







NS3562-8P-2S User Manual

Copyright	© 2019 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 NS3562-8P-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	<p>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.</p> <p>For more information on warranty disclaimers and product safety information, please check www.firesecurityproducts.com/policy/product-warning/ or scan the following code:</p>
	
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	4
	Product features	8
	Product specifications	11
Chapter 2	Installation	16
	Hardware description	16
	Installing the industrial managed switch	20
	Cabling	22
Chapter 3	Switch management	28
	Requirements	28
	Management access overview	28
	Web management	29
	SNMP-based network management	30
	Smart discovery utility	30
Chapter 4	Web configuration	32
	Main web page	33
	System	37
	Port management	57
	Link aggregation	69
	VLAN	77
	Spanning Tree Protocol (STP)	99
	Multicast	112
	Quality of Service (QoS)	130
	Security	139
	Access Control Lists (ACL)	174
	MAC address table	185
	LLDP	187
	Diagnostics	198
	RMON	202
	Power over Ethernet (PoE)	209
	Maintenance	217
Chapter 5	Switch operation	221
	Address table	221
	Learning	221
	Forwarding and filtering	221
	Store-and-forward	221
	Auto-negotiation	222

Chapter 6	PoE overview 223
	What is PoE? 223
	PoE system architecture 223
Chapter 7	Troubleshooting 225
Appendix A	Networking connection 226
	Glossary 228

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 NS3562-8P-2S model is as follows:

- Industrial L2+ 8-port 10/100/1000T 802.3at PoE+
- + 2-port 100/1000X SFP wall-mount managed switch

Unless specified, the term “industrial managed switch” mentioned in this user manual refers to the NS3562-8P-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
- 3-pin terminal block connector × 1
- DIN rail kit × 1
- Wall mounting kit × 1
- Magnet kit × 1
- SFP dust-proof cap × 2
- RJ45 dust-proof cap × 8

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

Easily deployed and expanded network

Designed to be installed in a wall enclosure or simply mounted on a wall in any convenient location, this innovative, wall-mount industrial managed Gigabit Ethernet

switch offers IPv6/IPv4 dual stack management, intelligent Layer 2 management functions, and a user-friendly interface. The IFS managed series is able to operate reliably, stably, and quietly in any environment without affecting its performance. Featuring ultra networking speed and an operating temperature ranging from -40 to 75°C in a compact but rugged IP30 metal housing, the IFS managed series is an ideal solution to meeting the demand for the following network applications:

- Building/Home automation network
- Internet of things (IoT)
- IP surveillance
- Wireless LAN

Innovative wall-mount installation

The IFS managed series is specially designed to be installed in a narrow environment, such as wall enclosure or electric weak box. The compact, flat, and wall-mounted design fits easily in any space-limited location. It adopts the user-friendly “Front Access” design, making the installing, cable wiring, LED monitoring, and maintenance of the wall-mount managed switch placed in an enclosure convenient for technicians. The IFS managed series can be installed by fixed wall mounting, magnetic wall mounting, or DIN rail, thereby making its usability more flexible.

IPv6/IPv4 dual stack

Supporting both IPv6 and IPv4 protocols, the industrial managed switch helps SMBs to step into the IPv6 era with a low investment as its network facilities need not be replaced or overhauled with the setup of IPv6 FTTx edge networks.

Robust layer 2 features

The industrial managed switch can be programmed for advanced switch management functions such as dynamic port link aggregation, 802.1Q VLAN and Q-in-Q VLAN, Multiple Spanning Tree Protocol (MSTP), Loop and BPDU Guard, and IGMP / MLD snooping. The industrial managed switch allows the operation of a high-speed trunk combining multiple ports such as a 16 Gbps fat pipe, and also supports fail-over. Also, the Link Layer Discovery Protocol (LLDP) is the Layer 2 protocol included to help discover basic information about neighboring devices on the local broadcast domain.



Efficient traffic control

The IFS managed series is loaded with robust QoS features and powerful traffic management to enhance services to business-class data, voice, and video solutions. The functionality includes broadcast / multicast storm control, per port bandwidth control, IP DSCP QoS priority, and remarking. It guarantees the best performance for VoIP and video stream transmission, and empowers enterprises to take full advantage of limited network resources.

Powerful security

The industrial switches offer comprehensive layer 2 to layer 4 access control list (ACL) for enforcing security to the edge. It can be used to restrict to network access by denying packets based on source and destination IP address, TCP/UDP port number, or defined typical network applications. Its protection mechanism also comprises 802.1X port-based user and device authentication, which can be deployed with RADIUS to ensure the port level security and block illegal users. With the Protected Port function, communication between edge ports can be prevented to guarantee user privacy. Furthermore, the Port Security function allows limiting the number of network devices on a given port.

Efficient management

For efficient management, the industrial managed switches are equipped with console, web, and SNMP management interfaces. With the built-in web-based management interface, the managed industrial switch offers an easy-to-use, platform-independent management and configuration facility. It supports standard Simple Network Management Protocol (SNMP) and can be managed by any management software. For text-based management mode, the industrial managed switch can be accessed via Telnet and the console port. Moreover, the industrial managed switches offer secure management remotely by supporting SSH, SSL, and SNMP v3 connections where the packet content can be encrypted at each session.

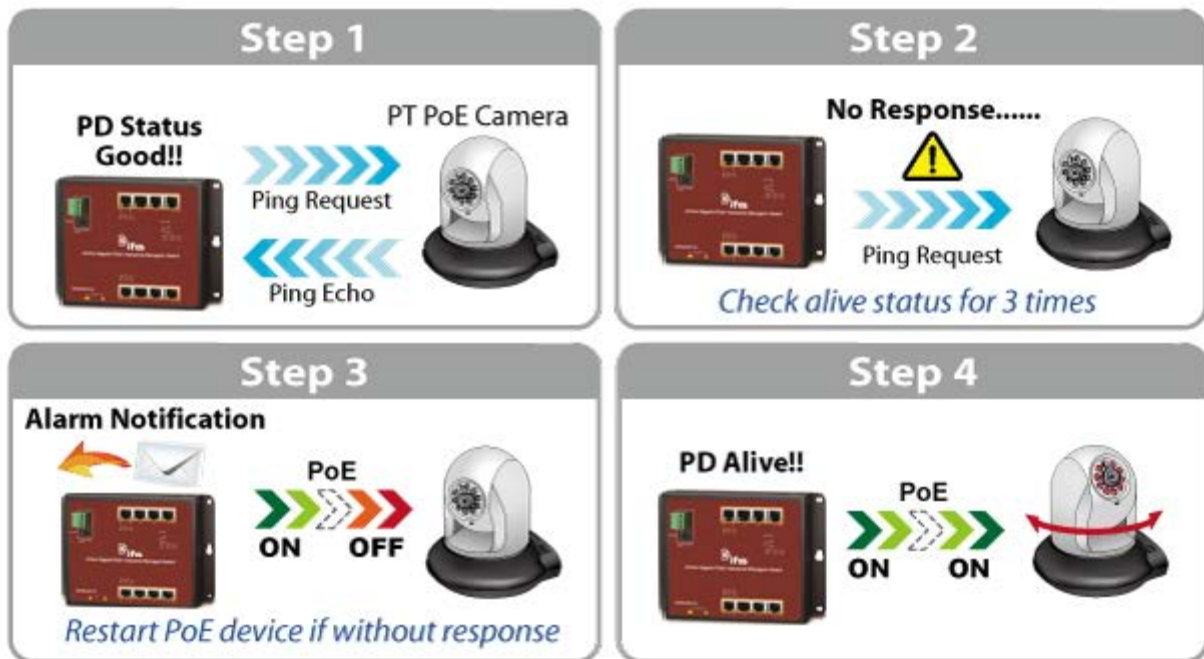
Built-in unique PoE functions for powered devices management

As a managed PoE switch for surveillance, wireless, and VoIP networks, the IFS PoE managed series features special PoE management functions:

- PD alive check
- Scheduled power recycling
- PoE schedule
- PoE usage monitoring

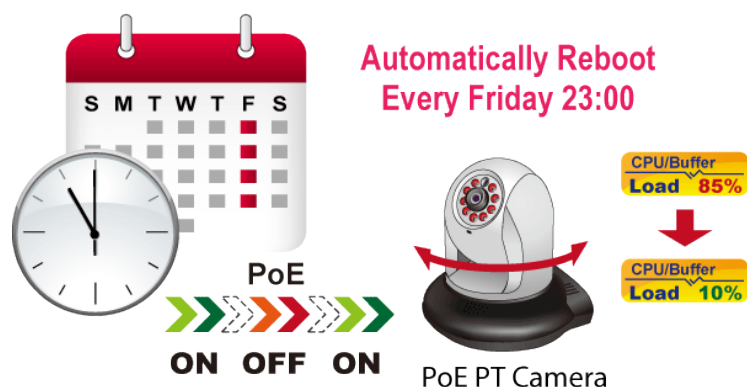
Intelligent powered device alive check

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.



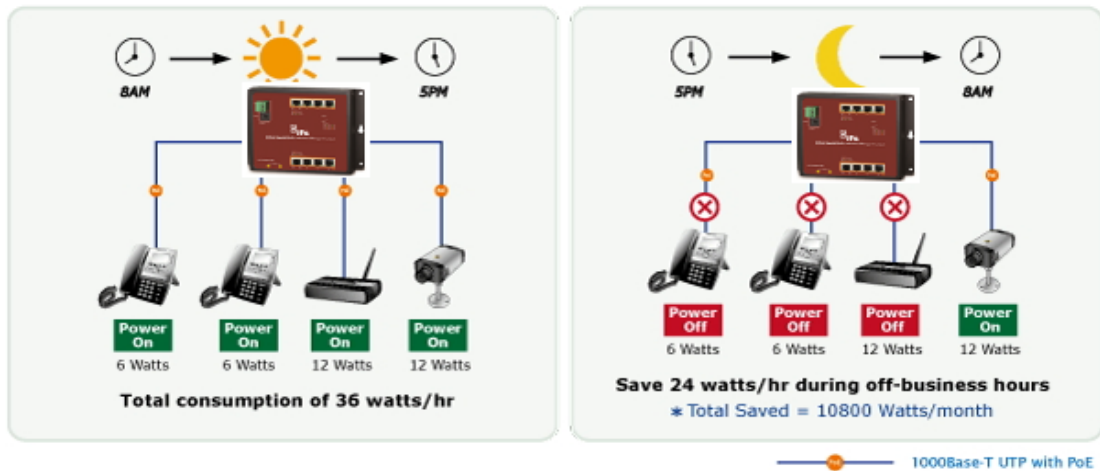
Scheduled power recycling

The IFS PoE managed series allows each of the connected PoE IP cameras or PoE wireless access points to reboot at a specific time each week. This reduces the chance of an IP camera or AP crash resulting from buffer overflow.



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. It also increases security by powering off PDs that should not be in use during non-business hours.



PoE usage monitoring

Via the power usage chart in the web management interface, the IFS PoE managed series enables the administrator to monitor the status of the power usage of the connected PDs in real time. Thus, it greatly enhances the management efficiency of the facilities..

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 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.

Product features

Physical port

- 10/100/1000BASE-T gigabit RJ45 copper
- 100/1000BASE-X mini-GBIC/SFP slots

Power over Ethernet

- Complies with IEEE 802.3at High Power over Ethernet end-span/mid-span PSE.
- Complies with IEEE 802.3af Power over Ethernet end-span PSE.
- IEEE 802.3af/IEEE 802.3at devices powered.
- Supports PoE power up to 36 W for each PoE port.

- 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 port power feeding priority
 - Per PoE port power limitation
 - PD classification detection
- Intelligent PoE features:
 - PD alive check
 - PoE schedule

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
- Provider bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
- Private VLAN
- Protocol-based VLAN
- MAC-based VLAN
- Voice VLAN
- Management VLAN
- GVRP

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)
- Loop protection to avoid broadcast loops

Quality of Service

- Ingress shaper and egress rate limit per port bandwidth control
- Storm control support
 - Broadcast/unknown unicast/unknown multicast
- Traffic classification:
 - IEEE 802.1p CoS
 - TOS / DSCP / IP Precedence of IPv4/IPv6 packets
- Strict priority and Weighted Round Robin (WRR) CoS policies

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

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)
 - 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
- 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)
- BOOTP and DHCP for IP address assignment
- User privilege levels control
- Link Layer Discovery Protocol (LLDP) and LLDP-MED
- Smart discovery utility for deploy management
- SNMP trap for interface Link Up and Link Down notification
- Smart fan with speed control
- Cable diagnostics
- Event message logging to remote Syslog server

Product specifications

Hardware Specifications	
Copper Ports	Eight 10/100/1000BASE-T RJ45 auto-MDI/MDI-X ports
SFP+ Slots	Two 100/1000BASE-X SFP interfaces Supports 100/1000Mbps dual mode and DDM
PoE Injector Ports	Eight ports with 802.3at/af PoE injector function (Port-1 to Port-8)
Switch Architecture	Store-and-Forward
Switch Fabric	20 Gbps / non-blocking
Throughput	14.8 Mpps @ 64 bytes
Address Table	8K entries
Shared Data Buffer	4.1 Mbits

Flow Control	IEEE 802.3x pause frame for full-duplex Back pressure for half-duplex
Jumbo Frame	10 Kb
Reset Button	< 5 seconds: System reboot > 5 seconds: Factory Default
Enclosure	Metal
Installation	DIN rail kit, wall-mount, and magnetic wall mount
Dimensions (WxDxH)	178 x 25 x 134 mm
Weight	640 g
Connector	Removable 3-pin terminal block for power input - Pin 1/2 for Power (Pin 1: V+ / Pin 2: V-) - Pin 3 for earth ground DC power jack with 2.0 mm central pole
LED	System: Power (Green) PoE Ports: PoE-in-Use (Orange) LNK/ACT (Green) LAN Port: 100 LNK/ACT (Orange) 1000 LNK/ACT (Green)
Power Requirement	48~56 VDC, 5A (max.) terminal block power input 48~56 DC, 5A (max.) DC jack power input Note: These two power input interfaces don't support the power redundant feature.
Power Consumption	Max 210 W / 716 BTU
ESD Protection	Contact discharge: 6K VDC Air discharge: 8K VDC
Power Over Ethernet	

PoE Standard	IEEE 802.3af/IEEE 802.3at Power over Ethernet/PSE
PoE Power Supply Type	End-span
PoE Power Output	IEEE 802.3af Standard - Per port 48–56 VDC (depending on the power supply), max. 15.4 W IEEE 802.3at Standard - Per port 50–56 VDC (depending on the power supply), max. 36 W
Power Pin Assignment	1/2(+), 3/6(-)
PoE Power Budget	200 W (depending on power input)
Max. number of Class 2 PDs	8
Max. number of Class 3 PDs	8
Max. number of Class 4 PDs	7
Layer 2 Functions	
Basic Management Interfaces	Telnet; Web browser; SNMP v1, v2c Up to 256 VLAN groups, out of 4094 VLAN IDs 802.1ad Q-in-Q tunneling (VLAN stacking) Voice VLAN Protocol VLAN Private VLAN (Protected port) GVRP Management VLAN
Secure Management Interfaces	SSH, SSL, SNMP v3
Port Mirroring	TX / RX / both 1-to-1 monitor
VLAN	802.1Q tagged-based VLAN Up to 256 VLAN groups, out of 4094 VLAN IDs 802.1ad Q-in-Q tunneling (VLAN stacking) Voice VLAN Protocol VLAN Private VLAN (Protected port) GVRP Management VLAN
Link Aggregation	IEEE 802.3ad LACP/static trunk Four groups with four ports per 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 256 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
Bandwidth Control	Ingress/egress limit per port bandwidth control
Standards Conformance	
Regulation Compliance	FCC Part 15 Class A, CE
Stability Testing	IEC60068-2-32 (free fall) IEC60068-2-27 (shock) IEC60068-2-6 (vibration)
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX/100BASE-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000BASE-T 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 RFC 768 UDP RFC 793 TFTP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP version 1 RFC 2236 IGMP version 2 RFC 3376 IGMP version 3 RFC 2710 MLD version 1 FRC 3810 MLD version 2
SNMP MIBs	RFC 1213 MIB-II RFC 1215 Generic Traps RFC 1493 Bridge MIB RFC 2674 Bridge MIB Extensions RFC 2737 Entity MIB (version 2) RFC 2819 RMON (1, 2, 3, 9) RFC 2863 Interface Group MIB RFC 3635 Ethernet-like MIB
Environment	
Operating	Temperature: -40 to 75°C

	Relative Humidity: 5 to 95% (non-condensing)
Storage	Temperature: -40 to 75°C Relative Humidity: 5 to 95% (non-condensing)

Chapter 2

Installation

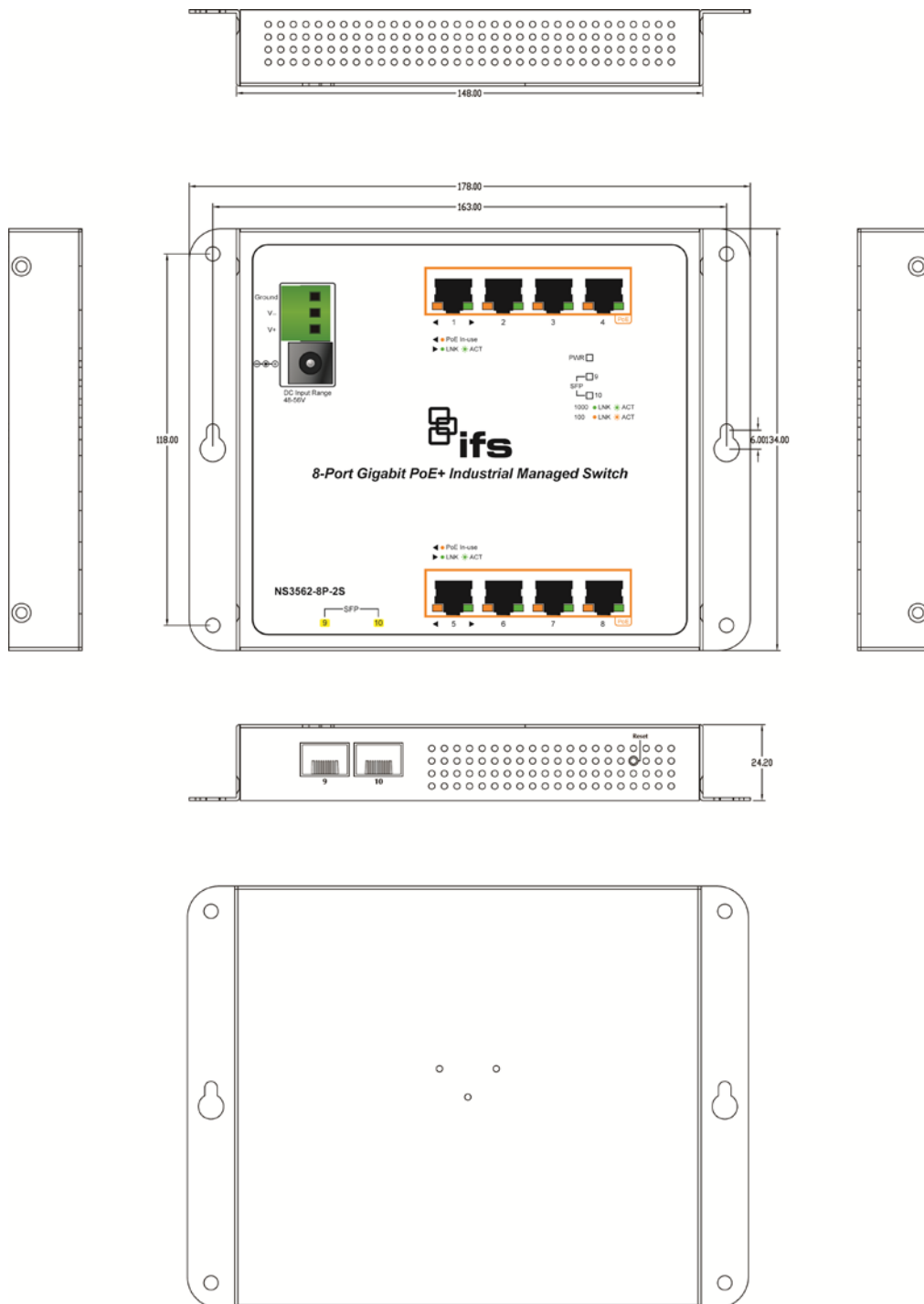
This section describes the hardware features of the industrial managed switch. For easier management and control of the industrial managed switch, familiarize yourself with its display indicators and ports. Front panel illustrations in this chapter display the unit LED indicators. Before connecting any 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): 178 x 25 x 134 mm



Dimensions (unit = 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).

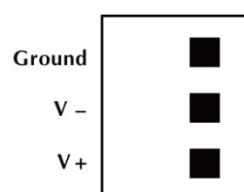
AC/DC power receptacle

The industrial managed switch features a strong dual power input system (terminal block and DC jack) incorporated into customer's automation network to enhance system reliability and uptime.

	3-pin Terminal Block	DC Jack
Power Input Range	48~56 VDC	48~56 VDC

To install the 3-pin terminal block connector on the wall-mount managed switch:

1. Insert the positive DC power wire into V+, negative DC power wire into V-, and the grounding wire into Ground.



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

Power Notice: In some areas, installing a surge suppression device may also help to protect your Managed Switch from being damaged by unregulated surge or current to the Managed Switch.

Reset button

Located on the 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
PWR	Green	Lit: indicates that the switch has power. Blinking: indicates the system of the switch is booting.

Per 10/100/1000BASE-T interfaces (Port-1 to Port-8)

LED	Color	Function
LNK/ACT	Green	Lit: indicates that the link through that port is successfully established. Blinking: indicates that the switch is actively sending or receiving data over that port.
PoE	Orange	Lit: indicates that the port is providing DC in-line power. Blinking: indicates that the connected device is not a PoE Powered Device (PD).

Per 100/1000X SFP interface (Port-9 to Port-10)

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	<p>Lit: indicates the port has successfully connected to the network at 100 Mbps.</p> <p>Blinking: indicates that the switch is actively sending or receiving data over that port.</p>

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.

Mounting

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

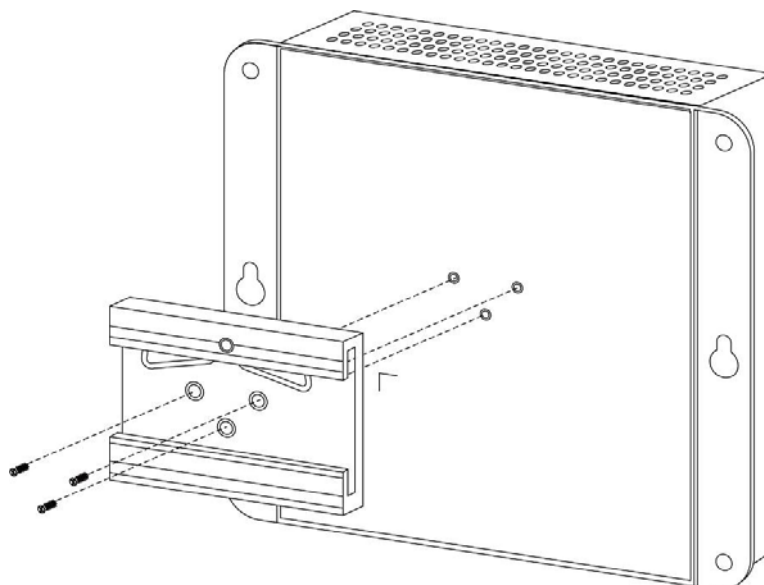
Note: Ensure that the industrial managed switch is mounted vertically with the air holes on the top and a minimum of three inches above and below the switch to allow for proper air flow. This device uses a convection flow of hot air which rises and brings cold air in from the bottom and out of the top of the device. Do not mount the switch horizontally as this does not allow air to flow up into the device and will result in damage to the switch. Do not tie DC1 to DC2. DC2 is for secondary power redundancy. Do not plug DC power into the device while the AC power cord is plugged in. This is not a hot-swappable switch. Hot-swapping this device will result in damage.

DIN-rail mounting

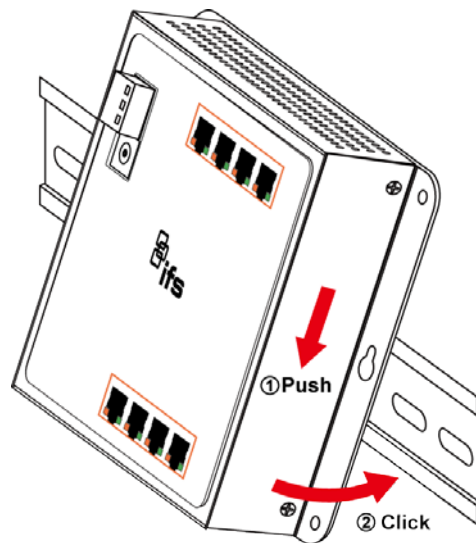
Note: Follow all the DIN-rail installation steps as shown in the example.

To install the DIN rails on the industrial managed switch:

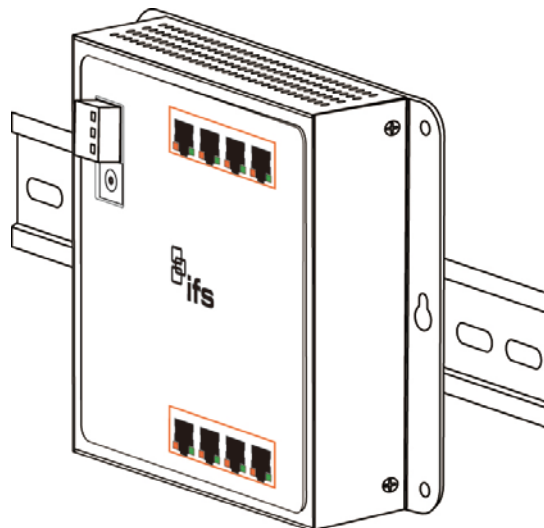
1. Screw the DIN-rail onto the industrial managed switch.



- Carefully slide the DIN-rail into the track.



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

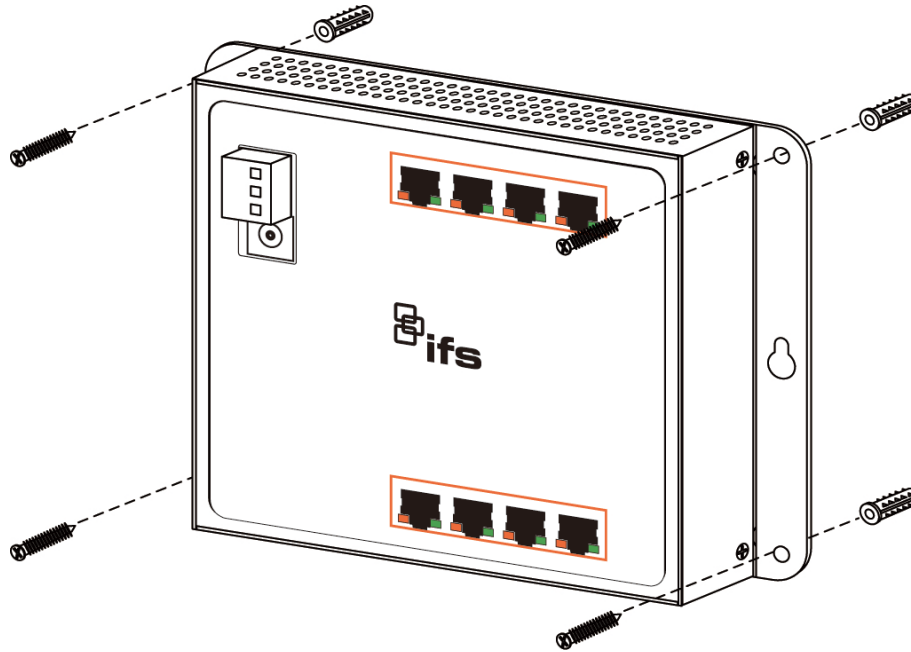


Wall mount plate mounting

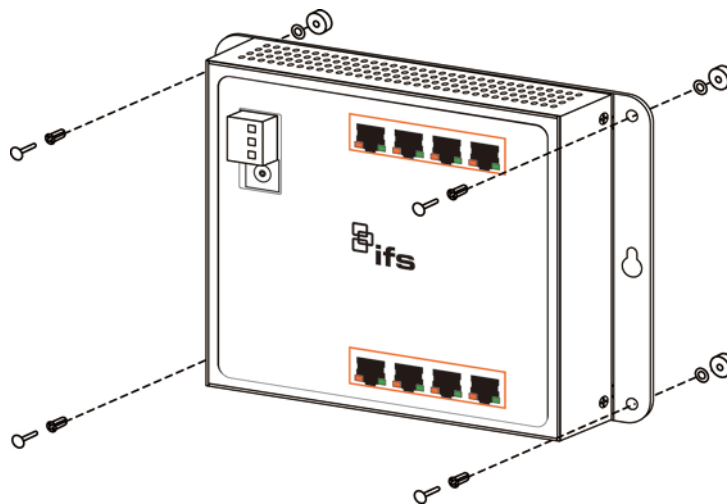
Note: Follow all the wall mount plate installation steps as shown in the example.

To install the industrial managed switch on the wall:

- Drill four 8 mm diameter holes in the wall, with a horizontal distance of 163 mm between each.
- Install a conductor pipe inside the board hole and flush the edge of the conductor pipe with the wall surface.
- Screw the bolts into the conductor pipe. The switch is between the bolts and the conductor pipe, as shown below.



To install the industrial managed switch on a magnetic surface:



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)

Part #	Fiber Connector	# of Fibers	Fiber Type	Max Distance	Wave Length	Optical Budget (dBm)	Optical Power (dBm)	Receiver Sensitivity (dBm)	Operating Temperature
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)
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									

Part #	Fiber Connector	# of Fibers	Fiber Type	Max Distance	Wave Length	Optical Budget (dBm)	Optical Power (dBm)	Receiver Sensitivity (dBm)	Operating Temperature
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:

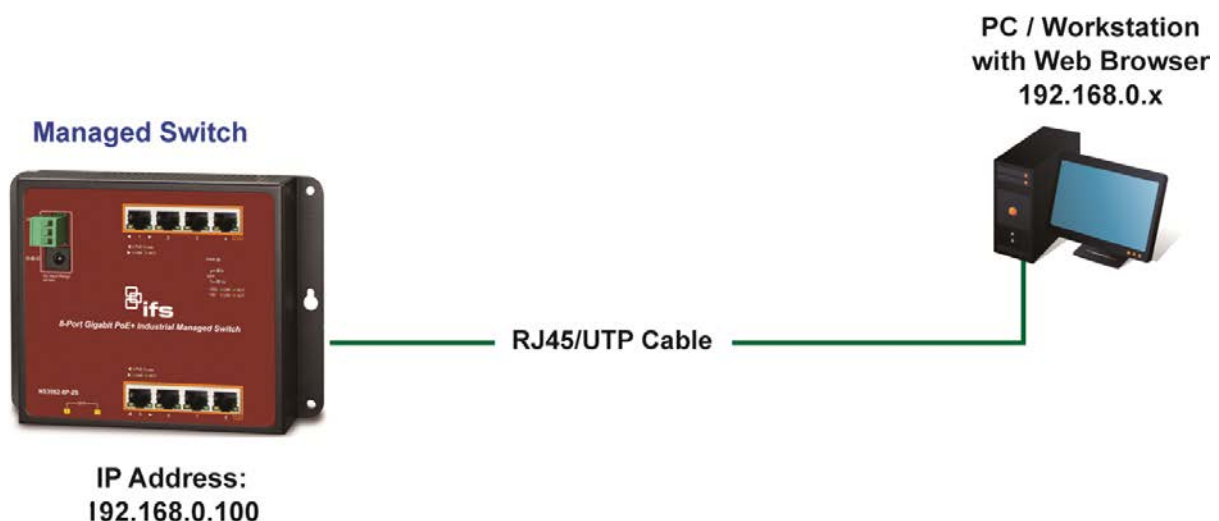
- Web browser interface
- An external SNMP-based network management application

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
Web browser	<ul style="list-style-type: none"> • Ideal for configuring the switch remotely. • Compatible with all popular browsers. • Can be accessed from any location. • Most visually appealing. 	<ul style="list-style-type: none"> • Security can be compromised (hackers need only know the IP address and subnet mask). • May encounter lag times on poor connections.
SNMP agent	<ul style="list-style-type: none"> • Communicates with switch functions at the MIB level. • Based on open standards. 	<ul style="list-style-type: none"> • 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).

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.

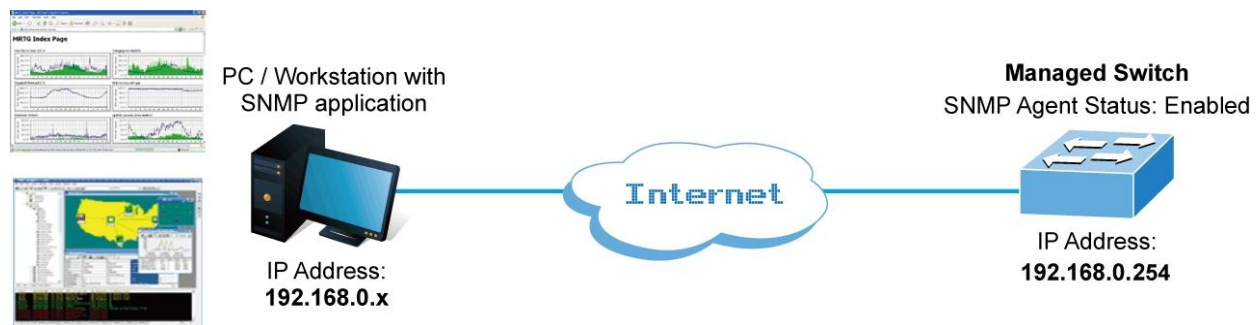


You can use a web browser to list and manage the industrial managed switch configuration parameters from one central location, just as if you were directly connected to the industrial managed switch's console port. Web management requires Microsoft Internet Explorer 11.0 or later.

