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized ▼	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized ▼	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized ▼	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized ▼	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized ▼	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize

The page includes the following fields:

System configuration

Object	Description
Mode	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.
Reauthentication Enabled	If selected, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the reauthentication period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port.
Reauthentication Period	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled check box is selected. Valid values are in the range 1 to 3600 seconds.
EAPOL Timeout	Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This has no effect on MAC-based ports.
Aging Period	This setting applies to the following modes (modes using port security functionality to secure MAC addresses): Single 802.1X Multi 802.1X MAC-Based Auth. When the NAS module uses the port security module to secure MAC addresses, the port security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds. If reauthentication is enabled and the port is in a 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port are removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries. For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect if the client is still attached, and the only way to free any resources is to age the entry.
Hold Time	This setting applies to the following modes (i.e., modes using the Port Security functionality to secure MAC addresses): Single 802.1X Multi 802.1X MAC-Based Auth. If a client is denied access, either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration > Security > AAA" Page), the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the The switch will ignore new frames coming

Object	Description
	from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.
RADIUS-Assigned QoS Enabled	RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature. The RADIUS-Assigned QoS Enabled check box provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When selected, the individual ports' ditto setting determines whether RADIUS-assigned QoS Class is enabled for that port. When deselected, RADIUS-server assigned QoS Class is disabled for all ports.
RADIUS-Assigned VLAN Enabled	RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature. The RADIUS-Assigned VLAN Enabled check box provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When selected, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled for that port. When deselected, RADIUS-server assigned VLAN is disabled for all ports.
Guest VLAN Enabled	A Guest VLAN is a special VLAN, typically with limited network access, on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The Guest VLAN Enabled check box provides a quick way to globally enable/disable Guest VLAN functionality. When selected, the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When deselected, the ability to move to the Guest VLAN is disabled for all ports.
Guest VLAN ID	This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range 1 to 4095.
Max. Reauth. Count	The number of times that the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range 1 to 255.
Allow Guest VLAN if EAPOL Seen	The switch remembers if an EAPOL frame has been received on the port for the lifetime of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (default setting), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the lifetime of the port. If enabled (selected), the switch considers entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.

Port configuration

The table has one row for each port on the selected switch and a number of columns, which are:

Object	Description
Port	The port number for which the configuration below applies.
Admin State	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available: Force Authorized In this mode, the switch sends one EAPOL success frame when the port link comes up, and any client on the port will be permitted network access without authentication. Force Unauthorized In this mode, the switch sends one EAPOL failure frame when the port link comes up, and any client on the port will be disallowed network access. Port-based 802.1X In the 802.1X, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible in that it allows for different authentication methods like MD5-Challenge, PEAP, and TLS. The authenticator (switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it. When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant. Note: Suppose two back end servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). In this case, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going back end authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next back end authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate. Single 802.1X In port-based 802.1X authentication, the whole port is opened for network traffic after a supplicant is successfully authenticated on a port. This allows other clients connected to the port (through a hub, for example) to piggy-back on the successfully authenticated client and get network access even though they really aren't authenticated. To overcome this security breach,

Object	Description
	use the Single 802.1X variant. Single 802.1X is really not an IEEE standard, but features many of the same characteristics as does port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communication between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link comes up will be the first one considered. If that supplicant doesn't provide valid credentials within a certain amount of time, another supplicant will get a chance. After a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address after successful authentication. Multi 802.1X Multi 802.1X is, like Single 802.1X, not an IEEE standard but a variant that features many of the same characteristics. In Multi 802.1X, one or more supplicants can get authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the port security module. In Multi 802.1X, it is not possible to use the multicast BPDU MAC address as destination MAC address for EAPOL frames sent from the switch towards the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL request identity frames using the BPDU multicast MAC address as destination to wake up any supplicants that might be on the port. The maximum number of supplicants that can be attached to a port can be limited using the port security limit control functionality. MAC-based authentication Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string in the format "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the port security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, therefore MAC-based authentication has nothing to do with the 802.1X standard. The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g., through a third party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by

Object	Description
	anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the port security limit control functionality.
RADIUS-Assigned QoS Enabled	When RADIUS-Assigned QoS is both globally enabled and enabled (selected) for a given port, the switch reacts to QoS Class information carried in the RADIUS access-accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS access-accept packet no longer carries a QoS Class, it is invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class immediately reverts to the original QoS Class (which may be changed by the administrator in the meantime without affecting the RADIUS-assigned). This option is only available for single-client modes (i.e., Port-based 802.1X and Single 802.1X). RADIUS attributes used in identifying a QoS Class: The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an access-accept packet. Only the first occurrence of the attribute in the packet will be considered and, to be valid, it must follow this rule: All eight octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the required QoS Class in the range [0; 7].
RADIUS-Assigned VLAN Enabled	When RADIUS-Assigned VLAN is both globally enabled and enabled (selected) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID immediately reverts to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes (i.e., Port-based 802.1X and Single 802.1X). For troubleshooting VLAN assignments, use the "Monitor > VLANs > VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. RADIUS attributes used in identifying a VLAN ID: RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used: The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet. The switch looks for the first set of these attributes that have the same Tag value and fulfill the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag): Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6). Value of Tunnel-Type must be set to "VLAN" (ordinal 13). Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the

Object	Description
	range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].
Guest VLAN Enabled	When Guest VLAN is both globally enabled and enabled (selected) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes (i.e., Port-based 802.1X, Single 802.1X, and Multi 802.1X) For troubleshooting VLAN assignments, use the "Monitor > VLANs > VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. Guest VLAN Operation: When a Guest VLAN enabled port link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meantime, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port is placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port is placed in the Guest VLAN. Otherwise, it will not move to the Guest VLAN but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout. Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN. While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the Allow Guest VLAN if EAPOL Seen check box is deselected.
Port State	The current state of the port. It can undertake one of the following values: Globally Disabled: NAS is globally disabled. Link Down: NAS is globally enabled, but there is no link on the port. Authorized: The port is in force authorized or a single-supplicant mode and the supplicant is authorized. Unauthorized: The port is in force unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. X Auth/Y Unauth: The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.
Restart	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode. Clicking these buttons will not cause settings changed on the page to take effect. Reauthenticate: Schedules a reauthentication to whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication is attempted immediately. The button only has an effect for successfully authenticated clients on the port and will not cause the clients to get temporarily unauthorized.

Object	Description
	Reinitialize: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients transfer to the unauthorized state while the reauthentication is in progress.

Buttons

- Click **Refresh** to refresh the page.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Network access overview

The Network Access Overview page provides an overview of the current NAS port states for the selected switch.

Network Access Server Switch Status						
Port	Admin State	Port State	Last Source	Last ID	QoS Class	Port VLAN ID
1	Force Authorized	Globally Disabled			-	
2	Force Authorized	Globally Disabled			-	
3	Force Authorized	Globally Disabled			-	
4	Force Authorized	Globally Disabled			-	
5	Force Authorized	Globally Disabled			-	
6	Force Authorized	Globally Disabled			-	
7	Force Authorized	Globally Disabled			-	
8	Force Authorized	Globally Disabled			-	

The page includes the following fields:

Object	Description
Port	The switch port number. Click to navigate to detailed NAS statistics.
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
Last Source	The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.
Last ID	The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.
QoS Class	QoS Class assigned to the port by the RADIUS server if enabled.
Port VLAN ID	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs here. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs here.

Buttons

- Click **Refresh** to refresh the page immediately.
- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.

Network access statistics

The Network Access Statistics page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it only shows selected back end server (RADIUS Authentication Server) statistics. Use the port drop-down menu to select the port details to be displayed.

NAS Statistics Port 1

Port 1 Auto-refresh ☐

Port State

Admin State	Force Authorized
Port State	Globally Disabled

The page includes the following fields:

Port state

Object	Description
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
QoS Class	The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.
Port VLAN ID	The VLAN ID that NAS has put the port in. The field is blank if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID.

Port counters

Object	Description			
EAPOL Counters	These supplicant frame counters are available for the following administrative states: Force Authorized Force Unauthorized Port-based 802.1X Single 802.1X Multi 802.1X			
	Direction	Name	IEEE Name	Description
	Rx	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
	Rx	Response ID	dot1xAuthEapolResponseFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
	Rx	Responses	dot1xAuthEapolResponseFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
	Rx	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
	Rx	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
	Rx	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
	Rx	Invalid Length	dot1xAuthEapolLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
	Tx	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
	Tx	Request ID	dot1xAuthEapolRequestIDFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.

	Tx	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.
Back end Server Counters	These back end (RADIUS) frame counters are available for the following administrative states: Port-based 802.1X Single 802.1X Multi 802.1X MAC-based Auth.			
	Direction	Name	IEEE Name	Description
	Rx	Access Challenges	dot1xAuthBackendAccessChallenges	802.1X-based: Counts the number of times that the switch receives the first request from the back end server following the first response from the supplicant. Indicates that the back end server has communication with the switch. MAC-based: Counts all Access Challenges received from the back end server for this port (left-most table) or client (right-most table).
	Rx	Other Requests	dot1xAuthBackendOtherRequestsToSupplicant	802.1X-based: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the back end server chose an EAP-method. MAC-based: Not applicable.
	Rx	Auth. Successes	dot1xAuthBackendAuthSuccesses	802.1X- and MAC-based: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the back end server.
	Rx	Auth. Failures	dot1xAuthBackendAuthFails	802.1X- and MAC-based: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not

	authenticated to the back end server. 802.1X-based: Counts the number of times that the switch attempts to send a supplicant's first response packet to the back end server. Indicates the switch attempted communication with the back end server. Possible retransmissions are not counted. MAC-based: Counts all the back end server packets sent from the switch towards the back end server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.		
	Tx	Responses	dot1xAuthBack endResponses
Last Supplicant/Client Info	Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states: Port-based 802.1X Single 802.1X Multi 802.1X MAC-based Auth.		
	Name	IEEE Name	Description
	MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
	VLAN ID	-	The VLAN ID on which the last frame from the last supplicant/client was received.
	Version	dot1xAuthLastEapolFrameVersion	802.1X-based: The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable.
	Identity	-	802.1X-based: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. MAC-based: Not applicable.

Selected counters

Object	Description
Selected Counters	The Selected Counters table is visible when the port is one of the following administrative states: Multi 802.1X MAC-based Auth. The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.

Attached MAC address

Object	Description
Identity	Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and back end server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached. This column is not available for MAC-based Auth.
MAC Address	For Multi 802.1X, this column holds the MAC address of the attached supplicant. For MAC-based Auth., this column holds the MAC address of the attached client. Clicking the link causes the client's back end server counters to be shown in the Selected Counters table. If no clients are attached, it shows no clients attached.
VLAN ID	This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.
State	The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the back end server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.
Last Authentication	Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear the counters for the selected port. This button is available in the following modes:
 - Force Authorized
 - Force Unauthorized
 - Port-based 802.1X

- Single 802.1X
- Click **Clear All** to clear both the port counters and all of the attached client's counters. Performing this action will not clear "Last Client." This button is available in the following modes:
 - Multi 802.1X
 - MAC-based Auth.X
- Click **Clear This** to clear only the currently selected client's counter. This button is available in the following modes:
 - Multi 802.1X
 - MAC-based Auth.X

RADIUS

Configure the RADIUS servers on the RADIUS Server Configuration page.

RADIUS Server Configuration

Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key		
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
Add New Server Apply Reset						

The page includes the following fields:

Global configuration

These settings are common for all of the RADIUS Servers.

Object	Description
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.
Retransmit	Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.
Dead Time	The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
Key	The secret key – up to 63 characters long – shared between the RADIUS server and the switch.
NAS-IP-Address	The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
NAS-IPv6-Address	The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.
NAS-Identifier	The identifier – up to 253 characters long – to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.

Server configuration

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

Object	Description
Delete	To delete a RADIUS server entry, check this box. The entry will be deleted during the next save.
Hostname	The IP address or hostname of the RADIUS server.
Auth Port	The UDP port to use on the RADIUS server for authentication.
Acct Port	The UDP port to use on the RADIUS server for accounting.
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
Retransmit	This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.
Key	This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

- Click **Add New Server** to add a new RADIUS server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to five servers are supported.
- Click **Delete** to undo the addition of the new server.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

TACACS+

The TACACS+ Server Configuration page permits configuration of the TACACS+ Servers.

The page includes the following fields:

Global configuration

These settings are common for all of the TACACS+ Servers.

Object	Description
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.
Dead Time	The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
Key	The secret key – up to 63 characters long – shared between the RADIUS server and the switch.

Server configuration

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

Object	Description
Delete	To delete a TACACS+ server entry, select this check box. The entry will be deleted during the next save.
Hostname	The IP address or hostname of the TACACS+ server.
Port	The TCP port to use on the TACACS+server for authentication.
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.
Key	This optional setting overrides the global key. Leaving it blank will use the global key.

Buttons

- Click **Add New Server** to add a new TACACS+server. An empty row is added to the table, and the RADIUS server can be configured as needed. Up to five servers are supported.
- Click **Delete** to undo the addition of the new server.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

RADIUS overview

The RADIUS Authentication/Accounting Server Overview page provides an overview of the status of the RADIUS servers configurable on the authentication configuration page.

RADIUS Authentication Server Status Overview

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:0	Disabled
2	0.0.0.0:0	Disabled
3	0.0.0.0:0	Disabled
4	0.0.0.0:0	Disabled
5	0.0.0.0:0	Disabled

Auto-refresh ☐

The page includes the following fields:

RADIUS authentication/accounting server status overview

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

Buttons

- Click **Refresh** to refresh the page immediately.
- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.

RADIUS details

The RADIUS Authentication Statistics for Server overview page provides detailed statistics for a particular RADIUS server.

RADIUS Authentication Statistics for Server #1

Server #1 ▼

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

RADIUS Accounting Statistics for Server #1

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

Auto-refresh ☐
Refresh
Clear

The page includes the following fields:

RADIUS authentication statistics

The statistics map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the back end servers to show details for each.

Object	Description			
Packet Counters	RADIUS authentication server packet counter. There are seven receive and four transmit counters.			
	Direction	Name	RFC4668 Name	Description
	Rx	Access Accepts	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
	Rx	Access Rejects	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
	Rx	Access Challenges	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
	Rx	Malformed Access Responses	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
	Rx	Bad Authenticators	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
	Rx	Unknown Types	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
	Rx	Packets Dropped	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
	Tx	Access Requests	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
	Tx	Access Retransmissions	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the

Other Info

Tx	ons	sions	RADIUS authentication server.
	Pending Requests	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Tx	Timeouts	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
This section contains information about the state of the server and the latest round-trip time.			
Name	RFC4668 Name	Description	
IP Address	-	IP address and UDP port for the authentication server in question.	
State	-	Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.	
Round-Trip Time	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication	

server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there has yet to be round-trip communication with the server.

RADIUS accounting statistics

The statistics map closely to those specified in RFC4670 - RADIUS Accounting Client MIB. Use the server check box to switch between the back end servers to show details for each.

Object	Description			
Packet Counters	RADIUS accounting server packet counter. There are five receive and four transmit counters.			
	Direction	Name	RFC4670 Name	Description
	Rx	Responses	radiusAccClientExtResponses	The number of RADIUS packets (valid or invalid) received from the server.
	Rx	Malformed Responses	radiusAccClientExtMalformedResponses	The number of malformed RADIUS packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or unknown types are not included as malformed access responses.
	Rx	Bad Authenticators	radiusAcctClientExtBadAuthenticators	The number of RADIUS packets containing invalid authenticators received from the server.
	Rx	Unknown Types	radiusAccClientExtUnknownTypes	The number of RADIUS packets of unknown types that were received from the server on the accounting port.
	Rx	Packets Dropped	radiusAccClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the accounting port and dropped for some other reason.
	Tx	Requests	radiusAccClientExtRequests	The number of RADIUS packets sent to the server. This does not include retransmissions.
	Tx	Retransmissions	radiusAccClientExtRetransmissions	The number of RADIUS packets retransmitted to the RADIUS accounting server.
	Tx	Pending	radiusAccClientEx	The number of RADIUS

	Requests		tPendingRequests	packets destined for the server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a response, timeout, or retransmission.
	Tx	Timeouts	radiusAccClientExtTimeouts	The number of accounting timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a request as well as a timeout.
Other Info	This section contains information about the state of the server and the latest round-trip time.			
	Name	RFC4670 Name	Description	
	IP Address	-	IP address and UDP port for the accounting server in question.	
	State	-	Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts. Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.	
	Round-Trip Time	radiusAccClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Response and the Request that matched it from the RADIUS accounting server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there has yet to be round-trip communication with the server.	

Buttons

- Select the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

Windows platform RADIUS server configuration

Set up the RADIUS server and assign the client IP address to the industrial managed switch (in this case, the field in the default IP address of the industrial managed switch with 192.168.0.100). Ensure that the shared secret key is as same as the one you had set at the industrial managed switch's 802.1x system configuration (12345678 in this case).

1. Configure the IP Address of remote RADIUS server and secret key.

RADIUS Server Configuration

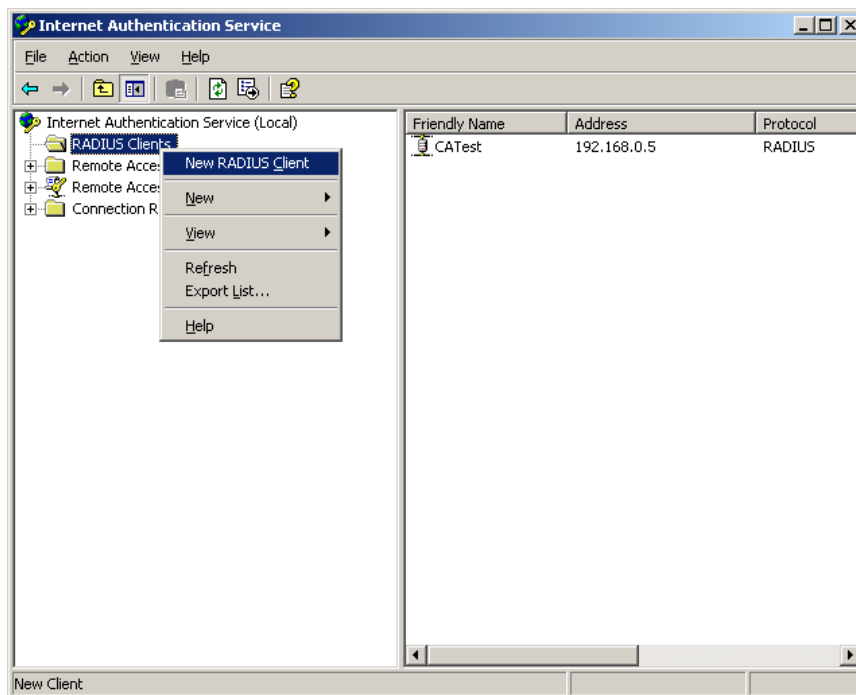
Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key		
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

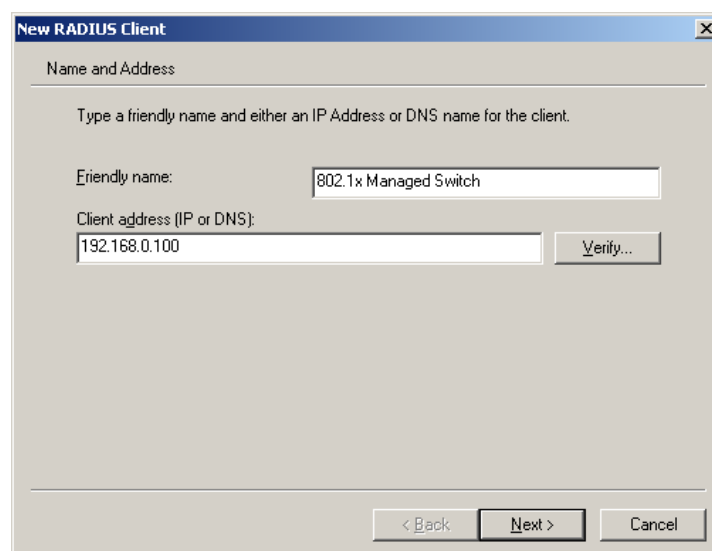
Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
☐	123	1812	1813	10	33	12345678

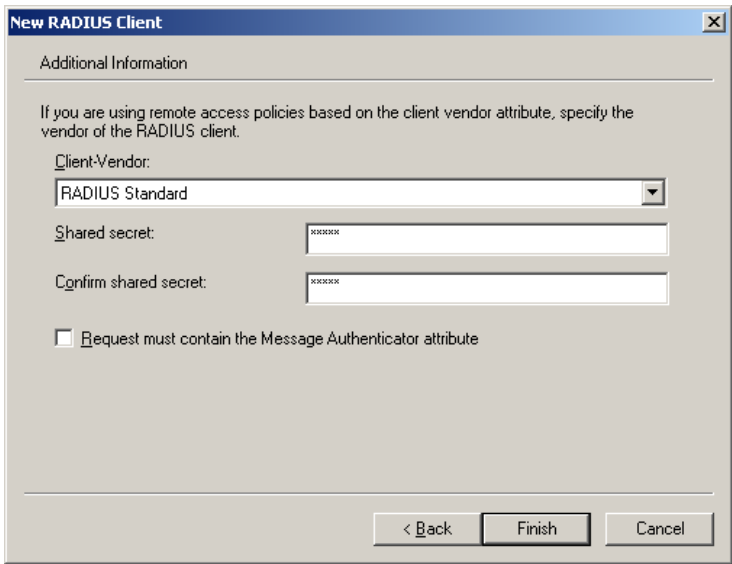
2. Click **New RADIUS Client** on the Windows 2003 server.



3. Assign the client IP address to the industrial managed switch.



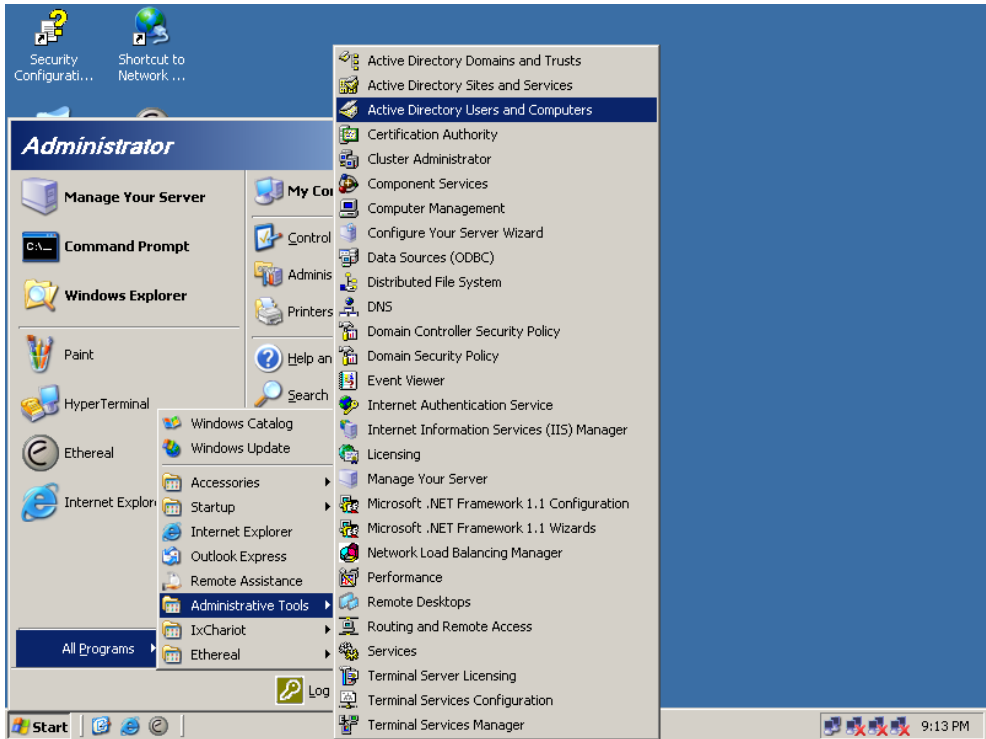
4. The shared secret key should be as same as the key configured on the industrial managed switch.



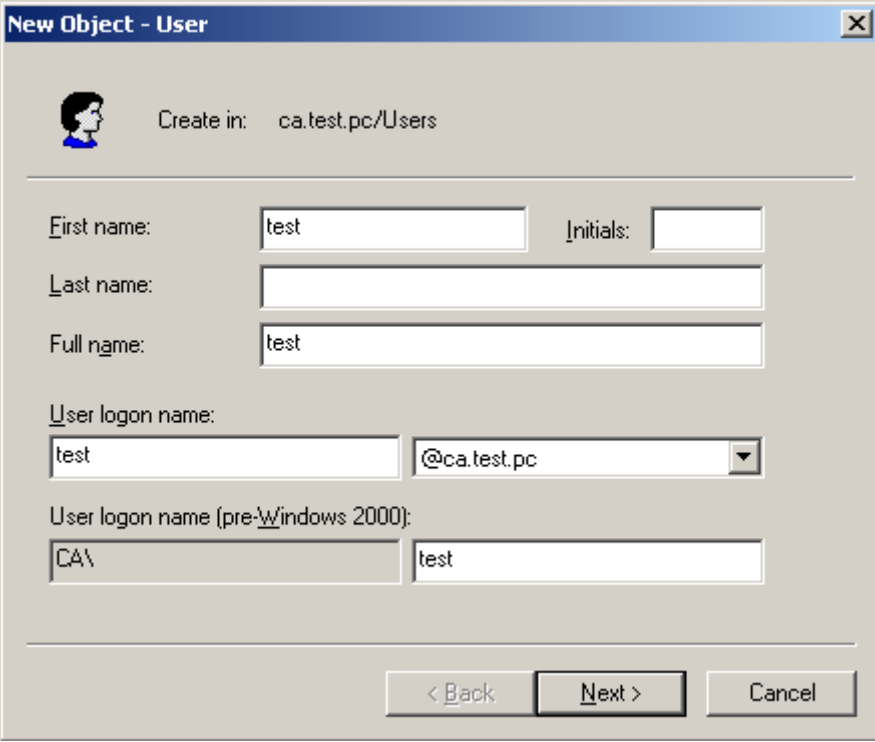
5. Configure ports attribute of 802.1X, the same as “802.1X Port Configuration.”

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
1	Port-based 802.1X	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize
2	Port-based 802.1X	☐	☐	☐	Globally Disabled	Reauthenticate	Reinitialize

6. Create user data. The establishment of the user data needs to be created on the Radius Server PC. For example, select **Active Directory Users and Computers** and create legal user data (Windows Server 2003).



7. Right-click a user that you created and then type in properties and configure settings.



New Object - User

Create in: ca.test.pc/Users

First name: test Initials:

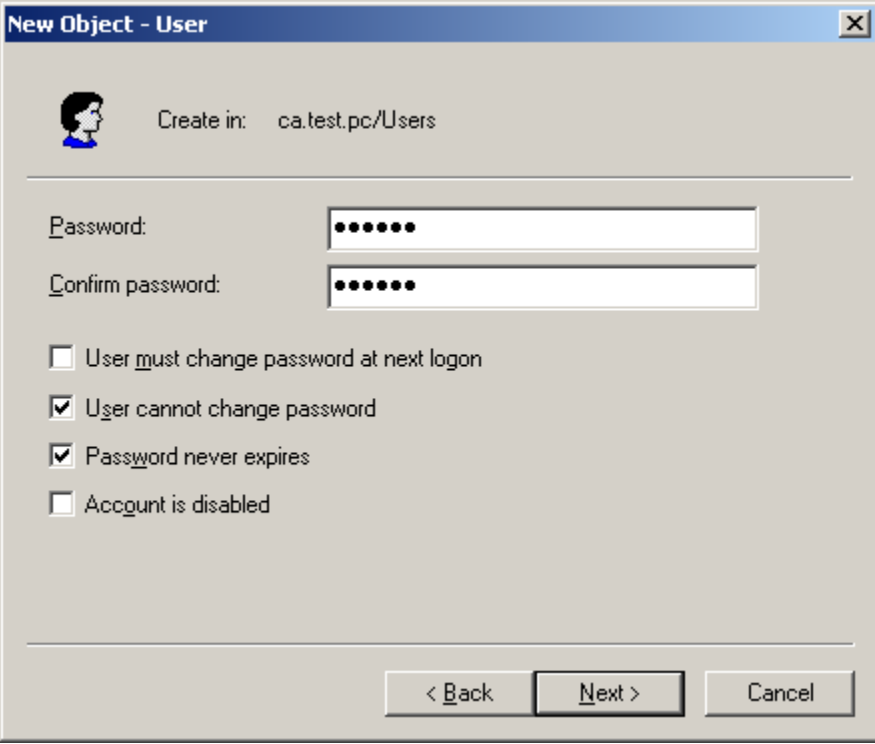
Last name:

Full name: test

User logon name: test @ca.test.pc

User logon name (pre-Windows 2000): CA\ test

< Back Next > Cancel



New Object - User

Create in: ca.test.pc/Users

Password:

Confirm password:

☐ User must change password at next logon

☒ User cannot change password

☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

Note: Set the Port Authenticate Status to “Force Authorized” if the port is connected to the RADIUS server or the port is an uplink port that is connected to another switch. Otherwise, the switch might not be able to access the RADIUS server after the 802.1X starts to work.

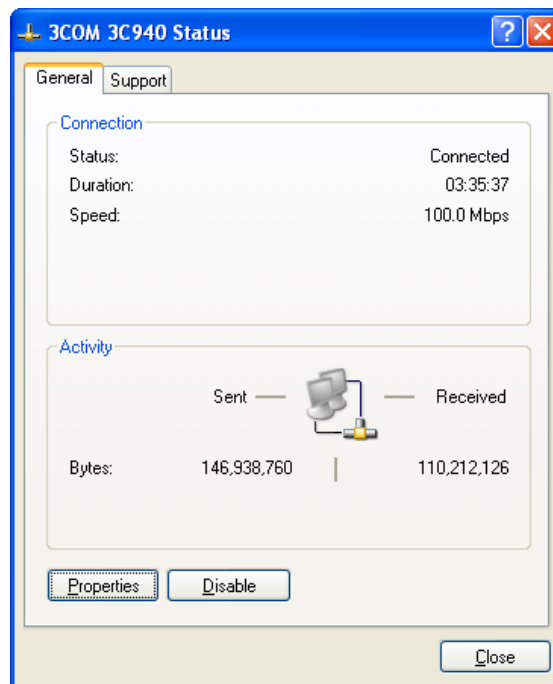
802.1X client configuration

Windows XP has native support for 802.1X. The following procedures show how to configure 802.1X Authentication in Windows XP.

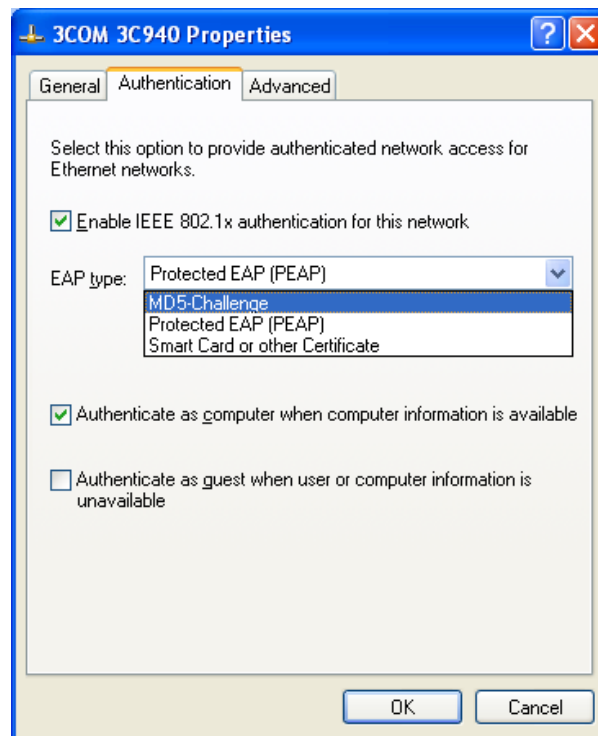
Please note that if you want to change the 802.1x authentication type of a wireless client, (i.e., switch to EAP-TLS from EAP-MD5), you must remove the current existing wireless network from your preferred connection first, and add it in again.