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

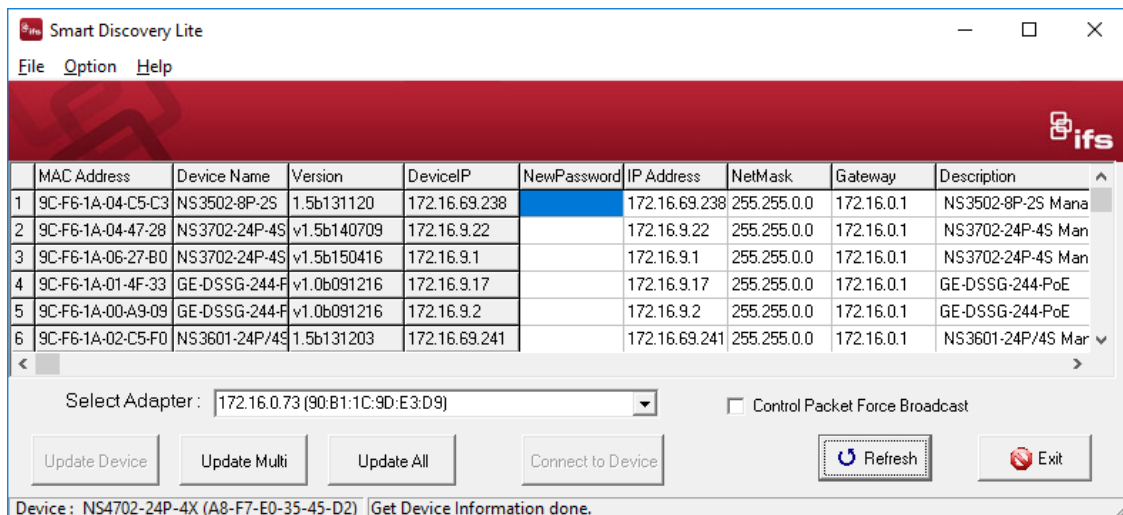
For easily listing the industrial managed switch in your Ethernet environment, the Smart Discovery utility included on the CD-ROM is an ideal solution.

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

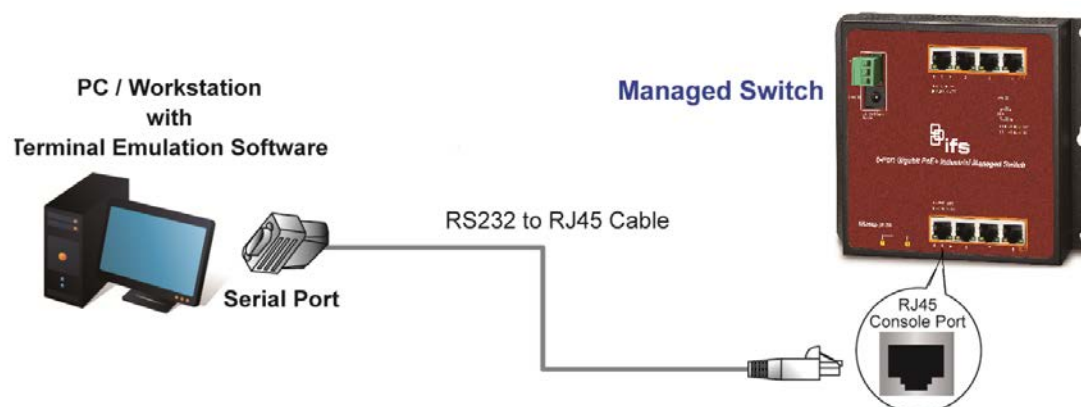
Web-based management of the industrial managed switch supports Internet Explorer 11.0 or later, and can be performed from any location on the network. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed, and present an easy viewing screen.

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.

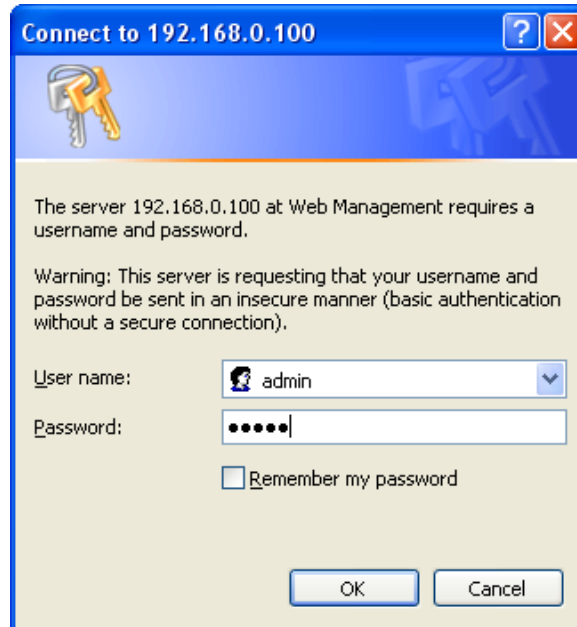
For example, if the default IP address of the industrial managed switch is 192.168.0.100, then the administrator computer should be set at 192.168.0.x (where x is a number between 1 and 254, except 100), and the default subnet mask is 255.255.255.0.

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 11.0 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
- 2. Copper port link status
- 3. SFP port link status
- 4. Main screen

Panel display

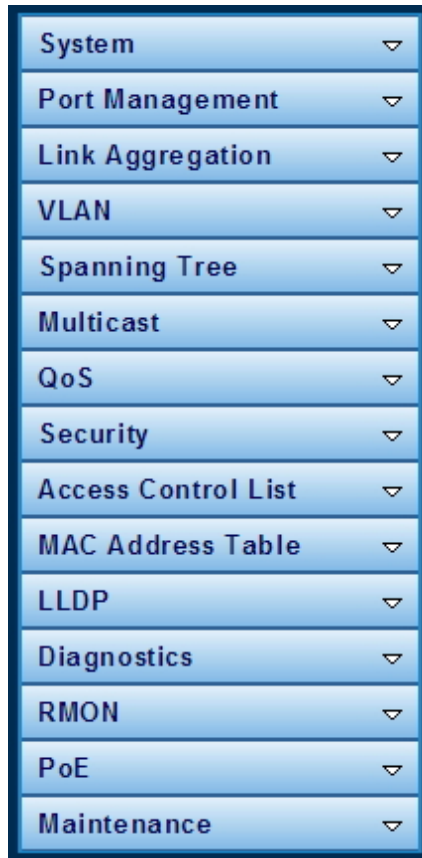
The web interface displays an image of the industrial managed switch's ports. The mode can be set to display different information for the ports, including Link up or Link down. Clicking on the image of a port opens the Port Statistics page.

Port status is indicated as follows:

State	Disabled	Down	Link	PoE in-use
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.



Buttons

Click **SAVE** to save changes or reset to default.

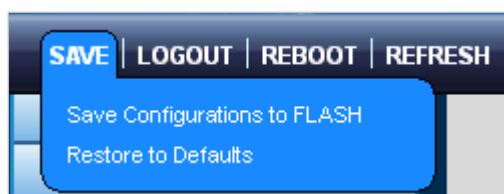
Click **LOGOUT** to logout of the managed switch.

Click **REBOOT** to reboot the managed switch.

Click **REFRESH** to refresh the page.

Save button

Click the **SAVE** button to save the running/startup/backup configuration or reset the switch to default parameters.



The page includes the following fields:

Item	Function
Save Configuration to FLASH	Saves the configuration. See xxx
Restore to Default	Resets the switch to default parameters. See xxx

Configuration manager

Save Configuration

Source File	<input checked="" type="radio"/> Running configuration <input type="radio"/> Startup configuration <input type="radio"/> Backup configuration
Destination File	<input checked="" type="radio"/> Startup configuration <input type="radio"/> Backup configuration

Apply

The page includes the following fields:

Item	Function
Running Configuration	<p>Refers to the running configuration sequence use in the switch. In the switch, the running configuration file stores in the RAM. In the current version, the running configuration sequence running-config can be saved from the RAM to FLASH by saving “Source File = Running Configuration” to “Destination File = Startup Configuration”, so that the running configuration sequence becomes the startup configuration file, which is called configuration save.</p> <p>To prevent illicit file upload and easier configuration, the switch names the running configuration file "running-config."</p>
Startup Configuration	<p>Refers to the configuration sequence used in switch startup. Startup configuration file is stored in nonvolatile storage, corresponding to the so-called configuration save. If the device supports multi-config file, name the configuration file as a .cfg file (the default is startup.cfg).</p> <p>If the device does not support multi-config files, it names the startup configuration file "startup-config."</p>
Backup Configuration	<p>The backup configuration is empty in FLASH; save the backup configuration first via Maintenance > Backup Manager.</p>

Buttons

- Click **Apply** to save the configuration.

Saving the configuration

The running configuration file stores in the managed switch’s RAM. In the current version, the running configuration sequence of running-config can be saved from the RAM to FLASH by "Save Configurations to FLASH" function, so that the running configuration sequence becomes the startup configuration file, which is called configuration save.

To save all applied changes and set the current configuration as a startup configuration requires the startup-configuration file to be loaded automatically across a system reboot.

1. Click **Save > Save Configurations to FLASH** to login to the Configuration Manager page.



2. Select Source File = **Running Configuration** and Destination File = **Startup Configuration**.

Save Configuration	
Source File	<input checked="" type="radio"/> Running configuration <input type="radio"/> Startup configuration <input type="radio"/> Backup configuration
Destination File	<input checked="" type="radio"/> Startup configuration <input type="radio"/> Backup configuration

3. Click **Apply** button to save the running configuration as a startup configuration.

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	Configure the industrial managed switch IP information on this page.
IPv6 Configuration	Configure the industrial managed switch IPv6 information on this page.
User Configuration	Configure a new user name and password on this page.
Time Settings	Configure SNTP on this page.
Log Management	The industrial managed switch system log information is provided here.
SNMP Management	Configure SNMP parameters on this page.

System information

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

Information Name	Information Value
System Name	Edit NS3562-8P-2S
System Location	Edit Default Location
System Contact	Edit Default Contact
MAC Address	09:4F:3b:1c:2b:3D
IP Address	192.168.0.109
Subnet Mask	255.255.255.0
Gateway	192.168.0.254
Loader Version	1.0.0.48161
Loader Date	Jan 15 2016 - 10:11:50
Firmware Version	V1.5b160519
Firmware Date	May 19 2016 - 15:29:23
System Object ID	1.3.6.1.4.1.26769.9.32
System Up Time	1 days, 20 hours, 57 mins, 29 secs

The page includes the following fields:

Item	Function
System Contact	The system contact configured in System Information.
System Name	The system name configured in System Information.
System Location	The system location configured in System Information.
MAC Address	The MAC Address of this industrial managed switch.
IP Address	The IP Address of this industrial managed switch.
Subnet Mask	The subnet mask of this industrial managed switch.
Gateway	The gateway of this industrial managed switch.
Loader Version	The loader version of this industrial managed switch.
Loader Date	The loader date of this industrial managed switch.
Firmware Version	The firmware version of this industrial managed switch.
Firmware Date	The firmware date of this industrial managed switch.
System Object ID	The system object ID of this industrial managed switch.
System Uptime	The period of time the device has been operational.

Buttons

- Click **Edit** to edit a parameter.

IP configuration

This page includes the IP address, subnet mask, and gateway. The configured column is used to view or change the IP configuration. Type in the IP address, subnet mask, and gateway as necessary.

IP Address Setting	
Mode	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
IP Address	<input type="text" value="192.168.0.109"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.0.254"/>
DNS Server 1	<input type="text" value="8.8.8.8"/>
DNS Server 2	<input type="text" value="8.8.8.8"/>

The page includes the following fields:

Item	Function
Mode	Indicates the IP address mode operation. Possible modes are: Static: Enables 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. DHCP: Enables DHCP client mode operation. Enable the DHCP client by selecting this box. If DHCP fails and the configured IP address is zero, DHCP will retry. If DHCP fails and the configured IP address is not zero, DHCP will stop and the configured IP settings will be used. The DHCP client announces the configured System Name as hostname to provide DNS lookup.
IP Address	Provides the IP address of the industrial managed switch in dotted decimal notation.
Subnet Mask	Provides the subnet mask of the industrial managed switch in dotted decimal notation.
Gateway	Provides the IP address of the router in dotted decimal notation.
DNS Server 1/2	Provides the IP address of the DNS server in dotted decimal notation.

Buttons

- Click **Apply** to apply changes.

IPv6 configuration

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.

IPv6 Address Setting	
Auto Configuration	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
IPv6 Address	<input type="text" value="::"/> / <input type="text" value="0"/>
Gateway	<input type="text" value="::"/>
DHCPv6 Client	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

The page includes the following fields:

Item	Function
Auto Configuration	<p>Select Enable to enable IPv6 auto-configuration. If it fails, the configured IPv6 address is zero. The router may delay responding to a router solicitation for a few seconds; the total time needed to complete auto-configuration can be significantly longer.</p>
IPv6 Address	<p>Provide the IPv6 address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::aaf7:e0ff:fe20:fd27.</p> <p>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 the following legal IPv4 address. For example, '::192.1.2.34'.</p> <p>Provide the IPv6 Prefix of this switch. The allowed range is 1 through 128.</p>
Gateway	<p>Provide the IPv6 gateway address of this switch. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::aaf7:e0ff:fe20:fd27.</p>
DHCPv6 Client	<p>To enable this Managed Switch to accept a configuration from a Dynamic Host Configuration Protocol version 6 (DHCPv6) server. By default, the Managed Switch does not perform DHCPv6 client actions. DHCPv6 clients request the delegation of long-lived prefixes that they can push to individual local hosts.</p>

Buttons

- Click **Apply** to apply changes.

User 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:

New User

User Name	Password Type	Password	Retype Password	Privilege Type	Privilege Value
<input type="text"/>	Clear Text <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	Admin <input type="button" value="v"/>	2 <input type="button" value="v"/>

This page includes the following fields:

Object	Description
User Name	The name identifying the user. Maximum length: 32 characters; Maximum number of users: 8
Password Type	The password type for the user.
Password	Type the user's new password here. (Range: 0-32 characters plain text, case sensitive)
Retype Password	Type the user's new password here again to confirm.
Privilege Level	The privilege level of the user. Options: <ul style="list-style-type: none"> • Admin • User • Other

Buttons

- Click **Apply** to apply changes.

Local Users

User Name	Password Type	Privilege Type	Privilege Value	Modify
admin	Encrypted	Admin	15	

This page includes the following fields:

Object	Description
Username	Displays the current user name.
Password Type	Displays the current password type.
Privilege Type	Displays the current privilege type.
Modify	Click to modify the local user entry. Click Delete to delete the current user.

Time settings

System time

Configure SNTP on this page. SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. You can specify SNTP servers and set the GMT time zone in this page.

System Time Setting

Enable SNTP	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Manual Time	Year <input type="text" value="2000"/> Month <input type="text" value="Jan"/> Day <input type="text" value="1"/> Hours <input type="text" value="0"/> Minutes <input type="text" value="0"/> Seconds <input type="text" value="0"/>
Time Zone	<input type="text" value="None"/>
Daylight Saving Time	<input type="text" value="Disable"/>
Daylight Saving Time Offset	<input type="text" value="60"/> (1 - 1440) Minutes
Recurring From	Day <input type="text" value="Sun"/> Week <input type="text" value="1"/> Month <input type="text" value="Jan"/> Hours <input type="text" value="0"/> Minutes <input type="text" value="0"/>
Recurring To	Day <input type="text" value="Sun"/> Week <input type="text" value="1"/> Month <input type="text" value="Jan"/> Hours <input type="text" value="0"/> Minutes <input type="text" value="0"/>
Non-recurring From	Year <input type="text" value="2000"/> Month <input type="text" value="Jan"/> Date <input type="text" value="1"/> Hours <input type="text" value="0"/> Minutes <input type="text" value="0"/>
Non-recurring To	Year <input type="text" value="2000"/> Month <input type="text" value="Jan"/> Date <input type="text" value="1"/> Hours <input type="text" value="0"/> Minutes <input type="text" value="0"/>

This page includes the following fields:

Object	Description
Enable SNTP	Indicates the SNTP mode operation. Possible modes are: Enabled: Enable SNTP mode operation. When enabling SNTP mode operation, the agent forwards and transfers SNTP messages between the clients and the server when they are not on the same subnet domain. Disabled: Disable SNTP 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).

Object	Description
Minute	Allows the user to input minute value. (0 to 59 minutes).
Second	Allows the user to input second value. (0 to 59 seconds).
Time Zone	Lists various Time Zones worldwide. Select the appropriate Time Zone from the drop-down menu and click Save .
Daylight Saving Time	This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Select Disable to disable the Daylight Saving Time configuration. Select Recurring and configure the Daylight Saving Time duration to repeat the configuration every year. Select Non-Recurring and configure the Daylight Saving Time duration for single time configuration. (Default: Disabled).
Daylight Saving Time Offset	Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

Buttons

- Click **Apply** to apply changes.

SNTP server settings

SNTP Server Settings

SNTP Server Address	<input style="width: 150px;" type="text"/>	(X.X.X.X or Hostname)
Server Port	<input style="width: 100px;" type="text" value="123"/>	(1 - 65535 Default : 123)

This page includes the following fields:

Object	Description
SNTP Server Address	Type the IP address or domain name of the SNTP server.
Server Port	Type the port number of the SNTP.

Buttons

- Click **Apply** to apply changes.

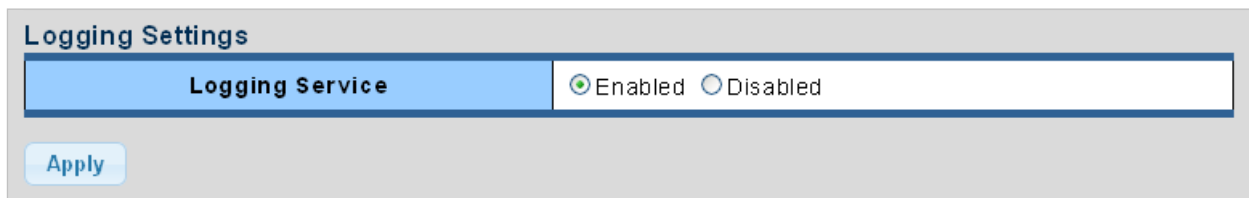
Log management

The industrial managed switch log management is provided here. The local logs permit the configuration and limiting of system messages that are logged to flash or RAM memory. The default is for event levels 0 to 3 are to be logged to flash and levels 0 to 6 are to be logged to RAM. The following table lists the event levels of the industrial managed switch:

Level	Severity Name	Description
7	Debug	Debuggin messages
6	Informational	Informational messages only.
5	Notice	Normal but significant condition, such as cold start.
4	Warning	Warning conditions (e.g., return false, unexpected return)
3	Error	Error conditions (e.g., invalid input, default used)
2	Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	Alert	Immediate action needed
0	Emergency	System unusable

Local log

The industrial managed switch local log information is provided here.

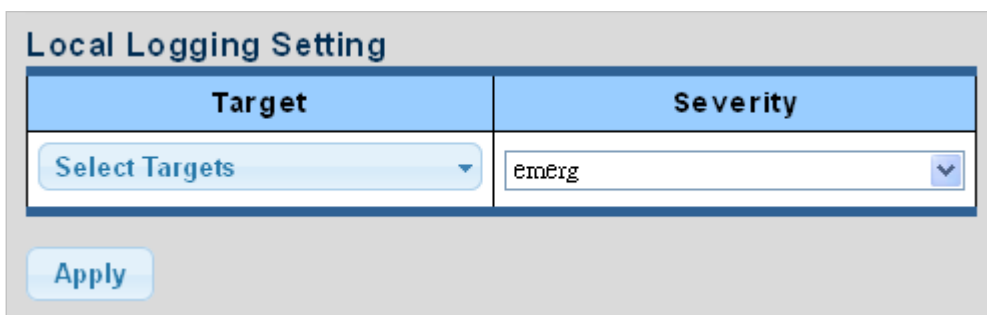


This page includes the following fields:

Object	Description
Logging Service	Enabled: Enable logging service operation. Disabled: Disable logging service operation.

Buttons

- Click **Apply** to apply changes.



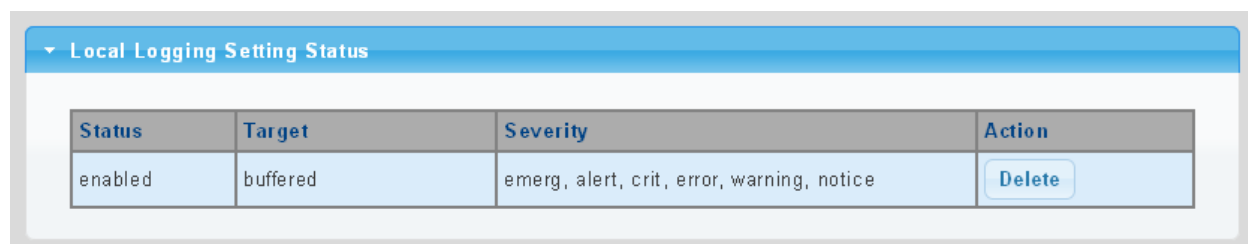
This page includes the following fields:

Object	Description
Target	The target of the local log entry. The following target types are supported: Buffered: Target the buffer of the local log. File: Target the file of the local log.

Object	Description
Severity	The severity of the local log entry. The following severity types are supported: emerg : Emergency level of the system unstable for local log. alert : Alert level of the immediate action needed for local log. crit : Critical level of the critical conditions for local log. error : Error level of the error conditions for local log. warning : Warning level of the warning conditions for local log. notice : Notice level of the normal but significant conditions for local log. info : Informational level of the informational messages for local log. debug : Debug level of the debugging messages for local log.

Buttons

- Click **Apply** to apply changes.

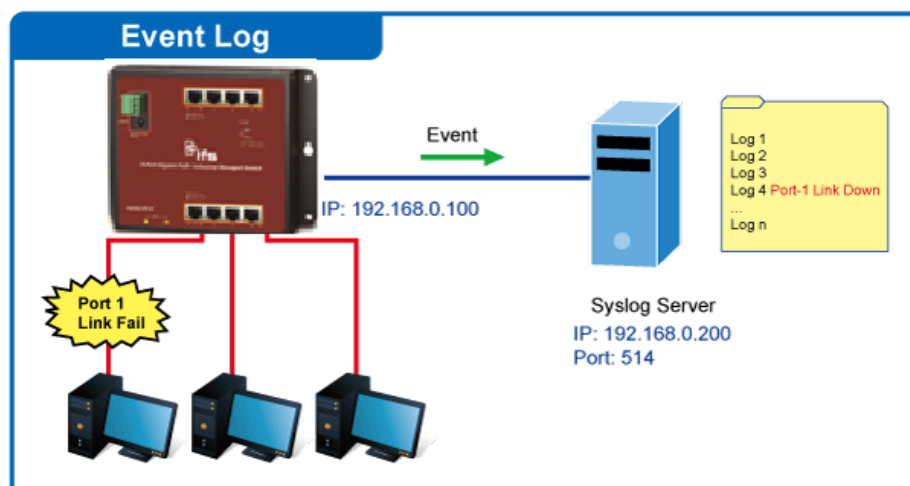


This page includes the following fields:

Object	Description
Status	Displays the current local log status.
Target	Displays the current local log target.
Severity	Displays the current local log severity.
Actions	Click Delete to delete the current status.

Remote syslog

The Remote Syslog page permits the configuration of the logging of messages that are sent to syslog servers or other management stations. You can also limit the event messages sent to only those messages below a specified level.



Remote Logging Setting

Server Address	Server Port	Severity	Facility
<input type="text"/>	514 (1-65535)	emerg ▼	local0 ▼

[Apply](#)

This page includes the following fields:

Object	Description
Server Address	Dsiplays the remote syslog IP address of this switch.
Server Port	Provides the port number of the remote syslog server. Default Port no.: 514
Severity	The severity of the local log entry. The following severity types are supported: emerg : Emergency level of the system unstable for local log. alert : Alert level of the immediate action needed for local log. crit : Critical level of the critical conditions for local log. error : Error level of the error conditions for local log. warning : Warning level of the warning conditions for local log. notice : Notice level of the normal but significant conditions for local log. info : Informational level of the informational messages for local log. debug : Debug level of the debugging messages for local log.
Facility	Local0~7 : local user 0~7

Buttons

- Click **Apply** to apply changes.

▼ Remote Logging Setting Status

Status	Server Info	Severity	Facility	Action

This page includes the following fields:

Object	Description
Status	Displays the current remote syslog status.
Server Info	Displays the current remote syslog server information.
Severity	Displays the current remote syslog severity. Displays the current remote syslog facility.
Actions	Click Delete to delete the remote server entry.

Log message

The switch log view is provided here:

Logging Filter Select

Target	Severity	Category
buffered ▼	Select Levels ▼	Select Categories ▼

This page includes the following fields:

Object	Description
Target	The target of the log view entry. The following target types are supported: Buffered: Target the buffered of the log view. File: Target the file of the log view.
Severity	The severity of the local log entry. The following severity types are supported: emerg: Emergency level of the system unstable for local log. alert: Alert level of the immediate action needed for local log. crit: Critical level of the critical conditions for local log. error: Error level of the error conditions for local log. warning: Warning level of the warning conditions for local log. notice: Notice level of the normal but significant conditions for local log. info: Informational level of the informational messages for local log. debug: Debug level of the debugging messages for local log.
Category	The category of the log view includes: AAA, ACL, CABLE_DIAG, DAI, DHCP_SNOOPING, Dot1X, GVRP, IGMP_SNOOPING, IPSG, L2, LLDP, Mirror, MLD_SNOOPING, Platform, PM, Port, PORT_SECURITY, QoS, Rate, SNMP and STP

Buttons

- Click **View** to view log.
- Click **Clear** to clear the log.
- Click **Refresh** to refresh the log.

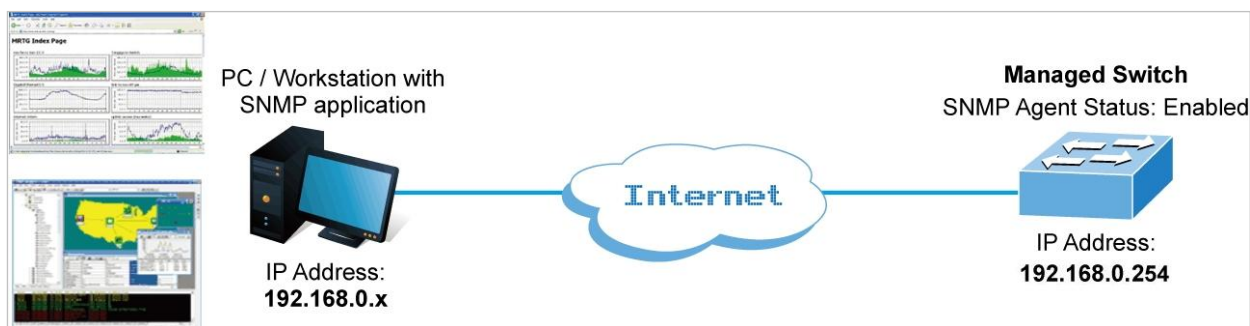
Simple Network Management Protocol (SNMP)

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)

SNMP system information

Configure SNMP settings on this page.

SNMP Global Setting

State	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
--------------	---

The page includes the following fields:

Object	Description
Status	Indicates the SNMP mode operation. Selections include: Enabled: Enable SNMP mode operation. Disabled: Disable SNMP mode operation.

Buttons

- Click **Apply** to apply changes.

SNMP view

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

View Table Setting

View Name	Subtree OID	Subtree OID Mask	View Type
<input type="text"/>	<input type="text"/>	all	<input checked="" type="radio"/> included <input type="radio"/> excluded

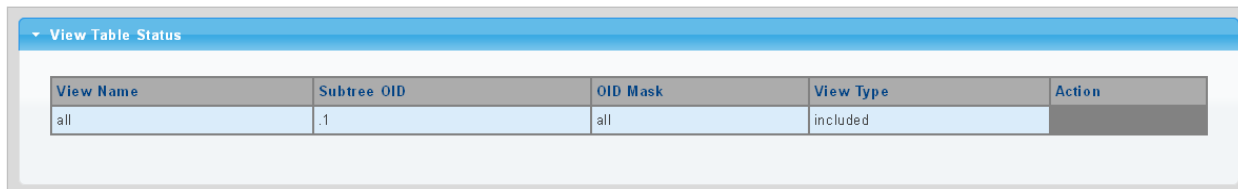
The page includes the following fields:

Object	Description
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 16.
Subtree OID	The OID defining the root of the subtree to add to the named view. The allowed string content is digital number or asterisk (*).
Subtree OID Mask	The bitmask identifies which positions in the specified object identifier are to be regarded as "wildcards" for the purpose of pattern-matching.
View Type	Indicates the view type that this entry should belong to. Possible view type are: included: An optional flag to indicate that this view subtree should be included. excluded: An optional flag to indicate that this view subtree should be excluded. General, if a view entry's view type is 'excluded', it should exist

Object	Description
	another view entry in which view type is 'included' and its OID subtree oversteps the 'excluded' view entry.

Buttons

- Click **Add** to add a new view entry.

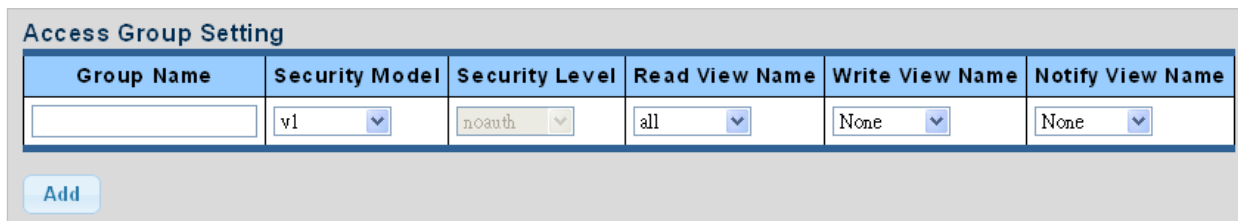


The page includes the following fields:

Object	Description
View Name	Display the current SNMP view name
Subtree OID	Display the current SNMP subtree OID
OID Mask	Display the current SNMP OID mask
View Type	Display the current SNMP view type
Action	Click Delete to delete the view table entry

SNMP access group

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



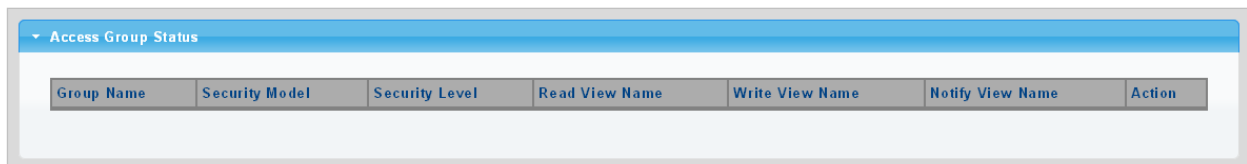
The page includes the following fields:

Object	Description
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 16.
Security Model	Indicates the security model that this entry should belong to. Possible security models are: v1 : Reserved for SNMPv1. v2c : Reserved for SNMPv2c. V3 : Reserved for SNMPv3 or User-based Security Model (USM)
Security Level	Indicates the security model that this entry should belong to. Possible security models are: Noauth : None authentication and none privacy security levels are

Object	Description
	assigned to the group. auth: Authentication and none privacy. priv: Authentication and privacy. Note: The Security Level applies to SNNPv3 only.
Read View Name	Read view name is the name of the view in which you can only view the contents of the agent. The allowed string length is 1 to 16.
Write View Name	Write view name is the name of the view in which you enter data and configure the contents of the agent. The allowed string length is 1 to 16.
Notify View Name	Notify view name is the name of the view in which you specify a notify, inform, or trap.

Buttons

- Click **Add** to add a new access entry.
- Click **Delete** to delete the entry.



The page includes the following fields:

Object	Description
Group Name	Display the current SNMP access group name
Security Model	Display the current security model
Security Level	Display the current security level
Read View Name	Display the current read view name
Write View Name	Display the current write view name
Notify View Name	Display the current notify view name
Action	Click Delete to delete the access group entry.

SNMP community

Configure the SNMP community on this page.

Community Setting

Community Name	Community Mode	Group Name	View Name	Access Right
<input type="text"/>	Basic <input type="button" value="v"/>	<input type="text"/>	all <input type="button" value="v"/>	ro <input type="button" value="v"/>

The page includes the following fields:

Object	Description
Community Name	Indicates the community read/write access string to permit access to SNMP agent. The allowed string length is 0 to 16.
Community Mode	Indicates the SNMP community supported mode. Possible versions are: Basic: Set SNMP community mode supported version 1 and 2c. Advanced: Set SNMP community mode supported version 3.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 16.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 16.
Access Right	Indicates the SNMP community type operation. Possible types are: RO=Read-Only: Set access string type in read-only mode. RW=Read-Write: Set access string type in read-write mode.

Buttons

- Click **Apply** to apply changes.

Community Status

Community Name	Group Name	View Name	Access Right	Action
public		all	rw	<input type="button" value="Delete"/>

The page includes the following fields:

Object	Description
Community Name	Displays the current community type
Group Name	Displays the current SNMP access group's name.
View Name	Displays the current view name.
Access Right	Displays the current access type
Delete	Click Delete to delete the community entry.

SNMP user

Configure SNMP users on this page. The entry index key is User Name.

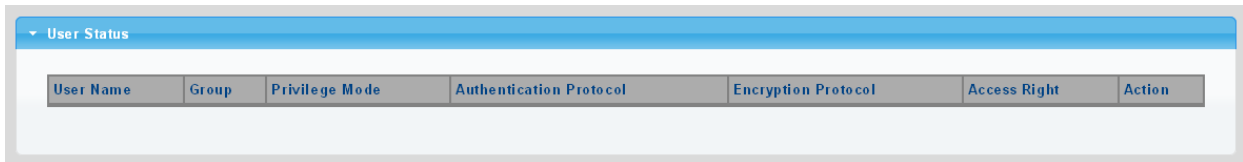
User Setting						
User Name	Group	Privilege Mode	Authentication Protocol	Authentication Password	Encryption Protocol	Encryption Key
<input type="text"/>	<input type="text" value=""/>	<input type="text" value="noauth"/>	<input type="text" value="None"/>	<input type="text" value=""/> (8 ~ 16 chars)	<input type="text" value="None"/>	<input type="text" value=""/> (8 ~ 16 chars)
<input type="button" value="Add"/>						

The page includes the following fields:

Object	Description
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 16.
Group	The SNMP Access Group. A string identifying the group name that this entry should belong to.
Privilege Mode	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 and SHA authentication options, the allowed string length is 8 to 16.
Encryption Protocol	Indicates the privacy protocol that this entry should belong to. Selections include: None: None privacy protocol. DES: An optional flag to indicate that this user using DES authentication protocol.
Encryption Key	A string identifying the privacy pass phrase. The allowed string length is 8 to 16.

Buttons

- Click **Add** to add a new user entry.

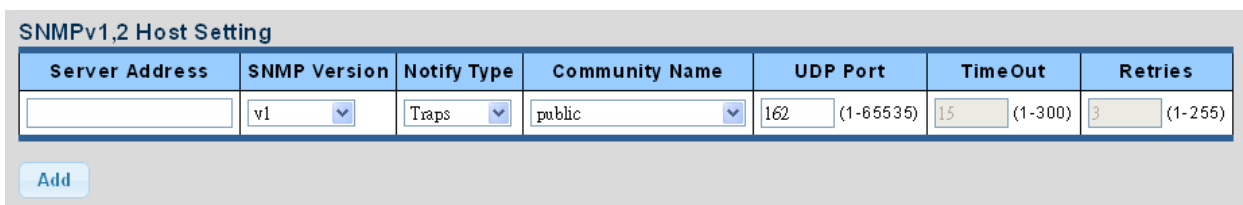


The page includes the following fields:

Object	Description
User Name	Displays the current user name
Group	Displays the current group
Privilege Mode	Displays the current privilege mode
Authentication Protocol	Displays the current authentication protocol
Encryption Protocol	Displays the current encryption protocol
Access Right	Displays the current access right
Action	Click Delete to delete the user entry.

SNMPv1, 2 notification recipients

Configure SNMPv1 and 2 notification recipients on this page.



The page includes the following fields:

Object	Description
Server Address	Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). It can also represent a legally valid IPv4 address. For example, ':::192.1.2.34'.
SNMP 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.
Notify Type	Set the notify type in traps or informs.
Community Name	Indicates the community access string when send SNMP trap packet.
UDP Port	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.
Time Out	Indicates the SNMP trap inform timeout. The allowed range is 1 to 300.
Retries	Indicates the SNMP trap inform retry times. The allowed range is 1 to 255.

Buttons

- Click **Add** to add a new SNMPv1, 2 host entry.

Server Address	SNMP Version	Notify Type	Community Name	UDP Port	Time Out	Retry	Action
----------------	--------------	-------------	----------------	----------	----------	-------	--------

The page includes the following fields:

Object	Description
Server Address	Displays the current server address
SNMP Version	Displays the current SNMP version
Notify Type	Displays the current notify type
Community Name	Displays the current community name
UDP Port	Displays the current UDP port
Time Out	Displays the current time out
Retries	Displays the current retry times
Action	Click Delete to delete the SNMPv1, 2 host entry

SNMPv3 notification recipients

Configure SNMPv3 notification recipients on this page.

Server Address	Notify Type	User Name	UDP Port	TimeOut	Retries
<input type="text"/>	Traps	<input type="text"/>	162 (1-65535)	15 (1-300)	3 (1-255)

The page includes the following fields:

Object	Description
Server Address	Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w'). It can also represent a legally valid IPv4 address. For example, ':::192.1.2.34'.
Notify Type	Set the notify type in traps or informs.
User Name	Indicates the user string when send SNMP trap packet.
UDP Port	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port, the port range is 1~65535.
Time Out	Indicates the SNMP trap inform timeout. The allowed range is 1 to 300.
Retries	Indicates the SNMP trap inform retry times. The allowed range is 1 to 255.

Buttons

- Click **Add** to add a new SNMPv3 host entry.

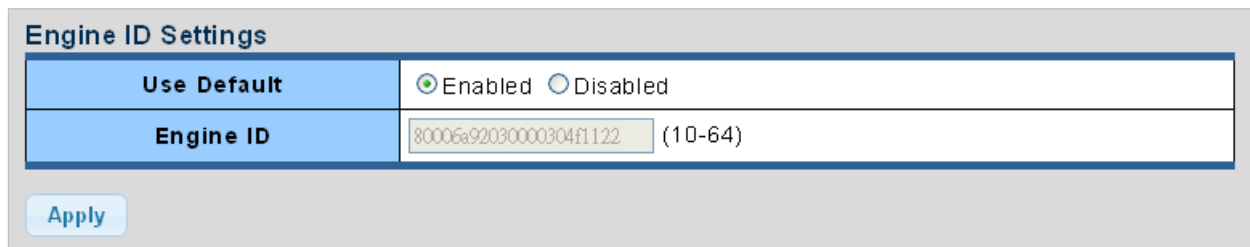


The page includes the following fields:

Object	Description
Server Address	Displays the current server address
Notify Type	Displays the current notify type
User Name	Displays the current community name
UDP Port	Displays the current UDP port
Time Out	Displays the current time out
Retries	Displays the current retry times
Action	Click Delete to delete the SNMPv3 host entry

SNMP engine ID

Configure the SNMPv3 engine ID on this page. The entry index key is Engine ID. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.



The page includes the following fields:

Object	Description
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed.

Buttons

- Click **Apply** to apply changes.

SNMP remote engine ID

Configure the SNMPv3 remote Engine ID on this page.

Remote IP Address	Engine ID
<input type="text"/>	<input type="text"/>

[Add](#)

The page includes the following fields:

Object	Description
Remote IP Address	Indicates the SNMP remote engine ID address. It allows a valid IP address in dotted decimal notation ('x.y.z.w').
Engine ID	An octet string identifying the engine ID that this entry should belong to.

Buttons

- Click **Apply** to apply changes.

Remote IP Address	Remote Engine ID	Action
-------------------	------------------	--------

The page includes the following fields:

Object	Description
Remote IP Address	Displays the current remote IP address.
Engine ID	Displays the current engine ID.
Action	Click Delete to delete the remote IP address entry.

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 Counters	Lists Ethernet and RMON port statistics
Bandwidth Utilization	Displays current bandwidth utilization
Port Mirroring	Sets the source and target ports for mirroring
Jumbo Frame	Sets the jumbo frame on the switch
Port Error Disable Configuration	Configures port error disable settings
Port Error Disabled Status	Disables port error status

Protected Ports	Configures protected ports settings
------------------------	-------------------------------------

Port configuration

Ports can be configured on the Port Configuration page.

Port Settings

Port Select	Enabled	Speed	Duplex	Flow Control
<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Select Ports ▼</div>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Auto ▼</div>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Auto ▼</div>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

The page includes the following fields:

Object	Description
Port Select	Select port number from this drop-down menu.
Enabled	Indicates the port state operation. Selections include: Enabled - Start up the port manually. Disabled – Shut down the port manually.
Speed	Select any available link speed for the given switch port. Draw the menu bar to select the mode. Auto - Set up Auto negotiation. Auto-10M - Set up 10M Auto negotiation. Auto-100M - Set up 100M Auto negotiation. Auto-1000M - Set up 1000M Auto negotiation. Auto-10/100M - Set up 10/100M Auto negotiation. 10M - Set up 10M Force mode. 100M - Set up 100M Force mode. 1000M - Set up 1000M Force mode.
Duplex	Select any available link duplex for the given switch port. Draw the menu bar to select the mode. Auto - Setup Auto negotiation. Full - Force sets Full-Duplex mode. Half - Force sets Half-Duplex mode.
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.

Buttons

- Click **Apply** to apply changes.

Port Status							
Port	Description	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
GE1	Edit	Enabled	UP	A-1000M	A-Full	Disabled	Disabled
GE2	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE3	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE4	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE5	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE6	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE7	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE8	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE9	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE10	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled

The page includes the following fields:

Object	Description
Port	The logical port number for this row
Description	Click Edit to indicate the port name
Enable State	Displays the current port state
Link Status	Displays the current link status
Speed	Displays the current speed status of the port
Duplex	Displays the current duplex status of the port.
Flow Control Configuration	Displays the current flow control configuration of the port
Flow Control Status	Display the current flow control status of the port

Port counters

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

Port MIB Counters Settings

Port	Mode
GE1 ▼	<input checked="" type="radio"/> All <input type="radio"/> Interface <input type="radio"/> Etherlike <input type="radio"/> RMON

The page includes the following fields:

Object	Description
Port	Select port number from this drop-down menu.
Mode	Select port counters mode. Options: All Interface Ether-link RMON

Interface Counters	Counters Value
Received Octets	0
Received Unicast Packets	0
Received Unknown Unicast Packets	0
Received Discards Packets	0
Transmit Octets	0
Transmit Unicast Packets	0
Transmit Unknown Unicast Packets	0
Transmit Discards Packets	0
Received Multicast Packets	0
Received Broadcast Packets	0
Transmit Multicast Packets	0
Transmit Broadcast Packets	0

Object	Description
Received Octets	The total number of octets received on the interface, including framing characters.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Received Unknown Unicast Packets	The number of packets received via the interface which is discarded because of an unknown or unsupported protocol.
Received Discards Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their delivery to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Transmit Octets	The total number of octets transmitted out of the interface, including framing characters.
Transmit Unicast Packets	The total number of packets that higher-level protocols requested is transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Transmit Unknown Unicast Packets	The total number of packets that higher-level protocols requested is transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Transmit Discards Packets	The number of inbound packets which is chosen to be discarded even though no errors have been detected to prevent from being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-) layer, is addressed to a multicast address at this sub-layer.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-) layer, addressed to a broadcast address at this sub-layer.
Transmit Multicast Packets	The total number of packets that higher-level protocols requested is transmitted and is addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Transmit Broadcast Packets	The total number of packets that higher-level protocols requested is transmitted, and addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.

Ethernet-link Counters	Counters Value
Alignment Errors	0
FCS Errors	0
Single Collision Frames	0
Multiple Collision Frames	0
Deferred Transmissions	0
Late Collision	0
Excessive Collision	0
Frame Too Longs	0
Symbol Errors	0
Control In Unknow Opcodes	0
In Pause Frames	0
Out Pause Frames	0

Object	Description
Alignment Errors	The number of alignment errors (missynchronized data packets).
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Late Collision	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collision	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increase when the interface is operating in full-duplex mode.
Frame Too Long	A count of frames received on a particular interface that exceeds the maximum permitted frame size.
Symbol Errors	The number of received and transmitted symbol errors
Control In Unknown Opcodes	The number of received control unknown opcodes
In Pause Frames	The number of received pause frames
Out Pause Frames	The number of transmitted pause frames

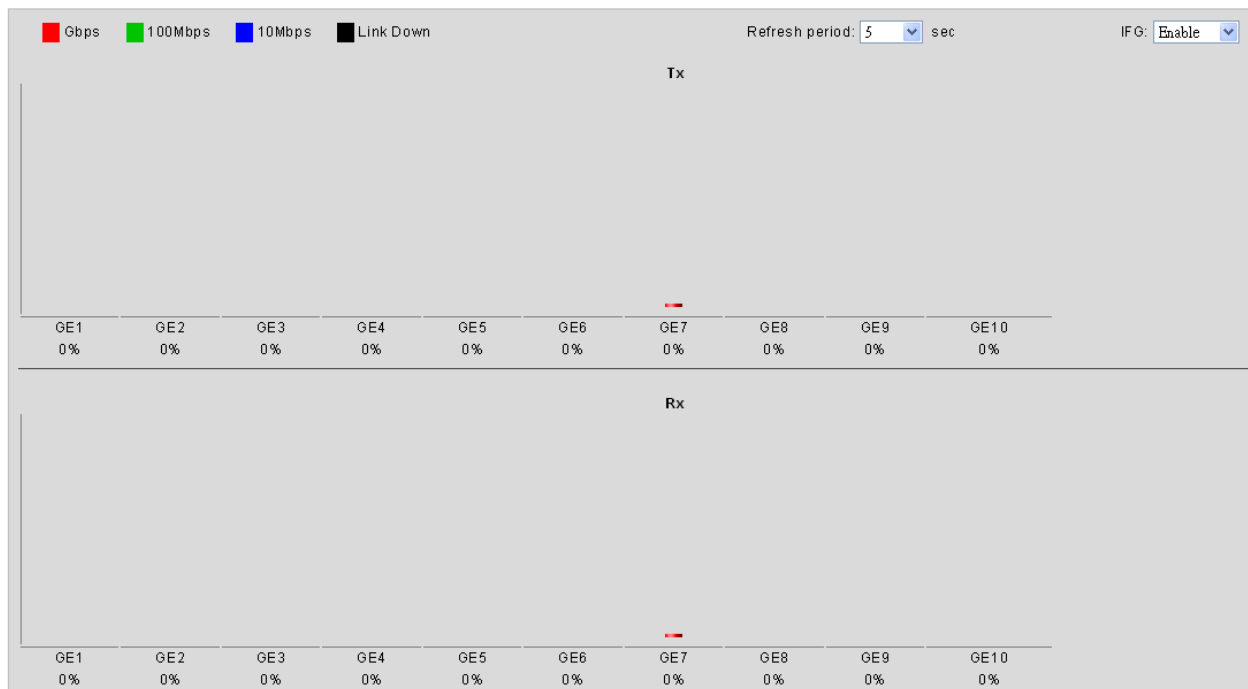
RMON Counters	Counters Value
Drop Events	0
Octets	0
Packets	0
Broadcast Packets	0
Multicast Packets	0
CRC / Alignment Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	0
64 Bytes Frame	0
65-127 Byte Frames	0
128-255 Byte Frames	0
256-511 Byte Frames	0
512-1023 Byte Frames	0
1024-1518 Byte Frames	0

Object	Description
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Octets	The total number of octets received and transmitted on the interface, including framing characters.
Packets	The total number of packets received and transmitted on the interface.
Broadcast Packets	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Packets	The total number of good frames received that were directed to this multicast address.
CRC / Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Undersize Packets	The total number of frames received that were less than 64 octets long(excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Packets	The total number of frames received that were longer than 1518 octets(excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.

Object	Description
64 Bytes Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets falls within the specified range (excluding framing bits but including FCS octets).

Bandwidth utilization

The Bandwidth Utilization page displays the percentage of the total available bandwidth being used on the ports. Bandwidth utilization statistics are represented with a line graph.



The page includes the following fields:

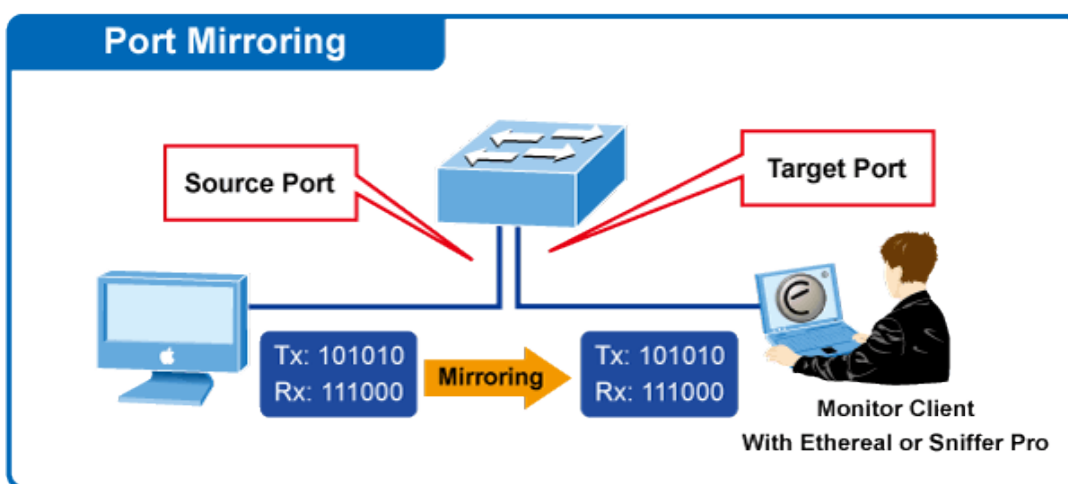
Object	Description
Refresh Period	This shows the period interval between last and next refresh. Options: 2 sec 5 sec 10 sec
IFG	Enable or Disable this function.

Port mirror

Configure port mirroring on this 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 Setting	
Session ID	Select Session <input type="button" value="v"/>
Monitor session state	Disable <input type="button" value="v"/>
Destination Port	GE1 <input type="button" value="v"/>
allow-ingress	Disable <input type="button" value="v"/>
Sniffer RX Ports	Select RX Ports <input type="button" value="v"/>
Sniffer TX Ports	Select TX Ports <input type="button" value="v"/>

The page includes the following fields:

Object	Description
Session ID	Set the port mirror session ID. Selections are: 1 to 4.
Monitor Session State	Enable or disable the port mirroring function.
Destination Port	Select the port to mirror destination port.
Allow-ingress	Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored to this port.
Sniffer TX Ports	Frames transmitted from these ports are mirrored to the mirroring port. Frames received are not mirrored.
Sniffer RX Ports	Frames received at these ports are mirrored to the mirroring port. Frames transmitted are not mirrored.

Buttons

- Click **Apply** to apply changes.

Jumbo frame

This page permits selection of the maximum frame size allowed for the switch port.

Jumbo Frame Setting

Jumbo Frame (Bytes)	<input style="width: 80%;" type="text" value="1522"/> (64-9216)
----------------------------	---

The page includes the following fields:

Object	Description
Jumbo Frame (Bytes)	Enter the maximum frame size allowed for the switch port, including FCS. The allowed range is 64 bytes to 9216 bytes.

Buttons

- Click **Apply** to apply changes.

Port error disabled configuration

Port error disable functions are configured on this page.

Error Disabled Recovery

Recovery Interval	<input style="width: 80%;" type="text" value="300"/> (Seconds)
BPDU Guard	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Self Loop	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Broadcast Flood	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Unknown Multicast Flood	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Unicast Flood	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
ACL	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Port Security Violation	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
DHCP rate limit	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
ARP rate limit	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

The page includes the following fields:

Object	Description
Recovery Interval	The period (in seconds) for which a port will be kept disabled in the event a port error is detected (and the port action shuts down the port).
BPDU Guard	Enable or disable the port error disabled function to check status by BPDU guard.
Self Loop	Enable or disable the port error disabled function to check status by self loop.
Broadcast Flood	Enable or disable the port error disabled function to check status by broadcast flood.
Unknown Multicast Flood	Enable or disable the port error disabled function to check status by unknown multicast flood.
Unicast Flood	Enable or disable the port error disabled function to check status by unicast flood.
ACL	Enable or disable the port error disabled function to check status by ACL.
Port Security Violation	Enable or disable the port error disabled function to check status by port security violation.
DHCP Rate Limit	Enable or disable the port error disabled function to check status by DHCP rate limit.
ARP Rate Limit	Enable or disable the port error disabled function to check status by ARP rate limit.

Buttons

- Click **Apply** to apply changes.

Port error disabled

This page displays port error disabled information. Ports can be disabled by some protocols such as BPDU Guard, Loopback and UDLD.



The screenshot shows a web interface with a blue header bar containing a dropdown menu labeled "Port Error Disabled Status". Below the header is a table with three columns: "Port Name", "Error Disabled Reason", and "Time Left (Seconds)". The table is currently empty.

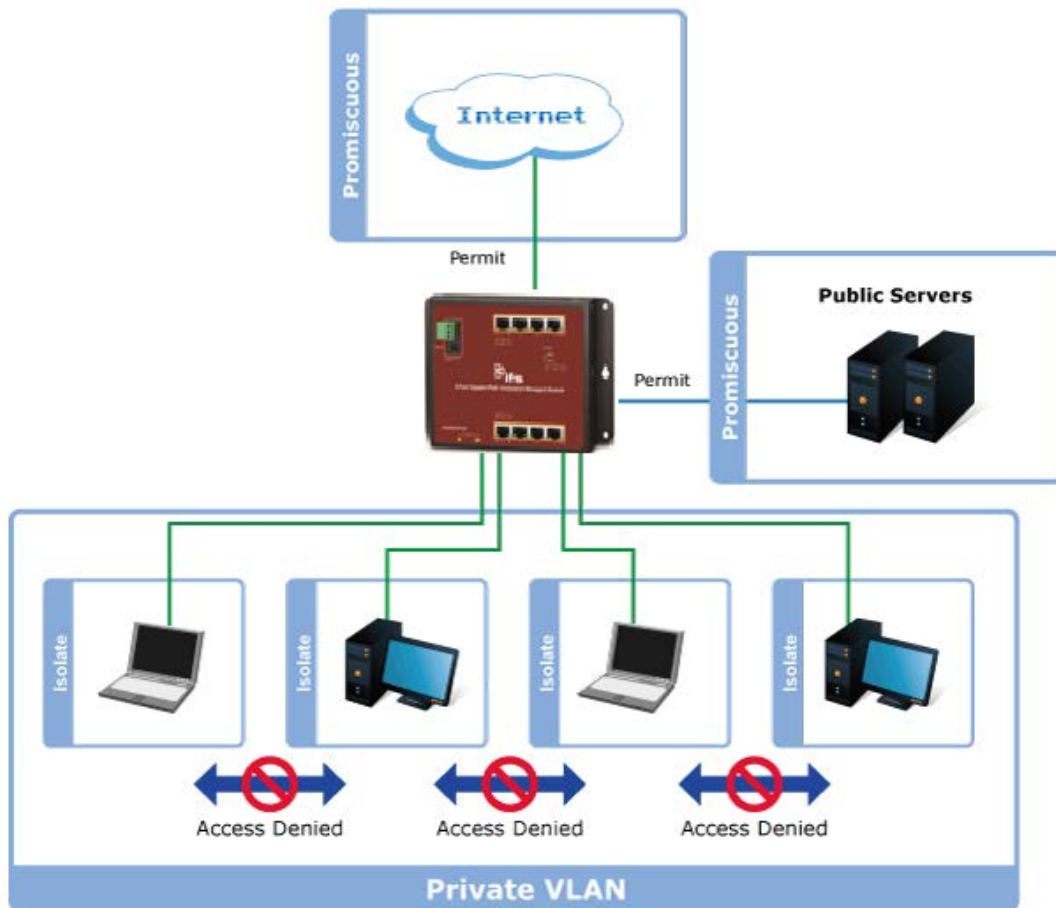
The displayed counters are:

Object	Description
Port Name	Shows the error disabled port.
Error Disable Reason	Shows the reason why the port was disabled.
Time Left (Seconds)	Shows the time left for port disable.

Protected ports

When a switch port is configured to be a member of a protected group (also called a private VLAN), communication between protected ports within that group can be prevented. Two application examples are provided in this section:

- Customers connected to an ISP can be members of the protected group, 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 protected port groups to be applied, the industrial managed switch must first be configured for standard VLAN operation. Ports in a protected port group fall into one of these two groups:

Promiscuous (Unprotected) ports

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

Isolated (Protected) ports

- Ports from which traffic can only be forwarded to promiscuous ports in the private VLAN
- Ports which 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 port forwarding to just the promiscuous ports within the private VLAN.

The page includes the following fields:

Object	Description
Port List	Select a port number from this drop-down menu.
Port Type	<p>Displays protected port types.</p> <p>Protected: A single stand-alone VLAN that contains one promiscuous port and one or more isolated (or host) ports. This VLAN conveys traffic between the isolated ports and a lone promiscuous port.</p> <p>Unprotected: A promiscuous port can communicate with all the interfaces within a private VLAN. This is the default setting.</p>

Buttons

- Click **Apply** to apply changes.

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.

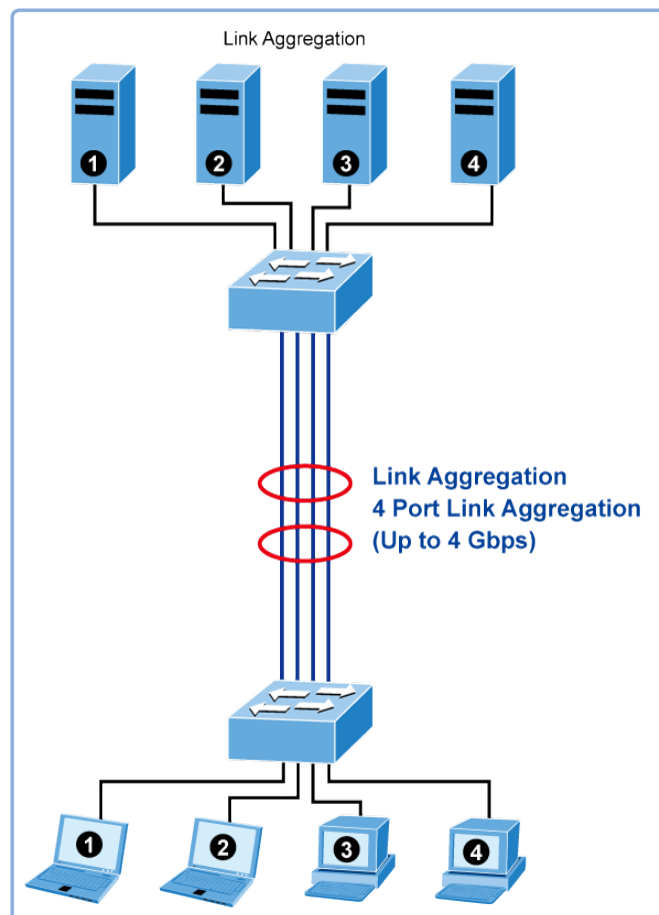
Each LAG is composed of ports of the same speed, set to full-duplex operations. Ports in a LAG can be of different media types (UTP/Fiber, or different fiber types), provided they operate at the same speed.

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 eight ports to be aggregated at the same time. The industrial managed switch supports Gigabit Ethernet ports (up to eight 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.

LAG setting

This page permits the configuration of load balance algorithm settings.

The page includes the following fields:

Object	Description
Load Balance Algorithm	<p>MAC Address: The MAC address can be used to calculate the port for the frame.</p> <p>IP/MAC Address: The IP and MAC address can be used to calculate the port for the frame.</p>

Buttons

- Click **Apply** to apply changes.

LAG management

Configure LAG management on this page.

LAG	Name	Type	Ports
LAG1	<input type="text"/>	<input checked="" type="radio"/> Static <input type="radio"/> LACP	Select Ports

The page includes the following fields:

Object	Description
LAG	Select a LAG number from the drop-down menu.
Name	Name of the LAG.
Type	Indicates the trunk type Static: Force aggregated selected ports to be a trunk group. LACP: LACP LAG 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.
Ports	Select port number from this drop-down menu to establish Link Aggregation

LAG	Name	Type	Link State	Active Member	Standby Member	Modify
LAG1		---	Not Present	-	-	Edit

The page includes the following fields:

Object	Description
LAG	The LAG for the settings contained in the same row.
Name	Displays the current name.
Type	Displays the current type.
Link State	Displays the link state.
Active Member	Displays the active member.
Standby Member	Displays the standby member.
Modify	Click Edit to modify LAG configuration.

LAG port setting

Configure each LAG on this page.

LAG Port settings

LAG Select	Enabled	Speed	Flow Control
<input type="text" value="Select LAGs"/>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	<input type="text" value="Auto"/>	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

The page includes the following fields:

Object	Description
LAG Select	Select the LAG number from this drop-down menu.
Enabled	Indicates the LAG state operation. Selections include: Enabled - Start up the port manually. Disabled – Shut down the port manually.
Speed	Select any available link speed for the given switch port. Draw the menu bar to select the mode. Auto - Set up Auto negotiation. Auto-10M - Set up 10M Auto negotiation. Auto-100M - Set up 100M Auto negotiation. Auto-1000M - Set up 1000M Auto negotiation. Auto-10/100M - Set up 10/100M Auto negotiation. 10M - Set up 10M Force mode. 100M - Set up 100M Force mode. 1000M - Set up 1000M Force mode.
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.

Buttons

- Click **Apply** to apply changes.

LACP port setting

Configure the LACP port setting on this page.

LACP Port Settings

Port Select	Priority	Timeout
<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Select Ports ▾</div>	<input style="width: 80px;" type="text" value="1"/> (1-65535)	<input checked="" type="radio"/> Long <input type="radio"/> Short

The page includes the following fields:

Object	Description
Port Select	Select the port number from this drop-down menu to set the LACP port.
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 will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.
Timeout	The Timeout controls the period between BPDU transmissions. Short transmits LACP packets each second, while Long waits for 30 seconds before sending an LACP packet.

Buttons

- Click **Apply** to apply changes.

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 Settings

Port Select	Priority	Timeout
<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Select Ports ▾</div>	<input style="width: 80px;" type="text" value="1"/> (1-65535)	<input checked="" type="radio"/> Long <input type="radio"/> Short

The page includes the following fields:

Object	Description
Port Select	Select the port number from this drop-down menu to set the LACP port.
Timeout	The Timeout controls the period between BPDU transmissions. Short transmits LACP packets each second, while Long waits for 30 seconds before sending an 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.

LAG 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.

LAG	Name	Type	Link State	Active Member	Standby Member
LAG1		---	Not Present	-	-

The page includes the following fields:

Object	Description
LAG	Displays the current trunk entry.
Name	Displays the current LAG name.
Type	Displays the current trunk type.
Link State	Displays the current link state.
Active Member	Displays the current active member.
Standby Member	Displays the current standby member.

LAG	Port	PartnerSysId	PnKey	AtKey	Sel	Mux	Receiv	PrdTx	AtState	PnState
LAG1	GE1	000000000000	03e8	03e8	U	DETACH	DFLT	FstPRD	A_G__F_	_TG_C_F_

The page includes the following fields:

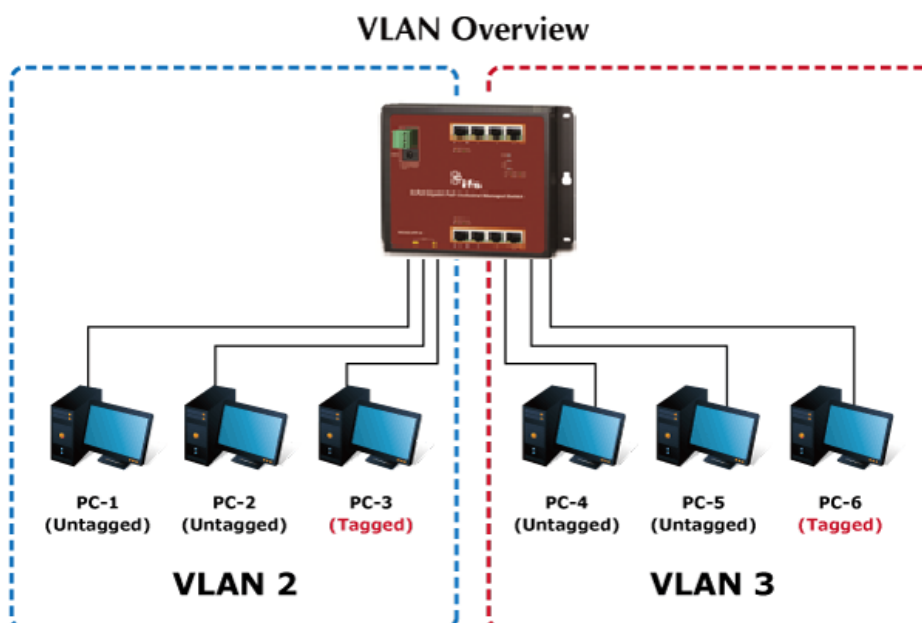
Object	Description
Trunk	Displays the current trunk ID.
Port	Displays the current port number.
PartnerSysId	The system ID of the link partner. This field is updated when the port receives LACP PDU from the link partner.
PnKey	Port key of the partner. This field is updated when the port receives LACP PDU from the link partner.
AtKey	Port key of actor. The key is designed to be the same as trunk ID.
Sel	LACP selection logic status of the port <input type="checkbox"/> "S" means selected <input type="checkbox"/> "U" means unselected <input type="checkbox"/> "D" means standby
Mux	LACP mux state machine status of the port <input type="checkbox"/> "DETACH" means the port is in detached state <input type="checkbox"/> "WAIT" means waiting state <input type="checkbox"/> "ATTACH" means attach state <input type="checkbox"/> "CLLCT" means collecting state <input type="checkbox"/> "DSTRBT" means distributing state
Receiv	LACP receive state machine status of the port <input type="checkbox"/> "INIT" means the port is in initialize state <input type="checkbox"/> "PORTDs" means port disabled state <input type="checkbox"/> "EXPR" means expired state <input type="checkbox"/> "LACPds" means LACP disabled state <input type="checkbox"/> "DFLT" means defaulted state <input type="checkbox"/> "CRRNT" means current state
PrdTx	LACP periodic transmission state machine status of the port <input type="checkbox"/> "no PRD" means the port is in no periodic state <input type="checkbox"/> "FstPRD" means fast periodic state <input type="checkbox"/> "SlwPRD" means slow periodic state <input type="checkbox"/> "PrdTX" means periodic TX state
AtState	The actor state field of LACP PDU description. The field from left to right describes: "LACP_Activity", "LACP_Timeout", "Aggregation", "Synchronization", "Collecting", "Distributing", "Defaulted", and "Expired". The contents could be true or false. If the contents are false, the web shows "_"; if the contents are true, the web shows "A", "T", "G", "S", "C", "D", "F" and "E" for each content respectively.
PnState	The partner state field of LACP PDU description. The field from left to right describes: "LACP_Activity", "LACP_Timeout", "Aggregation", "Synchronization", "Collecting", "Distributing", "Defaulted", and "Expired". The contents could be true or false. If the contents are false, the web will show "_"; if the contents are true, the Web shows "A", "T", "G", "S", "C", "D", "F" and "E" for each content respectively.