Configuration sample: EAP-MD5 authentication

1. Go to **Start > Control Panel**, and then double-click on **Network Connections**.
2. Right-click on the **Local Network Connection**.
3. Click **Properties** to open up the Properties setting window.



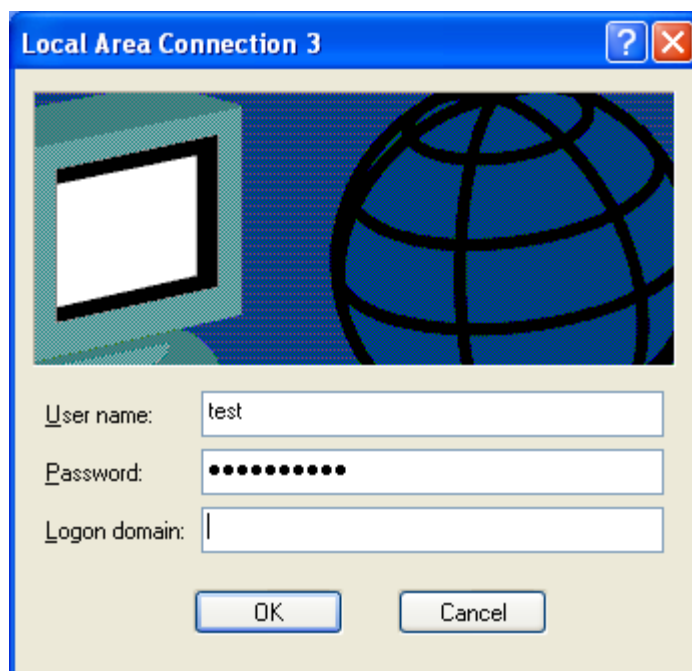
4. Click the **Authentication** tab.
5. Select **Enable network access control using IEEE 802.1X** to enable 802.1x authentication.
6. Select **MD-5 Challenge** from the drop-down list box for EAP type.



7. Click **OK**.
8. When the client has associated with the industrial managed switch, a user authentication notice appears in the system tray. Click on the notice to continue.



9. Type the user name, password and the logon domain that your account belongs to.
10. Click **OK** to complete the validation process.



Security

This section describes how to control access to the industrial managed switch, including user access and management control.

The Security page contains links to the following main topics:

- Port Limit Control
- Access Management
- HTTPs / SSH
- DHCP Snooping
- IP Source Guard
- ARP Inspection

Port limit control

The Port Limit Control Configuration page allows you to configure the port security limit control system and port settings. Limit control allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If limit control 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. The action can be one of the four different actions as described below.

The limit control module utilizes a lower-layer port security module that manages MAC addresses learned on the port. The limit control configuration consists of two sections, a system- and a port-wide.

Port Security Limit Control Configuration

System Configuration

Mode	Disabled ▼
Aging Enabled	☐
Aging Period	3600 seconds

Port Configuration

Port	Mode	Limit	Action	State	Re-open
*	<All> ▼	4	<All> ▼		
1	Disabled ▼	4	None ▼	Disabled	Reopen
2	Disabled ▼	4	None ▼	Disabled	Reopen
3	Disabled ▼	4	None ▼	Disabled	Reopen
4	Disabled ▼	4	None ▼	Disabled	Reopen
5	Disabled ▼	4	None ▼	Disabled	Reopen
6	Disabled ▼	4	None ▼	Disabled	Reopen
7	Disabled ▼	4	None ▼	Disabled	Reopen
8	Disabled ▼	4	None ▼	Disabled	Reopen

The page includes the following fields:

System configuration

Object	Description
Mode	Indicates if Limit Control is globally enabled or disabled on the switchstack. If globally disabled, other modules may still use the underlying functionality, but limit checks and corresponding actions are disabled.
Aging Enabled	If this check box is selected, secured MAC addresses are subject to aging as discussed under Aging Period.
Aging Period	If Aging Enabled is selected, then the aging period is controlled with this input. If other modules are using the underlying port security for securing MAC addresses, they may have other requirements to the aging period. The underlying port security will use the shorter requested aging period of all modules that use the functionality. The Aging Period can be set to a number between 10 and 10,000,000 seconds. To understand why aging may be required, consider the following scenario: Suppose an end-host is connected to a third party switch or hub, which in turn is connected to a port on this switch on which Limit Control is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, select Aging Enabled. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if these frames are not seen within the next aging period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.

Port configuration

The table has one row for each port on the selected switch and a number of columns, which are:

Object	Description
Port	The port number for which the configuration below applies.
Mode	Enable/disable Limit Control on this port. Both this and the Global Mode must be set to Enabled for Limit Control to be in effect. Note that other modules may still use the underlying port security features without enabling Limit Control on a given port.
Limit	The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1024. If the limit is exceeded, the corresponding action is taken. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a port security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted if the remaining ports have already used all available MAC addresses.
Action	If the limit is reached, the switch can take one of the following actions: None: Do not allow more than Limit MAC addresses on the port, but take no further action. Trap: If Limit + 1 MAC addresses are seen on the port, send an SNMP trap. If Aging is disabled, only one SNMP trap will be sent, but with Aging enabled, new SNMP traps will be sent every time the limit is exceeded. Shutdown: If Limit + 1 MAC addresses are seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port and no new addresses will be learned. Even if the link is physically disconnected and reconnected on the port (by disconnecting the cable), the port will remain shut down. There are three ways to re-open the port: 1. Boot the stack or elect a new master switch. 2. Disable and re-enable Limit Control on the port or the switch. 3. Click the Reopen button. Trap & Shutdown: If Limit + 1 MAC addresses are seen on the port, both the "Trap" and the "Shutdown" actions described above will be taken.
State	This column shows the current state of the port as seen from the Limit Control's point of view. The state takes one of four values: Disabled: Limit Control is either globally disabled or disabled on the port. Ready: The limit is not yet reached. This can be shown for all actions. Limit Reached: Indicates that the limit is reached on this port. This state can only be shown if Action is set to None or Trap. Shutdown: Indicates that the port is shut down by the Limit Control module. This state can only be shown if Action is set to Shutdown or Trap & Shutdown.
Re-open Button	If a port is shut down by this module, you may reopen it by clicking this button, which will only be enabled if this is the case. For other methods, refer to Shutdown in the Action section. Note: Clicking the reopen button causes the page to be refreshed, resulting in the loss of non-committed changes.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Click **Refresh** to refresh the page. Note that non-committed changes are lost.

Access management

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

The page includes the following fields:

Object	Description
Mode	Indicates the access management mode operation. Possible modes are: Enabled: Enable access management mode operation. Disabled: Disable access management mode operation.
Delete	Check to delete the entry. It will be deleted during the next apply .
VLAN ID	Indicates the VLAN ID for the access management entry.
Start IP address	Indicates the start IP address for the access management entry.
End IP address	Indicates the end IP address for the access management entry.
HTTP/HTTPS	Indicates the host can access the switch from the HTTP/HTTPS interface and that the host IP address matched the entry.
SNMP	Indicates the host can access the switch from the SNMP interface and that the host IP address matched the entry.
TELNET/SSH	Indicates the host can access the switch from the TELNET/SSH interface and that the host IP address matched the entry.

Buttons

- Click **Add New Entry** to add a new access management entry.
- Click **Apply** to apply changes.

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

Access management statistics

The Access Management Statistics page provides statistics for access management.

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

Auto-refresh ☐

The page includes the following fields:

Object	Description
Interface	The interface that allowed the remote host can access the switch.
Receive Packets	The received packets number from the interface under access management mode is enabled.
Allow Packets	The allowed packets number from the interface under access management mode is enabled.
Discard Packets	The discarded packets number from the interface under access management mode is enabled.

Buttons

- Click **Refresh** to refresh the page immediately.
- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Clear** to clear all statistics.

HTTPS

Configure HTTPS on the HTTPS Configuration page.

HTTPS Configuration

Mode	Enabled ▼
Automatic Redirect	Disabled ▼

The page includes the following fields:

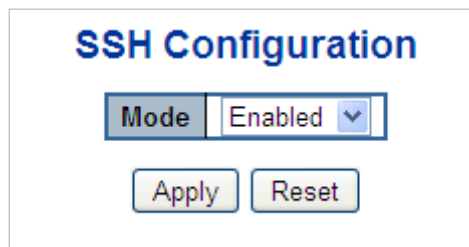
Object	Description
Mode	Indicates the HTTPS mode operation. When the current connection is HTTPS, applying the HTTPS disabled mode operation automatically redirects the web browser to an HTTP connection. Selections include: Enabled: Enable HTTPS mode operation. Disabled: Disable HTTPS mode operation.
Automatic Redirect	Indicates the HTTPS redirect mode operation. It is only significant if HTTPS mode Enabled is selected. It automatically redirects the web browser to an HTTPS connection when both HTTPS mode and Automatic Redirect are enabled or redirects web browser to an HTTP connection when both are disabled. Selections include: Enabled: Enable HTTPS redirect mode operation. Disabled: Disable HTTPS redirect mode operation.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

SSH

Configure SSH on the SSH Configuration page. This page shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other user modules. When a user module has enabled port security on a port, the port is set up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections – one with a legend of user modules and one with the actual port status.



The screenshot shows a web interface titled "SSH Configuration". Below the title is a "Mode" label followed by a dropdown menu currently showing "Enabled". Below the dropdown are two buttons: "Apply" and "Reset".

The page includes the following fields:

Object	Description
Mode	Indicates the SSH mode operation. Selections include: Enabled: Enable SSH mode operation. Disabled: Disable SSH mode operation..

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Port security status

The Port Security Status page shows the Port Security status. Port security is a module with no direct configuration. Configuration comes indirectly from other user modules. When a user module has enabled port security on a port, the port is set up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

The status page is divided into two sections – one with a legend of user modules and one with the actual port status.

Port Security Switch Status

User Module Legend

User Module Name	Abbr
Limit Control	L
802.1X	8
DHCP Snooping	D
Voice VLAN	V

Port Status

Port	Users	State	MAC Count	
			Current	Limit
1	----	Disabled	-	-
2	----	Disabled	-	-
3	----	Disabled	-	-
4	----	Disabled	-	-
5	----	Disabled	-	-
6	----	Disabled	-	-
7	----	Disabled	-	-
8	----	Disabled	-	-
9	----	Disabled	-	-
10	----	Disabled	-	-
11	----	Disabled	-	-
12	----	Disabled	-	-
13	----	Disabled	-	-
14	----	Disabled	-	-
15	----	Disabled	-	-
16	----	Disabled	-	-
17	----	Disabled	-	-
18	----	Disabled	-	-
19	----	Disabled	-	-
20	----	Disabled	-	-
21	----	Disabled	-	-
22	----	Disabled	-	-
23	----	Disabled	-	-
24	----	Disabled	-	-
25	----	Disabled	-	-
26	----	Disabled	-	-
27	----	Disabled	-	-
28	----	Disabled	-	-

Auto-refresh ☐

The page includes the following fields:

User module legend

The legend shows all user modules that may request Port Security services.

Object	Description
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 selected switch in the switch and a number of columns, which are:

Object	Description
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 if that module has enabled Port Security. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter has enabled port security.
State	Shows the current state of the port. It can take one of four values: Disabled: No user modules are currently using the Port Security service. Ready: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive. Limit Reached: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is reached and no more MAC addresses should be taken in. Shutdown: The Port Security service is enabled by at least the Limit Control user module, and that module has indicated that the limit is exceeded. No MAC addresses can be learned on the port until it is administratively re-opened on the Limit Control configuration web page.
MAC Count (Current, Limit)	The two columns indicate the number of currently learned MAC addresses (forwarding as well as blocked) 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 the Limit Control user module is not enabled on the port, the Limit column will show a dash (-).

Buttons

- Click **Refresh** to refresh the page immediately.
- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.

Port security detail

The Port Security Port Status page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other user modules. When a user module has enabled port security on a port, the port is set up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

Port Security Port Status Port 1

Port 1 ▼

MAC Address	VLAN ID	State	Time of Addition	Age/Hold
<i>No MAC addresses attached</i>				

Auto-refresh ☐ Refresh

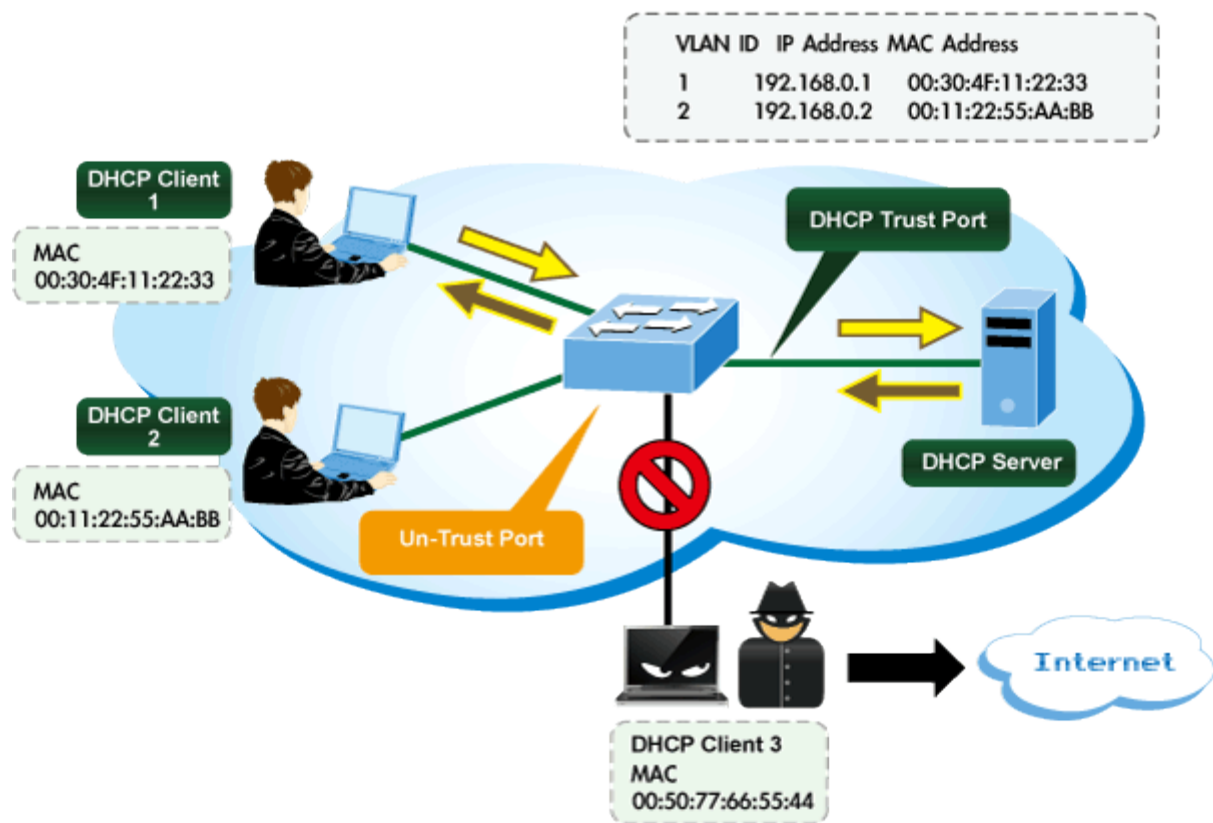
The page includes the following fields:

Object	Description
MAC Address & VLAN ID	The MAC address and VLAN ID 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 blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.
Time of Addition	Shows the date and time when this MAC address was first seen on the port.
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.