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:

Management VLAN	Configures the management VLAN
Create VLAN	Creates the VLAN group
Interface Settings	Configures mode and PVID on the VLAN port
Port to VLAN	Configures the VLAN membership
Port VLAN Membership	Displays the VLAN membership
Protocol VLAN Group Setting	Configures the protocol VLAN group
Protocol VLAN Port Setting	Configures the protocol VLAN port setting
GVRP Setting	Configures GVRP global setting
GVRP Port Setting	Configures GVRP port setting
GVRP VLAN	Displays the GVRP VLAN database
GVRP Statistics	Displays the GVRP port statistics

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.

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:

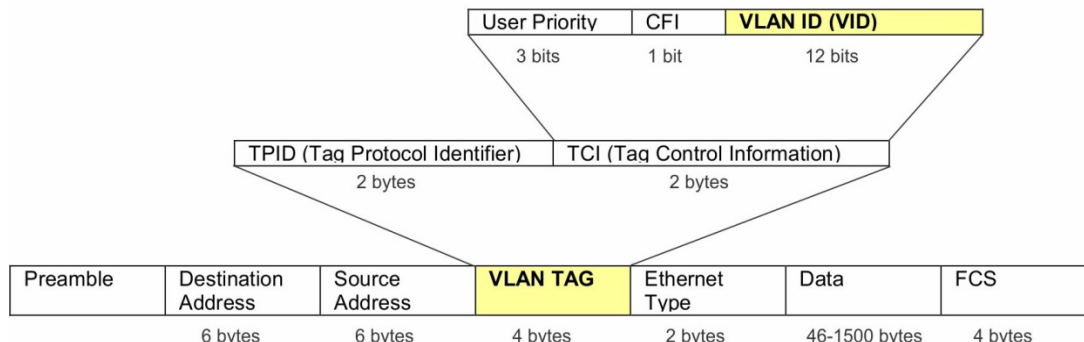
- **Tagging** – The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** – The act of stripping 802.1Q VLAN information out of the packet header.

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.

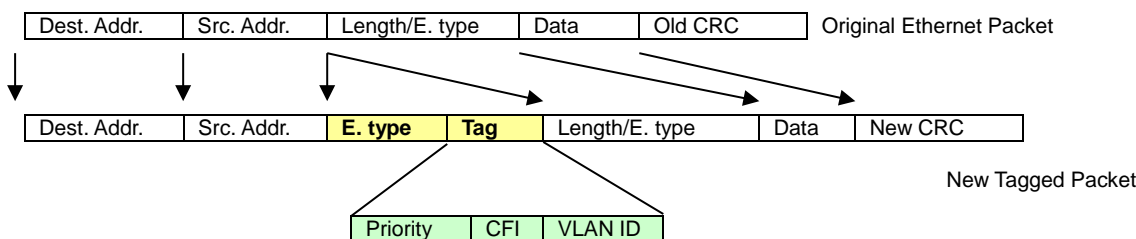
The tag is inserted into the packet header making the entire packet longer by four octets. All of the information originally contained in the packet is retained.

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.

Management VLAN

Configure Management VLAN on this page.



The screenshot shows a web configuration form titled "Management VLAN Setting". It features a single input field labeled "Management VLAN" with a dropdown menu currently showing "default(1)". Below the field is a blue "Apply" button.

The page includes the following fields:

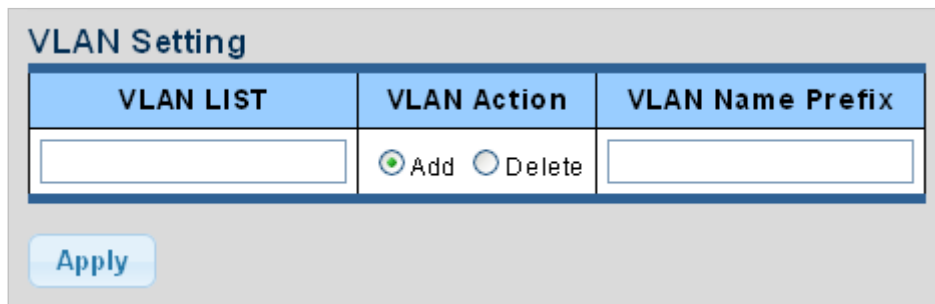
Object	Description
Management VLAN	Select the managed VLAN ID.

Buttons

- Click **Apply** to apply changes.

Create VLAN

Create and delete VLANs on this page.



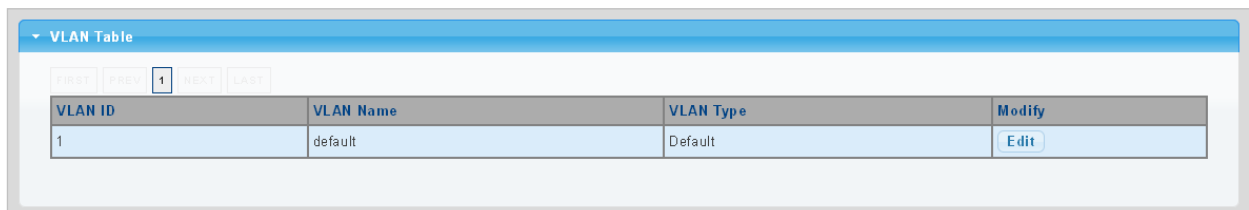
The screenshot shows a web configuration form titled "VLAN Setting". It contains three input fields: "VLAN LIST", "VLAN Action", and "VLAN Name Prefix". The "VLAN Action" field includes radio buttons for "Add" (selected) and "Delete". Below the fields is a blue "Apply" button.

The page includes the following fields:

Object	Description
VLAN List	Indicates the ID of this particular VLAN.
VLAN Action	This column allows users to add or delete VLANs.
VLAN Name Prefix	Indicates the name of this particular VLAN.

Buttons

- Click **Apply** to apply changes.



The screenshot shows a table titled "VLAN Table" with a table control above it. The table has four columns: "VLAN ID", "VLAN Name", "VLAN Type", and "Modify". The first row contains the values "1", "default", "Default", and an "Edit" button.

VLAN ID	VLAN Name	VLAN Type	Modify
1	default	Default	Edit

The page includes the following fields:

Object	Description
VLAN ID	Displays the current VLAN ID entry.
VLAN Name	Display the current VLAN ID name
VLAN Type	Display the current VLAN ID type
Modify	Click Edit to modify VLAN configuration

Interface settings

This 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.

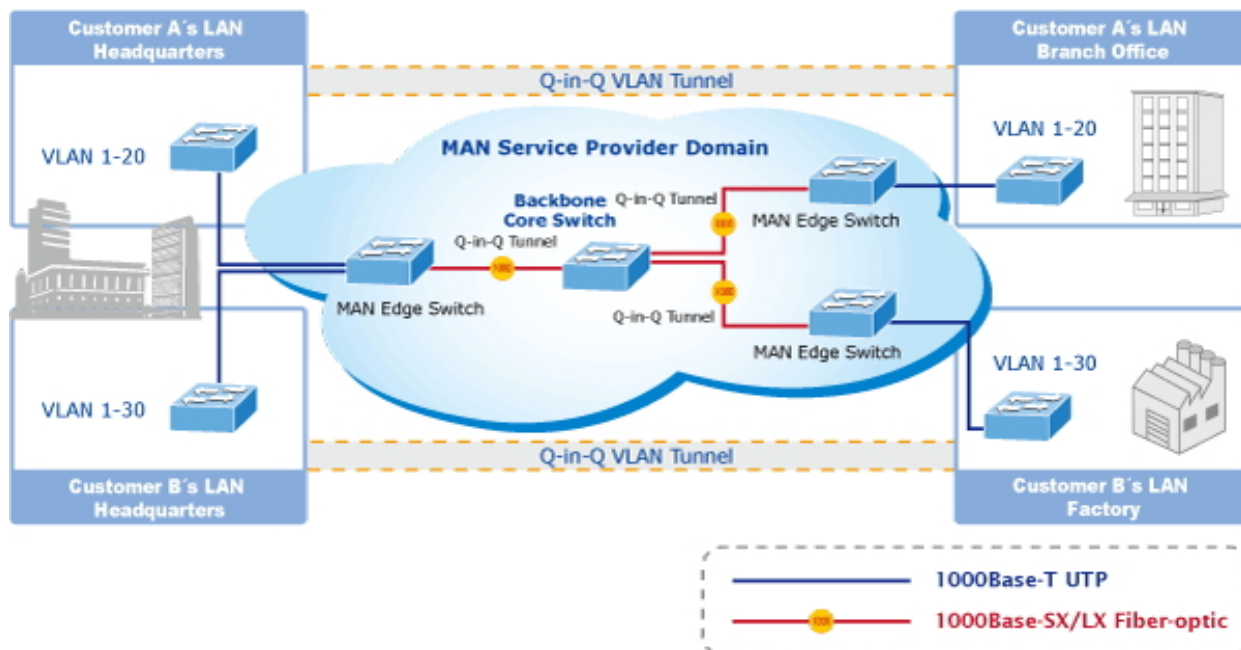
Untagged: Ports with untagging enabled strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port have no 802.1Q VLAN information (remember that the 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.

Edit interface setting

Port Select	Interface VLAN Mode	PVID	Accepted Type	Ingress Filtering	Uplink	TPID
Select Ports	<input checked="" type="radio"/> Hybrid Tunnel <input type="radio"/> Access <input type="radio"/> Trunk <input type="radio"/>	1 (1-4094)	<input checked="" type="radio"/> All <input type="radio"/> Tag Only <input type="radio"/> Untag <input type="radio"/> Only	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	0x8100

Apply

The page includes the following fields:

Object	Description
Interface VLAN Mode	<p>Set the port in access, trunk, hybrid and tunnel mode.</p> <p>Trunk means the port allows traffic of multiple VLANs.</p> <p>Access indicates the port belongs to one VLAN only.</p> <p>Hybrid means the port allows the traffic of multi-VLANs to pass in tag or untag mode.</p> <p>Tunnel configures IEEE 802.1Q tunneling for a downlink port to another device within the customer network.</p>
PVID	<p>Allows you to assign PVID to a selected port.</p> <p>The PVID will be inserted into all untagged frames entering the ingress port. The PVID must be the same as the VLAN ID that the port belongs to VLAN group, or the untagged traffic will be dropped. The range for the PVID is 1-4094.</p>
Accepted Type	<p>Determines whether 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 the port are discarded.</p> <p>Options:</p> <p>All</p> <p>Tag Only</p> <p>Untag Only</p> <p>By default, the field is set to All.</p>
Ingress Filtering	<p>If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded.</p> <p>If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.</p>
Uplink	Enable/disable uplink function in trunk port.
TPID	Configure the type (TPID) of the protocol of switch trunk port.

Buttons

- Click **Apply** to apply changes.

Port to VLAN

Port to VLAN Settings

VLAN ID : 1

Port	Interface VLAN Mode	Membership	PVID
GE1	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE2	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE3	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE4	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
LAG5	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
LAG6	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
LAG7	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
LAG8	Trunk	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>

Apply

The page includes the following fields:

Object	Description
VLAN ID	Select VLAN ID from this drop-down menu to assign VLAN membership.
Port	The switch port number of the logical port.
Interface VLAN Mode	Displays the current interface VLAN mode.
Membership	<p>Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:</p> <p>Forbidden: Interface is forbidden from automatically joining the VLAN via GVRP.</p> <p>Excluded: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.</p> <p>Tagged: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.</p> <p>Untagged: Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.</p>
PVID	Displays the current PVID.

Buttons

- Click **Apply** to apply changes.

Port VLAN membership

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

Port VLAN Membership Table				
Port	Mode	Administrative VLANs	Operational VLANs	Modify
GE1	Trunk	1UP	1UP	Edit
GE2	Trunk	1UP	1UP	Edit
GE3	Trunk	1UP	1UP	Edit
LAG5	Trunk	1UP	1UP	Edit
LAG6	Trunk	1UP	1UP	Edit
LAG7	Trunk	1UP	1UP	Edit
LAG8	Trunk	1UP	1UP	Edit

The page includes the following fields:

Object	Description
Port	The switch port number of the logical port.
Mode	Displays the current VLAN mode
Administrative VLANs	Displays the current administrative VLANs
Operational VLANs	Displays the current operational VLANs
Modify	Click Edit to modify VLAN membership

Protocol VLAN group setting

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this industrial managed switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

Command Usage

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use. Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.
2. Create a protocol group for each of the protocols you want to assign to a VLAN using the Protocol VLAN Configuration page.
3. Map the protocol for each interface to the appropriate VLAN using the Protocol VLAN Port Configuration page.

This page allows you to configure protocol-based VLAN group settings.

Add Protocol VLAN Group

Group ID (1-8)	<input type="text" value="1"/>
Frame Type	<input type="text" value="Ethernet_II"/>
Protocol Value (0x0600-0xFFFE)	<input type="text"/>

The page includes the following fields:

Object	Description
Group ID	Protocol Group ID assigned to the Special Protocol VLAN Group.
Frame Type	Frame Type can have one of the following values: Ethernet II IEEE802.3_LL_C_Other RFC_1042 Note: On changing the Frame type field, valid value of the following text field will vary depending on the new frame type you selected.
Protocol Value (0x0600-0xFFFE)	Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu. Valid values for frame type ranges from 0x0600-0xfffe

Buttons

- Click **Apply** to apply changes.

Protocol VLAN Group State

Group ID	Frame Type	Protocol Value	Delete

The page includes the following fields:

Object	Description
Group ID	Displays the current group ID
Frame Type	Display the current frame type
Protocol Value	Display the current protocol value
Delete	Click Delete to delete the group ID entry

Protocol VLAN port setting

This page permits mapping an already configured Group Name to a VLAN/port for the switch.

The page includes the following fields:

Object	Description
Port	Select a port from this drop-down menu to assign a protocol VLAN port
Group	Select a group ID from this drop-down menu to protocol VLAN group
VLAN	VLAN ID assigned to the Special Protocol VLAN Group

Buttons

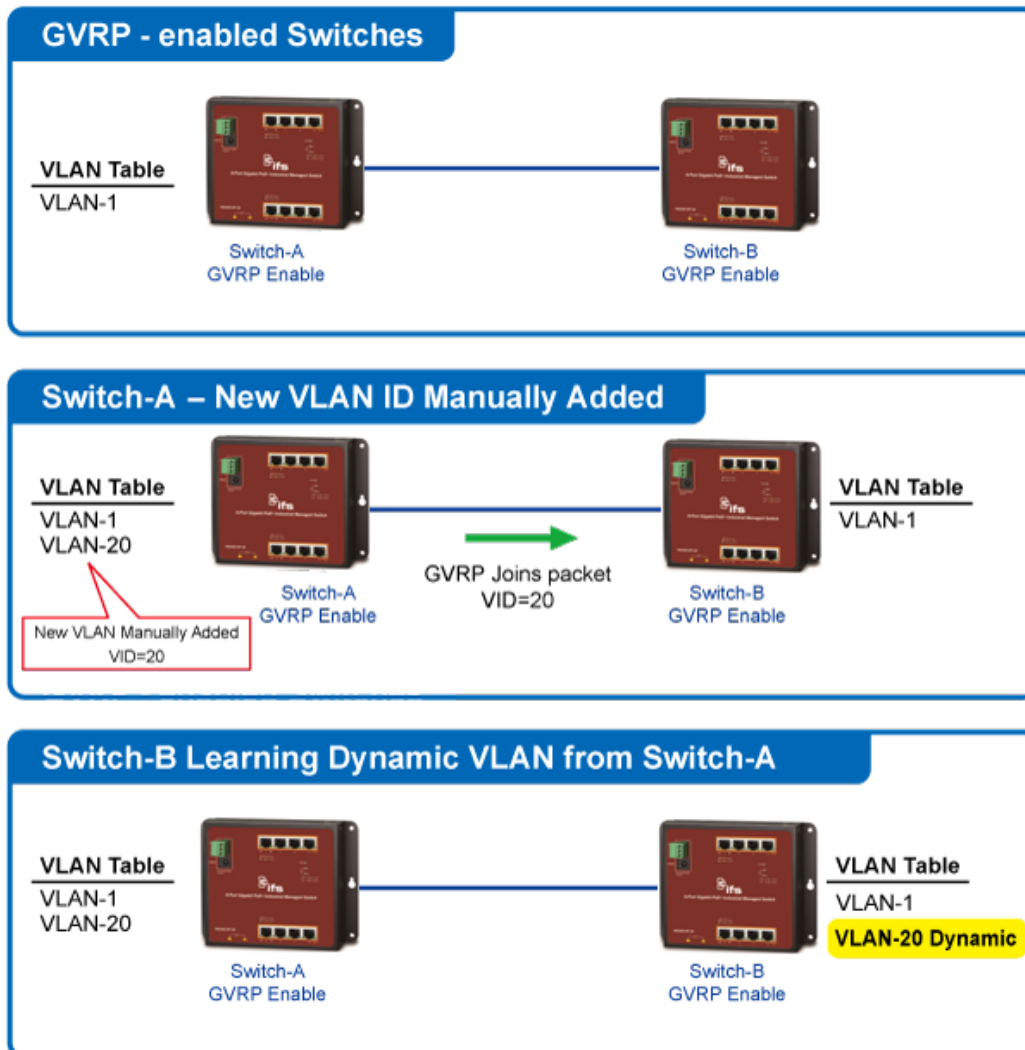
- Click **Add** to add a protocol VLAN port entry.

The page includes the following fields:

Object	Description
Port	Displays the current port
Group ID	Displays the current group ID
VLAN ID	Displays the current VLAN ID
Delete	Click Delete to delete the group ID entry

GVRP setting

GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network.



VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

GVRP Global Setting

GVRP	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Join Timeout	<input type="text" value="20"/> (20-16375 centiseconds)
Leave Timeout	<input type="text" value="60"/> (45-32760 centiseconds)
LeaveAll Timeout	<input type="text" value="1000"/> (65-32765 centiseconds)

The page includes the following fields:

Object	Description
GVRP	Enable or Disable GVRP on this switch.
Join Timeout	The interval between transmitting requests/queries to participate in a VLAN group. Range: 20-16375 centiseconds Default: 20 centiseconds
Leave Timeout	The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. Range: 45-32760 centiseconds Default: 60 centiseconds
LeaveAll Timeout	The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. Range: 65-32765 centiseconds; Default: 1000 centiseconds

Note: Timer settings must follow this rule: $2 \times (\text{join timer}) < \text{leave timer} < \text{leaveAll timer}$

Buttons

- Click **Apply** to apply changes.

GVRP port setting

Configure GVRP port settings on this page.

Port settings

Port Select	GVRP Enabled	Registration Mode	Vlan Creation
<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Select Ports ▾</div>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Normal ▾</div>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

The page includes the following fields:

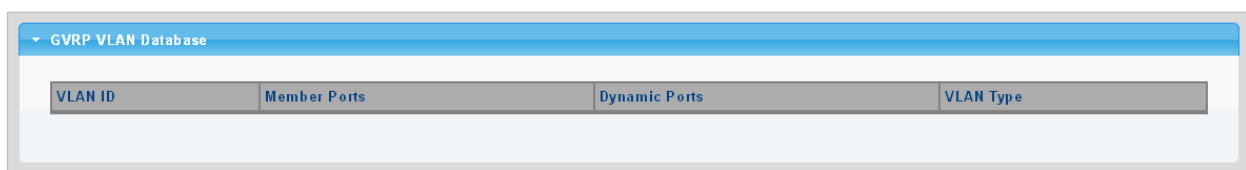
Object	Description
Port Select	Select a port from this drop-down menu to assign a protocol VLAN port.
GVRP Enabled	Enable or Disable on the port.
Registration Mode	By default, GVRP ports are in normal registration mode. These ports use GVRP join messages from neighboring switches to prune the VLANs running across the 802.1Q trunk link. If the device on the other side is not capable of sending GVRP messages, or if you do not want to allow the switch to prune any of the VLANs, use the fixed

Object	Description
	mode. Fixed mode ports will forward for all VLANs that exist in the switch database. Ports in forbidden mode forward only for VLAN 1.
VLAN Creation	GVRP can dynamically create VLANs on switches for trunking purposes. By enabling GVRP dynamic VLAN creation, a switch will add VLANs to its database when it receives GVRP join messages about VLANs it does not have.

Buttons

- Click **Apply** to apply changes.

GVRP VLAN



The page includes the following fields:

Object	Description
VLAN ID	Displays the current VLAN ID
Member Ports	Displays the current member ports
Dynamic Ports	Displays the current dynamic ports
VLAN Type	Displays the current VLAN type

GVRP statistics

Port	Join Empty (Rx/Tx)	Empty (Rx/Tx)	Leave Empty (Rx/Tx)	Join In (Rx/Tx)	Leave In (Rx/Tx)	Leave All (Rx/Tx)
GE1	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
GE2	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
GE3	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
GE4	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0

The page includes the following fields:

Object	Description
Port	The switch port number of the logical port
Join Empty (Rx/Tx)	Displays the current join empty (TX/RX) packets
Empty (Rx/Tx)	Displays the current empty (TX/RX) packets
Leave Empty (Rx/Tx)	Displays the current leave empty (TX/RX) packets

Object	Description
Join In (Rx/Tx)	Displays the current join in (TX/RX) packets
Leave In (Rx/Tx)	Displays the current leave in (TX/RX) packets
LeaveAll (Rx/Tx)	Displays the current leaveall (TX/RX) packets

Port	Invalid Protocol ID	Invalid Attribute Type	Invalid Attribute Value	Invalid Attribute Length	Invalid Event
GE1	0	0	0	0	0
GE2	0	0	0	0	0
GE3	0	0	0	0	0
GE4	0	0	0	0	0

The page includes the following fields:

Object	Description
Port	The switch port number of the logical port
Invalid Protocol ID	Displays the current invalid protocol ID
Invalid Attribute Type	Displays the current invalid attribute type
Invalid Attribute Value	Displays the current invalid attribute value
Invalid Attribute Length	Displays the current invalid attribute length
Invalid Event	Displays the current invalid event

Buttons

- Click **Clear** to clear error statistics.
- Click **Refresh** to refresh the error statistics.

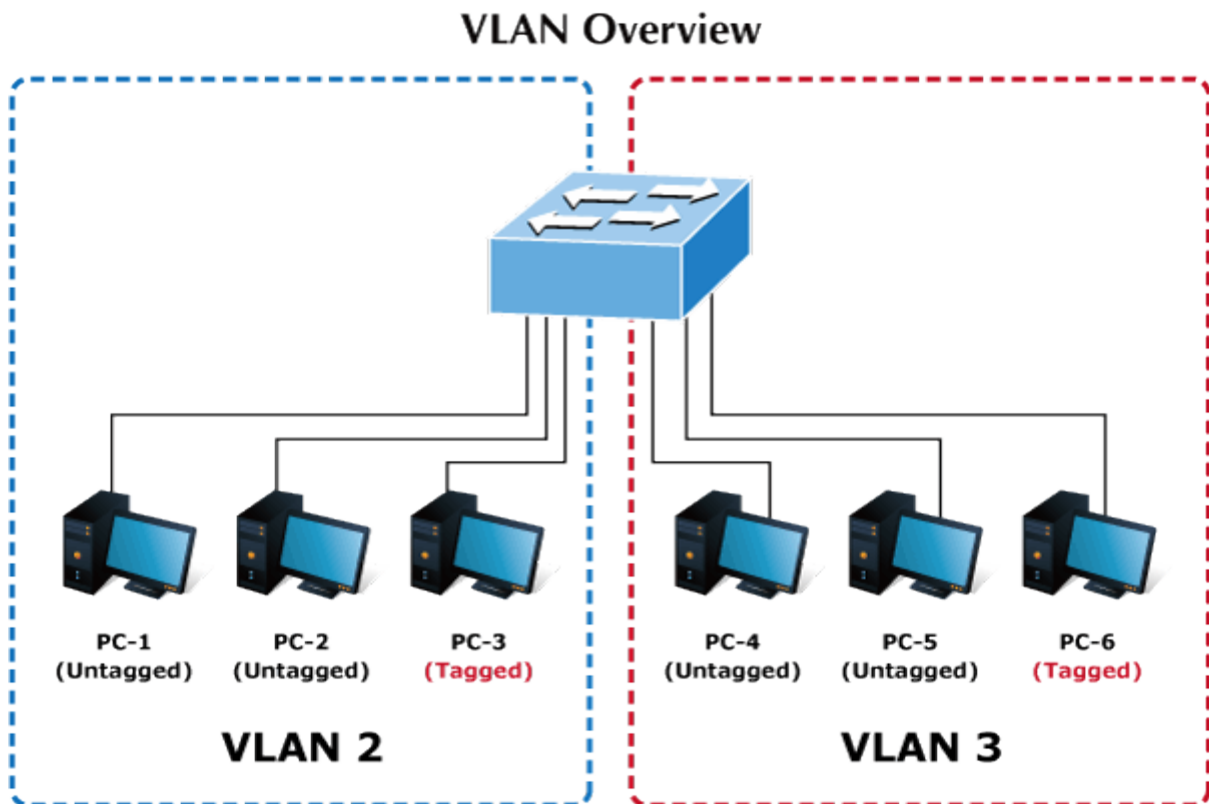
VLAN setting examples

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.

VLAN ID	VLAN Name	VLAN Type
1	default	Default
2	20002	Static
3	30003	Static

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

Port	Interface VLAN Mode	PVID	Accept Frame Type
GE1	Hybrid	2	ALL
GE2	Hybrid	2	ALL
GE3	Hybrid	2	ALL
GE4	Hybrid	3	ALL
GE5	Hybrid	3	ALL
GE6	Hybrid	3	ALL

3. Enable VLAN Tag for specific ports

VLAN ID = 2:

Port-1 & 2 = Untagged,
 Port-3 = Tagged,
 Port -4~6 = Excluded..

Port to VLAN Settings

VLAN ID : 2

Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE2	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE3	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE4	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE5	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE6	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>

VLAN ID = 3:
 Port-4 & 5 = Untagged,
 Port -6 = Tagged,
 Port-1~3 = Excluded.

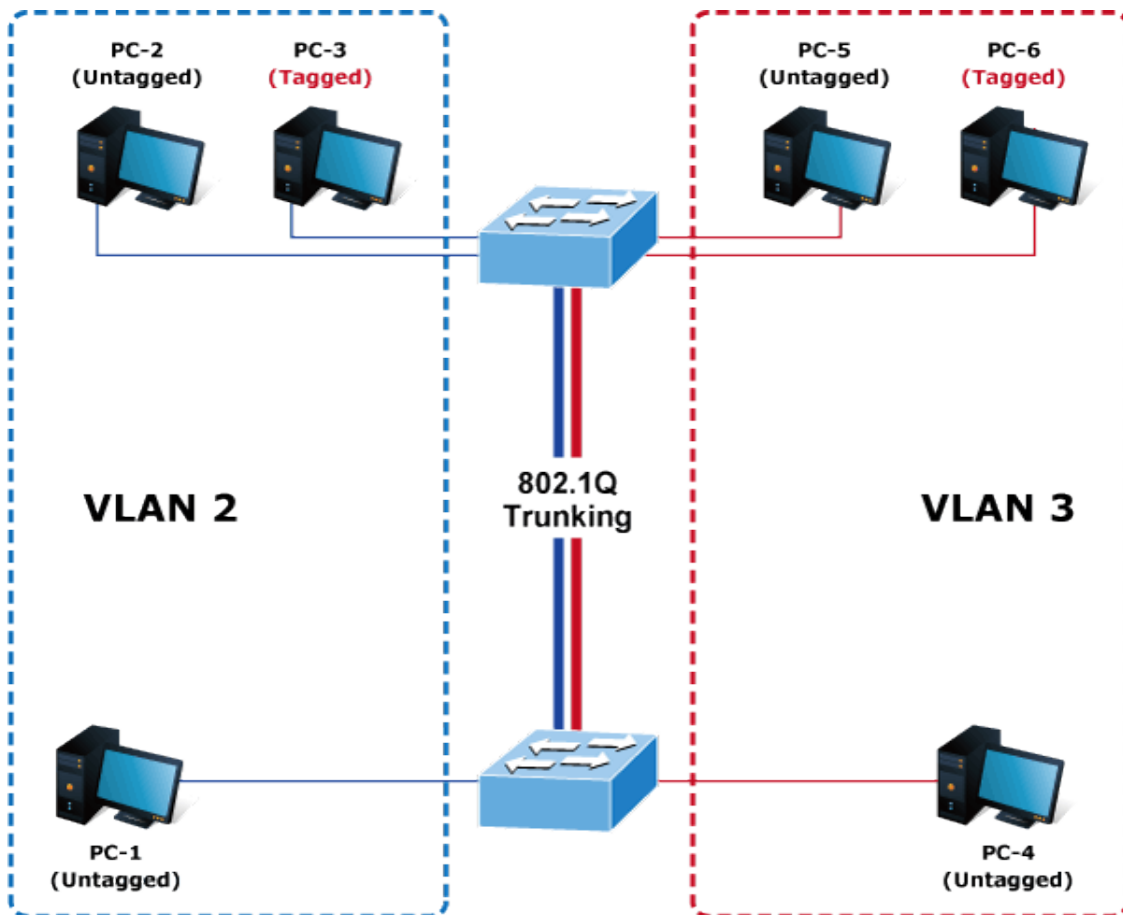
Port to VLAN Settings

VLAN ID : 3

Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE2	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE3	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE4	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE5	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE6	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input checked="" type="checkbox"/>

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.

VLAN Table		
VLAN ID	VLAN Name	VLAN Type
1	default	Default
2	20002	Static
3	30003	Static

2. Assign VLAN members and PVIDs to each port:

VLAN 2: Port-1, Port-2 and Port-3, VLAN Mode = Hybrid

VLAN 3: Port-4, Port-5 and Port-6, VLAN Mode = Hybrid

VLAN 1: Port-7, VLAN Mode = Hybrid

Port	Interface VLAN Mode	PVID	Accept Frame Type
GE1	Hybrid	2	ALL
GE2	Hybrid	2	ALL
GE3	Hybrid	2	ALL
GE4	Hybrid	3	ALL
GE5	Hybrid	3	ALL
GE6	Hybrid	3	ALL
GE7	Hybrid	1	ALL

3. Assign Tagged/Untagged to each port:

VLAN ID = 1:

Port-1~6 = Untagged,

Port -7 = Excluded..

Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input type="checkbox"/>
GE2	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input type="checkbox"/>
GE3	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input type="checkbox"/>
GE4	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input type="checkbox"/>
GE5	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input type="checkbox"/>
GE6	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input type="checkbox"/>
GE7	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input checked="" type="checkbox"/>

VLAN ID = 2:

Port-1 & 2 = Untagged,

Port-3 & 7 = Tagged,

Port -4~6 = Excluded.

Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE2	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE3	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE4	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE5	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE6	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE7	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>

VLAN ID = 3:

Port-4 & 5 = Untagged,

Port -6 & 7= Tagged,

Port-1~3 = Excluded.

Port to VLAN Settings			
VLAN ID : 3			
Port	Interface VLAN Mode	Membership	PVID
GE1	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE2	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE3	Hybrid	<input type="radio"/> Forbidden <input checked="" type="radio"/> Excluded <input type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>
GE4	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE5	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input type="radio"/> Tagged <input checked="" type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE6	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input checked="" type="checkbox"/>
GE7	Hybrid	<input type="radio"/> Forbidden <input type="radio"/> Excluded <input checked="" type="radio"/> Tagged <input type="radio"/> Untagged	<input type="checkbox"/>

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

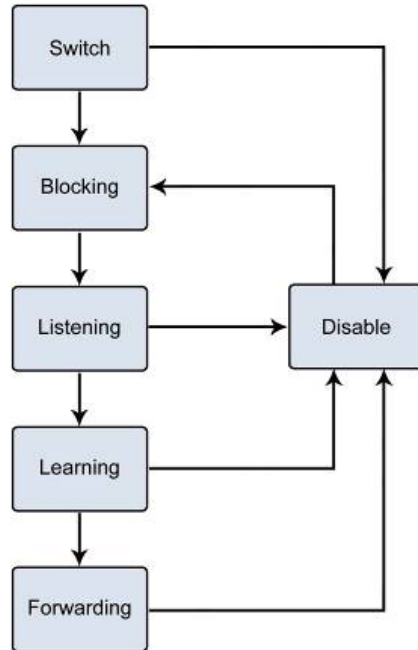
The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a blocking state to a forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout 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.

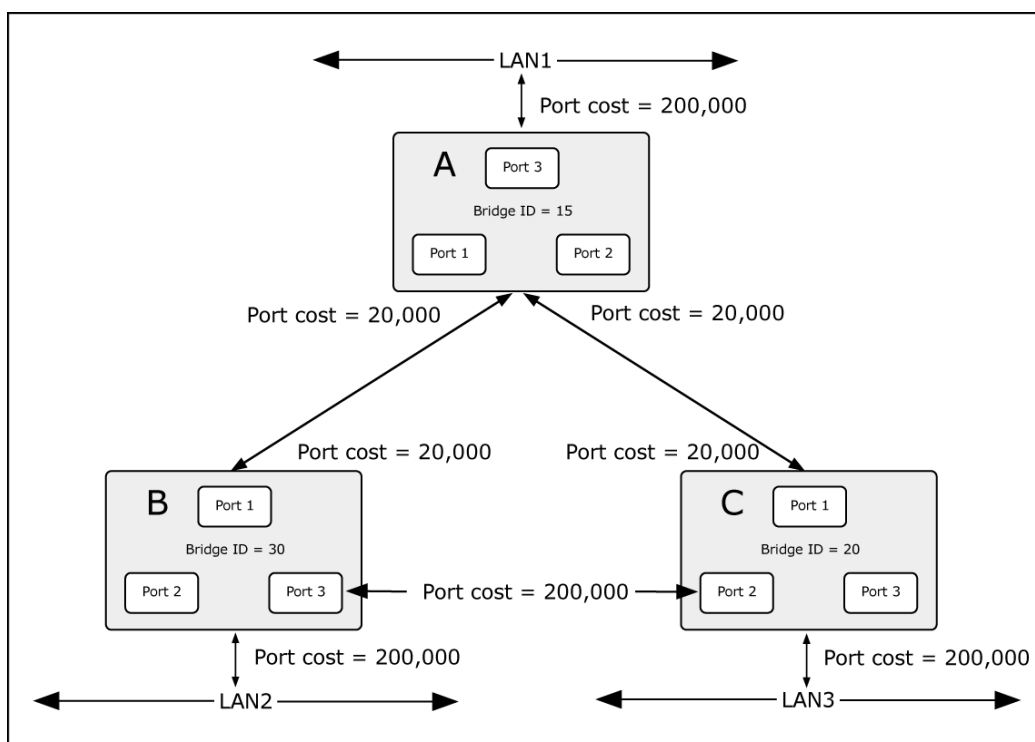
- **Forward Delay Timer** – The forward delay can be from 4 to 30 seconds. This is the time any port on the switch spends in the listening state while moving from the blocking state to the forwarding state.

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

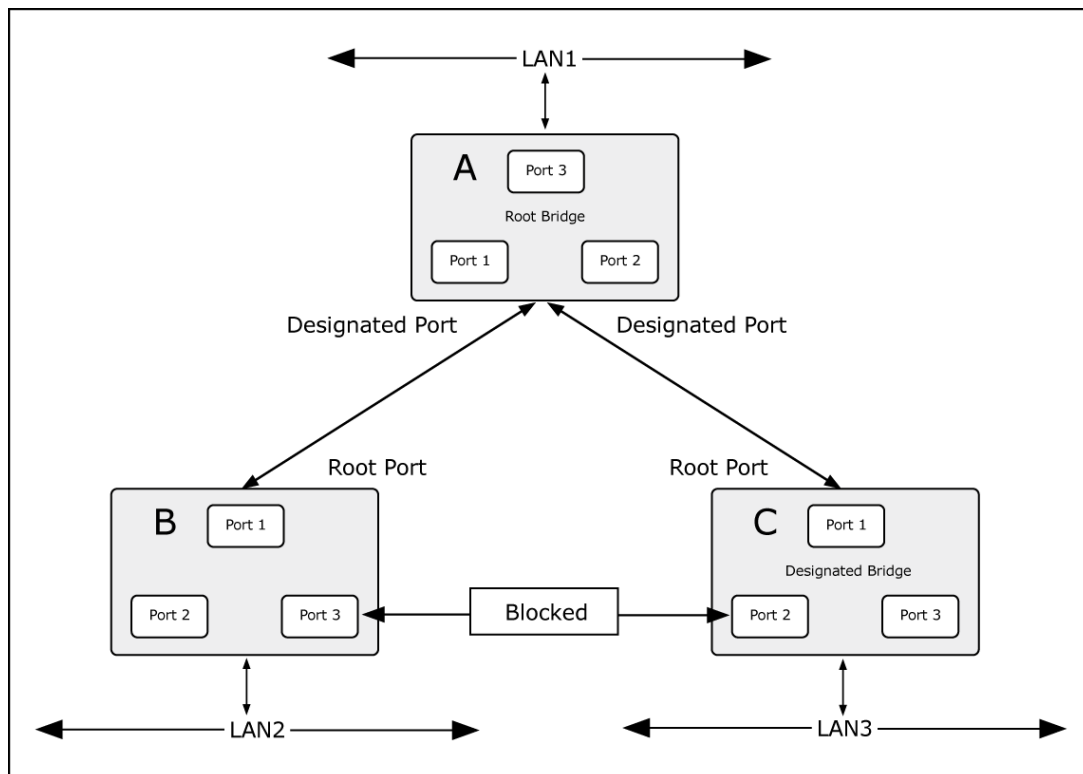
A simple illustration of three switches connected in a loop is depicted in the following diagram. In this example, you can anticipate some major network problems if the STP assistance is not applied.



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 global settings

This 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.

Global Setting	
Enabled	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
BPDU Forward	<input checked="" type="radio"/> flooding <input type="radio"/> filtering
PathCost Method	<input type="radio"/> short <input checked="" type="radio"/> long
Force Version	RSTP-Operation <input type="button" value="v"/>
Configuration Name	<input type="text" value="00:00:30:4F:11:22"/> (Max.32 charactor)
Configuration Revision	<input type="text" value="0"/> (0 - 65535)

The page includes the following fields:

Object	Description
Enable	STP function Enabled or Disabled . The default value is Disabled .
BPDU Forward	Set the BPDU forward method.
PathCost Method	The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
Force Version	The STP protocol version setting. Valid values are STP-Compatible, RSTP-Operation and MSTP-Operation.
Configuration Name	Identifier used to identify the configuration currently being used.
Configuration Revision	Identifier used to identify the configuration currently being used. The values allowed are between 0 and 65535. The default value is 0.

Buttons

- Click **Apply** to apply changes.

STP port setting

This page permits the user to inspect and change the current per port STP settings.

STP Port Setting

Port Select	External Path Cost (0 = Auto)	Edge Port	BPDU Filter	BPDU Guard	P2P MAC	Migrate
<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Select Ports ▾</div>	<input style="width: 50px;" type="text" value="0"/>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">No ▾</div>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">No ▾</div>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">No ▾</div>	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Yes ▾</div>	<input type="checkbox"/>

[Apply](#)

The page includes the following fields:

Object	Description
Port Select	Select a port number from this drop-down menu.
External Cost (0 = Auto)	<p>Controls the path cost incurred by the port.</p> <p>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.</p> <p>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.</p>
Edge Port	Determines if the operEdge flag should start as being set or cleared. (The initial operEdge state when a port is initialized).
BPDU Filter	Determines if a port explicitly configured as Edge will transmit and receive BPDUs.
BPDU Guard	<p>Determines if a port explicitly configured as Edge will disable itself upon reception of a BPDU.</p> <p>The port will enter the error-disabled state, and will be removed from the active topology.</p>
P2P MAC	<p>Determines if the port connects to a point-to-point LAN rather than a shared medium.</p> <p>This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.</p> <p>(This applies to physical ports only. Aggregations are always forced Point2Point).</p>
Migrate	<p>If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode.</p> <p>However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces.</p> <p>(Default: Disabled)</p>

Buttons

- Click **Apply** to apply changes.

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 802.1w 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

CIST instance settings

This page permits the user to inspect and change the CIST instance settings.

CIST Instance Setting	
Priority	32768
Max Hops	20 (1-40)
Forward Delay	15 (4-30)
Max Age	20 (6-40)
Tx Hold Count	6 (1-10)
Hello Time	2 (1-10)

Apply

The page includes the following fields:

Object	Description
Priority	<p>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.</p> <p>For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.</p>
Max Hops	<p>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 of 6 to 40 hops.</p>
Forward Delay	<p>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 4 to 30 seconds</p> <p>Default: 15</p> <p>Minimum: The higher of 4 or $[(\text{Max. Message Age} / 2) + 1]$</p> <p>Maximum: 30</p>
Max Age	<p>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.</p> <p>Default: 20</p> <p>Minimum: The higher of 6 or $[2 \times (\text{Hello Time} + 1)]$.</p> <p>Maximum: The lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$</p>
Tx Hold Count	<p>The number of BPDUs a bridge port can send per second. When exceeded, transmission of the next BPDU is delayed. Valid values are in the range 1 to 10 BPDUs per second.</p>
Hello Time	<p>The time that controls the switch to send out the BPDU packet to check STP current status.</p> <p>Enter a value between 1 through 10.</p>

Buttons

- Click **Apply** to apply changes.

CIST port setting

This page permits the user to configure per port CIST priority and cost.

Port Select	Priority	Internal Path Cost (0 = Auto)
Select Ports	128	0

Apply

The page includes the following fields:

Object	Description
Port Select	Select the port number from this drop-down menu.
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
Internal Path Cost (0 = Auto)	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.

Buttons

- Click **Apply** to apply changes.

MST instance configuration

Configure the MST instance settings on this page.

MSTI ID (1-15)	VLAN List (1-4094)	Priority
1		32768

Apply

The page includes the following fields:

Object	Description
MSTI ID	Assign an MSTI ID. The range for the MSTI ID is 1-15.
VLAN List (1-4096)	Assign a VLAN list to a special MSTI ID. The range for the VLAN list is 1-4094.
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.

MST port setting

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 global.

MST Port Setting

MST ID	Port Select	Priority	Internal Path Cost (0 = Auto)
1 ▼	Select Ports ▼	128 ▼	0

The page includes the following fields:

Object	Description
MST ID	Select the special MST ID to configure path cost and priority.
Port Select	Select the port number from this drop-down menu.
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
Internal Path Cost (0 = Auto)	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network.

Object	Description
	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.

Buttons

- Click **Apply** to apply changes.

STP statistics

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

Port	Configuration BPDUs Received	TCN BPDUs Received	MSTP BPDUs Received	Configuration BPDUs Transmitted	TCN BPDUs Transmitted	MSTP BPDUs Transmitted
GE1	0	0	0	0	0	0
GE2	0	0	0	0	0	0
GE3	0	0	0	0	0	0

The page includes the following fields:

Object	Description
Port	The switch port number of the logical STP port.
Configuration BPDUs Received	The current configuration BPDUs received.
TCN BPDUs Received	The current TCN BPDUs received.
MSTP BPDUs Received	The current MSTP BPDUs received.
Configuration BPDUs Transmitted	The configuration BPDUs transmitted.
TCN BPDUs Transmitted	The current TCN BPDUs transmitted.
MSTP BPDUs Transmitted	The current BPDUs transmitted.

Multicast

Properties

Configure multicast properties on this page.

PropertiesSetting	
Unknown Multicast Action	<input type="radio"/> Drop <input checked="" type="radio"/> Flood <input type="radio"/> Router Port
IPv4 Forward Method	<input checked="" type="radio"/> MAC <input type="radio"/> Src-Dst-Ip
IPv6 Forward Method	<input checked="" type="radio"/> MAC <input type="radio"/> Src-Dst-Ip

The page includes the following fields:

Object	Description
Unknown Multicast Action	Unknown multicast traffic method: Drop , Flood or send to Router Port .
IPv4 Forward Method	Configure the IPv4 multicast forward method.
IPv6 Forward Method	Configure the IPv6 multicast forward method.

Buttons

- Click **Apply** to apply changes.

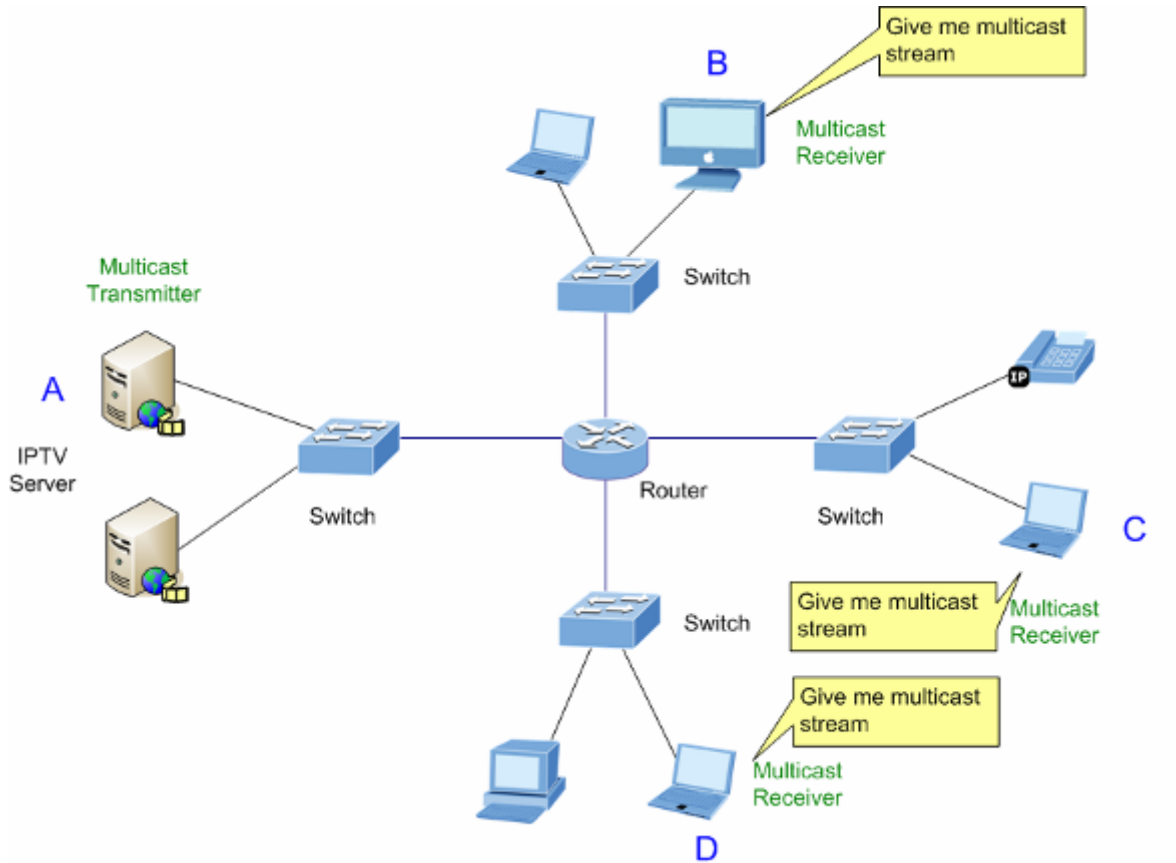
IGMP snooping

The Internet Group Management Protocol (IGMP) allows hosts and routers to 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.

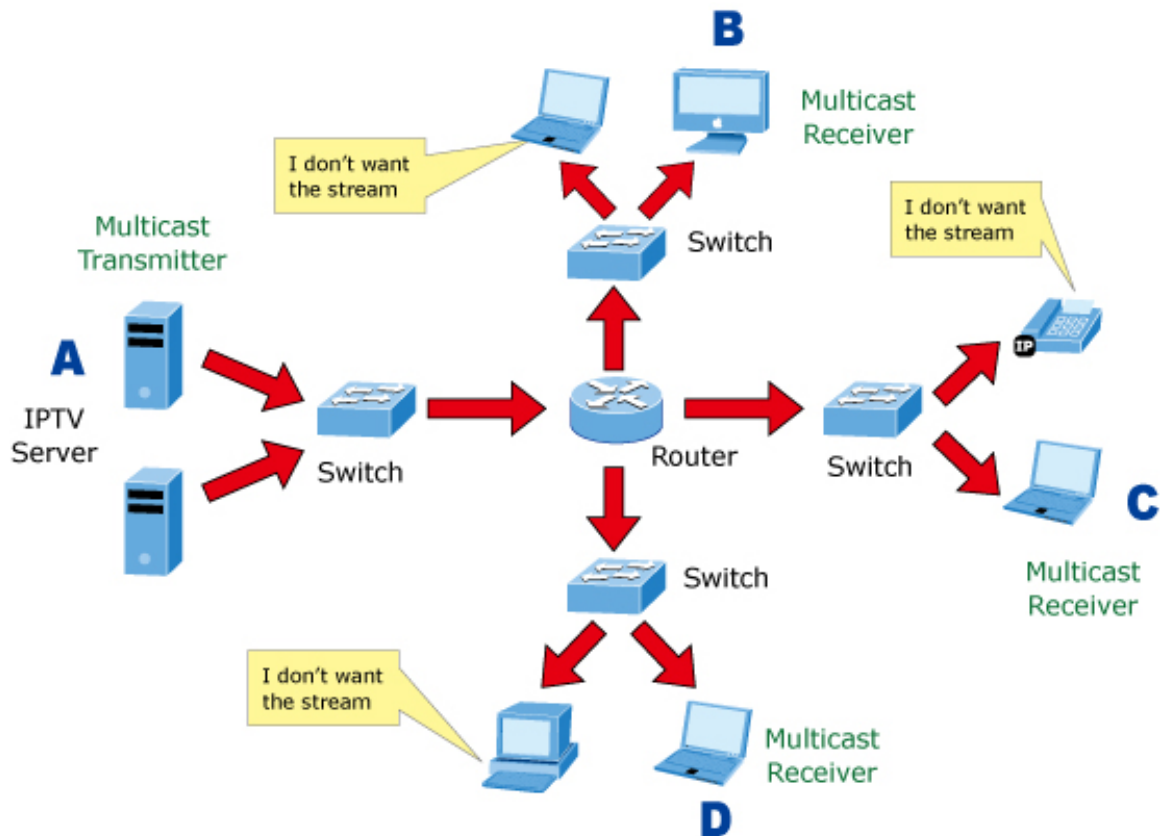
About IGMP snooping

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 'queried.' 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.

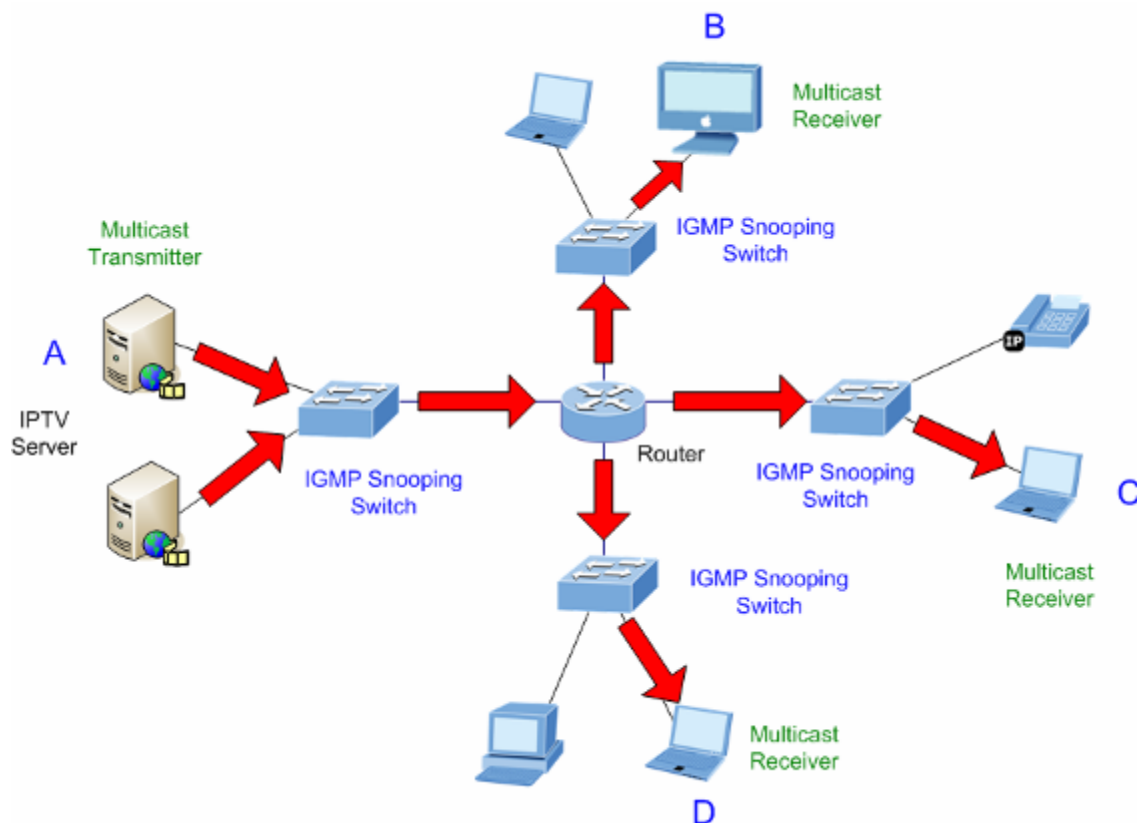
Multicast service



Multicast flooding



IGMP snooping multicast stream control

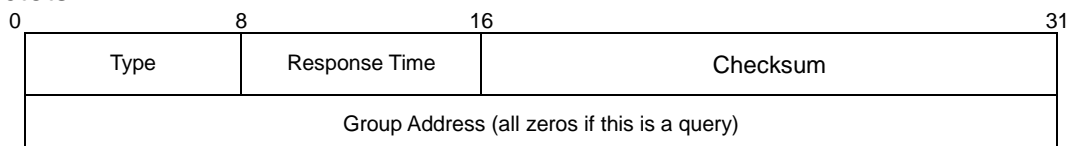


IGMP versions 1 and 2

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.

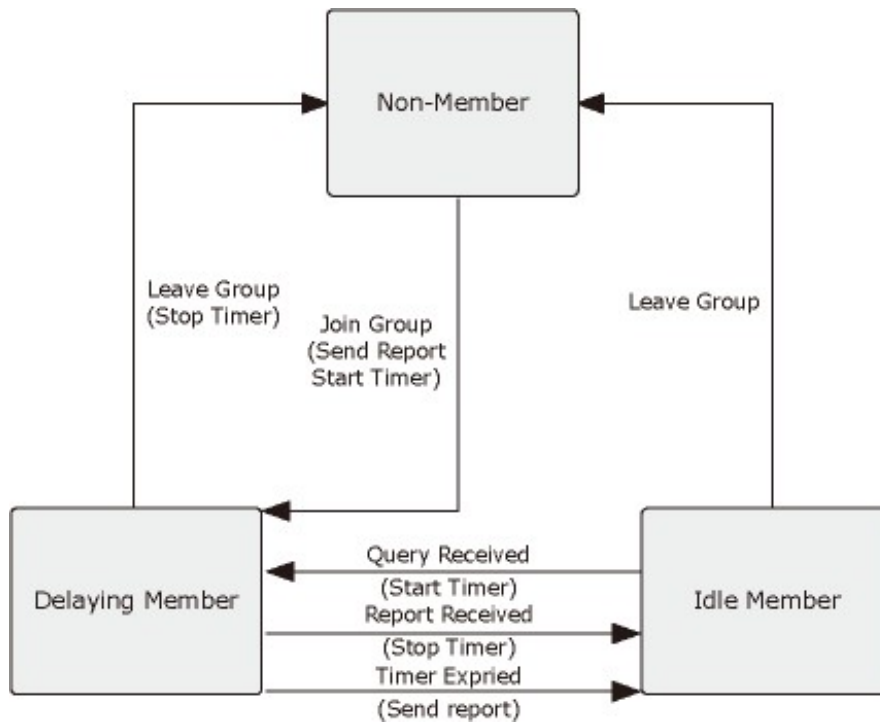
- A host sends an IGMP “report” to join a group
- A host will never send a report when it wants to leave a group (for version 1).
- A host will send a “leave” report when it wants to leave a group (for version 2).

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.

IGMP settings

This page provides IGMP snooping-related configuration options. Most of the settings are global, whereas the Router Port configuration is related to the current unit, as reflected by the page header.

IGMP Snooping	
IGMP Snooping Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IGMP Snooping Version	<input checked="" type="radio"/> v2 <input type="radio"/> v3
IGMP Snooping Report Suppression	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

[Apply](#)

The page includes the following fields:

Object	Description
IGMP Snooping Status	Enable or Disable IGMP snooping. The default value is Disable .
IGMP Snooping Version	Sets the IGMP Snooping operation version. Possible versions are: v2 : Set IGMP Snooping supported IGMP version 2. v3 : Set IGMP Snooping supported IGMP version 3.
IGMP Snooping Report Suppression	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all IGMP reports are sent as-is to multicast-capable routers. The default is Enable .

Buttons

- Click **Apply** to apply changes.
- Click **Edit** to edit parameters.

IGMP querier setting

IGMP Querier Setting		
VLAN ID	Querier State	Querier Version
Select VLANs	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input checked="" type="radio"/> v2 <input type="radio"/> v3

Apply

The page includes the following fields:

Object	Description
VLAN ID	Select VLAN ID from this drop-down menu.
Querier State	Enable or disable the querier state. The default value is "Disabled".
Querier Version	Sets the querier version for compatibility with other devices on the network. Version: 2 or 3; Default: 2

Buttons

- Click **Apply** to apply changes.

IGMP static group

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in previous sections. For certain applications that require tighter control, you may need to statically configure a multicast service on the

industrial managed switch. First, add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

- Static multicast addresses are never aged out.
- When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

VLAN ID	Group IP Address	Member Ports
Select VLANs		Select Ports

Add

The page includes the following fields:

Object	Description
VLAN ID	Select the VLAN ID from this drop-down menu.
Group IP Address	The IP address for a specific multicast service.
Member Ports	Select a port number from this drop-down menu.

Buttons

- Click **Add** to add an IGMP router port entry.
- Click **Edit** to edit parameters.

IGMP router setting

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the industrial managed switch.

VLAN ID	Type	Static Ports Select	Forbid Ports Select
Select VLANs	<input checked="" type="radio"/> Static <input type="radio"/> Forbid	Select Static Ports	Select Forbid Ports

Add

The page includes the following fields:

Object	Description
VLAN ID	Selects the VLAN to propagate all multicast traffic coming from the attached

Object	Description
	multicast router.
Type	Sets the Router port type: Static Forbid
Static Ports Select	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.
Forbid Port Select	Forbid certain ports from acting as router ports.

Buttons

- Click **Add** to add a IGMP router port entry.
- Click **Edit** to edit parameters.
- Click **Delete** to delete the group ID entry.

IGMP forward all

Forward All

VLAN ID : 1

Port	Membership
GE1	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE2	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE3	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None

Apply

The page includes the following fields:

Object	Description
VLAN ID	Select the VLAN ID from this drop-down menu to assign IGMP membership.
Port	The switch port number of the logical port.
Membership	Select IGMP membership for each interface: Forbidden: Interface is forbidden from automatically joining the IGMP via MVR. None: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface. Static: Interface is a member of the IGMP.

Buttons

- Click **Apply** to apply changes.

IGMP snooping statistics

This page provides IGMP snooping statistics.

Statistics Packets	Counter
Total RX	18
Valid RX	8
Invalid RX	10
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Specail Group Query RX	0
Specail Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Specail Group Query TX	0
Specail Group & Source Query TX	0

The page includes the following fields:

Object	Description
Total RX	The current total RX.
Valid RX	The current valid RX.
Invalid RX	The current invalid RX.
Other RX	The current other RX.
Leave RX	The current leave RX.
Report RX	The current report RX.
General Query RX	The current general query RX
Special Group Query RX	The current special group query RX
Special Group & Source Query RX	The current special group & source query RX.
Leave TX	The current leave TX
Report TX	The current report TX

Object	Description
General Query TX	The current general query TX
Special Group Query TX	The current special group query TX
Special Group & Source Query TX	The current special group & source query TX

Buttons

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

MLD snooping

MLD setting

This page provides MLD snooping-related configuration options. Most of the settings are global, whereas the Router Port configuration is related to the current unit, as reflected by the page header.

MLD Snooping

MLD Snooping Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MLD Snooping Version	<input checked="" type="radio"/> v1 <input type="radio"/> v2
MLD Snooping Report Suppression	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

The page includes the following fields:

Object	Description
MLD Snooping Status	Enable or disable the MLD snooping. The default value is Disable .
MLD Snooping Version	Sets the MLD Snooping operation version. Possible versions are: v1 : Set MLD Snooping supported MLD version 1. v2 : Set MLD Snooping supported MLD version 2.
MLD Snooping Report Suppression	Limits the membership report traffic sent to multicast-capable routers. When you disable report suppression, all MLD reports are sent as-is to multicast-capable routers. The default is Enable .

Buttons

- Click **Apply** to apply changes.
- Click **Edit** to edit parameters in the MLD snooping table.

MLD static group

Add Mld Static Group

VLAN ID	Group IP Address	Member Ports
<input type="text" value="Select VLANs"/>	<input type="text" value="::"/>	<input type="text" value="Select Ports"/>

The page includes the following fields:

Object	Description
VLAN ID	Select the VLAN ID from this drop-down menu.
Group IP Address	The IP address for a specific multicast service.
Member Ports	Select a port number from this drop-down menu.

Buttons

- Click **Apply** to apply changes.
- Click **Edit** to edit parameters in the MLD Static Groups table.

MLD router setting

Depending on your network connections, MLD snooping may not always be able to locate the MLD querier. Therefore, if the MLD querier is a known multicast router/switch connected over the network to an interface (port or trunk) on the industrial managed switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

Add Router Port

VLAN ID	Type	Static Ports Select	Forbid Ports Select
<input type="text" value="Select VLANs"/>	<input checked="" type="radio"/> Static <input type="radio"/> Forbid	<input type="text" value="Select Static Ports"/>	<input type="text" value="Select Forbid Ports"/>

The page includes the following fields:

Object	Description
VLAN ID	Selects the VLAN to propagate all multicast traffic coming from the attached multicast router.
Type	Sets the Router port type: Static Forbid

Object	Description
Static Ports Select	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.
Forbid Port Select	Forbid certain ports from acting as router ports.

Buttons

- Click **Add** to add a IGMP router port entry.
- Click **Edit** to edit parameters in the MLD Router Port Status table.
- Click **Delete** to delete the group ID entry in the MLD Router Port Status table.

MLD routing table

This page includes the Dynamic Router, Static Router, and Forbidden Router table information.

Dynamic Router Table		
VLAN ID	Port	Expiry Time (Sec)

Static Router Table	
VLAN ID	PortMask

Forbidden Router Table	
VLAN ID	PortMask

MLD forward all

Forward All

VLAN ID : 1

Port	Membership
GE1	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE2	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None
GE3	<input type="radio"/> Static <input type="radio"/> Forbidden <input checked="" type="radio"/> None

Apply

The page includes the following fields:

Object	Description
VLAN ID	Select the VLAN ID from this drop-down menu to assign MLD membership.
Port	The switch port number of the logical port.
Membership	Select MLD membership for each interface: Forbidden: Interface is forbidden from automatically joining the MLD via MVR. None: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface. Static: Interface is a member of the MLD.

Buttons

- Click **Apply** to apply changes.

MLD snooping statistics

This page provides MLD snooping statistics.

Statistics Packets	Counter
Total RX	0
Valid RX	0
Invalid RX	0
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Specail Group Query RX	0
Specail Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Specail Group Query TX	0
Specail Group & Source Query TX	0

The page includes the following fields:

Object	Description
Total RX	The current total RX.
Valid RX	The current valid RX.
Invalid RX	The current invalid RX.
Other RX	The current other RX.
Leave RX	The current leave RX.
Report RX	The current report RX.
General Query RX	The current general query RX
Special Group Query RX	The current special group query RX
Special Group & Source Query RX	The current special group & source query RX.
Leave TX	The current leave TX
Report TX	The current report TX
General Query TX	The current general query TX
Special Group Query TX	The current special group query TX
Special Group & Source Query TX	The current special group & source query TX

Buttons

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

Multicast throttling setting

Multicast 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 multicast 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.

After configuring multicast profiles, you can assign them to interfaces on the industrial managed switch. The multicast throttling number can also be set to limit the number of multicast groups an interface can join at the same time.

IP Type	Port Select	Max Groups	Action
ipv4	Select Ports	256 (0-256)	<input checked="" type="radio"/> Deny <input type="radio"/> Replace

Apply

The page includes the following fields:

Object	Description
IP Type	Select IPv4 or IPv6 from this drop-down menu.
Port Select	Select a port number from this drop-down menu.
Max Groups	Sets the maximum number of multicast groups an interface can join at the same time. Range: 0-256; Default: 256
Action	Sets the action to take when the maximum number of multicast groups for the interface has been exceeded. (Default: Deny) Deny - The new multicast group join report is dropped Replace - The new multicast group replaces an existing group

Buttons

- Click **Apply** to apply changes.

Multicast filter

In certain switch applications, the administrator may want to control the multicast services available to end users. For example, an IP/TV service is based on a specific subscription plan. The multicast filtering feature fulfills this requirement by restricting access to specified multicast services on a switch port.

Multicast filtering enables you to assign a profile to a switch port that specifies multicast groups that are permitted or denied on the port. A multicast filter profile can contain one

or more, or a range of multicast addresses; but only one profile can be assigned to a port. When enabled, multicast join reports received on the port are checked against the filter profile. If a requested multicast group is permitted, the multicast join report is forwarded as normal. If a requested multicast group is denied, the multicast join report is dropped.

When you have created a Multicast profile number, you can then configure the multicast groups to filter and set the access mode.

Command Usage

- Each profile has only one access mode; either permit or deny.
- When the access mode is set to permit, multicast join reports are processed when a multicast group falls within the controlled range.
- When the access mode is set to deny, multicast join reports are only processed when the multicast group is not in the controlled range.