DHCP snooping

DHCP snooping is used to block intruders on the untrusted ports of DUT when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DHCP Snooping Overview



Configure DHCP Snooping on the DHCP Snooping Configuration page.

DHCP Snooping Configuration

Snooping Mode

Disabled

Port Mode Configuration

Port	Mode
*	<All>
1	Trusted
2	Trusted
3	Trusted
4	Trusted
5	Trusted
6	Trusted
7	Trusted
8	Trusted

The page includes the following fields:

Object	Description
Snooping Mode	Indicates the DHCP snooping mode operation. Possible modes are: Enabled: Enable DHCP snooping mode operation. When the DHCP snooping mode operation is enabled, the request DHCP messages will be forwarded to trusted ports and only allow reply packets from trusted ports. Disabled: Disable the DHCP snooping mode operation.
Port Mode Configuration	Indicates the DHCP snooping port mode. Possible port modes are: Trusted: Configures the port as trusted sources of the DHCP message. Untrusted: Configures the port as untrusted sources of the DHCP message.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Snooping table

The Dynamic DHCP Snooping Table page displays the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients that obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

Dynamic DHCP Snooping Table

Auto-refresh ☐
Refresh
|<<
>>

Start from MAC address

, VLAN

with

entries per page.

Buttons

- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **>>** to use the last entry of the currently displayed table as a basis for the next lookup. "No more entries" is shown in the table.
- Click **|<<** to start over.

IP source guard configuration

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. The IP Source Guard Configuration page provides IP Source Guard-related configuration data.

IP Source Guard Configuration

Mode: Disabled

[Translate Dynamic to Static](#)

Port Mode Configuration

Port	Mode	Max Dynamic Clients
*	<All>	<All>
1	Disabled	Unlimited
2	Disabled	Unlimited
3	Disabled	Unlimited
4	Disabled	Unlimited
5	Disabled	Unlimited
6	Disabled	Unlimited
7	Disabled	Unlimited
8	Disabled	Unlimited

The page includes the following fields:

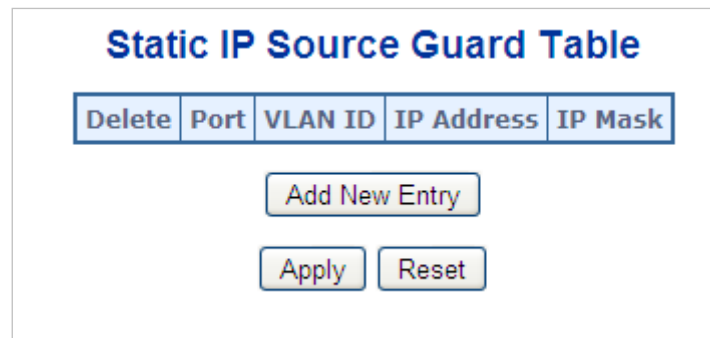
Object	Description
Mode of IP Source Guard Configuration	Enable/disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.
Port Mode Configuration	Specify on which ports IP Source Guard is enabled. Only when both Global Mode and Port Mode on a given port are enabled will IP Source Guard be enabled on this port.
Max Dynamic Clients	Specify the maximum number of dynamic clients that can be learned on given ports. This value can be 0, 1, 2, and unlimited. If the port mode is enabled and the value of max dynamic client is equal 0, it only allows the forwarding of IP packets that are matched in static entries on the specific port.

Buttons

- Click **Translate Dynamic to Static** to translate all dynamic entries to static entries.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

IP source guard static table

The Static IP Source Guard Table page appears as below:



The interface for the Static IP Source Guard Table. It features a title 'Static IP Source Guard Table' in blue. Below the title is a table with five columns: 'Delete', 'Port', 'VLAN ID', 'IP Address', and 'IP Mask'. Underneath this table is a button labeled 'Add New Entry'. At the bottom of the interface are two buttons: 'Apply' and 'Reset'.

The page includes the following fields:

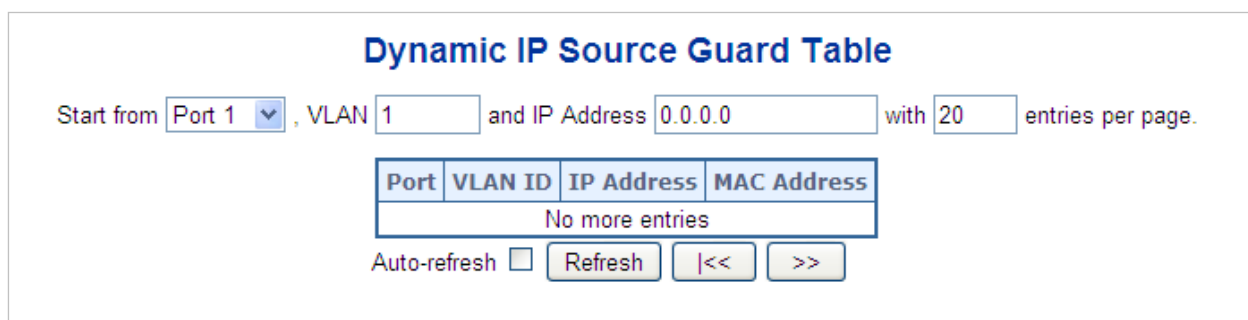
Object	Description
Delete	Select to delete the entry. It will be deleted during the next save.
Port	The logical port for the settings.
VLAN ID	The VLAN ID for the settings.
IP Address	Allowed Source IP address.
MAC Address	Allowed Source MAC address.

Buttons

- Click **Add New Entry** to add a new entry to the Static IP Source Guard table.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Dynamic IP source guard table

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by IP mask.



The interface for the Dynamic IP Source Guard Table. It features a title 'Dynamic IP Source Guard Table' in blue. Below the title is a search bar with the text 'Start from Port 1, VLAN 1 and IP Address 0.0.0.0 with 20 entries per page.' Below the search bar is a table with four columns: 'Port', 'VLAN ID', 'IP Address', and 'MAC Address'. The table contains the text 'No more entries'. Below the table are four buttons: 'Auto-refresh' (with a checkbox), 'Refresh', '<<', and '>>'.

Navigating the dynamic IP source guard table

Each page shows up to 99 entries from the Dynamic IP source guard table, selected through the "entries per page" input field (default is 20). When first visited, the web page will show the first 20 entries from the beginning of the table. The first entry

displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the table.

The **Start from** port address, **IP Address**, and **VLAN** input fields allow the user to select the starting point in the table. Clicking the **Refresh** button updates the displayed table starting from that or the closest next Dynamic IP source guard table match.

In addition, the two input fields will, after clicking the **Refresh** button, 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/IP 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 **I<<** button to start over.

The page includes the following fields:

Object	Description
Port	The port number for which the status applies. Click the port number to see the status for this particular port.
VLAN ID	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
IP Address	The IP address of the entry.

Buttons

- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the displayed table starting from the **MAC address** and **VLAN** input fields.
- Click **Clear** to flush all dynamic entries.
- Click **I<<** to update the table starting from the first entry in the MAC table (i.e., the entry with the lowest VLAN ID and MAC address).
- Click **>>** to update the table, starting with the entry after the last entry currently displayed.

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 DUT. The ARP Inspection Configuration page provides ARP Inspection related configuration.

ARP Inspection Configuration

Mode: Disabled

[Translate Dynamic to Static](#)

Port Mode Configuration

Port	Mode	Check VLAN	Log Type
*	<All>	<All>	<All>
1	Disabled	Disabled	None
2	Disabled	Disabled	None
3	Disabled	Disabled	None
4	Disabled	Disabled	None
5	Disabled	Disabled	None
6	Disabled	Disabled	None
7	Disabled	Disabled	None
8	Disabled	Disabled	None

The page includes the following fields:

Object	Description
Mode of ARP Inspection Configuration	Enable/disable the Global ARP Inspection.
Port Mode Configuration	Specify the ports on which ARP Inspection is enabled. Only when both Global Mode and Port Mode on a given port are enabled will ARP Inspection be enabled on this port. Possible modes are: Enabled: Enable ARP Inspection operation. Disabled: Disable ARP Inspection operation. To inspect the VLAN configuration, select Enabled under Check VLAN. The default setting of Check VLAN is disabled. When Check VLAN is set to Disabled, the log type of ARP Inspection refers to the port setting. When Check VLAN is set to Enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible modes are: Enabled: Enable check VLAN operation. Disabled: Disable check VLAN operation. When the Global Mode and Port Mode on a given port are set to Enabled, and Check VLAN is set to Disabled, the log type of ARP Inspection will refer to the port setting. There are four log types which are: None: Log nothing. Deny: Log denied entries. Permit: Log permitted entries. ALL: Log all entries.

Buttons

- Click **Translate Dynamic to Static** to translate all dynamic entries to static entries.
- Click **Apply** to apply changes.

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

ARP inspection static table

The Static ARP Inspection Table page provides Static ARP Inspection data.

The page includes the following fields:

Object	Description
Delete	Select 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

- Click **Add New Entry** to add a new entry to the Static ARP inspection table.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Dynamic ARP inspection table

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 1024 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address.

Navigating the ARP inspection table

Each page shows up to 99 entries from the Dynamic ARP inspection table, selected through the "entries per page" input field (default is 20). When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP inspection table. The first entry displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the table.

The **Start from** port address, **MAC Address**, **IP Address** and **VLAN** input fields allow the user to select the starting point in the table. Clicking the **Refresh** button updates the displayed table starting from that or the closest next Dynamic ARP inspection match.

In addition, the two input fields will, after clicking the **Refresh** button, 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 **I<<** button to start over.

The page includes the following fields:

Object	Description
Port	The port number for which the status applies. Click the port number to see the status for this particular port.
VLAN ID	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
IP Address	The IP address of the entry.

Buttons

- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the displayed table starting from the **MAC address** and **VLAN** input fields.
- Click **Clear** to flush all dynamic entries.
- Click **I<<** to update the table starting from the first entry in the MAC table (i.e., the entry with the lowest VLAN ID and MAC address).
- Click **>>** to update the table, starting with the entry after the last entry currently displayed.

MAC address table

Switching of frames is based upon the DMAC address contained in the frame. The industrial managed 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) that 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.

MAC table configuration

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

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging

☐

Aging Time

300

seconds

MAC Table Learning

	Port Members																											
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Auto	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	
Disable	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Secure	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Static MAC Table Configuration

			Port Members																											
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Add New Static Entry

Apply

Reset

The page includes the following fields:

Aging configuration

Object	Description
Disable Automatic Aging	Enables/disables the automatic aging of dynamic entries
Aging Time	The time after which a learned entry is discarded. By default, dynamic entries are removed from the MAC after 300 seconds. This removal is also called aging. (Range: 10-10000000 seconds; Default: 300 seconds)

MAC table learning

If the learning mode for a given port is greyed out, another module is in control of the mode so that it cannot be changed by the user. An example of such a module is the MAC-Based Authentication under 802.1X.

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

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.

Object	Description
Delete	Select 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. Select or deselect as needed to modify the entry.
Adding a New Static Entry	Click Add New Static Entry to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click Save .

Buttons

- Click **Apply** to apply changes.

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

MAC address table status

Dynamic 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.

MAC Address Table

Start from VLAN and MAC Address with entries per page.

Query by:

☐ Interface

☐ VLAN

☐ MAC Address

CPU

Type	VLAN	MAC Address	Port Members																											
			CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Static	1	33-33-FF-00-00-00	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dynamic	1	40-61-86-04-18-69	✓																											
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Auto-refresh ☐

Refresh

Clear

◀◀

▶▶

Navigating the MAC table

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

The "Start from MAC address" and **VLAN** input fields allow the user to select the starting point in the MAC Table. Clicking the **Refresh** button updates the displayed table starting from that or the closest next MAC Table match.

In addition, the two input fields will, after clicking the **Refresh** button, assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The **>>** button uses 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.

The page includes the following fields:

Object	Description
Type	Indicates if the entry is a static or 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

- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the displayed table starting from the **MAC address** and **VLAN** input fields.
- Click **Clear** to flush all dynamic entries.
- Click **◀** to update the table starting from the first entry in the MAC table (i.e., the entry with the lowest VLAN ID and MAC address).
- Click **>** to update the table, starting with the entry after the last entry currently displayed.

LLDP

Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities, and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Link Layer Discovery Protocol – Media Endpoint Discovery (LLDP-MED) is an extension of LLDP intended for managing endpoint devices such as Voice over IP (VoIP) phones and network switches. The LLDP-MED TLVs advertise information such as network policy, power, inventory, and device location details. LLDP and LLDP-MED information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

LLDP configuration

The LLDP Configuration page allows the user to inspect and configure the current LLDP port settings.

LLDP Configuration

LLDP Parameters

Tx Interval	30	seconds
Tx Hold	4	times
Tx Delay	2	seconds
Tx Reinit	2	seconds

LLDP Port Configuration

			Optional TLVs				
Port	Mode	CDP Aware	Port Description	System Name	System Description	System Capabilities	Management Address
*	<All>	☐	☐	☐	☐	☐	☐
1	Disabled	☐	☒	☒	☒	☒	☒
2	Disabled	☐	☒	☒	☒	☒	☒
3	Disabled	☐	☒	☒	☒	☒	☒
4	Disabled	☐	☒	☒	☒	☒	☒
5	Disabled	☐	☒	☒	☒	☒	☒
6	Disabled	☐	☒	☒	☒	☒	☒
7	Disabled	☐	☒	☒	☒	☒	☒
8	Disabled	☐	☒	☒	☒	☒	☒

The page includes the following fields:

LLDP parameters

Object	Description
Tx Interval	The switch is periodically transmitting 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. Default: 30 seconds This attribute must comply with the following rule: (Transmission Interval * Hold Time Multiplier) ≤65536, and Transmission Interval ≥ (4 * Delay Interval)
Tx Hold	Each LLDP frame contains information about how long 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. TTL in seconds is based on the following rule: (Transmission Interval * Holdtime Multiplier) ≤ 65536. Therefore, the default TTL is 4*30 = 120 seconds.
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. This attribute must comply with the rule: (4 * Delay Interval) ≤Transmission Interval

Object	Description
Tx Reinit	When a port 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 is no longer valid. Tx Reinit controls the amount of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.

LLDP port configuration

The LLDP port settings relate to the current unit, as reflected by the page header.

Object	Description
Port	The switch port number of the logical LLDP port.
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, and 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 port 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 neighbours' 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 neighbours 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 ports have CDP awareness disabled, the switch forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled, all CDP frames are terminated by the switch. Note: When CDP awareness on a port is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.
Port Description	Optional TLV: When selected, the "port description" is included in LLDP information transmitted.
System Name	Optional TLV: When selected, the "system name" is included in LLDP information transmitted.
System Description	Optional TLV: When selected, the "system description" is included in LLDP

Object	Description
	information transmitted.
System Capabilities	Optional TLV: When selected, the "system capability" is included in LLDP information transmitted.
Management Address	Optional TLV: When selected, the "management address" is included in LLDP information transmitted.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

LLDP-MED configuration

The LLDP-MED Configuration page permits configuration of the LLDP-MED.

LLDP-MED Configuration

Fast Start Repeat Count

Fast start repeat count

Coordinates Location

Latitude ° North Longitude ° East Altitude Meters Map Datum WGS84

Civic Address Location

Country code		State		County	
City		City district		Block (Neighborhood)	
Street		Leading street direction		Trailing street suffix	
Street suffix		House no.		House no. suffix	
Landmark		Additional location info		Name	
Zip code		Building		Apartment	
Floor		Room no.		Place type	
Postal community name		P.O. Box		Additional code	

Emergency Call Service

Emergency Call Service

Policies

Delete	Policy ID	Application Type	Tag	VLAN ID	L2 Priority	DSCP
No entries present						

The page includes the following fields:

Fast start repeat count

Object	Description
Fast start repeat count	Rapid startup and Emergency Call Service Location Identification Discovery of endpoints is a critically important aspect of VoIP systems. In addition, it is best to advertise only those pieces of information which are specifically relevant to particular endpoint types (e.g., only advertise the voice network policy to permitted voice-capable devices), both in order to conserve the limited LLDPDU 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 port. 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 to 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, we recommend repeating 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 four times, given that four LLDP frames with a one 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.