Multicast profile setting

Add Profile

Ip Type	ipv4 <input type="button" value="v"/>
Profile Index	<input type="text" value="1"/> (1-128)
Group from	<input type="text"/>
Group to	<input type="text"/>
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny

The page includes the following fields:

Object	Description
IP Type	Select IPv4 or IPv6 from this drop-down menu
Profile Index	Indicates the ID of this particular profile
Group from	Specifies multicast groups to include in the profile. Specify a multicast group range by entering a start IP address.
Group to	Specifies multicast groups to include in the profile. Specify a multicast group range by entering an end IP address.
Action	<p>Sets the access mode of the profile; either permit or deny.</p> <p>Permit Multicast join reports are processed when a multicast group falls within the controlled range.</p> <p>Deny When the access mode is set to, multicast join reports are only processed when the multicast group is not in the controlled range.</p>

Buttons

Click **Add** to add a multicast profile entry.

- Click **Edit** to edit parameters in the IGMP/MLD Profile Status page.
- Click **Delete** to delete the IGMP/MLD profile entry in the IGMP/MLD Profile Status page.

IBMP filter setting

The page includes the following fields:

Object	Description
Port Select	Select a port number from this drop-down menu.
Filter Profile ID	Select a filter profile ID from this drop-down menu.

Buttons

- Click **Apply** to apply changes.
- Click **Show** to display parameters in the Port Filter Status page.
- Click **Delete** to delete the IGMP profile entry in the Port Filter Status page.

MLD filter setting

The page includes the following fields:

Object	Description
Port Select	Select a port number from this drop-down menu.
Filter Profile ID	Select a filter profile ID from this drop-down menu.

Buttons

- Click **Apply** to apply changes.
- Click **Show** to display parameters in the Port Filter Status page.

- Click **Delete** to delete the MLD profile entry in the Port Filter Status page.

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.

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).

The QoS page of the industrial managed switch contains three types of QoS mode, all of which rely on predefined fields within the packet to determine the output queue:

- **802.1p Tag Priority** – The output queue assignment is determined by the IEEE 802.1p VLAN priority tag.
- **IP DSCP** – The output queue assignment is determined by the TOS or DSCP field in the IP packets.

- **Port-Base Priority** – Any packet received from the specify high priority port will treated as a high priority packet.

The industrial managed switch supports an eight priority level queue, and the queue service rate is based on the WRR(Weight Round Robin) and WFQ (Weighted Fair Queuing) alorithm. The WRR ratio of high-priority and low-priority can be set to 4:1 and 8:1.

General

QoS properties

QoS Global Setting

QoS Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Basic
-----------------	--

The page includes the following fields:

Object	Description
QoS Mode	Enable or disable QoS mode.

Buttons

- Click **Apply** to apply changes.

QoS port settings

Port Port Settings

Port	CoS Value	Remark CoS	Remark DSCP	Remark IP Precedence
<input type="button" value="Select Ports"/>	0	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

The page includes the following fields:

Object	Description
Port Select	Select a port number from this drop-down menu.
CoS Value	Select CoS value from this drop-down menu
Remark CoS	Disable or enable remark CoS
Remark DSCP	Disable or enable remark DSCP
Remark IP Precedence	Disable or enable remark IP Precedence

Buttons

- Click **Apply** to apply changes.

Queue settings

Queue Table				
Queue	Scheduling Method			
	Strict Priority	WRR	Weight	% of WRR Bandwidth
1	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="1"/>	
2	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="2"/>	
3	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="3"/>	
4	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="4"/>	
5	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="5"/>	
6	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="9"/>	
7	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="13"/>	
8	<input checked="" type="radio"/>	<input type="radio"/>	<input type="text" value="15"/>	

The page includes the following fields:

Object	Description
Queue	The current queue ID.
Strict Priority	Determines if the scheduler mode is "Strict Priority" on this switch port.
WRR	Determines if the scheduler mode is "Weighted" on this switch port
Weight	Determines the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".
% of WRR Bandwidth	The current bandwidth for each queue.

Buttons

- Click **Apply** to apply changes.

CoS mapping

CoS to Queue Mapping								
Class of Service	0	1	2	3	4	5	6	7
Queue	<input type="text" value="2"/>	<input type="text" value="1"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="5"/>	<input type="text" value="6"/>	<input type="text" value="7"/>	<input type="text" value="8"/>

Queue to CoS Mapping								
Queue	1	2	3	4	5	6	7	8
Class of Service	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="5"/>	<input type="text" value="6"/>	<input type="text" value="7"/>

The page includes the following fields:

Object	Description
Queue	Select a Queue value from this drop-down menu.
Class of Service	Select a CoS value from this drop-down menu.

Buttons

- Click **Apply** to apply changes.

DSCP mapping

DSCP to Queue Mapping

DSCP	Queue
Select DSCP	1

Queue to DSCP Mapping

Queue	1	2	3	4	5	6	7	8
DSCP	0	8	16	24	32	40	48	56

[Apply](#)

The page includes the following fields:

Object	Description
Queue	Select a Queue value from this drop-down menu.
DSCP	Select DSCP value from this drop-down menu.

Buttons

- Click **Apply** to apply changes.

IP precedence mapping

IP Precedence to Queue Mapping

IP Precedence	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

Queue to IP Precedence Mapping

Queue	1	2	3	4	5	6	7	8
IP Precedence	0	1	2	3	4	5	6	7

[Apply](#)

The page includes the following fields:

Object	Description
Queue	Select a Queue value from this drop-down menu.
IP Precedence	Select IP Precedence value from this drop-down menu.

Buttons

- Click **Apply** to apply changes.

QoS basic mode

Global settings

The page includes the following fields:

Object	Description
Trust Mode	Set the QoS mode.

Buttons

- Click **Apply** to apply changes.

Port settings

The page includes the following fields:

Object	Description
Port	Select a port number from this drop-down menu.
Trust Mode	Set the trust mode to Enabled or Disabled .

Buttons

- Click **Apply** to apply changes.

Rate Limit

Configure the switch port rate limit for the switch port on this page.

Ingress bandwidth control

Select the ingress bandwidth preamble on this page.

Ingress Bandwidth Control Settings

Port	State	Rate(Kbps)
<input type="text" value="Select Ports"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input style="width: 100%;" type="text"/> (0-1000000, must a multiple of 16)

The page includes the following fields:

Object	Description
Port	Select a port number from this drop-down menu.
State	Enable or Disable the port rate policer. The default value is Disabled .
Rate (Kbps)	Configure the rate for the port policer. The default value is "unlimited". Valid values are in the range 0 to 1000000.

Buttons

- Click **Apply** to apply changes.

Egress bandwidth control

Select the egress bandwidth preamble on this page.

Egress Bandwidth Control Settings

Port	State	Rate(Kbps)
<input type="text" value="Select Ports"/>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input style="width: 100%;" type="text"/> (0-1000000, must a multiple of 16)

The page includes the following fields:

Object	Description
Port	Select a port number from this drop-down menu.
State	Enable or Disable the port rate policer. The default value is Disabled .
Rate (Kbps)	Configure the rate for the port policer. The default value is "unlimited". Valid values are in the range 0 to 1000000.

Buttons

- Click **Apply** to apply changes.

Egress queue

Select the egress queue bandwidth control settings on this page.

Egress Queue Bandwidth Control Settings

Port	Queue	State	CIR(Kbps)
GE1 ▼	1 ▼	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<input style="width: 100%;" type="text"/> (0-1000000, must a multiple of 16)

The page includes the following fields:

Object	Description
Port	Select a port number from this drop-down menu.
Queue	Select a queue number from this drop-down menu.
State	Enable or Disable the port rate policer. The default value is Disabled .
CIR (Kbps)	Configure the CIR for the port policer. The default value is "unlimited". Valid values are in the range 0 to 1000000.

Buttons

- Click **Apply** to apply changes.

Voice VLAN

Introduction

Configure the switch port rate limit for the switch port on this page.

Voice VLAN is specially configured for user voice data traffic. By setting a Voice VLAN and adding the ports of the connected voice equipment to Voice VLAN, the user can to configure QoS (Quality of service) service for voice data, and improve voice data traffic transmission priority to ensure calling quality.

The switch can judge if the data traffic is the voice data traffic from specified equipment according to the source MAC address field of the data packet entering the port. The packet with the source MAC address complying with the system defined voice equipment OUI (Organizationally Unique Identifier) will be considered the voice data traffic and transmitted to the Voice VLAN.

The configuration is based on the MAC address, acquiring a mechanism in which every piece of voice equipment transmitting information through the network has its own unique MAC address. VLAN traces the address belonging to the specified MAC. By this means, VLAN permits the voice equipment to always belong to Voice VLAN when relocated physically. The greatest advantage of the VLAN is that the equipment can be automatically placed into Voice VLAN according to its voice traffic which will be transmitted at a specified priority. Meanwhile, when voice equipment is physically relocated, it still belongs to the Voice VLAN without any further configuration modification, which is because it is based on voice equipment other than the switch port.

Note: The Voice VLAN feature enables the voice traffic to forward on the Voice VLAN, and then the switch can be classified and scheduled to network traffic. We recommend two VLANs on a port -- one for voice and one for data.

Note: 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.

Properties

Properties	
Voice VLAN State	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Voice VLAN Id	<input type="text" value=""/> <input type="checkbox"/> Enable
Remark Cos/802.1p	<input type="text" value="6"/> <input type="button" value="v"/>
1p remark	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Aging Time(30-65536 min)	<input type="text" value="1440"/>

The page includes the following fields:

Object	Description
Voice VLAN State	Indicates the Voice VLAN mode operation. The MSTP feature must be disabled before Voice VLAN is enabled to avoid an ingress filter conflict. Selections include: Enabled: Enable Voice VLAN mode operation. Disabled: Disable Voice VLAN mode operation
Voice VLAN ID	Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is conflict configuration if the value equal management VID, MVR VID, PVID, etc. The allowed range is 1 to 4095.
Remark CoS/802.1p	Select 802.1p value from this drop-down menu
1p remark	Enabled or Disabled 802.1p remark
Aging Time (30-65536 min)	The time after which a port is removed from the Voice VLAN when VoIP traffic is no longer received on the port. (\Default: 1440 minutes).

Buttons

- Click **Apply** to apply changes.

Telephony OUI MAC setting

The page includes the following fields:

Object	Description
OUI Address	A 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	User-defined text that identifies VoIP devices.

Buttons

- Click **Apply** to apply changes.
- Click **Edit** to edit voice VLAN OUI group parameters on the Voice VLAN OUI Group page.
- Click **Delete** to delete voice VLAN OUI group parameters.

Telephony OUI port setting

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN so that the switch can classify and schedule network traffic. We recommend 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.

The page includes the following fields:

Object	Description
Port	Select a port number from this drop-down menu
State	Enable or disable the voice VLAN port setting. The default value is Disabled .

Object	Description
CoS Mode	Select the current CoS mode

Buttons

- Click **Apply** to apply changes.

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:

- 802.1x
- Radius Server
- TACACS+ Server
- AAA
- Access
- Management Access Method
- DHCP Snooping
- Dynamic ARP Inspection
- IP Source Guard
- Port Security
- DoS
- Storm Control

802.1X

In the 802.1X protocol, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (Extensible Authentication Protocol over LAN) 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 (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange

frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. In addition to 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 User Authentication

The industrial managed switch can be configured to authenticate users logging into the system for management access using local or remote authentication methods, such as telnet and web browser. This 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

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 available any services offered by the switch or the LAN.

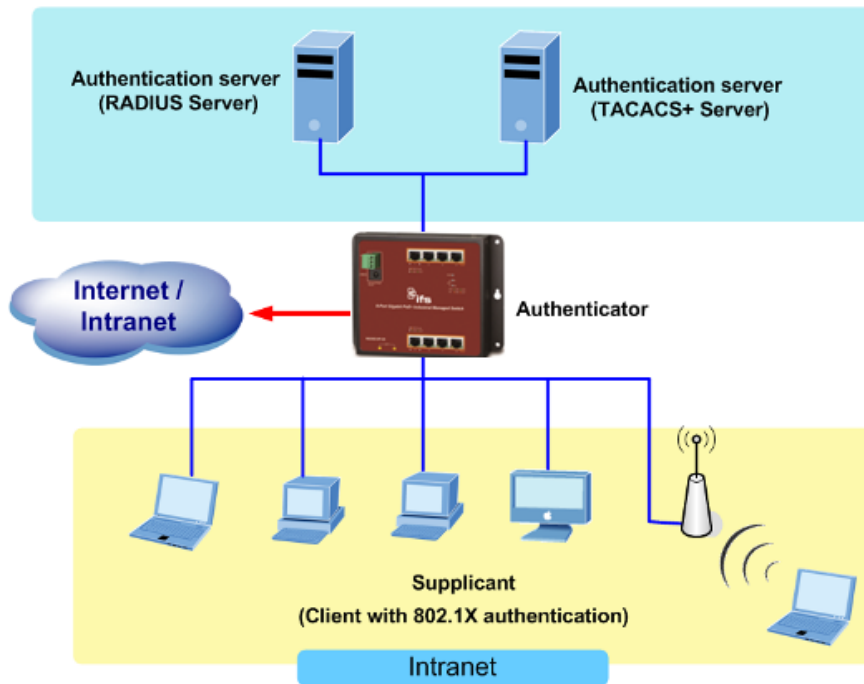
Until the client is authenticated, 802.1X access control allows only EAPOL traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

This section includes this conceptual information:

- Device Roles
- Authentication Initiation and Message Exchange
- Ports in Authorized and Unauthorized States

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 Windows 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; it is available in 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.

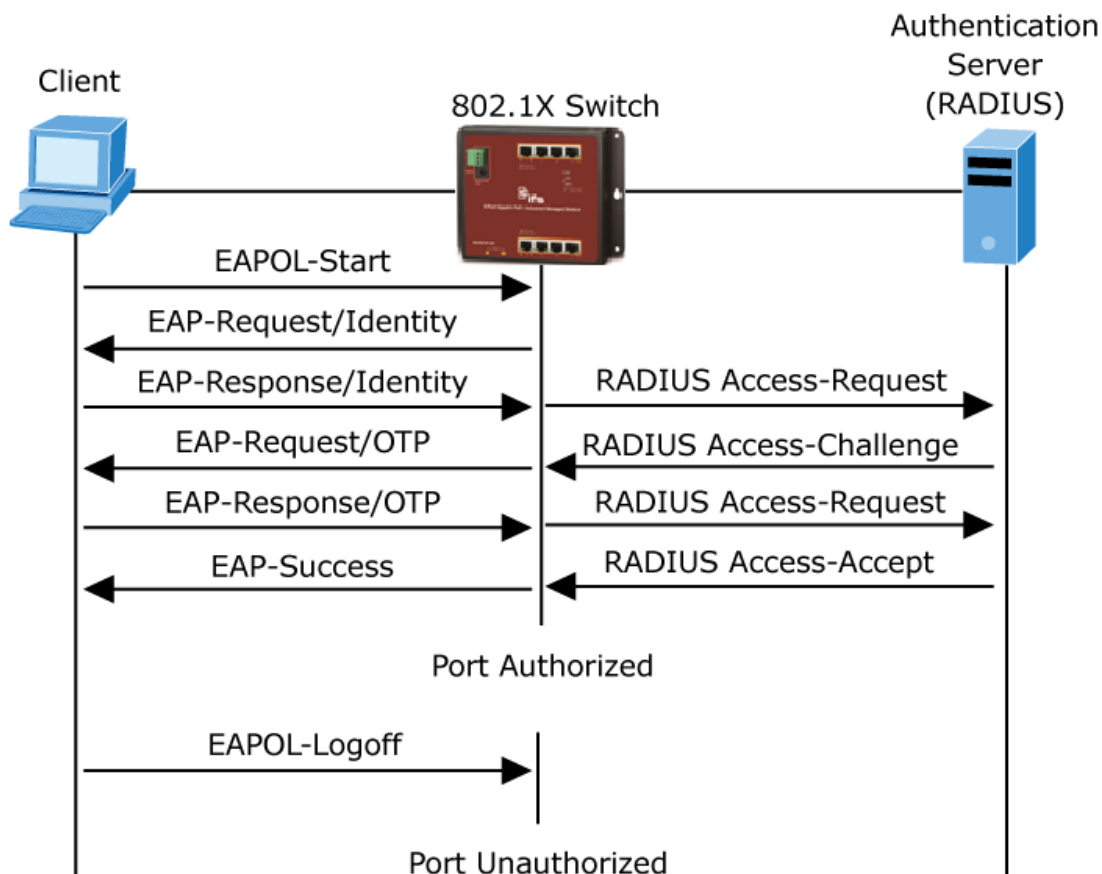
Authentication initiation and message exchange

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.

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 is 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 a fixed number of times. If 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.

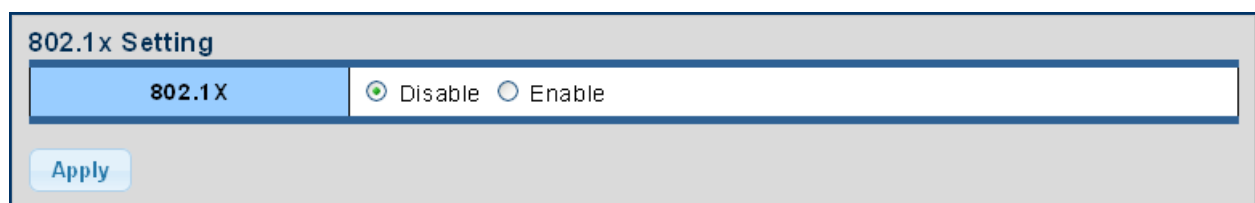
When a client logs off, it sends an EAPOL-logoff message, causing the switch port to transition to the unauthorized state.

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.

802.1X setting

Configure the IEEE 802.1X authentication system on this 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, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "Security→802.1X Access Control→802.1X Setting" page. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations as demonstrating in the following sections.



The screenshot shows a web configuration interface for 802.1X settings. The title is "802.1x Setting". Below the title is a blue header bar containing the text "802.1X" and two radio buttons: "Disable" (which is selected) and "Enable". Below the header bar is an "Apply" button.

The page includes the following fields:

Object	Description
802.1X	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports allow frame forwarding.

Buttons

- Click **Apply** to apply changes.

802.1X port setting

Configure the IEEE 802.1X port settings on this page.

802.1x Port Setting

Port	Select Ports ▼
Mode	No Authentication ▼
Reauthentication Enable	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Reauthentication Period	<input type="text" value="3600"/> (Range 30 - 65535, Default: 3600)
Quiet Period	<input type="text" value="60"/> (Range 0 - 65535, Default: 60)
Supplicant Period	<input type="text" value="30"/> (Range 1 - 65535, Default: 30)
Maximum Request Retries	<input type="text" value="2"/> (Range 1 - 10, Default: 2)

The page includes the following fields:

Object	Description
Port	Select a port from the drop-down menu.
Mode	<p>If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:</p> <p>No Authentication</p> <p>Authentication</p> <p>Force Authorized</p> <p>In this mode, the switch will send one EAPOL Success frame when the port link appears, and any client on the port will be permitted to access the network without authentication.</p> <p>Force Unauthorized</p> <p>In this mode, the switch sends one EAPOL Failure frame when the port link appears, and any client on the port will not be permitted to access the network.</p>
Reauthentication Enable	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.

Object	Description
Reauthentication Period	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 30 to 65535 seconds.
Quiet Period	Sets the amount of time to keep silent on supplicant authentication failure.
Supplicant Period	Sets the interval for the supplicant to re-transmit EAP request/identify frame.
Maximum Request Retries	The number of times that the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN. The value can only be changed if the Guest VLAN option is globally enabled.

Buttons

- Click **Apply** to apply changes.
- Click **Edit** to edit port parameters in the Modify column.

Guest VLAN setting

When a Guest VLAN enabled port's link is recognized, 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 will be 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 will be 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" is disabled.

The page includes the following fields:

Object	Description
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 can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1~4094].
Guest VLAN Enabled	A Guest VLAN is a special VLAN - typically with limited network access - where 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 ID Enable checkbox 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 Port Setting	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).

Buttons

- Click **Apply** to apply changes.

Authenticated host table

The page includes the following fields:

Object	Description
User Name	The current user name.
Port	The current port number.

Object	Description
Session Time	The current session time.
Authentication Method	The current authentication method.
MAC Address	The current MAC address.

RADIUS server

Configure the RADIUS servers on the RADIUS settings page.

Use Default Parameters

IP Version	Version 6 Version 4
Retries	<input type="text" value="3"/> (Range 1 - 10, Default: 3)
Timeout for Reply	<input type="text" value="3"/> sec. (Range 1 - 30, Default: 3)
Dead Time	<input type="text" value="0"/> min. (Range 0 - 2000, Default: 0)
Key String	<input type="text"/> (0/63 ASCII Alphanumeric Characters Used)

The page includes the following fields:

Object	Description
Retries	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.
Timeout for Reply	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	<p>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.</p> <p>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.</p>
Key String	The secret key – up to 63 characters long – shared between the RADIUS server and the switch.

Buttons

- Click **Apply** to apply changes.

New Radius server configuration

New Radius Server

Server Definition	<input checked="" type="radio"/> By IP address <input type="radio"/> By name
Server IP	<input type="text"/>
Authentication Port	<input type="text" value="1812"/> (0 - 65535)
Acct Port	<input type="text" value="1813"/> (0 - 65535)
Key String	<input checked="" type="checkbox"/> Use Default <input type="text"/>
Timeout for Reply	<input checked="" type="checkbox"/> Use Default <input type="text"/> (1-30) secs
Retries	<input checked="" type="checkbox"/> Use Default <input type="text"/> (1 - 10)
Server Priority	<input type="text" value="1"/> (0 - 65535)
Dead Time	<input type="text" value="0"/> (0 - 2000)
Usage Type	<input type="radio"/> Login <input type="radio"/> 802.1X <input checked="" type="radio"/> All

The page includes the following fields:

Object	Description
Server Definition	Set the server definition.
Server IP	Address of the Radius server IP/name
Authentication Port	The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.
Acct Port	The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.
Retries	Timeout is the number of seconds, in the range 1 to 10, to wait for a reply from a RADIUS server before retransmitting the request.
Timeout for Reply	Retransmit is the number of times, in the range 1 to 30, 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	<p>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.</p> <p>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.</p>
Key String	The secret key – up to 63 characters long – shared between the RADIUS server and the switch.
Server Priority	Set the server priority.
Usage Type	Set the usage type. The following modes are available: Login

Object	Description
	802.1X
	All

Buttons

- Click **Apply** to apply changes.
- Click **Edit** to edit port parameters in the Modify column.
- Click **Delete** to delete a login interface entry.

TACACS+ server

The TACACS+ Server Configuration page permits configuration of the TACACS+ Servers.

Use Default Parameters

IP Version	Version 6 Version 4
Key String	<input type="text"/> (0/63 ASCII Alphanumeric Characters Used)
Timeout for Reply	<input type="text" value="5"/> sec. (Range 1 - 30, Default: 5)

The page includes the following fields:

Object	Description
Timeout for Reply	Retransmit is the number of times, in the range 1 to 30, a TACACS+ 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.
Key String	The secret key – up to 63 characters long – shared between the RADIUS server and the switch.

Buttons

- Click **Apply** to apply changes.

New TACACS+ server configuration

New Tacacs+ Server

Server Definition	<input checked="" type="radio"/> By IP address <input type="radio"/> By name
Server IP	<input type="text"/>
Server Port	<input type="text" value="49"/> (0 - 65535)
Server Key	<input checked="" type="checkbox"/> Use Default <input type="text"/>
Server Timeout	<input checked="" type="checkbox"/> Use Default <input type="text"/> (1-30) secs
Server Priority	<input type="text" value="1"/> (0 - 65535)

The page includes the following fields:

Object	Description
Server Definition	Set the server definition
Server IP	Address of the TACACS+ server IP/name
Server Port	Network (TCP) port of TACACS+ server used for authentication messages. (Range: 1-65535; Default: 49)
Server Key	The key- shared between the TACACS+ Authentication Server and the switch.
Server Timeout	The number of seconds the switch waits for a reply from the server before it resends the request.
Server Priority	Set the server priority

Buttons

- Click **Add** to add a new TACACS+server.
- Click **Edit** to edit port parameters in the Modify column.
- Click **Delete** to delete a login interface entry.

AAA

Authentication, authorization, and accounting (AAA) provides a framework for configuring access control on the industrial managed switch. Its three security functions can be summarized as follows:

- **Authentication** — Identifies users that request access to the network.
- **Authorization** — Determines if users can access specific services.
- **Accounting** — Provides reports, auditing, and billing for services that users have accessed on the network.

The AAA functions require the use of configured RADIUS or TACACS+ servers in the network. The security servers can be defined as sequential groups that are then

applied as a method for controlling user access to specified services. For example, when the switch attempts to authenticate a user, a request is sent to the first server in the defined group, if there is no response the second server will be tried, and so on. If at any point a pass or fail is returned, the process stops.

The industrial managed switch supports the following AAA features:

- Accounting for IEEE 802.1X authenticated users that access the network through the industrial managed switch.
- Accounting for users that access management interfaces on the industrial managed switch through the Telnet.
- Accounting for commands that users enter at specific CLI privilege levels. Authorization of users that access management interfaces on the industrial managed switch through the Telnet.

To configure AAA on the industrial managed switch, follow this general process:

1. Configure RADIUS and TACACS+ server access parameters. See “Configuring Local/Remote Logon Authentication”.
2. Define RADIUS and TACACS+ server groups to support the accounting and authorization of services.
3. Define a method name for each service to which you want to apply accounting or authorization and specify the RADIUS or TACACS+ server groups to use. Apply the method names to port or line interfaces.

Note: This guide assumes that RADIUS and TACACS+ servers have already been configured to support AAA. Refer to the documentation provided with the RADIUS or TACACS+ server software for further server software configuration details.

Login list

Configure login list parameters on this page.

New Authentication List

List Name	Method 1	Method 2	Method 3	Method 4
<input style="width: 100%;" type="text"/>	Empty ▼	Empty ▼	Empty ▼	Empty ▼

The page includes the following fields:

Object	Description
List Name	Defines a name for the authentication list.
Method 1-4	Set the login authentication method: Empty / None / Local / TACACS+ / RADIUS / Enable

Buttons

- Click **Add** to add a new authentication list.
- Click **Edit** to edit login authentication list parameters in the Modify column.
- Click **Delete** to delete a login authentication list entry.

Enable list

Configure login list parameters on this page.

The page includes the following fields:

Object	Description
List Name	Defines a name for the authentication list.
Method 1-3	Set the login authentication method: Empty / None / TACACS+ / RADIUS / Enable

Buttons

- Click **Add** to add a new authentication list.
- Click **Edit** to edit login authentication list parameters in the Modify column.
- Click **Delete** to delete a login authentication list entry.

Access

Configure the access management of the industrial managed switch via four different methods: Telnet, SSH, HTTP, and HTTPs.

Telnet

Telnet Settings	
Telnet Service	Disabled <input type="button" value="v"/>
Login Authentication List	default <input type="button" value="v"/>
Enable Authentication List	default <input type="button" value="v"/>
Session Timeout	<input type="text" value="10"/> (0-65535) minutes
Password Retry Count	<input type="text" value="3"/> (0-120)
Silent Time	<input type="text" value="0"/> (0-65535) seconds

The page includes the following fields:

Object	Description
Telnet Service	Disable or enable telnet service
Login Authentication List	Select login authentication list from this drop-down menu.
Enable Authentication List	Select enable authentication list from this drop-down menu.
Session Timeout	Set the session timeout value.
Password Retry Count	Set the password retry count value.
Silent Time	Set the silent time value.

Buttons

- Click **Apply** to apply changes.
- Click **Disconnect** to disconnect Telnet communication.
- Click **Delete** to delete a login authentication list entry.

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.

SSH Settings	
SSH Service	Disabled <input type="button" value="v"/>
Login Authentication List	default <input type="button" value="v"/>
Enable Authentication List	default <input type="button" value="v"/>
Session Timeout	<input type="text" value="10"/> (0-65535) minutes
Password Retry Count	<input type="text" value="3"/> (0-120) minutes
Silent Time	<input type="text" value="0"/> (0-65535) seconds

The page includes the following fields:

Object	Description
SSH Service	Disable or enable SSH service.
Login Authentication List	Select login authentication list from this drop-down menu.
Enable Authentication List	Select enable authentication list from this drop-down menu.
Session Timeout	Set the session timeout value.
Password Retry Count	Set the password retry count value.
Silent Time	Set the silent time value.

Buttons

- Click **Apply** to apply changes.
- Click **Disconnect** to disconnect Telnet communication.

HTTP

HTTP Settings	
HTTP Service	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Login Authentication List	default <input type="button" value="v"/>
Session Timeout	<input type="text" value="10"/> (0-86400) minutes

The page includes the following fields:

Object	Description
HTTP Service	Disable or enable HTTP service.
Login Authentication List	Select login authentication list from this drop-down menu.
Session Timeout	Set the session timeout value.

Buttons

- Click **Apply** to apply changes.

HTTPs

Configure HTTPs on the HTTPs Configuration page.

HTTPS Settings

HTTPS Service	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Login Authentication List	default ▼
Session Timeout	10 (0-86400) minutes

The page includes the following fields:

Object	Description
HTTPs Service	Disable or enable HTTPs service.
Login Authentication List	Select login authentication list from this drop-down menu.
Session Timeout	Set the session timeout value.

Buttons

- Click **Apply** to apply changes.

Access management

Profile rules

Profile Rule Table Setting

Access Profile Name (1-32 characters)	Priority(1-65535)	Management Method	Action	Port	IP-Source
<input type="text"/>	1	All ▼	Permit ▼	Select Ports ▼	<input checked="" type="radio"/> All <input type="radio"/> IPv4/Mask 0.0.0.0 <input type="text" value="0.0.0.0"/> <input type="radio"/> IPv6/Prefix 0.0:0.0 <input type="text" value=""/> 128 <input type="text" value=""/>

The page includes the following fields:

Object	Description
Access Profile Name (1-32 characters)	Indicates the access profile name.
Priority (1-65535)	Set priority The allowed value is from 1 to 65535
Management Method	Indicates the host can access the switch from HTTP/HTTPS/telnet/SSH/SNMP/All interface that the host IP address matched the entry.
Action	An IP address can contain any combination of permit or deny rules. (Default: Permit rules) Sets the access mode of the profile; either Permit or Deny .
Port	Select a port from this drop-down menu.
IP-Source	Indicates the IP address for the access management entry.

Buttons

- Click **Apply** to apply changes.
- Click **Edit** to edit profile rules in the Modify column.
- Click **Delete** to delete a profile rules list entry in the Modify column.

Access rules

Access Profile: Active Deactive

The page includes the following fields:

Object	Description
Access Profile	Select an access profile from this drop-down menu.

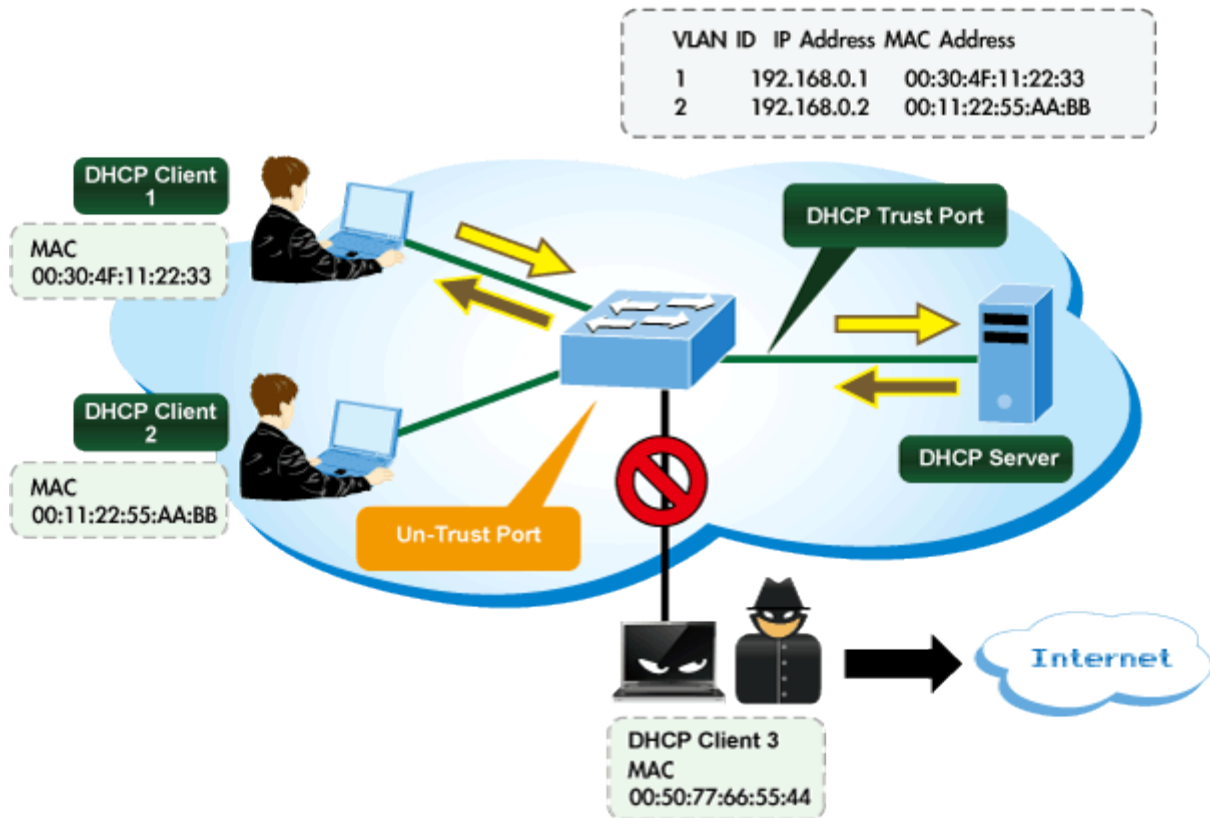
Buttons

- Click **Apply** to apply changes.
- Click **Delete** to delete a access profile entry.

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



Command usage

Table entries are only learned for trusted interfaces. An entry is added or removed dynamically to the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.

When DHCP snooping is enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.

Filtering rules are implemented as follows:

- If the global DHCP snooping is disabled, all DHCP packets are forwarded.
- If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a trusted port. If the received packet is a DHCP ACK message, a dynamic DHCP snooping entry is also added to the binding table.

If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, but the port is not trusted, it is processed as follows:

- If the DHCP packet is a reply packet from a DHCP server (including OFFER, ACK or NAK messages), the packet is dropped.
- If the DHCP packet is from a client, such as a DECLINE or RELEASE message, the switch forwards the packet only if the corresponding entry is found in the binding table.

- If the DHCP packet is from a client, such as a DISCOVER, REQUEST, INFORM, DECLINE or RELEASE message, the packet is forwarded if MAC address verification is disabled. However, if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.
- If the DHCP packet is not a recognizable type, it is dropped.
- If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.
- If a DHCP packet from a server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.
- If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

Additional considerations when the switch itself is a DHCP client:

- The port(s) through which the switch submits a client request to the DHCP server must be configured as trusted. Note that the switch will not add a dynamic entry for itself to the binding table when it receives an ACK message from a DHCP server.
- Also, when the switch sends out DHCP client packets for itself, no filtering takes place. However, when the switch receives any messages from a DHCP server, any packets received from untrusted ports are dropped.

Global setting

Configure DHCP Snooping on the DHCP Snooping Configuration page.

The page includes the following fields:

Object	Description
DHCP Snooping	<p>Indicates the DHCP snooping mode operation. Possible modes are:</p> <p>Enabled: Enable DHCP snooping mode operation.</p> <p>When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports.</p> <p>Disabled: Disable DHCP snooping mode operation.</p>

Buttons

- Click **Apply** to apply changes.

DHCP snooping VLAN setting

When DHCP snooping is enabled globally on the switch, and enabled on the specified VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.

When the DHCP snooping is globally disabled, DHCP snooping can still be configured for specific VLANs, but the changes will not take effect until DHCP snooping is globally enabled.

When DHCP snooping is globally enabled, and DHCP snooping is then disabled on a VLAN, all dynamic bindings learned for this VLAN are removed from the binding table.

The page includes the following fields:

Object	Description
VLAN List	Indicates the ID of this particular VLAN.
DHCP Snooping	Indicates the DHCP snooping mode operation. Possible modes are: Enabled: Enable DHCP snooping mode operation. When enabling the DHCP snooping mode operation, the request DHCP messages are forwarded to trusted ports and only permit reply packets from trusted ports. Disabled: Disable DHCP snooping mode operation.

Buttons

- Click **Apply** to apply changes.

Port setting

A trusted interface is an interface that is configured to receive only messages from within the network. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall.

When DHCP snooping enabled both globally and on a VLAN, DHCP packet filtering will be performed on any untrusted ports within the VLAN.

When an untrusted port is changed to a trusted port, all the dynamic DHCP snooping bindings associated with this port are removed.

Set all ports connected to DHCP servers within the local network or firewall to **Trusted**. Set all other ports outside the local network or firewall to **Untrusted**.

Port	Type	Chaddr Check
Select Ports	<input checked="" type="radio"/> Un Trusted <input type="radio"/> Trusted	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Apply

The page includes the following fields:

Object	Description
Port	Select a port from this drop-down menu.
Type	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.
Chaddr Check	Indicates that the Chaddr check function is enabled on selected port. Chaddr: Client hardware address.

Buttons

- Click **Apply** to apply changes.

Statistics

Port	Forwarded	Chaddr Check Dropped	Untrust Port Dropped	Untrust Port With Option82 Dropped	Invalid Dropped
GE1	0	0	0	0	0
GE2	0	0	0	0	0
GE3	0	0	0	0	0
GE4	0	0	0	0	0

The page includes the following fields:

Object	Description
Port	Select a port from this drop-down menu.
Forwarded	The current forwarded packets.
Chaddr Check Dropped	Dropped chaddr checks.
Untrusted Port Dropped	Untrusted ports dropped.
Untrusted Port with Option82 Dropped	Untrusted ports with option82 dropped.
Invalid Dropped	Invalid dropped packets.

Buttons

- Click **Apply** to apply changes.

Database agent

When DHCP snooping is enabled, the switch uses the DHCP snooping binding database to store information about untrusted interfaces. The database can have up to 8192 bindings.

Each database entry (binding) has an IP address, an associated MAC address, the lease time (in hexadecimal format), the interface to which the binding applies, and the VLAN to which the interface belongs. A checksum value, the end of each entry, is the number of bytes from the start of the file to end of the entry. Each entry is 72 bytes, followed by a space and then the checksum value.

To keep the bindings when the switch reloads, you must use the DHCP snooping database agent. If the agent is disabled, dynamic ARP or IP source guard is enabled, and the DHCP snooping binding database has dynamic bindings, the switch loses its connectivity. If the agent is disabled and only DHCP snooping is enabled, the switch does not lose its connectivity, but DHCP snooping might not prevent DHCP spoofing attacks.

The database agent stores the bindings in a file at a configured location. When reloading, the switch reads the binding file to build the DHCP snooping binding database. The switch keeps the file current by updating it when the database changes.

When a switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database. The switch also updates the entries in the binding file. The frequency at which the file is updated is based on a configurable delay, and the updates are batched. If the file is not updated in a specified time (set by the write-delay and abort-timeout values), the update stops.

DHCP Snooping Database	
Database Type	None <input type="button" value="v"/>
FileName	<input type="text"/>
Remote Server	<input type="text"/> (X.X.X.X or Hostname)
Write Delay	300 (15 ~ 86400 Second)
Timeout	300 (0 ~ 86400 Second)

The page includes the following fields:

Object	Description
Database Type	Select a database type from the drop-down menu.
File Name	The name of file image.
Remote Server	Fill in the remote server IP address
Write Delay	Specify the duration for which the transfer should be delayed after the binding database changes. The range is from 15 to 86400 seconds. The default is 300 seconds (5 minutes).
Timeout	Specify when to stop the database transfer process after the binding database changes. The range is from 0 to 86400. Use 0 for an infinite duration. The default is 300 seconds (5 minutes).

Buttons

- Click **Apply** to apply changes.

Rate limit

After enabling DHCP snooping, the switch monitors all the DHCP messages and implements software transmission. Configure the DHCP Rate Limit Setting on this page.

DHCP Rate Limit Setting

Port	State	Rate Limit (pps)
<div style="border: 1px solid #ccc; border-radius: 4px; padding: 2px; display: inline-block;">Select Ports ▾</div>	<input checked="" type="radio"/> Default <input type="radio"/> User-Define	<div style="border: 1px solid #ccc; border-radius: 4px; padding: 2px; display: inline-block;">Unlimited</div> (1~300 pps)

Apply

The page includes the following fields:

Object	Description
Port	Select a port from the drop-down menu.
State	The name of file image.
Rate Limit (pps)	Configure the rate limit for the port policer. The default value is Unlimited . Valid values are in the range 1 to 300.

Buttons

- Click **Apply** to apply changes.

Option82 Global Setting

DHCP provides a relay mechanism for sending information about the switch and its DHCP clients to DHCP servers. Known as DHCP Option 82, it allows compatible DHCP servers to use the information when assigning IP addresses, or to set other services or policies for clients. It is also an effective tool in preventing malicious network attacks

from attached clients on DHCP services, such as IP Spoofing, Client Identifier Spoofing, MAC Address Spoofing, and Address Exhaustion.

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)
- Remote ID (option 2)

The Circuit ID sub-option includes information specific to which circuit the request came in on.

The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

After enabling DHCP snooping, the switch monitors all the DHCP messages and implement software transmission.

The page includes the following fields:

Object	Description
State	Set the option2 (remote ID option) content of option 82 added by DHCP request packets. Default is the default VLAN MAC format. User-Define is the remote-id content of option 82 specified by users

Buttons

- Click **Apply** to apply changes.

Option82 port setting

This function is used to set the retransmitting policy of the system for the received DHCP request message which contains option82.

- The drop mode means that if the message has option82, then the system will drop it without processing.
- The keep mode means that the system will keep the original option82 segment in the message, and forward it to the server to process
- The replace mode means that the system will replace the option 82 segment in the existing message with its own option 82, and forward the message to the server to process.

Option82 Port Setting

Port	Enable	Allow UnTrusted
<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Select Ports ▾</div>	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Keep ▾</div>

Apply

The page includes the following fields:

Object	Description
Port	Select a port from the drop-down menu.
Enable/Disable	Enable or Disable option82 on the port.
Allow Untrusted	Select modes from this drop-down menu. The following modes are available: Drop Keep Replace

Buttons

- Click **Apply** to apply changes.

Option82 circuit ID setting

By setting a creation method for option82, users can custom-define the parameters of the circuit-id suboption.

Option82 Port Circuit-ID Setting

Port	Vlan	Circuit ID
<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">Select Ports ▾</div>	<input checked="" type="checkbox"/> <input type="checkbox"/> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block; margin-left: 5px;">1</div>	<input checked="" type="radio"/> Default <input type="radio"/> User-Define <div style="border: 1px solid #ccc; width: 80px; height: 15px; display: inline-block;"></div>

Apply

The page includes the following fields:

Object	Description
Port	Select a port from the drop-down menu.
VLAN	Indicates the ID of this particular VLAN
Circuit ID	Set the option1 (Circuit ID) content of option 82 added by DHCP request packets.

Buttons

- Click **Apply** to apply changes.

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.

Note: A Dynamic ARP prevents the untrusted ARP packets based on the DHCP Snooping Database.

Global setting

DAI Setting

DAI
 Enabled Disabled

The page includes the following fields:

Object	Description
DAI	Set Dynamic ARP Inspection to Enabled or Disabled .

Buttons

- Click **Apply** to apply changes.

VLAN setting

DAI VLAN Setting

VLAN LIST	Status
1	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

The page includes the following fields:

Object	Description
VLAN ID	Indicates the ID of this particular VLAN.
Status	Enables Dynamic ARP Inspection on the specified VLAN Options: Enable Disable

Buttons

- Click **Apply** to apply changes.

Port setting

Configure switch ports as DAI trusted or untrusted, and select check modes on this page.

DAI Port Setting

Port	Type	Src-Mac Chk	Dst-Mac Chk	IP Chk	IP Allow Zero
Select Ports ▾	<input checked="" type="radio"/> Un Trusted <input type="radio"/> Trusted	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled

The page includes the following fields:

Object	Description
Port	Select a port from the drop-down menu.
Type	Specify which ports ARP Inspection is enabled on. ARP Inspection is only enabled when both Global Mode and Port Mode on a given port are enabled. All interfaces are untrusted by default.
Src-Mac Chk	Enable or disable to check the source MAC address in the Ethernet header against the sender MAC address in the ARP body. This check is performed on both ARP requests and responses. When enabled, packets with different MAC addresses are classified as invalid and dropped.
Dst-Mac Chk	Enable or disable to check the destination MAC address in the Ethernet header against the target MAC address in ARP body. This check is performed for ARP responses. When enabled, packets with different MAC addresses are classified as invalid and are dropped.
IP Chk	Enable or disable to check the source and destination IP addresses of ARP packets. The all-zero, all-one or multicast IP addresses are considered invalid and the corresponding packets are discarded.
IP Allow Zero	Enable or disable to check all-zero IP addresses.

Buttons

- Click **Apply** to apply changes.

Statistics

Dynamic ARP Inspection Statistics						
Port	Forwarded	Source MAC Failures	Dest MAC Failures	SIP Validation Failures	DIP Validation Failures	IP-MAC Mismatch Failures
GE1	0	0	0	0	0	0
GE2	0	0	0	0	0	0
GE3	0	0	0	0	0	0
GE4	0	0	0	0	0	0

The page includes the following fields:

Object	Description
Port	The switch port number of the logical port.
Forwarded	The current forwarded packets.
Source MAC Failures	The current source MAC failures
Dest MAC Failures	The current destination MAC failures
SIP Validation Failures	The current SIP Validation failures
DIP Validation Failure	The current DIP Validation failures
IP-MAC Mismatch Failures	The current IP-MAC mismatch failures

Buttons

- Click **Clear** to clear the statistics.
- Click **Refresh** to refresh the statistics.

Rate limit

ARP Rate Limit Setting		
Port	State	Rate Limit (pps)
Select Ports	<input checked="" type="radio"/> Default <input type="radio"/> User-Define	<input type="text" value="Unlimited"/> (up to 50 pps)

Apply

The page includes the following fields:

Object	Description
Port	Select a switch port number from the drop-down menu.
State	Select Default or User-Define .
Rate Limit (pps)	Configure the rate limit for the port policer. The default value is Unlimited .

Buttons

- Click **Apply** to apply changes.

IP source guard configuration

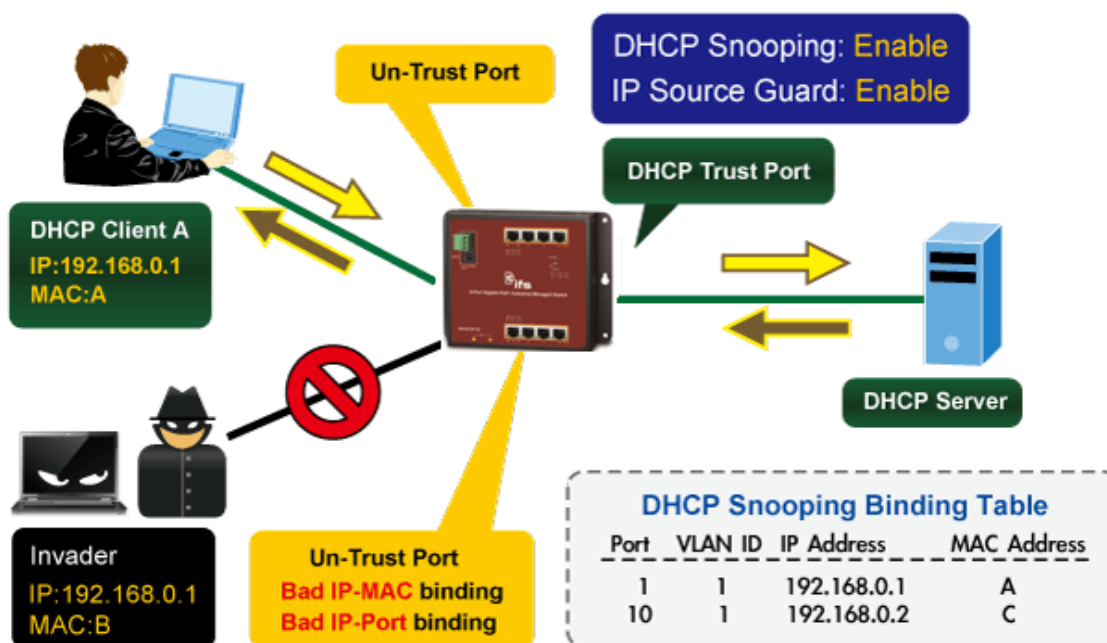
IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

After receiving a packet, the port looks up the key attributes (including IP address, MAC address, and VLAN tag) of the packet in the binding entries of the IP source guard. If there is a matching entry, the port will forward the packet. Otherwise, the port will abandon the packet.

IP source guard filter packets are based on the following types of binding entries:

- IP-port binding entry
- MAC-port binding entry
- IP-MAC-port binding entry

IP Source Guard Overview



The IP Source Guard port setting page provides IP Source Guard-related configuration data.

IP Source Guard Port Setting

Port	Status	Verify Source	Max Binding Entry
Select Ports	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	<input checked="" type="radio"/> IP <input type="radio"/> IP and MAC	No-limited

Apply

The page includes the following fields:

Object	Description
Port	Select a port from the drop-down menu.
Status	Enable or disable the IP source guard
Verify Source	Configures the switch to filter inbound traffic-based IP addresses, or IP addresses and MAC addresses. None Disables IP source guard filtering on the switch. IP Enables traffic filtering based on IP addresses stored in the binding table. IP and MAC Enables traffic filtering based on IP addresses and the corresponding MAC addresses stored in the binding table.
Max Binding Entry	The maximum number of IP source guards that can be secured on this port

Buttons

- Click **Apply** to apply changes.

Binding table

Ip Source Guard Static Binding Entry

Port	VLAN ID	MAC Address	IP Address
GE1	1 (1-4094)	<input checked="" type="checkbox"/>	<input type="text"/>

The page includes the following fields:

Object	Description
Port	Select a port from the drop-down menu.
VLAN ID	Indicates the ID of this particular VLAN.
MAC Address	Sourcing MAC address is permitted.
IP Address	Sourcing IP address is permitted.

- Click **Add** to add an IP source guard static binding table entry.
- Click **Delete** to delete an IP source guard static binding table entry.

Port security

This page allows you to configure the Port Security Limit Control system and port settings. Limit Control permits limitation of 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 Limit Control module is one of the modules that utilize a lower-layer module while the Port Security module manages MAC addresses learned on the port.

The Limit Control configuration consists of two sections: system- and a port-wide.

Port Security Settings			
Port Select	Security	Max L2 Entry	Action
Select Ports ▾	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	Unlimited	Forward ▾

Apply

The page includes the following fields:

Object	Description
Port	The port number for which the status applies.
Security	Enable or disable port security.
Mac L2 Entry	<p>The maximum number of MAC addresses that can be secured on this port. If the limit is exceeded, the corresponding action is taken.</p> <p>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.</p>
Action	<p>If a limit is reached, the switch can take one of the following actions:</p> <p>Forward: Do not allow more than Limit MAC addresses on the port, but take no further action.</p> <p>Shutdown: If Limit + 1 MAC addresses is seen on the port, shut down the port. This implies that all secured MAC addresses will be removed from the port, and no new ones 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:</p> <ol style="list-style-type: none"> 1) Disable and re-enable Limit Control on the port or the switch, 2) Click the Reopen button. <p>Discard: If Limit + 1 MAC addresses is seen on the port, it will not learn the new MAC address and drop the package.</p>

Buttons

- Click **Apply** to apply changes.

DoS

DoS (Denial of Service) is a simple but effective destructive attack on the internet. The server under DoS attack will drop normal user data packets due to the non-stop processing of the attacker's data packet, leading to denial of the service and could lead to a leak of sensitive data from the server.

Protocol check is an application that can protect the server from attacks such as DoS. The protocol check allows the user to drop matched packets based on specified conditions. This type of security feature provides several simple and effective protections against DoS attacks while having no influence on the linear forwarding performance of the switch.

Global DoS Setting	
DMAC = SMAC	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Land	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
UDP Blat	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
TCP Blat	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
POD	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
IPv6 Min Fragment	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled Byte: <input type="text" value="1240"/> (0-65535)
ICMP Fragments	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
IPv4 Ping Max Size	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
IPv6 Ping Max Size	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Ping Max Size Setting	Byte: <input type="text" value="512"/> (0-65535)
Smurf Attack	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled Netmask Length: <input type="text" value="0"/> (0-32)
TCP Min Hdr Size	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled Bytes: <input type="text" value="20"/> (0-31)
TCP-SYN(SPORT<1024)	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Null Scan Attack	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
X-Mas Scan Attack	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
TCP SYN-FIN Attack	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
TCP SYN-RST Attack	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
TCP Fragment (Offset = 1)	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

The page includes the following fields:

Object	Description
DMAC = SMAC	Enable or disable DoS check mode by DMAC = SMAC
Land	Enable or disable DoS check mode by land
UDP Blat	Enable or disable DoS check mode by UDP blat
TCP Blat	Enable or disable DoS check mode by TCP blat
POD	Enable or disable DoS check mode by POD
IPv6 Min Fragment	Enable or disable DoS check mode by IPv6 min fragment
ICMP Fragments	Enable or disable DoS check mode by ICMP fragment
IPv4 Ping Max Size	Enable or disable DoS check mode by IPv4 ping max size
IPv6 Ping Max Size	Enable or disable DoS check mode by IPv6 ping max size
Ping Max Size Setting	Set the max size for ping
Smurf Attack	Enable or disable DoS check mode by smurf attack

Object	Description
TCP Min Hdr Size	Enable or disable DoS check mode by TCP min hdr size
TCP-SYN (SPORT < 1024)	Enable or disable DoS check mode by TCP-syn (sport < 1024)
Null Scan Attack	Enable or disable DoS check mode by null scan attack
X-mas Scan Attack	Enable or disable DoS check mode by x-mas scan attack
TCP SYN-FIN Attack	Enable or disable DoS check mode by TCP syn-fin attack
TCP SYN-RST Attack	Enable or disable DoS check mode by TCP syn-rst attack
TCP Fragment (Offset = 1)	Enable or disable DoS check mode by TCP fragment (offset = 1)

Buttons

- Click **Apply** to apply changes.

DoS port setting

STP Port Setting

Port Select	DoS Protection
<input type="text" value="Select Ports"/>	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

The page includes the following fields:

Object	Description
Port Select	Select a port from this drop-down menu.
DoS Protection	Enable or disable per port DoS protection.

Buttons

- Click **Apply** to apply changes.

Storm control

Storm control for the switch is configured on this page.

There is an unknown unicast storm rate control, unknown 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).

Storm Control Global Setting

Unit	<input type="radio"/> pps <input checked="" type="radio"/> bps
Preamble & IFG	<input checked="" type="radio"/> Excluded <input type="radio"/> Included

The page includes the following fields:

Object	Description
Unit	Controls the unit of measure for the storm control rate as "pps" or "bps." The default value is "bps."
Preamble & IFG	Set the excluded or included interframe gap.

Buttons

- Click **Apply** to apply changes.

Port setting

Storm control for the switch is configured on this page. There are three types of storm rate control:

- Broadcast storm rate control
- Unknown Unicast storm rate control
- Unknown Multicast storm rate control

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

Storm Control Setting

Port	Port State	Action	Type Enable	Rate (Kbps)
<div style="border: 1px solid #ccc; padding: 2px; display: inline-block; border-radius: 4px;">Select Ports ▾</div>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block; border-radius: 4px;">drop ▾</div>	<input type="checkbox"/> Broadcast <input type="checkbox"/> Unknown Multicast <input type="checkbox"/> Unknown Unicast	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block; border-radius: 4px; width: 80px; text-align: center;">10000</div> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block; border-radius: 4px; width: 80px; text-align: center;">10000</div> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block; border-radius: 4px; width: 80px; text-align: center;">10000</div>

Apply

The page includes the following fields:

Object	Description
Port	Select a port from this drop-down menu.
Port State	Enable or disable the storm control status for the given storm type.
Action	Configures the action performed when storm control is over rate on a port. Valid values are Shutdown or Drop.
Type Enable	The settings in a particular row apply to the frame type listed here: Broadcast Unknown unicast Unknown multicast
Rate (kbps/pps)	Configure the rate for the storm control. The default value is "10,000."

Buttons

- Click **Apply** to apply changes.

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

This 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.

MAC-Based ACL

ACL Name	<input style="width: 90%;" type="text"/>
-----------------	--

The page includes the following fields:

Object	Description
ACL Name	Type a named MAC-based ACL list.

Buttons

- Click **Add** to add an ACL name.
- Click **Delete** to delete an ACL name entry.

MAC-based ACE

MAC-Based ACE	
ACL Name	<input type="text" value=""/>
Sequence	<input type="text" value=""/> (Range: 1 - 2147483647, 1 is first processed)
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown
DA MAC	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
DA MAC Value	<input type="text" value=""/>
DA MAC Mask	<input type="text" value=""/> (0s for matching, 1s for no matching)
SA MAC	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
SA MAC Value	<input type="text" value=""/>
SA MAC Mask	<input type="text" value=""/> (0s for matching, 1s for no matching)
VLAN ID	<input type="text" value=""/> (Range: 1 - 4094)
802.1p	<input type="checkbox"/> Include
802.1p Value	<input type="text" value=""/> (Range: 0-7)
802.1p Mask	<input type="text" value=""/>
Ethertype(Range:0x05DD-0xFFFF)	<input type="text" value=""/> (Range: 0x05DD-0xFFFF)

The page includes the following fields:

Object	Description
ACL Name	Select an ACL name from this drop-down menu.
Sequence	Set the ACL sequence
Action	<p>Indicates the forwarding action of the ACE.</p> <p>Permit: Frames matching the ACE may be forwarded and learned.</p> <p>Deny: Frames matching the ACE are dropped.</p> <p>Shutdown: Port shutdown is disabled for the ACE.</p> <p>DA MAC Specify the destination MAC filter for this ACE.</p> <p>Any: No DA MAC filter is specified.</p> <p>User Defined: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DA MAC value appears.</p>
DA MAC Value	When User Defined is selected for the DA MAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this DA MAC value.
DA MAC Mask	Specify whether frames can hit the action according to their sender hardware

Object	Description
	address field (SHA) settings. 0: ARP frames where SHA is not equal to the DA MAC address. 1: ARP frames where SHA is equal to the DA MAC address.
SA MAC	Specify the source MAC filter for this ACE. Any: No SA MAC filter is specified. User Defined: If you want to filter a specific source MAC address with this ACE, choose this value. A field for typing a SA MAC value appears.
SA MAC Value	When User Defined is selected for the SA MAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx". A frame that hits this ACE matches this SA MAC value.
SA MAC Mask	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 SA MAC address. 1: ARP frames where SHA is equal to the SA MAC address.
VLAN ID	Indicates the ID of this particular VLAN.
802.1p	Include or exclude the 802.1p value.
802.1p Value	Set the 802.1p value.
802.1p Mask	0: The frame is not equal to the 802.1p value. 1: The frame is equal to the 802.1p value.
EtherType (Range:0x05DD – 0xFFFF)	You can type a specific EtherType value. The allowed range is 0x05DD to 0xFFFF. A frame that hits this ACE matches this EtherType value.

Buttons

- Select the **Add** to add a MAC-based ACE.
- Click **Edit** to edit a MAC-based ACL parameter.
- Click **Delete** to delete a MAC-based ACL entry.

IPv4-based ACL

This page shows the ACL status of different ACL users. Each row describes the ACE that is defined. If a specific ACE is not applied to the hardware due to hardware limitations, it creates a conflict.

IPv4-Based ACL

ACL Name	<input style="width: 90%;" type="text"/>
-----------------	--

The page includes the following fields:

Object	Description
ACL Name	Create a named IPv4-based ACL list.

Buttons

- Select the **Add** to add an ACL name list.
- Click **Delete** to delete an ACL name entry.

IPv4-based ACE

An ACE consists of several parameters. Different parameter options appear depending on the frame type selected.

IPv4-Based ACE	
ACL Name	<input type="text"/>
Sequence	<input type="text"/> (Range: 1 - 2147483647, 1 is first processed)
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown
Protocol	<input checked="" type="radio"/> Any(IP) <input type="radio"/> Select from list <input type="text" value="icmp"/> <input type="radio"/> Protocol ID to match <input type="text" value="1"/>
Source IP Address	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
Source IP Address Value	<input type="text"/>
Source IP Wildcard Mask	<input type="text"/> (0s for matching, 1s for no matching)
Destination IP Address	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
Destination IP Address Value	<input type="text"/>
Destination IP Wildcard Mask	<input type="text"/> (0s for matching, 1s for no matching)
Source Port	<input checked="" type="radio"/> Any <input type="radio"/> Single <input type="text" value="0"/> (Range: 0 - 65535) <input type="radio"/> Range <input type="text" value="0"/> - <input type="text" value="65535"/> (Range: 0 - 65535)
Destination Port	<input checked="" type="radio"/> Any <input type="radio"/> Single(Range: 0 - 65535) <input type="text" value="0"/> (Range: 0 - 65535) <input type="radio"/> Range(Range: 0 - 65535) <input type="text" value="0"/> - <input type="text" value="65535"/> (Range: 0 - 65535)
TCP Flags	Urg <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Ack <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Psh <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Rst <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Syn <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Fin <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care
Type of Service	<input checked="" type="radio"/> Any <input type="radio"/> DSCP to match <input type="text" value="0"/> (Range: 0 - 63) <input type="radio"/> IP Precedence to match <input type="text" value="0"/> (Range: 0 - 7)
ICMP	<input checked="" type="radio"/> Any <input type="radio"/> Select from list <input type="text" value="Echo Reply"/> <input type="radio"/> Protocol ID to match <input type="text" value="0"/> (Range: 0 - 255)
ICMP Code	<input checked="" type="radio"/> Any <input type="radio"/> User Defined <input type="text" value="0"/> (Range: 0 - 255)

The page includes the following fields:

Object	Description
ACL Name	Select ACL name from this drop-down menu.
Sequence	Set the ACL sequence.
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. Shutdown: Port shutdown is disabled for the ACE.
Protocol	Specify the protocol filter for this ACE. Any(IP): No protocol filter is specified. Select from list: If you want to filter a specific protocol with this ACE, choose this value and select protocol from this drop-down menu. Protocol ID to match: If you want to filter a specific protocol with this ACE, choose this value and set current protocol ID.
Source IP Address	Specify the Source IP address filter for this ACE. Any: No source IP address filter is specified. User Defined: If you want to filter a specific source IP address with this ACE, choose this value. A field for entering a source IP address value appears.
Source IP Address Value	When "User Defined" is selected for the source IP address filter, you can enter a specific source IP address. The legal format is "xxx.xxx.xxx.xxx". A frame that hits this ACE matches this source IP address value.
Source IP Wildcard Mask	When User Defined is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
Destination IP Address	Specify the Destination IP address filter for this ACE. Any: No destination IP address filter is specified. User Defined: If you want to filter a specific destination IP address with this ACE, choose this value. A field for entering a source IP address value appears.
Destination IP Address Value	When "User Defined" is selected for the destination IP address filter, you can enter a specific destination IP address. The legal format is "xxx.xxx.xxx.xxx". A frame that hits this ACE matches this destination IP address value.
Destination IP Wildcard Mask	When User Defined is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.
Source Port	Specify the source port for this ACE. Any: No specific source port is specified (source port status is "don't-care"). Single: If you want to filter a specific source port with this ACE, you can enter a specific source port value. A field for entering a source port value appears. The allowed range is 0 to 65535. A frame that hits this ACE matches this source port value. Range: If you want to filter a specific source port range filter with this ACE, you can enter a specific source port range value. A field for entering a source port value appears. The allowed range is 0 to 65535. A frame that hits this ACE matches this source port value.
Destination Port	Specify the destination port for this ACE. Any: No specific destination port is specified (destination port status is "don't-care"). Single: If you want to filter a specific destination port with this ACE, you can

Object	Description
	<p>enter a specific destination port value. A field for entering a destination port value appears. The allowed range is 0 to 65535. A frame that hits this ACE matches this destination port value.</p> <p>Range: If you want to filter a specific destination port range filter with this ACE, you can enter a specific destination port range value. A field for entering a destination port value appears.</p>
Type of Service	<p>Specify the type of service for this ACE.</p> <p>Any: No specific type of service is specified (destination port status is "don't-care").</p> <p>DSCP: If you want to filter a specific DSCP with this ACE, you can enter a specific DSCP value. A field for entering a DSCP value appears. The allowed range is 0 to 63. A frame that hits this ACE matches this DSCP value.</p> <p>IP Precedence: If you want to filter a specific IP precedence with this ACE, you can enter a specific IP precedence value. A field for entering an IP precedence value appears. The allowed range is 0 to 7. A frame that hits this ACE matches this IP precedence value.</p>
ICMP	<p>Specify the ICMP for this ACE.</p> <p>Any: No specific ICMP is specified (destination port status is "don't-care").</p> <p>List: If you want to filter a specific list with this ACE, you can select a specific list value.</p> <p>Protocol ID: If you want to filter a specific protocol ID filter with this ACE, you can enter a specific protocol ID value. A field for entering a protocol ID value appears. The allowed range is 0 to 255. A frame that hits this ACE matches this protocol ID value.</p>
ICMP Code	<p>Specify the ICMP code filter for this ACE.</p> <p>Any: No ICMP code filter is specified (ICMP code filter status is "don't-care").</p> <p>User Defined: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.</p>

TCP flags

Object	Description
URG	<p>Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.</p> <p>Set: TCP frames where the URG field is set must be able to match this entry.</p> <p>Unset: TCP frames where the URG field is set must not be able to match this entry.</p> <p>Don't Care: Any value is allowed ("don't-care").</p>
ACK	<p>Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.</p> <p>Set: TCP frames where the ACK field is set must be able to match this entry.</p> <p>Unset: TCP frames where the ACK field is set must not be able to match this entry.</p> <p>Don't Care: Any value is allowed ("don't-care").</p>
PSH	<p>Specify the TCP "Push Function" (PSH) value for this ACE.</p>

Object	Description
	<p>Set: TCP frames where the PSH field is set must be able to match this entry.</p> <p>Unset: TCP frames where the PSH field is set must not be able to match this entry.</p> <p>Don't Care: Any value is allowed ("don't-care").</p>
RST	<p>Specify the TCP "Reset the connection" (RST) value for this ACE.</p> <p>Set: TCP frames where the RST field is set must be able to match this entry.</p> <p>Unset: TCP frames where the RST field is set must not be able to match this entry.</p> <p>Don't Care: Any value is allowed ("don't-care").</p>
SYN	<p>Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.</p> <p>Set: TCP frames where the SYN field is set must be able to match this entry.</p> <p>Unset: TCP frames where the SYN field is set must not be able to match this entry.</p> <p>Don't Care: Any value is allowed ("don't-care").</p>
FIN	<p>Specify the TCP "No more data from sender" (FIN) value for this ACE.</p> <p>Set: TCP frames where the FIN field is set must be able to match this entry.</p> <p>Unset: TCP frames where the FIN field is set must not be able to match this entry.</p> <p>Don't Care: Any value is allowed ("don't-care").</p>

Buttons

- Click **Add** to add a ACE list.
- Click **Edit** to edit a IPv4-based ACL parameter.
- Click **Delete** to delete a IPv4-based ACL entry.