Coordinates location

Object	Description
Latitude	Latitude SHOULD be normalized to within 0-90° with a maximum of four 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° with a maximum of four 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 -32767 to 32767 with a maximum of four 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 of 0.0 is meaningful even

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

Civic address location

IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI).

Object	Description
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

Object	Description
Place type	Place type - Example: Office
Postal community name	Postal community name - Example: Leonia
P.O. Box	Post office box (P.O. BOX) - Example: 12345
Additional code	Additional code - Example: 1320300003

Emergency call service

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

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

Policies

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

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

The network policy attributes advertised are:

- 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 / Signaling (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.

Object	Description
Delete	Select this check box to delete the policy. It will be deleted during the next save.
Policy ID	ID for the policy. This is auto generated and is used when selecting the polices mapped to the specific ports.
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 Signaling (conditional) – For use in network topologies that require a different policy for the voice signaling 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 Signaling (conditional) – For use in network topologies that require a different policy for the guest voice signaling 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 Signaling (conditional) – For use in network topologies that require a separate policy for the video signaling 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.

Object	Description
Tag	Tag indicates if 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 port 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 behavior 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 Add New Policy 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

Port policies configuration

Every port may advertise a unique set of network policies or different attributes for the same network policies based on the authenticated user identity or port configuration.

Object	Description
Port	The port number for which the configuration applies.
Policy ID	The set of policies for a given port. The set of policies is selected by selecting the check boxes that correspond to the policies

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

LLDP-MED neighbor

The LLDP-MED Neighbor Information page provides a status overview of all LLDP-MED neighbors. The table contains a row for each port on which an LLDP neighbor is detected. The columns hold the following information:

LLDP-MED Neighbour Information

Port 1					
Device Type	Capabilities				
Endpoint Class III	LLDP-MED Capabilities, Network Policy, Extended Power via MDI - PD, Inventory				
Application Type	Policy	Tag	VLAN ID	Priority	DSCP
Voice	Defined	Untagged	-	-	46
Voice Signaling	Defined	Untagged	-	-	32
Auto-negotiation	Auto-negotiation status	Auto-negotiation Capabilities		MAU Type	
Supported	Enabled	1000BASE-T half duplex mode, 1000BASE-X, -LX, -SX, -CX full duplex mode, Asymmetric and Symmetric PAUSE for full-duplex inks, Symmetric PAUSE for full-duplex links		100BaseTXFD - 2 pair category 5 UTP, full duplex mode	

The page includes the following fields:

Fast start repeat count

Object	Description
Port	The port on which the LLDP frame was received.
Device Type	LLDP-MED Devices are comprised of two primary Device Types: Network Connectivity Devices and Endpoint Devices. LLDP-MED Network Connectivity Device Definition LLDP-MED Network Connectivity Devices, as defined in TIA-1057, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies: 1. LAN Switch/Router 2. IEEE 802.1 Bridge 3. IEEE 802.3 Repeater (included for historical reasons) 4. IEEE 802.11 Wireless Access Point 5. Any device that supports the IEEE 802.1AB and MED extensions defined by TIA-1057 and can relay IEEE 802 frames via any method. LLDP-MED Endpoint Device Definition 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 but 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)

Object	Description
	The LLDP-MED Media Endpoint (Class II) definition is applicable to all endpoint products that have IP media capabilities but 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, etc. 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: 1. LLDP-MED capabilities 2. Network Policy 3. Location Identification 4. Extended Power via MDI - PSE 5. Extended Power via MDI - PD 6. Inventory 7. Reserved
Application Type	Application Type indicating the primary function of the application(s) defined for this network policy, advertised by an Endpoint or Network Connectivity Device. The possible application types are as follows: 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 – Supports 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

Object	Description
	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.
TAG	TAG is indicating 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 port 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 port is used instead.
Priority	Priority is the Layer 2 priority to be used for the specified application type. One of eight priority levels (0 through 7).
DSCP	DSCP is the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474. Contain one of 64 code point values (0 through 63).
Auto-negotiation	Auto-negotiation identifies if MAC/PHY auto-negotiation is supported by the link partner.
Auto-negotiation status	Auto-negotiation status identifies if auto-negotiation is currently enabled at the link partner. If Auto-negotiation is supported and Auto-negotiation status is disabled, the 802.3 PMD operating mode will be determined by the operational MAU type field value rather than by auto-negotiation.

Buttons

- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

Neighbor

The LLDP Neighbor Information page provides a status overview for all LLDP neighbors. The displayed table contains a row for each port on which an LLDP neighbor is detected.

LLDP Neighbor Information

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

Auto-refresh ☐
Refresh

The page includes the following fields:

Object	Description
Local Port	The port on which the LLDP frame was received.
Chassis ID	The identification of the neighbor's LLDP frames.
Port ID	The identification of the neighbor port.
Port Description	The port description advertised by the neighbor unit.
System Name	The name advertised by the neighbor unit.
System Capabilities	System Capabilities describes the neighbor unit's capabilities. The possible capabilities are: 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
Management Address	The neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could, for instance, hold the neighbor's IP address.

Buttons

- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

Port statistics

The LLDP Global/Statistics Local Counters page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters are counters that refer to the switch, while local counters refers to counters for the currently selected switch.

LLDP Global Counters

Global Counters	
Neighbor entries were last changed 1970-01-01 Thu 00:00:00+00:00 (385 secs. ago)	
Total Neighbors Entries Added	0
Total Neighbors Entries Deleted	0
Total Neighbors Entries Dropped	0
Total Neighbors Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

The page includes the following fields:

Global counters

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

LLDP statistics local counters

The displayed table contains a row for each port. The columns hold the following information:

Object	Description
Local Port	The port on which LLDP frames are received or transmitted.
Tx Frames	The number of LLDP frames transmitted on the port.
Rx Frames	The number of LLDP frames received on the port.
Rx Errors	The number of received LLDP frames containing some kind of error.
Frames Discarded	If an LLDP frame is received on a port, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many 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 port links down, an LLDP shutdown frame is received, or when the entry ages out.

Object	Description
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.
Org. Discarded	The number of organizationally TLVs received.
Age-Outs	Each LLDP frame contains information about how long time the LLDP information is valid (age-out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.

Buttons

- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.
- Click **Clear** to clear the local counters. All counters (including global counters) are cleared upon reboot.

Network diagnostics

This section provides the physical layer and IP layer network diagnostics tools for troubleshooting. The diagnostic tools are designed for network managers to help them quickly diagnose problems and better service customers.

Use the Diagnostics menu items to display and configure basic administrative details of the industrial managed switch. Under System, the following topics are provided to configure and view the system information:

- Ping
- IPv6 Ping
- Remote IP Ping
- Cable Diagnostics

Ping

The ping and IPv6 ping permit the issuance of ICMP PING packets to troubleshoot IP connectivity issues. The industrial managed switch transmits ICMP packets, and the sequence number and roundtrip time are displayed upon reception of a reply.

Cable diagnostics

Cable diagnostics performs tests on copper cables. These functions have the ability to identify the cable length and operating conditions, and to isolate a variety of common faults that can occur on the Cat5 twisted-pair cabling. There might be two states, which are as follows:

- If the link is established on the twisted-pair interface in 1000BASE-T mode, the cable diagnostics can run without disruption of the link or of any data transfer.
- If the link is established in 100BASE-TX or 10BASE-T, the cable diagnostics cause the link to drop while the diagnostics are running.

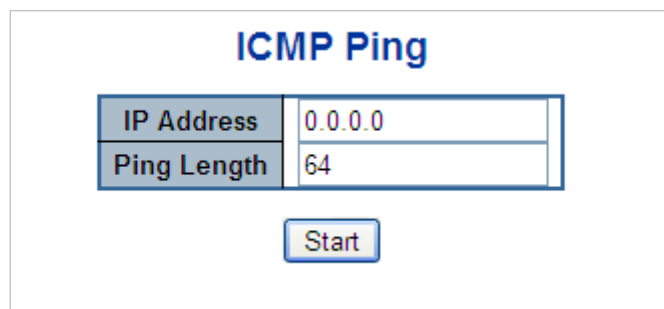
After the diagnostics are finished, the link is re-established and the following functions are available.

- Coupling between cable pairs
- Cable pair termination
- Cable Length

Ping

The ICMP Ping page allows you to issue ICMP ping packets to troubleshoot IP connectivity issues.

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



The page includes the following fields:

Object	Description
IP Address	The destination IP Address.
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.

Note: Be sure the target IP address is within the same network subnet of the industrial managed switch, otherwise the correct gateway IP address must be set up.

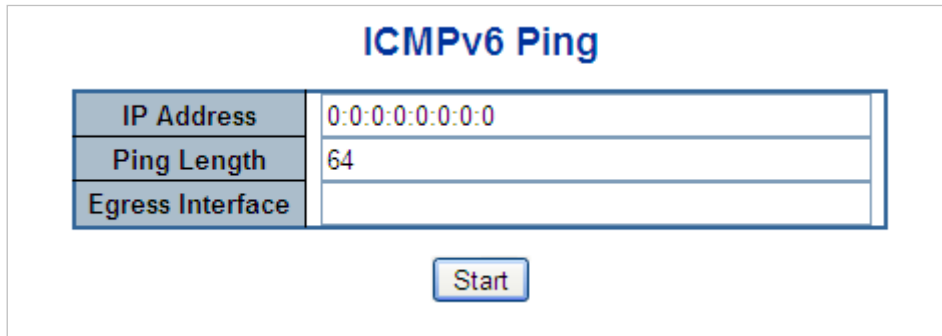
Buttons

- Click **Start** to transmit ICMP packets.
- Click **New Ping** to re-start diagnostics with ping.

IPv6 ping

The ICMPv6 Ping page allows you to issue ICMPv6 ping packets to troubleshoot IPv6 connectivity issues. After clicking **Start**, five ICMPv6 packets are transmitted, and the

sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.



The image shows a web form titled "ICMPv6 Ping". It contains three input fields: "IP Address" with the value "0:0:0:0:0:0:0:0", "Ping Length" with the value "64", and "Egress Interface" which is empty. Below these fields is a "Start" button.

The page includes the following fields:

Object	Description
IP Address	The destination IP address.
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Egress Interface	The VLAN ID (VID) of the specific egress IPv6 interface to which the ICMP packet goes. The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. When the egress interface is not provided, PING6 finds the best match interface for destination. Do not specify an egress interface for loopback addresses. Do specify an egress interface for link-local or multicast addresses.

Buttons

- Click **Start** to transmit ICMP packets.
- Click **New Ping** to re-start diagnostics with ping.

Remote IP ping test

This Remote ICMP Ping Test page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues on a special port. After clicking **Test**, five ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

Port	Remote IP Address	Ping Size	Ping Button	Result
1	0.0.0.0	64	Ping	
2	0.0.0.0	64	Ping	
3	0.0.0.0	64	Ping	
4	0.0.0.0	64	Ping	
5	0.0.0.0	64	Ping	
6	0.0.0.0	64	Ping	
7	0.0.0.0	64	Ping	
8	0.0.0.0	64	Ping	

The page includes the following fields:

Object	Description
Port	The logical port for the settings.
Remote IP Address	The destination IP address.
Ping Size	The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.
Result	Display the ping result.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.
- Click **Clear** to clear the IP address and the result of the ping value.

Cable diagnostics

The VeriPHY Cable Diagnostics page is used for running cable diagnostics.

Click **Start** to run the diagnostics. This will take approximately five seconds. If all ports are selected, this can take approximately 15 seconds. When completed, the page refreshes automatically, and the cable diagnostics results appear in the cable status table. Note that cable diagnostics is only accurate for cables of 7–140 meters in length.

10 and 100 Mbps ports are linked down while running cable diagnostics. Therefore, running cable diagnostics on a 10 or 100 Mbps management port causes the switch to stop responding until VeriPHY is complete. The ports belong to the current unit, as reflected by the page header.

VeriPHY Cable Diagnostics

Cable Status									
Port	Description	Pair A(1,2)	Length A	Pair B(3,6)	Length B	Pair C(4,5)	Length C	Pair D(7,8)	Length D
1		--	--	--	--	--	--	--	--
2		--	--	--	--	--	--	--	--
3		--	--	--	--	--	--	--	--
4		--	--	--	--	--	--	--	--
5		--	--	--	--	--	--	--	--
6		--	--	--	--	--	--	--	--
7		--	--	--	--	--	--	--	--
8		--	--	--	--	--	--	--	--

The page includes the following fields:

Object	Description
Port	The port where you are requesting cable diagnostics.
Description	Display per port description.
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

Buttons

- Click **Start** to run the diagnostics.

Loop protection

This section describes the enable loop protection function that provides loop protection to prevent broadcast loops in the industrial managed switch.

Loop protection configuration

The Loop Protection Configuration page allows the user to inspect and change the current loop protection configurations.

Loop Protection Configuration

General Settings

Global Configuration			
Enable Loop Protection	Disable ▾		
Transmission Time	5		seconds
Shutdown Time	180		seconds

Port Configuration

Port	Enable	Action	Tx Mode
*	☐	<All> ▾	<All> ▾
1	☒	Shutdown Port ▾	Enable ▾
2	☒	Shutdown Port ▾	Enable ▾
3	☒	Shutdown Port ▾	Enable ▾
4	☒	Shutdown Port ▾	Enable ▾
5	☒	Shutdown Port ▾	Enable ▾
6	☒	Shutdown Port ▾	Enable ▾
7	☒	Shutdown Port ▾	Enable ▾
8	☒	Shutdown Port ▾	Enable ▾

This page includes the following fields:

General settings

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

Port configuration

Object	Description
Port	The switch port number.
Enable	Controls loop protection enable/disable on this switch port.
Action	Configures the action performed when a loop is detected on a port.

Object	Description
	Selections include Shutdown Port , Shutdown Port and Log or Log Only .
Tx Mode	Controls if the port is actively generating loop protection PDUs or if it is just passively looking for looped PDU's.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Loop protection status

The Loop Protection Status page shows the loop protection port status of the switch.

Loop Protection Status

Auto-refresh ☐ Refresh

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
No ports enabled						

This page includes the following fields:

Object	Description
Port	The 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	Indicates if a loop is currently detected on the port.
Time of Last Loop	The time of the last loop event detected.

Buttons

- Click **Auto-refresh** to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **Refresh** to refresh the page immediately.

RMON

RMON is an expansion of standard SNMP. RMON is a set of MIB definitions used to define standard network monitor functions and interfaces, enabling communication

between SNMP management terminals and remote monitors. RMON provides a highly efficient method to monitor actions inside the subnets.

The MID of RMON consists of 10 groups. The switch supports the most frequently used groups:

- **Statistics:** Maintain basic usage and error statistics for each subnet monitored by the agent.
- **History:** Record periodical statistic samples.
- **Alarm:** Allow management console users to set any count or integer for sample intervals and alert thresholds for RMON agent records.
- **Event:** A list of all events generated by the RMON agent.

Alarm depends on the implementation of an event. **Statistics** and **History** display current or history subnet statistics. **Alarm** and **Event** provide a method to monitor any integer data change in the network, and provide some alerts upon abnormal events (sending Trap or record in logs).

RMON alarm configuration

Configure RMON alarm table on the RMON Alarm Configuration page. The entry index key is **ID**.

RMON Alarm Configuration

Delete	ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
Add New Entry Apply Reset										

The page includes the following fields:

Object	Description
Delete	Select the Delete check box to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2 ³¹ -1.
Variable	Indicates the particular variable to be sampled. The possible variables are: InOctets: 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 broadcast and multicast packets delivered to a higher-layer protocol. InDiscards: The number of inbound packets that are discarded when the packets are normal. InErrors: The number of inbound packets that contained errors preventing

Object	Description
	them from being deliverable to a higher-layer protocol. InUnknownProtos: The number of inbound packets that were discarded because of an unknown or unsupported protocol. OutOctets: The number of octets transmitted out of the interface, including framing characters. OutUcastPkts: The number of unicast packets that requested to transmit. OutNUcastPkts: The number of broadcast and multicast packets that requested to transmit. OutDiscards: The number of outbound packets that are discarded when the packets are 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: Triggers alarm when the first value is larger than the rising threshold. Falling: Triggers alarm when the first value is less than the falling threshold. RisingOrFalling: Triggers alarm when the first value is larger than the rising threshold or less than the falling threshold (default).
Rising Threshold	Rising threshold value (-2147483648-2147483647).
Rising Index	Rising event index (1-65535).
Falling Threshold	Falling threshold value (-2147483648-2147483647)
Falling Index	Falling event index (1-65535).

Buttons

- Click **Add New Entry** to add a new community entry.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

RMON alarm status

The RMON Alarm Overview page provides an overview of RMON Alarm entries. Each page shows up to 99 entries from the Alarm table (default is 20 entries per page). The range of entries per page can be typed into the **Start from Control Index** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the Alarm table. The first entry shown will be the one with the lowest ID found in the Alarm table.

RMON Alarm Overview

Auto-refresh ☐ Refresh |<< >>

Start from Control Index with entries per page.

ID	Interval	Variable	Sample Type	Value	Startup Alarm	Rising Threshold	Rising Index	Falling Threshold	Falling Index
No more entries									

The page includes the following fields:

Object	Description
ID	Indicates the index of alarm control entry.
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold.
Variable	Indicates the particular variable to be sampled
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds.
Value	The value of the statistic during the last sampling period.
Startup Alarm	The alarm that may be sent when this entry is first set to valid.
Rising Threshold	Rising threshold value.
Rising Index	Rising event index.
Falling Threshold	Falling threshold value.
Falling Index	Falling event index.

Buttons

- Click **Refresh** to refresh the page immediately.
- Click the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **|<<** to update the table starting from the first entry in the alarm table (i.e., the entry with the lowest ID).
- Click **>>** to update the table starting with the entry after the last entry currently displayed.

RMON event configuration

Configure the RMON Event table on the RMON Event Configuration page. The entry index key is **ID**.

The page includes the following fields:

Object	Description
Delete	Select to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Desc	Indicates the event. The string length is from 0 to 127, default is a null string.
Type	Indicates the notification of the event. The possible types are: none : The total number of octets received on the interface, including framing characters. log : The number of unicast packets delivered to a higher-layer protocol. snmptrap : The number of broadcast and multicast packets delivered to a higher-layer protocol. logandtrap : The number of inbound packets that are discarded when the packets are normal.
Community	Specify the community when trap is sent. The string length is from 0 to 127, default is "public."
Event Last Time	Indicates the value of sysUpTime at the time this event entry last generated an event.

Buttons

- Click **Add New Entry** to add a new community entry.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

RMON event status

The RMON Event Overview page provides an overview of RMON Event table entries. Each page shows up to 99 entries from the Event table (default is 20 entries per page). The range of entries per page can be typed into the **Start from Control Index** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the Event table. The first entry shown will be the one with the lowest ID found in the Event table

RMON Event Overview

Auto-refresh ☐ Refresh ◀ ▶

Start from Control Index and Sample Index with entries per page.

Event Index	LogIndex	LogTime	LogDescription
No more entries			

The page includes the following fields:

Object	Description
Event Index	Indicates the index of the event entry.
Log Index	Indicates the index of the log entry.
LogTime	Indicates event log time.
LogDescription	Indicates the event description.

Buttons

- Click **Refresh** to refresh the page immediately.
- Click the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **◀** to update the table starting from the first entry in the alarm table (i.e., the entry with the lowest ID).
- Click **▶** to update the table starting with the entry after the last entry currently displayed.

RMON history configuration

Configure RMON History on the RMON History Configuration page. The entry index key is **ID**.

RMON History Configuration

Delete	ID	Data Source	Interval	Buckets	Buckets Granted
Add New Entry Apply Reset					

The page includes the following fields:

Object	Description
Delete	Select to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Data Source	Indicates the port ID to be monitored. If in the switch, the value must add 1000*(switch ID-1). For example, if the port is switch 3 port 5, the value is 2005.
Interval	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
Buckets	Indicates the maximum data entries associated with this history control entry stored in RMON. The range is from 1 to 3600, default value is 50.
Buckets Granted	The number of data to be saved in the RMON.

Buttons

- Click **Add New Entry** to add a new community entry.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

RMON history status

The RMON History Overview page provides details of RMON history entries.

RMON History Overview

Auto-refresh ☐ Refresh |<< >>|

Start from Control Index and Sample Index with entries per page.

History Index	Sample Index	Sample Start	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	Utilization
No more entries														

The page includes the following fields:

Object	Description
History Index	Indicates the index of history control entry.
Sample Index	Indicates the index of the data entry associated with the control entry.
Sample Start	The value of sysUpTime at the start of the interval over which this sample was measured.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.

Object	Description
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 1518 octets.
Frag.	The number of frames with a size less than 64 octets received with invalid CRC.
Jabb.	The number of frames with a size larger than 64 octets received with invalid CRC.
Coll.	The best estimate of the total number of collisions on this Ethernet segment.
Utilization	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Buttons

- Click **Refresh** to refresh the page immediately.
- Click the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **1<<** to update the table starting from the first entry in the alarm table (i.e., the entry with the lowest ID).
- Click **>>** to update the table starting with the entry after the last entry currently displayed.

RMON statistics configuration

Configure the RMON Statistics table on the RMON Statistics Configuration page. The entry index key is **ID**.

The screenshot shows a web interface titled "RMON Statistics Configuration". Below the title, there are two rows of buttons. The first row contains three buttons: "Delete", "ID", and "Data Source". The second row contains three buttons: "Add New Entry", "Apply", and "Reset".

The page includes the following fields:

Object	Description
Delete	Select to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Data Source	Indicates the port ID to be monitored. If in the switch, the value must add 1000*(switch ID-1). For example, if the port is switch 3 port 5, the value is 2005.

Buttons

- Click **Add New Entry** to add a new community entry.
- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

RMON statistics status

The RMON Statistics Status Overview page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table (default is 20 entries per page). The range of entries per page can be typed into the **Start from Control Index** and **entries per page** fields. When initially accessing the page, it shows the first 20 entries from the beginning of the Statistics table. The first entry shown will be the one with the lowest ID found in the Statistics table

RMON Statistics Status Overview

Auto-refresh ☐ Refresh |<< >>

Start from Control Index with entries per page.

ID	Data Source (ifIndex)	Drop	Octets	Pkts	Broad-cast	Multi-cast	CRC Errors	Under-size	Over-size	Frag.	Jabb.	Coll.	64 Bytes	65 ~ 127	128 ~ 255	256 ~ 511	512 ~ 1023	1024 ~ 1588
No more entries																		

The page includes the following fields:

Object	Description
ID	Indicates the index of statistics entry.
Data Source (ifIndex)	The port ID to be monitored.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broadcast	The total number of good packets received that were directed to the broadcast address.

Object	Description
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.
Undersize	The total number of packets received that were less than 64 octets.
Oversize	The total number of packets received that were longer than 1518 octets.
Frag.	The number of frames with a size less than 64 octets received with invalid CRC.
Jabb.	The number of frames with a size larger than 64 octets received with invalid CRC.
Coll.	The best estimate of the total number of collisions on this Ethernet segment.
64 Bytes	The total number of packets (including bad packets) received that were 64 octets in length.
65~127	The total number of packets (including bad packets) received that were between 65 to 127 octets in length.
128~255	The total number of packets (including bad packets) received that were between 128 to 255 octets in length.
256~511	The total number of packets (including bad packets) received that were between 256 to 511 octets in length.
512~1023	The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.
1024~1518	The total number of packets (including bad packets) received that were between 1024 to 1518 octets in length.

Buttons

- Click **Refresh** to refresh the page immediately.
- Click the **Auto-refresh** check box to refresh the page automatically. Automatic refresh occurs every three seconds.
- Click **1<<** to update the table starting from the first entry in the alarm table (i.e., the entry with the lowest ID).
- Click **>>** to update the table starting with the entry after the last entry currently displayed.

Power over Ethernet (PoE)

Providing up to 24 PoE in-line power interfaces, the industrial managed switch can easily build a power central-controlled IP phone system, IP camera system, and Access Point (AP) group for the enterprise. For example, 24 cameras/APs can be installed for company surveillance demands, or to build a wireless roaming environment in the office. Without power-socket limitation, the industrial managed switch makes the installation of cameras or WLAN APs simple and efficient.

PoE Powered Devices (PD)

 3~5 Watts	Voice over IP phones Enterprises can install POE VoIP phones, ATA, and other Ethernet/non-Ethernet end-devices to the central location where UPS is installed for uninterrupted power systems and power control systems.
 6~12 Watts	Wireless LAN Access Points Museums, airports, hotels, campuses, factories, warehouses, etc. can install APs in any location.
 10~12 Watts	IP Surveillance Enterprises, museums, campuses, hospitals, banks, etc. can install IP cameras regardless of installation location without the need to install AC sockets.
 3~12 Watts	PoE Splitter PoE splitters split the PoE 52 VDC over the Ethernet cable into a 5/12 VDC power output. It frees the device deployment from restrictions due to power outlet locations, which eliminate the costs for additional AC wiring and reduces the installation time.
 3~25 Watts	High Power PoE Splitter High PoE splitters split the PoE 56 VDC over the Ethernet cable into a 24/12V DC power output. It frees the device deployment from restrictions due to power outlet locations, which eliminate the costs for additional AC wiring and reduces the installation time.
 30 Watts	High Power Speed Dome This state-of-the-art design is designed to fit into various network environments like traffic centers, shopping malls, railway stations, warehouses, airports, and production facilities for the most demanding outdoor surveillance applications without the need to install AC sockets.

Note: Since the industrial managed switch PoE ports support 56 VDC PoE power output, ensure that the PD's acceptable DC power range is from 56 VDC. Otherwise, it will damage the PD.

In a PoE system, operating power is applied from a power source (PSU-power supply unit) over the LAN infrastructure to powered devices (PDs), which are connected to ports. Under some conditions, the total output power required by PDs can exceed the maximum available power provided by the PSU. The system may include a PSU capable of supplying less power than the total potential power consumption of all the PoE ports in the system. To keep the majority of the ports active, power management is implemented.

The PSU input power consumption is monitored by measuring voltage and current, and is equal to the system's aggregated power consumption. The power management concept allows all ports to be active and activates additional ports, as long as the aggregated power of the system is lower than the power level at which additional PDs

cannot be connected. When this value is exceeded, ports will be deactivated according to user-defined priorities. The power budget is managed according to the following user-definable parameters:

- Maximum available power
- Ports priority
- Maximum allowable power per port

There are five modes for configuring how the ports/PDs may reserve power and when to shut down ports.

Classification mode

In this mode, each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist: 4, 7, 15.4, and 30.8 W.

Class	Usage	Range of maximum power used by the PD	Class Description
0	Default	0.44 to 12.95 W	Classification unimplemented
1	Optional	0.44 to 3.84 W	Very low power
2	Optional	3.84 to 6.49 W	Low power
3	Optional	6.49 to 12.95 W (or to 15.4 W)	Mid power
4	Optional	12.95 to 25.50 W (or to 30.8 W)	High power

Note:

1. The maximum power fields have no effect in classification mode.
2. The PD69012 PoE chip is designed so that Class level 0 will be assigned to 15.4 W by AF mode and 30.8 W by AT mode under classification power limit mode. It is hardware limited.

Allocation mode

In this mode, the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the maximum power fields. The ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver.

Note: In this mode, the port power is not turned on if the PD requests more available power.

LLDP mode

In this mode, the PoE power ports are managed and determined by LLDP Media protocol.

PoE configuration

Inspect and configure the current PoE configuration settings on the Power over Ethernet Configuration page.

Power Over Ethernet Configuration

System PoE Admin Mode	Enable ▼
PoE Temperature Protection	Enable ▼
PoE Management Mode	allocation-consumption ▼
Power Supply Budget [W]	440
Temperature Threshold	70 Degrees C
PoE Usage Threshold	85 %

The page includes the following fields:

Object	Description
System PoE Admin Mode	Enables/disables the PoE function, determining whether or not the PoE ports supply power.
PoE Temperature Protection	Enables/disables PoE temperature protection.
PoE Management Mode	There are six modes for configuring how the ports/PDs may reserve power and when to shut down ports. Class-Consumption mode: System offers PoE power according to PD real power consumption. Class-Reserved-Power mode: System reserves PoE power to PD according to PoE class level. Allocation-Consumption mode: System offers PoE power according to PD real power consumption. Allocation-Reserved-Power mode: Users can assign how much PoE power for per port and the system reserves PoE power to the PD. LLDP-Consumption mode: System offers PoE power according to PD real power consumption. LLDP-Reserved-Power mode: System reserves PoE power to the PD according to LLDP configuration.
Power Supply Budget [W]	Sets the limit value of the total PoE port provided power to the PDs. The industrial managed switch available maximum value is 440.
Temperature Threshold	Sets the temperature protection threshold value. If the system temperature is over this value, then the system lowers the total PoE power budget automatically.
PoE Usage Threshold	Sets the PoE power budget limitation.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

PD classifications

A PD may be classified by the PSE based on the classification information provided by the PD. The intent of PD classification is to provide information about the maximum power required by the PD during operation. The PD provides a signature about Class level to improve power management at the PSE.

The PD is classified based on power. The classification of the PD is the maximum power that the PD draws across all input voltages and operational modes.

A PD will return to Class 0 to 4 in accordance with the maximum power draw as specified below:

Class	Usage	Range of maximum power used by the PD	Class Description
0	Default	12.95 W (or to 15.4 W for AF mode) 25.5 W (or to 30.8 W for AT mode)	Mid power or high power
1	Optional	0.44 to 3.84 W	Very low power
2	Optional	3.84 to 6.49 W	Low power
3	Optional	6.49 to 12.95 W (or to 15.4 W)	Mid power
4	Optional	12.95 to 25.50 W (or to 30.8 W)	High power

Port sequential

The Port Sequential Power up Interval page permits the user to configure the PoE ports' start up interval time. The PoE ports start up one by one.

Port Sequential Power up Interval

Sequential Power up Option	Enable ▼
Sequential Power up Interval	5 (3 ~ 30) seconds
Sequential Power up Port Option	By port ▼

Apply
Reset

Note: The PoE port will start up after the system program has completely finished running.

The page includes the following fields:

Object	Description
--------	-------------

Object	Description
Sequential Power up Option	Enables/disables the sequential power-up function.
Sequential Power up Interval	Configures the PoE port start up interval time.
Sequential Power up Port Option	There are two modes for starting up the PoE port: By Port: The PoE port will start up by following the port number. By Priority: The PoE Port will start up by following the PoE priority.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Port configuration

Inspect and configure the current PoE port settings on the PoE Ethernet Configuration page.

Power Over Ethernet Configuration

Port	PoE Mode	Schedule	AF/AT Mode	Priority	Power Allocation[W]
*	Enable ▼	<All> ▼	<All> ▼	<All> ▼	30.8
1	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
2	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
3	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
4	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
5	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
6	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
7	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
8	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
9	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
10	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
11	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
12	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
13	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
14	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
15	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
16	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
17	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
18	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
19	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
20	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
21	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
22	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
23	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8
24	Enable ▼	Profile 1 ▼	802.3at ▼	High ▼	30.8

Apply
Reset

The page includes the following fields:

Object	Description
PoE Mode	There are three PoE modes: Enable : Enables the PoE function. Disable : Disables the PoE function Schedule : Enables the PoE function in schedule mode
Schedule	Indicates the schedule profile mode. Possible profiles are: Profile1 Profile2 Profile3 Profile4
AF/AT Mode	Permits the user to select 802.3at or 802.3af compatibility mode. The default value is 802.3at mode. This function affects PoE power reservation on Classification power limit mode only. In 802.3af mode, the system is going to reserve 15.4W maximum for the PD that supports Class 3 level. In IEEE 802.3at mode, the system is going to reserve 30.8W for the PD that supports Class 4 level. Class 1 to Class 3 level in 802.3at mode reserves the same PoE power as 802.3af mode.
Priority	Priority represents PoE port priority. There are three levels of power priority: Low , High , and Critical . Priority is used when total power consumption is over the total power budget. In this case, the port with the lowest priority is turned off and power is provided to the port with higher priority.
Power Allocation	Limits the port PoE supply Watts. The per port maximum value must be less than 30.8W, and total port values must be less than the power reservation value. After a power overload has been detected, the port automatically shuts down and remains in detection mode until the PD's power consumption is lower than the power limit value.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

PoE status

Inspect the total power consumption, total power reserved, and current status for all PoE ports on the PoE Status page.

Power Over Ethernet Status

PoE System Status

Sequential Power On	Enable
System Power Budget	440 Watts
Operation mode	allocation-consumption
Current Budget	440 Watts
Current ports in used	16 ports
Class 1 ports	0
Class 2 ports	0
Class 3 ports	0
Class 4 ports	16
Power Consumption	424.7 Watts (96%)
Reserved Power(Reserved mode)	--
PoE Temperature	
Port 1 - 12	45°C / 113°F
Port 13 - 24	44°C / 111°F

Current Power Consumption  96% 424.7 / 440 W

PoE Port Status

Local Port	PD Class	Power Used [W]	Current Used [mA]	Priority	Port Status	AF/AT Mode
1	4	31.9	557	High	PoE ON	AT
2	4	26	460	High	PoE ON	AT
3	4	26	460	High	PoE ON	AT
4	4	26.4	468	High	PoE ON	AT
5	4	25.4	452	High	PoE ON	AT
6	4	26	462	High	PoE ON	AT
7	4	25.7	455	High	PoE ON	AT
8	4	25.7	456	High	PoE ON	AT
9	4	25.7	456	High	PoE ON	AT
10	4	25.7	456	High	PoE ON	AT
11	4	25.7	456	High	PoE ON	AT
12	4	25.7	456	High	PoE ON	AT
13	4	25.7	456	High	PoE ON	AT
14	4	25.7	456	High	PoE ON	AT
15	4	25.7	456	High	PoE ON	AT
16	4	25.7	456	High	PoE ON	AT
17	4	25.7	456	High	PoE ON	AT
18	4	25.7	456	High	PoE ON	AT
19	4	25.7	456	High	PoE ON	AT
20	4	26.2	463	High	PoE ON	AT
21	0	0	0	High	PoE Search	--
22	0	0	0	High	PoE Search	--
23	0	0	0	High	PoE Search	--
24	0	0	0	High	PoE Search	--
Total		424.7 [W]	7511 [mA]			

Auto Refresh ☐

The page includes the following fields:

Object	Description
Sequential Power On	Displays the current sequential power on mode.
System Power Budget	Displays the maximum PoE power budget.
Operation mode	Displays the current PoE operation mode.
Current Budget	Displays the current maximum PoE budget.
Current ports in used	Displays the current PoE in-use ports.
Class 1 ~ 4 ports	Displays the current PoE class 1 ~ 4 ports.
Power Consumption	Displays the current power consumption (total Watts and percentage).
Reserved Power (Reserved mode)	Shows how much the total power is reserved for all PDs.
PoE Temperature	Displays the current operating temperature of the first PoE chip unit. Chipset 1 = port 1 ~ 12 Chipset 2 = port 13 ~ 24
Current Power Consumption	Shows the total W usage of the industrial managed switch.
Local Port	This is the logical port number for this row.
PD Class	Displays the class of the PD attached to the port as established by the classification process. Class 0 is the default for PDs. The PD is powered based on PoE class level if the system is working in classification mode. A PD will return Class 0 to 4 in accordance with the maximum power draw as specified in "PD classifications" on page 294.
Power Used [W]	Shows how much power the PD is currently using.
Current Used [mA]	Shows how much current the PD is currently using.
Priority	Shows the port's priority configured by the user.
Port Status	Shows the port's status.
AF / AT Mode	Displays per PoE ports operating in 802.3af or 802.3at mode.
Total	Shows the total power and current usage of all PDs.

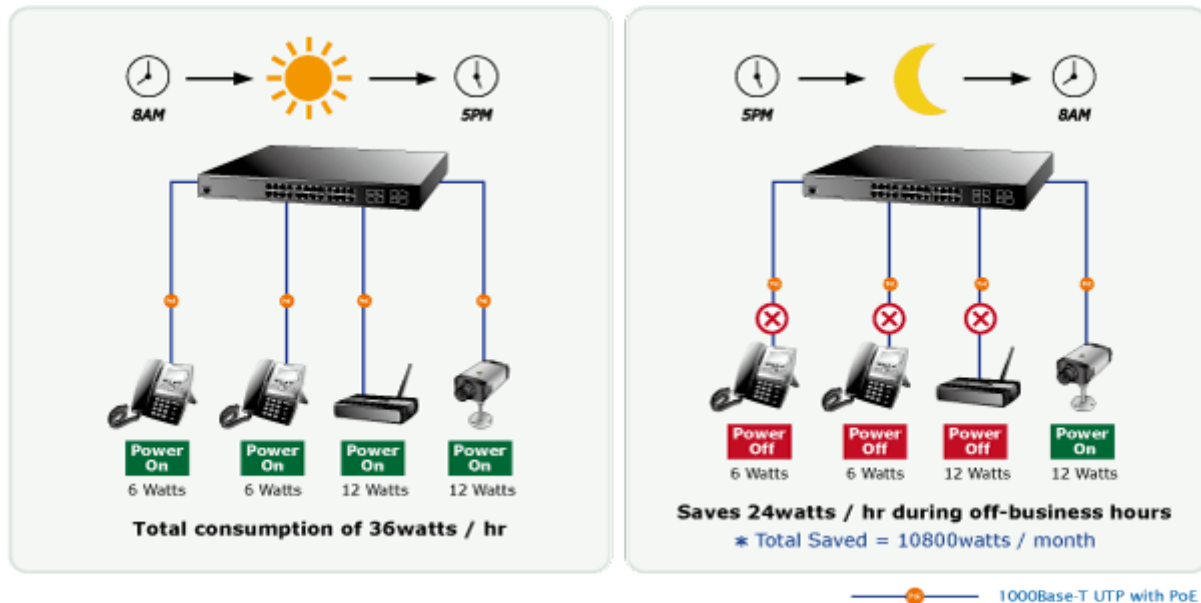
Buttons

- Select the **Auto-refresh** check box to enable an automatic refresh of the page at regular intervals.
- Click **Refresh** to refresh the page immediately.

PoE schedule

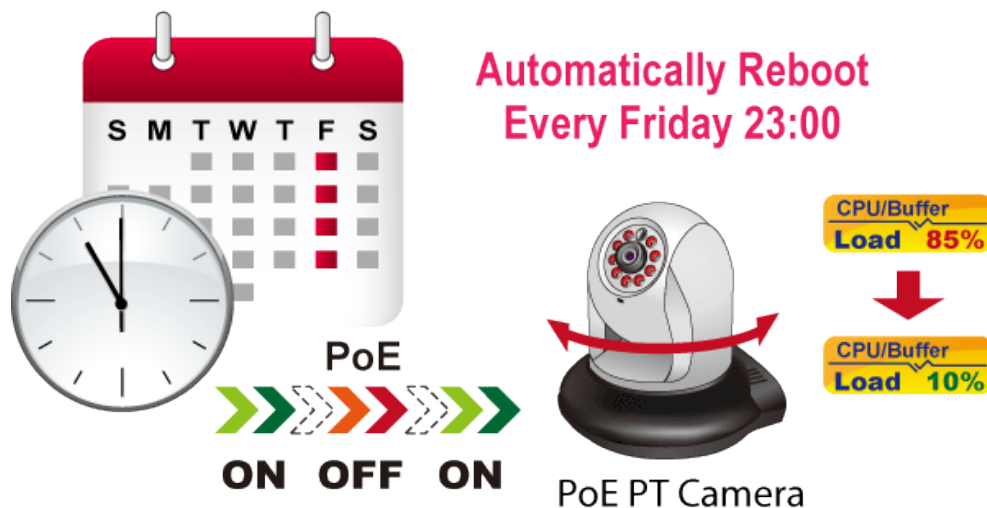
In addition to its functional use for IP surveillance, the industrial managed switch can also be implemented in any PoE network including VoIP and Wireless LAN. Under the trend of energy saving worldwide and contributing to worldwide environmental protection, the industrial managed switch can effectively control power supply in

addition to its capability to provide high Watt power. The PoE schedule function can enable or disable PoE power feeding for each PoE port during specified time intervals, and is a powerful function to help SMB or Enterprises save power and reduce cost.



Scheduled power recycling

The managed switch allows each of the connected PoE IP cameras to reboot at a specific time each week, thus reducing the chance of IP camera crashes resulting from buffer overflow.



Define the PoE schedule and schedule power recycling on the PoE Schedule page.

Power Over Ethernet Schedule

Profile

Profile 1

Delete	Week Day	Start Hour	Start Min	End Hour	End Min	Reboot Enable	Reboot Only	Reboot Hour	Reboot Min
--------	----------	------------	-----------	----------	---------	---------------	-------------	-------------	------------

Add New Rule

Apply

Sta

Fri

Thu

Wed

Tue

Mon

Sun

PoE Schedule

PoE Reboot

00h

01h

02h

03h

04h

05h

06h

07h

08h

09h

10h

11h

12h

13h

14h

15h

16h

17h

18h

19h

20h

21h

22h

23h

00h

Click the **Add New Rule** button to start setting the PoE schedule function. Click **Apply** after creating a schedule for the selected profile. Then, go to the PoE Port Configuration page and select **Schedule** from the PoE Mode drop-down list, and the profile number from the Schedule drop-down list, for each port to which you want to apply the schedule profile.

The page includes the following fields:

Object	Description
Profile	Set the schedule profile mode. Possible profiles are: Profile1 Profile2 Profile3 Profile4
Week Day	Set the weekday for enabling the PoE function.
Start Hour	Set the hour for enabling the PoE function.
Start Min	Set the minute for enabling the PoE function.
End Hour	Set the hour for disabling the PoE function.
End Min	Set the minute for disabling the PoE function.
Reboot Enable	Enables or disables a PoE port reboot according to the PoE reboot schedule. Note that if you want the PoE schedule and PoE reboot schedule to work at the same time, use this function and do not use the Reboot Only function. This function permits the administrator to reboot the PoE device at the indicated time as required.

300

NS3553-4P-1T-2S Industrial Managed Switch User Manual

Object	Description
Reboot Only	Permits a reboot of the PoE function according to the PoE reboot schedule. Note that if the administrator enables this function, the PoE schedule will not set the time to a profile. This function only applies to PoE port reset at the indicated time.
Reboot Hour	Sets the hour for PoE reboots. This function is only for the PoE reboot schedule.
Reboot Min	Sets what the minute for PoE reboots. This function is only for the PoE reboot schedule.

Buttons

- Click **Add New Rule** to set the PoE schedule function.
- Click **Apply** to apply changes.
- Click **Delete** to delete the entry.

LLDP PoE neighbors

The LLDP Neighbor PoE Information page provides a status overview for all LLDP PoE neighbors. The displayed table contains a row for each port on which an LLDP PoE neighbor is detected.

LLDP Neighbor Power Over Ethernet Information				
Local Port	Power Type	Power Source	Power Priority	Maximum Power
1	PD Device	Unknown	Unknown	6.3 [W]
Auto-refresh ☒ Refresh				

The administrator must enable the LLDP port in the LLDP Configuration page (see below). In this example, the LLDP function from port 1 to port 2 was enabled. After plugging in a PD that supports the PoE LLDP function, the PD's PoE information appears in the LLDP Neighbor PoE Information page.

LLDP Port Configuration							
Port	Mode	CDP Aware	Optional TLVs				
			Port Description	System Name	System Description	System Capabilities	Management Address
*	<All>	☐	☐	☐	☐	☐	☐
1	Enabled	☒	☒	☒	☒	☒	☒
2	Enabled	☒	☒	☒	☒	☒	☒
3	Disabled	☐	☒	☒	☒	☒	☒

PoE alive check configuration

The industrial managed switch can be configured to monitor a connected PD's status in real-time via ping action. After the PD stops working and does not respond, the industrial managed switch restarts PoE port power so that the PD is once again recognized and working.

Configure PD alive check on the PD Ping Alive Check page.

PD Ping Alive Check

Port	Mode	Ping PD IP Address	Interval Time(10~300s)	Retry Count(1~5)	Action	Reboot Time(30~180s)	
*	<All> ▼	0.0.0.0		30	2	<All> ▼	90
1	Disable ▼	0.0.0.0		30	2	None ▼	90
2	Disable ▼	0.0.0.0		30	2	None ▼	90
3	Disable ▼	0.0.0.0		30	2	None ▼	90
4	Disable ▼	0.0.0.0		30	2	None ▼	90
5	Disable ▼	0.0.0.0		30	2	None ▼	90
6	Disable ▼	0.0.0.0		30	2	None ▼	90
7	Disable ▼	0.0.0.0		30	2	None ▼	90
8	Disable ▼	0.0.0.0		30	2	None ▼	90
9	Disable ▼	0.0.0.0		30	2	None ▼	90
10	Disable ▼	0.0.0.0		30	2	None ▼	90
11	Disable ▼	0.0.0.0		30	2	None ▼	90
12	Disable ▼	0.0.0.0		30	2	None ▼	90
13	Disable ▼	0.0.0.0		30	2	None ▼	90
14	Disable ▼	0.0.0.0		30	2	None ▼	90
15	Disable ▼	0.0.0.0		30	2	None ▼	90
16	Disable ▼	0.0.0.0		30	2	None ▼	90
17	Disable ▼	0.0.0.0		30	2	None ▼	90
18	Disable ▼	0.0.0.0		30	2	None ▼	90
19	Disable ▼	0.0.0.0		30	2	None ▼	90
20	Disable ▼	0.0.0.0		30	2	None ▼	90
21	Disable ▼	0.0.0.0		30	2	None ▼	90
22	Disable ▼	0.0.0.0		30	2	None ▼	90
23	Disable ▼	0.0.0.0		30	2	None ▼	90
24	Disable ▼	0.0.0.0		30	2	None ▼	90

The page includes the following fields:

Object	Description
Mode	Enables/disables the per port PD alive check function. All ports are disabled by default.
Ping PD IP Address	Set the PoE device IP address in this field. The PD's IP address must be set to the same network segment as the industrial managed switch.
Interval Time (10~300s)	Set the length of time a ping request should be issued to the PD. Interval time range is from 10 to 300 seconds.
Retry Count (1~5)	Set the number of times that system retry pings to the PD. For example, if the count is set to 2, and the system retries pings to the PD and the PD doesn't respond continuously, the PoE port will be reset.
Action	Set the action to be applied if the PD does not respond. Action selections are as follows: PD Reboot: The system resets the PoE port that connected the PD. Reboot & Alarm: The system resets the PoE port and issues an alarm message via syslog, SMTP. Alarm: The system issues an alarm message via syslog, SMTP.
Reboot Time (30~180s)	Set the PoE device rebooting time. This is useful due to the different rebooting time of PoE devices. The PD alive check is not a defining standard, so the PoE device doesn't report reboot complete information to the industrial managed switch. As a result, the user must ensure how long the PD reboot takes, and then set the time value in this column.

Object	Description
	The system checks the PD again according to the reboot time. If you cannot determine the precise booting time, we suggest set it to a longer time.

Buttons

- Click **Apply** to apply changes.
- Click **Reset** to undo any changes made locally and revert to previously saved values.

Port identification

Configure each port response time for TruVision Navigator in the port identification Configuration page.

Configuration

Discovery Response Time (1-9). Sec

Port	Device type
1	Other ▼
2	Other ▼
3	Other ▼
4	Other ▼
5	Other ▼
6	Other ▼
7	Other ▼
8	Other ▼
9	Other ▼
10	Other ▼
11	Other ▼
12	Other ▼
13	Other ▼
14	Other ▼
15	Other ▼
16	Other ▼
17	Other ▼
18	Other ▼
19	Other ▼
20	Other ▼
21	Other ▼
22	Other ▼
23	Other ▼
24	Other ▼

Chapter 5

Switch operation

Address table

The industrial managed switch is implemented with an address table. This address table is composed of many entries. Each entry is used to store the address information of some node in network, including MAC address, port number, etc. This information comes from the learning process of the industrial managed switch.

Learning

When one packet comes in from any port, the industrial managed switch records the source address, port number, and the other related information in the address table. This information will be used to decide either forwarding or filtering for future packets.

Forwarding and filtering

When one packet comes from a port of the industrial managed switch, it checks the destination address as well as the source address learning. The industrial managed switch will look up the address table for the destination address. If not found, this packet will be forwarded to all the other ports except the port that this packet comes from. These ports will transmit this packet to the network it is connected to. If found, and the destination address is located at a different port from the one this packet comes from, the industrial managed switch will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port that this packet comes in, then this packet will be filtered, thereby increasing the network throughput and availability.

Store-and-forward

Store-and-Forward is a packet-forwarding technique. A Store-and-Forward switch stores the incoming frame in an internal buffer and completes error checking before

transmission. Therefore, no erroneous packets will occur, making it the best choice when a network needs efficiency and stability.

The industrial managed switch scans the destination address from the packet header and searches the routing table provided for the incoming port and forwards the packet if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. However, the switch is most commonly used to segment existing hubs, which nearly always improves the overall performance. Ethernet switching can be easily configured in any Ethernet network environment to significantly boost bandwidth using conventional cabling and adapters.

Owing to the learning function of the industrial managed switch, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain and reduces the overall load on the network.

The industrial managed switch performs Store-and-Forward, preventing erroneous packets and reducing the re-transmission rate. No packet loss will occur.

Auto-negotiation

The STP ports on the industrial managed switch have built-in auto-negotiation. This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detecting the modes and speeds of both devices that are connected. Both the 10BASE-T and 100BASE-TX devices can connect with the port in either half- or full-duplex mode. 1000BASE-T can be only connected in full-duplex mode.

Chapter 6

PoE overview

What is PoE?

PoE is an abbreviation for Power over Ethernet. PoE technology permits a system to pass data and electrical power safely on an Ethernet UTP cable. The IEEE standard for PoE technology requires a category 5 cable or higher for high power PoE levels, but can operate with a category 3 cable for low power levels. Power is supplied in common mode over two or more of the differential pairs of wires found in Ethernet cables and comes from a power supply within a PoE-enabled networking device such as an Ethernet switch or can be injected into a cable run with a mid-span power supply.

The original IEEE 802.3af-2003 PoE standard provides up to 15.4 W of DC power (minimum 44 VDC and 350 mA) to each device. Only 12.95 W is assured to be available at the powered device as some power dissipates in the cable. The updated IEEE 802.3at-2009 PoE standard, also known as PoE+ or PoE plus, provides up to 25.5 W of power. The 2009 standard prohibits a powered device from using all four pairs for power. The 802.3af/802.3at standards define two types of source equipment:

Mid-Span – A mid-span device is placed between a legacy switch and the powered device (PD). Mid-span taps the unused wire pairs 4/5 and 7/8 to carry power. The other four pairs are for data transmission.

End-Span – An end-span device connects directly to the PD. End-span taps the 1/2 and 3/6 wire pairs.

PoE system architecture

The PoE specification typically requires two devices: the Powered Source Equipment (PSE) and the PD. The PSE is either an end-span or a mid-span, while the PD is a PoE-enabled terminal such as an IP phone, Wireless LAN, etc. Power can be delivered over data pairs or spare pairs of standard CAT-5 cabling.

Powered Source Equipment (PSE)

A PSE is a device such as a switch that provides (sources) power on the Ethernet cable. The maximum allowed continuous output power per cable in IEEE 802.3af is

15.40 W. A later specification, IEEE 802.3at, offers 25.50 W. When the device is a switch, it is commonly called an end-span, although IEEE 802.3af refers to it as endpoint. Otherwise, if it's an intermediary device between a non PoE capable switch and a PoE device, it's called a mid-span. An external PoE injector is a mid-span device.

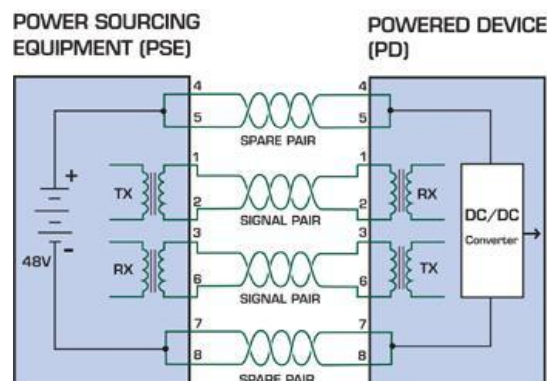
Powered Device (PD)

A PD is a device powered by a PSE and thus consumes energy. Examples include wireless access points, IP phones, and IP cameras. Many powered devices have an auxiliary power connector for an optional external power supply. Depending on the PD design, some, none, or all power can be supplied from the auxiliary port, with the auxiliary port sometimes acting as backup power in case of PoE-supplied power failure.

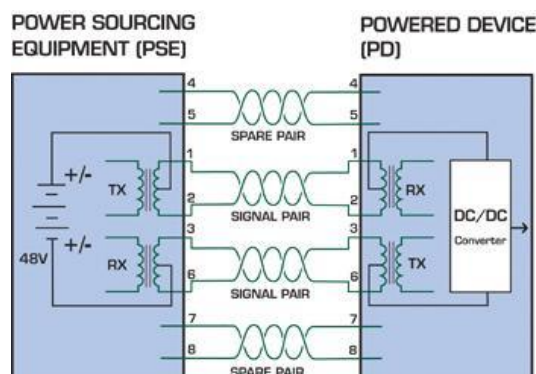
How power is transferred through the cable

A standard CAT5 Ethernet cable has four twisted pairs, but only two of these are used for 10BASE-T and 100BASE-TX. The specification allows two options for using these cables for power.

The spare pairs are used. The diagram below shows the pair on pins 4 and 5 connected together and forming the positive supply, and the pair on pins 7 and 8 connected together and forming the negative supply. (either polarity can be used).



The data pairs are used. Since Ethernet pairs are transformer-coupled at each end, it is possible to apply DC power to the center tap of the isolation transformer without interrupting the data transfer. In this mode of operation, the pair on pins 3 and 6 and the pair on pins 1 and 2 can be of either polarity.



Chapter 7

Troubleshooting

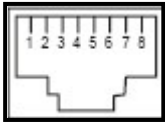
This chapter contains information to help you solve issues. If the industrial managed switch is not functioning properly, ensure that it was set up according to the instructions in this manual.

Issue	Solution
The link LED does not illuminate	Check the cable connection and remove duplex mode of the industrial managed switch.
Some stations cannot talk to other stations located on the other port.	Check the VLAN settings, trunk settings, or port enabled/disabled status.
Poor performance	Check the full duplex status of the industrial managed switch. If the industrial managed switch is set to full duplex and the partner is set to half duplex, then the performance will be poor. Also check the in/out rate of the port.
The industrial managed switch doesn't connect to the network	1. Check the LNK/ACT LED on the industrial managed switch. 2. Try another port on the industrial managed switch. 3. Make sure the cable is installed properly. 4. Make sure the cable is the right type. 5. Turn off the power. After a while, turn on power again.
The 1000BASE-T port link LED illuminates, but the traffic is irregular	Check that the attached device is not set to dedicate full duplex. Some devices use a physical or software switch to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.
The industrial managed switch does not power up.	1. Check to ensure that the AC power cord is not faulty and that it is inserted properly. 2. If the cord is inserted correctly, replace the power cord. 3. Check that the AC power source is working by connecting a different device in place of the switch. 4. If that device does not work, check the AC power

Appendix A

Networking connection

PoE RJ45 port pin assignments

	Pin Number	RJ45 Power Assignment
	1	Power +
	2	Power +
	3	Power -
	6	Power -

RJ45 port pin assignments – 1000Mbps, 1000BASE-T

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

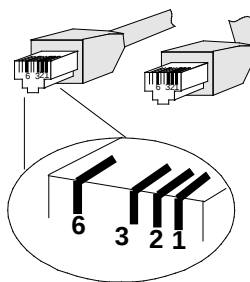
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

10/100Mbps, 10/100BASE-TX

When connecting the industrial managed switch to another Fast Ethernet switch, a bridge, or a hub, a straight or crossover cable is necessary. Each port of the industrial managed switch supports auto-MDI (Media Dependent Interface)/MDI-X (Media Dependent Interface Cross) detection. This makes it possible to directly connect the industrial managed switch to any Ethernet device without making a crossover cable. The following table and diagram show the standard RJ45 receptacle/ connector and their pin assignments.

Pin number	MDI	MDI-X
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5		Not used
6	Rx + (receive)	Tx + (transmit)
7, 8		Not used

The standard RJ45 receptacle/connector:



There are eight wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and the color of the straight cable and crossover cable connection:

Straight Cable		SIDE 1	SIDE 2
	SIDE 1	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown
	SIDE 2		
Crossover Cable		SIDE 1	SIDE 2
	SIDE 1	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown	1 = White / Green 2 = Green 3 = White / Orange 4 = Blue 5 = White / Blue 6 = Orange 7 = White / Brown 8 = Brown
	SIDE 2		

Ensure that connected cables are with the same pin assignment and color as the above diagram before deploying the cables into the network.

Glossary

A

ACE	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). ACE also contains many detailed, different parameter options that are available for individual application.
ACL	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 if there are specific traffic object access rights. 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. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are three web pages associated with the manual ACL configuration:

Access Control List (ACL): The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). The table is empty by default. 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, one 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" web page. There are number of parameters that can be configured with an ACE. Read the web page help text to obtain further information for each of them. The maximum number of ACEs is 64.

ACL Port Configuration: The ACL ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic policy is created under the "Access Control List" page. You can 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 getting matched, however. 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: This page can be used to configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per second. The "Ports" and "Access Control List" web pages can be used to assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES	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	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 preferred media.
APS	Automatic Protection Switching. This protocol is used to secure that switching is done bidirectionally 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.
ARP	Address Resolution Protocol. It is a protocol 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 address of its neighbors is 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	Continuity Check. This is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.
CCM	Continuity Check Message. This is an OAM frame transmitted from a MEP to its peer MEP and used to implement CC functionality.
CDP	Cisco Discovery Protocol

D

DEI	Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.
DES	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	Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network. DHCP is 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 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 DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from 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 is 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 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 to the DHCP relay agent's MAC address.
DHCP Snooping	DHCP snooping is used to block an intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet into a legitimate conversation between the DHCP client and server.
DNS	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	Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting network sites or a 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.
DSCP	Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

E

EEE	Energy Efficient Ethernet as defined in IEEE 802.3az.
EPS	Ethernet Protection Switching as defined in ITU/T G.8031.

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.
---------------	---

F

FTP	File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.
-----	--

Fast Leave	IGMP snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is 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.
------------	--

H

HTTP	Hypertext Transfer Protocol. It is a protocol that 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, entering a URL in a browser 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	Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection. HTTPS provides 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 the use of 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.
-------	---

I

ICMP	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	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.
IMAP	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 IMAP 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 email messages on the server rather than downloading them to a computer. To remove your messages from the server, use the mail client to generate local folders, copy messages to the local hard drive, and then delete and expunge the messages from the server.

IP	Internet Protocol. It is a protocol used for communicating data across a internet network. IP is a "best effort" system, which means that no packet of information sent over it 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 IP address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network. The most widely used version of the Internet protocol is IPv4, which has 32-bit IP addresses allowing for over four billion unique addresses. There is a substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bit IP 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	IP MultiCast
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.

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.
LLDP	Link Layer Discovery Protocol is an IEEE 802.1ab standard protocol. The LLDP specified in this standard allows stations attached to an IEEE 802 LAN to advertise to other stations attached to the same IEEE 802 LAN the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station's 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 extendstion of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).
LOC	LOC is an acronym for Loss Of Connectivity and is detected by a MEP and indicates 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), that 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	Message-Digest algorithm 5. MD5 is a message digest algorithm using 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	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.
MVR	Multicast VLAN Registration. It 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.

N

NAS	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	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 provides each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, as well as the session and transport services described in the Open Systems Interconnection (OSI) model.
NFS	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	Network Time Protocol. A network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as the transport layer.

O

OAM	Operation Administration and Maintenance. It is a protocol described in ITU-T Y.1731 used to implement carrier Ethernet functionality. MEP functionality like CC and RDI is based on this.
Optional TLVs	A LLDP frame contains multiple TLVs For some TLVs it is configurable if the switch includes the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled, the corresponding information is not included in the LLDP frame.
OUI	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 that forms the first 24 bits of a MAC address.

P

PCP	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.
PD	Powered Device. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.
PHY	Physical Interface Transceiver. It is the device that implements 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 email 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 email and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send email with SMTP, and a mail handler receives it on the recipient's behalf. Then, the mail is read using POP or IMAP.
PPPoE	Point-to-Point Protocol over Ethernet. It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames (Wikipedia). It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks.
Private VLAN	In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.
PTP	Precision Time Protocol. A network protocol for synchronizing the clocks of computer systems.

Q

QCE	QoS Control Entry. It describes the QoS class associated with a particular QCE ID. There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of four different QoS classes: "Low", "Normal," "Medium," and "High" for individual application.
-----	--

QCL	QoS Control List. It is the list table of QCEs, containing QoS control entries that classify a specific QoS class on specific traffic objects. Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.
QL	QL In SyncE 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	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, and QoS can help to provide this.
QoS Class	Every incoming frame is classified to a QoS class, 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 QoS class. There is a one to one mapping between QoS class, queue, and priority. A QoS class of 0 (zero) has the lowest priority.

R

RARP	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	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 to and use a network service.
RDI	Remote Defect Indication. It is a OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP.
Router Port	A router port is a port on the Ethernet switch that connects it to the Layer 3 multicast device.
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 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 and most common Unix platforms. Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".
SHA	SHA is an acronym for Secure Hash Algorithm. It 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	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	SubNetwork Access Protocol (SNAP). It is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, 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	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	Simple Network Time Protocol. A network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as a transport layer.
SPROUT	Stack Protocol using Routing Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform the shortest path forwarding within the stack.

SSID	Service Set Identifier. It 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.
SSH	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.
SSM	SSM In SyncE is an abbreviation for Synchronization Status Message and contains 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 obsoleted by RSTP.
SyncE	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

TACACS+	Terminal Access Controller Access Control System Plus. It is a networking protocol that 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.
Tag Priority	Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.
TCP	Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange 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 email 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), email, and File Transfer Protocol (FTP).

TELNET	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	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 provides directory service and security features.
ToS	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 six 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	Type Length Value. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as a TLV.
TKIP	Temporal Key Integrity Protocol. It is 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.

U

UDP	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 doesn't 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	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 that stores the priority level for the 802.1Q frame.

V

VLAN	Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications: VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags. VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames. Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.
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, QoS-related configuration for voice data can be performed, ensuring the transmission priority of voice traffic and voice quality.

W

WEP	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, WEP was intended to provide data confidentiality comparable to that of a traditional wired network (Wikipedia).
Wi-Fi	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	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	Wi-Fi Protected Access - Pre Shared Key. WPA was designed to enhance the security of wireless networks. There are two types 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 a 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.
WPA-Radius	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.
WPS	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.
WRED	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 DP level is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.
WTR	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.