IPv6-based ACL

This page shows the ACL status of different ACL users. Each row describes the ACE that is defined. If a specific ACE is not applied to the hardware due to hardware limitations, it creates a conflict.

IPv6-Based ACL

ACL Name	<input style="width: 90%;" type="text"/>
-----------------	--

The page includes the following fields:

Object	Description
ACL Name	Create a named IPv6-based ACL list.

Buttons

- Select the **Add** to add an ACL name list.

- Click **Delete** to delete an ACL name entry.

IPv6-based ACE

An ACE consists of several parameters. Different parameter options appear depending on the frame type selected.

IPv6-Based ACE	
ACL Name	<input type="text" value=""/>
Sequence	<input type="text" value=""/> (Range: 1 - 2147483647, 1 is first processed)
Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown
Protocol	<input checked="" type="radio"/> Any(IP) <input type="radio"/> Select from list <input type="text" value="tcp"/>
Source IP Address	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
Source IP Address Value	<input type="text" value=""/>
Source IP Prefix Length	<input type="text" value="0"/> (Range: 0 - 128)
Destination IP Address	<input checked="" type="radio"/> Any <input type="radio"/> User Defined
Destination IP Address Value	<input type="text" value=""/>
Destination IP Prefix Length	<input type="text" value="0"/> (0s for matching, 1s for no matching)
Source Port	<input checked="" type="radio"/> Any <input type="radio"/> Single <input type="text" value="0"/> (Range: 0 - 65535) <input type="radio"/> Range <input type="text" value="0"/> - <input type="text" value="65535"/> (Range: 0 - 65535)
Destination Port	<input checked="" type="radio"/> Any <input type="radio"/> Single(Range: 0 - 65535) <input type="text" value="0"/> (Range: 0 - 65535) <input type="radio"/> Range(Range: 0 - 65535) <input type="text" value="0"/> - <input type="text" value="65535"/> (Range: 0 - 65535)
TCP Flags	Urg <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Ack <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Psh <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Rst <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Syn <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care Fin <input checked="" type="radio"/> Set <input type="radio"/> Unset <input type="radio"/> Don't Care
Type of Service	<input checked="" type="radio"/> Any <input type="radio"/> DSCP to match <input type="text" value="0"/> (Range: 0 - 63) <input type="radio"/> IP Precedence to match <input type="text" value="0"/> (Range: 0 - 7)
ICMP	<input checked="" type="radio"/> Any <input type="radio"/> Select from list <input type="text" value="destination"/> <input type="radio"/> Protocol ID to match <input type="text" value="0"/> (Range: 0 - 255)
ICMP Code	<input checked="" type="radio"/> Any <input type="radio"/> User Defined <input type="text" value="0"/> (Range: 0 - 255)

The page includes the following fields:

Object	Description
ACL Name	Select ACL name from this drop-down menu.
Sequence	Set the ACL sequence.
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. Shutdown: Port shutdown is disabled for the ACE.
Protocol	Specify the protocol filter for this ACE. Any(IP): No protocol filter is specified. Select from list: If you want to filter a specific protocol with this ACE, choose this value and select protocol from this drop-down menu. Protocol ID to match: If you want to filter a specific protocol with this ACE, choose this value and set current protocol ID.
Source IP Address	Specify the Source IP address filter for this ACE. Any: No source IP address filter is specified. User Defined: If you want to filter a specific source IP address with this ACE, choose this value. A field for entering a source IP address value appears.
Source IP Address Value	When "User Defined" is selected for the source IP address filter, you can enter a specific source IP address. The legal format is "xxx.xxx.xxx.xxx". A frame that hits this ACE matches this source IP address value.
Source IP Wildcard Mask	When User Defined is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.
Destination IP Address	Specify the Destination IP address filter for this ACE. Any: No destination IP address filter is specified. User Defined: If you want to filter a specific destination IP address with this ACE, choose this value. A field for entering a source IP address value appears.
Destination IP Address Value	When "User Defined" is selected for the destination IP address filter, you can enter a specific destination IP address. The legal format is "xxx.xxx.xxx.xxx". A frame that hits this ACE matches this destination IP address value.
Destination IP Wildcard Mask	When User Defined is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.
Source Port	Specify the source port for this ACE. Any: No specific source port is specified (source port status is "don't-care"). Single: If you want to filter a specific source port with this ACE, you can enter a specific source port value. A field for entering a source port value appears. The allowed range is 0 to 65535. A frame that hits this ACE matches this source port value. Range: If you want to filter a specific source port range filter with this ACE, you can enter a specific source port range value. A field for entering a source port value appears. The allowed range is 0 to 65535. A frame that hits this ACE matches this source port value.
Destination Port	Specify the destination port for this ACE. Any: No specific destination port is specified (destination port status is "don't-care").

Object	Description
	<p>Single: If you want to filter a specific destination port with this ACE, you can enter a specific destination port value. A field for entering a destination port value appears. The allowed range is 0 to 65535. A frame that hits this ACE matches this destination port value.</p> <p>Range: If you want to filter a specific destination port range filter with this ACE, you can enter a specific destination port range value. A field for entering a destination port value appears.</p>
Type of Service	<p>Specify the type of service for this ACE.</p> <p>Any: No specific type of service is specified (destination port status is "don't-care").</p> <p>DSCP: If you want to filter a specific DSCP with this ACE, you can enter a specific DSCP value. A field for entering a DSCP value appears. The allowed range is 0 to 63. A frame that hits this ACE matches this DSCP value.</p> <p>IP Precedence: If you want to filter a specific IP precedence with this ACE, you can enter a specific IP precedence value. A field for entering an IP precedence value appears. The allowed range is 0 to 7. A frame that hits this ACE matches this IP precedence value.</p>
ICMP	<p>Specify the ICMP for this ACE.</p> <p>Any: No specific ICMP is specified (destination port status is "don't-care").</p> <p>List: If you want to filter a specific list with this ACE, you can select a specific list value.</p> <p>Protocol ID: If you want to filter a specific protocol ID filter with this ACE, you can enter a specific protocol ID value. A field for entering a protocol ID value appears. The allowed range is 0 to 255. A frame that hits this ACE matches this protocol ID value.</p>
ICMP Code	<p>Specify the ICMP code filter for this ACE.</p> <p>Any: No ICMP code filter is specified (ICMP code filter status is "don't-care").</p> <p>User Defined: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears. The allowed range is 0 to 255. A frame that hits this ACE matches this ICMP code value.</p>

TCP flags

Object	Description
URG	<p>Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE.</p> <p>Set: TCP frames where the URG field is set must be able to match this entry.</p> <p>Unset: TCP frames where the URG field is set must not be able to match this entry.</p> <p>Don't Care: Any value is allowed ("don't-care").</p>
ACK	<p>Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE.</p> <p>Set: TCP frames where the ACK field is set must be able to match this entry.</p> <p>Unset: TCP frames where the ACK field is set must not be able to match this entry.</p> <p>Don't Care: Any value is allowed ("don't-care").</p>

Object	Description
PSH	Specify the TCP "Push Function" (PSH) value for this ACE. Set: TCP frames where the PSH field is set must be able to match this entry. Unset: TCP frames where the PSH field is set must not be able to match this entry. Don't Care: Any value is allowed ("don't-care").
RST	Specify the TCP "Reset the connection" (RST) value for this ACE. Set: TCP frames where the RST field is set must be able to match this entry. Unset: TCP frames where the RST field is set must not be able to match this entry. Don't Care: Any value is allowed ("don't-care").
SYN	Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. Set: TCP frames where the SYN field is set must be able to match this entry. Unset: TCP frames where the SYN field is set must not be able to match this entry. Don't Care: Any value is allowed ("don't-care").
FIN	Specify the TCP "No more data from sender" (FIN) value for this ACE. Set: TCP frames where the FIN field is set must be able to match this entry. Unset: TCP frames where the FIN field is set must not be able to match this entry. Don't Care: Any value is allowed ("don't-care").

Buttons

- Click **Add** to add a ACE list.
- Click **Edit** to edit a IPv6-based ACL parameter.
- Click **Delete** to delete a IPv6-based ACL entry.

ACL binding

Bind the policy content to the appropriate ACLs on this page.

The page includes the following fields:

Object	Description
Binding Port	Select port from this drop-down menu.
ACL Select	Select ACL list from this drop-down menu.

Buttons

- Click **Apply** to apply changes.
- Click **Edit** to edit ACL binding table parameters.
- Click **Delete** to delete an ACL binding entry.

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.

Static MAC setting

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.

MAC Address	VLAN	Port
00:00:00:00:00:00	default	GE1

[Add](#)

This page includes the following fields:

Object	Description
VLAN	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
Port Members	Select a port from this drop-down menu.

Buttons

- Click **Add** to add a new static MAC address.
- Click **Delete** to delete a static MAC status entry.

MAC filtering

Use MAC filtering to filter the per-configured MAC address and increase security.

MAC Address	VLAN (1~4094)
00:00:00:00:00:00	1

Add

This page includes the following fields:

Object	Description
MAC Address	The MAC address of the entry.
VLAN (1~4096)	Indicates the ID of this particular VLAN.

Buttons

- Click **Add** to add a new MAC filtering setting.
- Click **Delete** to delete a static MAC status entry.

Dynamic address setting

By default, dynamic entries are removed from the MAC table after 300 seconds.

Aging Time
300 (Range: 10 - 630)

Apply

This page includes the following fields:

Object	Description
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: 10-630 seconds; Default: 300 seconds)

Buttons

- Click **Apply** to apply changes.
- Click **Delete** to delete a static MAC status entry.

Dynamic learned

The dynamic learned MAC table is shown on this page. The MAC table is sorted first by VLAN ID and then by MAC address.

This page includes the following fields:

Object	Description
VLAN	The VLAN ID of the entry.
MAC Address	The MAC address of the entry.
Port	Select a port from this drop-down menu.

Buttons

- Click **View** to refresh the table.
- Click **Clear** to flush all dynamic entries.
- Click **Add to Static MAC table** to add a dynamic MAC address to the static MAC address.

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 global settings

The LLDP Configuration page allows the user to inspect and configure the current LLDP port settings.

Global Settings	
Enabled	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
LLDP PDU Disable Action	<input type="radio"/> Filtering <input type="radio"/> Bridging <input checked="" type="radio"/> Flooding
Transmission Interval	<input type="text" value="30"/> (5-32768)
Holdtime Multiplier	<input type="text" value="4"/> (2-10)
Reinitialization Delay	<input type="text" value="2"/> (1-10)
Transmit Delay	<input type="text" value="2"/> (1-8192)
LLDP-MED Fast Start Repeat Count	<input type="text" value="3"/> (1-10)

The page includes the following fields:

Object	Description
Enable	Globally enable or disable the LLDP function.
LLDP PDU Disable Action	Set the LLDP PDU disable action. Filtering: discard all LLDP PDU. Bridging: transmit LLDP PDU in the same VLAN. Flooding: transmit LLDP PDU for all ports.
Transmission 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)
Holdtime Multiplier	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.
Reinitialization Delay	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.
Transmit 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

Object	Description
	<p>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.</p> <p>This attribute must comply with the rule: $(4 * \text{Delay Interval}) \leq \text{Transmission Interval}$</p>
LLDP-MED Fast Start Repeat Count	<p>Configures the amount of LLDP MED Fast Start LLDPDUs to transmit during the activation process of the LLDP-MED Fast Start mechanism.</p> <p>Range: 1-10 packets; Default: 3 packets</p> <p>The MED Fast Start Count parameter is part of the timer which ensures that the LLDP-MED Fast Start mechanism is active for the port. LLDP-MED Fast Start is critical to the timely startup of LLDP, and therefore integral to the rapid availability of Emergency Call Service.</p>

Buttons

- Click **Apply** to apply changes.

LLDP port configuration

Use the LLDP Port Configuration to specify the message attributes for individual interfaces, including if messages are to be transmitted, received, or both transmitted and received.

LLDP Port Configuration

Port Select	State
Select Ports ▾	Disable ▾

Apply

Optional TLVs Selection

Port Select	Optional TLV Select
Select Ports ▾	Select Optional TLVs ▾

Apply

The page includes the following fields:

Object	Description
Port Select	Select a port from these drop-down menus.
State	<p>Enables LLDP messages transmit and receive modes for LLDP Protocol Data Units. Options:</p> <p>Tx only Rx only TxRx</p>

Object	Description
	Disabled
Optional TLV Select	<p>Configures the information included in the TLV field of advertised messages.</p> <p>System Name: When selected, the "System Name" is included in LLDP information transmitted.</p> <p>Port Description: When selected, the "Port Description" is included in LLDP information transmitted.</p> <p>System Description: When selected, the "System Description" is included in LLDP information transmitted.</p> <p>System Capability: When selected, the "System Capability" is included in LLDP information transmitted.</p> <p>802.3 MAC-PHY: When selected, the "802.3 MAC-PHY" is included in LLDP information transmitted.</p> <p>802.3 Link Aggregation: When selected, the "802.3 Link Aggregation" is included in LLDP information transmitted.</p> <p>802.3 Maximum Frame Size: When selected, the "802.3 Maximum Frame Size" is included in LLDP information transmitted.</p> <p>Management Address: When selected, the "Management Address" is included in LLDP information transmitted.</p> <p>802.1 PVID: When selected, the "802.1 PVID" is included in LLDP information transmitted.</p>

Buttons

- Click **Apply** to apply changes.

VLAN name TLV VLAN status

VLAN Name TLV VLAN Selection

Port Select	VLAN Select
<input type="text" value="Select Ports"/>	<input type="text" value="Select VLANs"/>

The page includes the following fields:

Object	Description
Port Select	Select a port from this drop-down menu.
VLAN Select	Select a VLAN from this drop-down menu.

Buttons

- Click **Apply** to apply changes.

LLDP local device

Use the LLDP Local Device Information screen to display information about the switch such as its MAC address, chassis ID, management IP address, and port information.

Local Device Summary	
Chassis ID Subtype	MAC Address
Chassis ID	09:4F:3C:00:1d:5c
System Name	GSD-1002M
System Description	V1
Capabilities Supported	Bridge
Capabilities Enabled	Bridge
Port ID Subtype	Interface name

LLDP remote device

This page provides a status overview for all LLDP remote devices. The table contains a row for each port on which a LLDP neighbor is detected.

LLDP Remote Device							
Detail Delete Refresh							
Sel	Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name	Time to Live

The page includes the following fields:

Object	Description
Local Port	The switch port number of the logical LLDP port.
Chassis ID Subtype	The current chassis ID subtype
Chassis ID	The Chassis ID is the identification of the neighbor's LLDP frames
Port ID Subtype	The current port ID subtype
Port ID	The Remote Port ID is the identification of the neighbor port
System Name	System Name is the name advertised by the neighbor unit
Time to Live	The current time to live

Buttons

- Click **Refresh** to refresh a LLDP remote device.
- Click **Delete** to delete a LLDP remote device entry.

MED network 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.

Voice Auto Mode Configuration

LLDP MED Policy for Voice Application Auto Manual

Network Policy Configuration

Network Policy Number	1
Application	Voice
VLAN ID	1 (1-4094)
VLAN Tag	<input checked="" type="radio"/> Tagged <input type="radio"/> Untagged
L2 Priority	0 (0-7)
DSCP Value	0 (0-63)

The page includes the following fields:

Object	Description
LLDP MED Policy for Voice Application	Set the LLDP MED policy for voice application mode.
Network Policy Number	Select the network policy number from this drop-down menu.
Application Type	<p>Intended use of the application types:</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Video Conferencing – For use by dedicated video conferencing equipment and other similar appliances supporting real-time interactive video/audio services.</p> <p>Streaming Video – For use by broadcast or multicast based video content</p>

Object	Description
	<p>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.</p> <p>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.</p>
Tag	<p>Tag indicates if the specified application type is using a 'tagged' or an 'untagged' VLAN.</p> <p>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.</p> <p>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.</p>
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.

Buttons

- Click **Apply** to apply changes.
- Click **Delete** to delete a LLDP MED network policy table entry.

MED port setting

Port LLDP MED Configuration

Port Select	MED Enable	MED Optional TLVs	MED Network Policy
Select Ports ▾	Enable ▾	Select Optional TLVs ▾	Select Optional TLVs ▾

Apply

The page includes the following fields:

Object	Description
Port Select	Select a port from this drop-down menu.
MED Enable	Enable or disable MED configuration
MED Optional TVLs	Configures the information included in the MED TLV field of advertised messages. Network Policy – This option advertises network policy configuration information, aiding in the discovery and diagnosis of VLAN configuration mismatches on a port. Improper network policy configurations frequently result in voice quality degradation or complete service disruption. Location – This option advertises location identification details. Inventory – This option advertises device details useful for inventory management, such as manufacturer, model, software version and other pertinent information.
MED Network Policy	Select MED network policy from this drop-down menu.

Buttons

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

MED location configuration

MED Location Configuration

Ports	<input type="text" value="Select Ports"/>
Location Coordinate	<input type="text"/> (16 pairs of hexadecimal characters)
Location Civic Address	<input type="text"/> (6-160 pairs of hexadecimal characters)
Location ECS ELIN	<input type="text"/> (10-25 pairs of hexadecimal characters)

The page includes the following fields:

Object	Description
Port	Select a port from this drop-down menu.
Location Coordinate	A string identifying the Location Coordinate that this entry should belong to.
Location Civic Address	A string identifying the Location Civic Address that this entry should belong to.
Location ESC ELIN	A string identifying the Location ESC ELIN that this entry should belong to.

Buttons

- Click **Apply** to apply changes.

LLDP overloading

LLDP Port Overloading Table												
Interface	Total(Bytes)	Left to Send(Bytes)	Status	Status								
				Mandatory TLVs	MED Capabilities	MED Location	MED Network Policy	MED Extended Power via MDI	802.3 TLVs	Optional TLVs	MED Inventory	802.1 TLVs
GE1	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE2	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE3	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE4	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE5	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE6	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE7	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE8	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE9	48	1440	Not Overloading	21(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)
GE10	49	1439	Not Overloading	22(Transmitted)	9(Transmitted)		10(Transmitted)					8(Transmitted)

The page includes the following fields:

Object	Description
Interface	The switch port number of the logical port
Total (Bytes)	Total number of bytes of LLDP information that is normally sent in a packet.
Left to Send (Bytes)	Total number of available bytes that can also send LLDP information in a packet.
Status	Provides the status of the TLVs.
Mandatory TLVs	The mandatory group of TLVs that were transmitted or overloaded
MED Capabilities	The capabilities packets that were transmitted or overloaded
MED Location	The location packets that were transmitted or overloaded
MED Network Policy	The network policies packets that were transmitted or overloaded
MED Extended Power via MDI	The extended power via MDI packets that were transmitted or overloaded.
802.3 TLVs	The 802.3 TLVs that were transmitted or overloaded.
Optional TLVs	The LLDP MED extended power via MDI packets that were sent or overloaded.
MED Inventory	The mandatory group of TLVs that was transmitted or overloaded.
802.1 TLVs	The 802.1 TLVs that were transmitted or overloaded

LLDP statistics

The LLDP Device Statistics screen displays general statistics for LLDP-capable devices attached to the switch, and for LLDP protocol messages transmitted or received on all local interfaces.

LLDP Global Statistics	
Insertions	0
Deletions	0
Drops	0
Age Outs	0

The page includes the following fields:

Object	Description
Insertions	Shows the number of new entries added since switch reboot.
Deletions	Shows the number of new entries added since switch reboot.
Drops	Shows the number of LLDP frames dropped due to the entry table being full.
Age Outs	Shows the number of entries deleted due to Time-To-Live expiring.

Buttons

- Click **Refresh** to refresh the statistics.
- Click **Clear** to clear the statistics.

Port statistics

Port	TX Frames	RX Frames			RX TLVs		RX Age outs
	Total	Total	Discarded	Errors	Discarded	Unrecognized	Total
GE1	136	0	0	0	0	0	0
GE2	0	0	0	0	0	0	0
GE3	0	0	0	0	0	0	0
GE4	0	0	0	0	0	0	0
GE5	0	0	0	0	0	0	0
GE6	0	0	0	0	0	0	0
GE7	0	0	0	0	0	0	0
GE8	0	0	0	0	0	0	0
GE9	0	0	0	0	0	0	0
GE10	0	0	0	0	0	0	0

The page includes the following fields:

Object	Description
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.
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.
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.

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 Test
- IPv6 Ping Test
- Trace Route
- Cable Diagnostics

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

Note: Cable Diagnostics is only accurate for cables of length from 15 to 100 meters.

The page includes the following fields:

Object	Description
Port	The port where you are requesting cable diagnostics.

Buttons

- Click **Copper Test** to run the diagnostics.

Port	Channel A	Cable Length A	Channel B	Cable Length B	Channel C	Cable Length C	Channel D	Cable Length D	Result
GE2	NORMAL		NORMAL		NORMAL		NORMAL		PASS

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.

Ping test

This page allows you to issue ICMP ping packets to troubleshoot IP connectivity issues.

After clicking **Apply**, ICMP packets are transmitted, and the sequence number and roundtrip time appear upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

Ping Test Setting	
IP Address	<input type="text"/> (x.x.x.x or hostname)
Count	<input type="text" value="4"/> (1 - 5 Default : 4)
Interval (in sec)	<input type="text" value="1"/> (1 - 5 Default : 1)
Size (in bytes)	<input type="text" value="56"/> (8 - 5120 Default : 56)
Ping Results	<div style="border: 1px solid gray; height: 100px;"></div>

The page includes the following fields:

Object	Description
IP Address	The destination IP Address.
Count	Number of echo requests to send.
Interval (in sec)	Send interval for each ICMP packet.
Size (in bytes)	The payload size of the ICMP packet. Values range from 8 bytes to 5120 bytes.
Ping Results	Display the current ping result.

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 **Apply** to transmit ICMP packets.

IPv6 ping

The ICMPv6 Ping page allows you to issue ICMPv6 ping packets to troubleshoot IPv6 connectivity issues. After clicking **Apply**, 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.

Ping test Setting

IPv6 Address	<input type="text"/> (XX:XX:XX:XX)
Count	<input type="text" value="4"/> (1 - 5 Default : 4)
Interval (in sec)	<input type="text" value="1"/> (1 - 5 Default : 1)
Size (in bytes)	<input type="text" value="56"/> (8 - 5120 Default : 56)
Ping Results	<div style="border: 1px solid #ccc; height: 60px; width: 100%;"></div>

The page includes the following fields:

Object	Description
IP Address	The destination IPv6 Address.
Count	Number of echo requests to send.
Interval (in sec)	Send interval for each ICMP packet.
Size (in bytes)	The payload size of the ICMP packet. Values range from 8 bytes to 5120 bytes.
Ping Results	Display the current ping result.

Buttons

- Click **Apply** to transmit ICMPv6 packets.

Trace router

The trace route function tests the gateways through which the data packets travel from the source device to the destination device, checking network accessibility and locating network failure.

The execution procedure of the trace route function sends a data packet with TTL at 1 to the destination address. If the first hop returns an ICMP error message saying that this packet cannot be sent due to a TTL timeout, a data packet with TTL at 2 is sent. The send hop may be a TTL timeout return, but the procedure carries on until the data packet is sent to its destination. These procedures are for recording every source address that returns an ICMP TTL timeout message, thus describing the path the IP data packets traveled to reach the destination.

Trace Route Setting

IP Address	<input style="width: 80%;" type="text" value="192.168.1.100"/> (x.x.x.x or hostname)
Max Hop	<input style="width: 80%;" type="text" value="30"/> (2 - 255 Default : 30)
Trace Route Results	<div style="background-color: #f0f0f0; width: 100%; height: 100%;"></div>

The page includes the following fields:

Object	Description
IP Address	The destination IP address.
Max Hop	The maximum gateway number allowed by trace route function.
Trace Route Results	The current trace route result.

Buttons

- Click **Apply** to transmit ICMPv6 packets.

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 statistics status

The RMON Statistics Status Overview page provides an overview of RMON Statistics entries.

The screenshot shows a web interface titled "Port GE1 RMON Statistics". It features a dropdown menu for "Port" set to "GE1" and a "Clear" button. Below this is a table with two columns: "RMON Counters" and "Value".

RMON Counters	Value
Drop Events	0
Octets	5192377
Packets	36210
Broadcast Packets	508
Multicast Packets	156
CRC / Alignment Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	0
64 Bytes Frame	23107
65-127 Byte Frames	5685
128-255 Byte Frames	227
256-511 Byte Frames	7161
512-1023 Byte Frames	30
1024-1518 Byte Frames	0

The page includes the following fields:

Object	Description
Port	Select a port from this drop-down menu.
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.
Packets	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 Packets	The total number of packets received that were less than 64 octets.
Oversize packets	The total number of packets received that were longer than 1518 octets.
Fragments	The number of frames with a size less than 64 octets received with invalid CRC.
Jabbers	The number of frames with a size larger than 64 octets received with invalid CRC.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Bytes Frame	The total number of packets (including bad packets) received that were 64 octets in length.
65~127 Frame	The total number of packets (including bad packets) received that were between 65 to 127 octets in length.
128~255 Frame	The total number of packets (including bad packets) received that were between 128 to 255 octets in length.
256~511 Frame	The total number of packets (including bad packets) received that were between 256 to 511 octets in length.
512~1023 Frame	The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.
1024~1518 Frame	The total number of packets (including bad packets) received that were between 1024 to 1518 octets in length.

Buttons

- Click **Clear** to clear the RMON statistics.

RMON event configuration

Configure the RMON Event table on the RMON Event Configuration page.

RMON Event

Select Index	<input type="text" value="Create New"/> ▼
Index	<input type="text" value="0"/> (1-65535)
Type	<input type="text" value="None"/> ▼
Community	<input type="text" value=""/>
Owner	<input type="text" value=""/> (0~31 Characters)
Description	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> ⋮ (0~127 Characters)

The page includes the following fields:

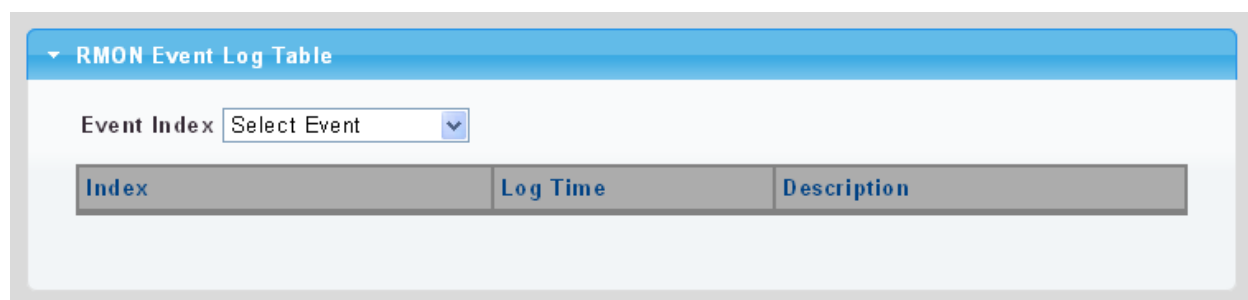
Object	Description
Select Index	Select index from this drop-down menu to create new index or modify index.
Index	Indicates the index of the entry. The range is from 1 to 65535.
Desc	Indicates the event. The string length is from 0 to 127, default is a null string.
Type	Indicates the notification of the 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."
Owner	Indicates the owner of this event. The string length is from 0 to 127, default is a null string.
Description	Indicates the description of this event. The string length is from 0 to 127, default is a null string.

Buttons

- Click **Apply** to apply changes.

RMON event log

The RMON Event Log Table page provides an overview of RMON Event table entries.



The page includes the following fields:

Object	Description
Select Index	Select the index from this drop-down menu.
Index	Indicates the index of the log entry.
Log Time	Indicates event log time.
Description	Indicates the event description.

RMON alarm

Configure RMON alarm table on the RMON Alarm page.

RMON Alarm

Select Index	Create New <input type="button" value="v"/>
Index	0 <input type="text"/> (1-65535)
Sample Port	GE1 <input type="button" value="v"/>
Sample Variable	DropEvents <input type="button" value="v"/>
Sample Interval	0 <input type="text"/> (1-2147483647)
Sample Type	<input type="radio"/> absolute <input type="radio"/> delta
Rising Threshold	0 <input type="text"/> (0-2147483647)
Falling Threshold	0 <input type="text"/> (0-2147483647)
Rising Event	0: None (Unassigned) <input type="button" value="v"/>
Falling Event	0: None (Unassigned) <input type="button" value="v"/>
Owner	<input type="text"/> (0~31 Characters)

The page includes the following fields:

Object	Description
Select Index	Select the index from this drop-down menu.
Index	Indicates the index of the alarm entry. The range is from 1 to 65535.
Sample Port	Select a port from this drop-down menu.
Sample Variable	Indicates the particular variable to be sampled, the possible variables are: DropEvents: The total number of events in which packets were dropped due to lack of resources. Octets: The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits. Pkts: The total number of frames (bad, broadcast and multicast) received and transmitted. BroadcastPkts: The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets. MulticastPkts: The total number of good frames received that were directed to this multicast address.

Object	Description
	<p>CRCAlignErrors: The number of CRC/alignment errors (FCS or alignment errors).</p> <p>UnderSizePkts: The total number of frames received that were less than 64 octets long(excluding framing bits, but including FCS octets) and were otherwise well formed.</p> <p>OverSizePkts: The total number of frames received that were longer than 1518 octets(excluding framing bits, but including FCS octets) and were otherwise well formed.</p> <p>Fragments: The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.</p> <p>Jabbers: The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.</p> <p>Collisions: The best estimate of the total number of collisions on this Ethernet segment.</p> <p>Pkts64Octets: The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).</p> <p>Pkts64to172Octets: The total number of frames (including bad packets) received and transmitted where the number of octets falls within the specified range (excluding framing bits but including FCS octets).</p> <p>Pkts158to255Octets: The total number of frames (including bad packets) received and transmitted where the number of octets falls within the specified range (excluding framing bits but including FCS octets).</p> <p>Pkts256to511Octets: The total number of frames (including bad packets) received and transmitted where the number of octets falls within the specified range (excluding framing bits but including FCS octets).</p> <p>Pkts512to1023Octets: The total number of frames (including bad packets) received and transmitted where the number of octets falls within the specified range (excluding framing bits but including FCS octets).</p> <p>Pkts1024to1518Octets: The total number of frames (including bad packets) received and transmitted where the number of octets falls within the specified range (excluding framing bits but including FCS octets).</p>
Sample Interval	Sample interval (1–2147483647)
Sample Type	<p>The method of sampling the selected variable and calculating the value to be compared against the thresholds. Possible sample types are:</p> <p>Absolute: Get the sample directly.</p> <p>Delta: Calculate the difference between samples (default).</p>
Rising Threshold	Rising threshold value (0-2147483647).
Falling Threshold	Falling threshold value (0-2147483647)
Rising Event	Event to fire when the rising threshold is crossed.
Falling Event	Event to fire when the falling threshold is crossed.
Owner	Specify an owner for the alarm.

Buttons

- Click **Apply** to apply changes.

RMON history

Configure RMON history on the RMON History page.

RMON History	
Select Index	Create New
Index	0 (1-65535)
Sample Port	GE1
Bucket Requested	50 (1-50, Default 50)
Interval	1800 (1-3600 Default 1800)
Owner	(0~31 Characters)

Apply

The page includes the following fields:

Object	Description
Select Index	Select the index from this drop-down menu.
Index	Indicates the index of the history entry. The range is from 1 to 65535.
Sample Port	Select a port from this drop-down menu.
Bucket Requested	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 50, default value is 50.
Interval	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.
Owner	Specify an owner for the history.

Buttons

- Click **Apply** to apply changes.
- Click **Delete** to delete the RMON history entry.

RMON history log

The RMON History Table page provides details of RMON history entries.

RMON History Table

History Index Select History

No data available!

The page includes the following fields:

Object	Description
History Index	Indicates the index of history control entry.







Buttons

- Click **Apply** to apply changes.

Power over Ethernet (PoE)

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, 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	<p>Voice over IP phones</p> <p>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.</p>
 6~12 Watts	<p>Wireless LAN Access Points</p> <p>Museums, airports, hotels, campuses, factories, warehouses, etc. can install APs in any location.</p>
 10~12 Watts	<p>IP Surveillance</p> <p>Enterprises, museums, campuses, hospitals, banks, etc. can install IP cameras regardless of installation location without the need to install AC sockets.</p>
 3~12 Watts	<p>PoE Splitter</p> <p>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.</p>
 3~25 Watts	<p>High Power PoE Splitter</p> <p>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.</p>
 30 Watts	<p>High Power Speed Dome</p> <p>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.</p>

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.

System configuration

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.

PoE configuration

Inspect and configure the current PoE configuration settings on the PoE Configuration page.

PoE Configuration

PoE Configuration

System PoE Admin Mode	Enable ▾
PoE Management Mode	Consumption ▾
Temperature Threshold	120 Degrees C
PoE Temperature	43°C / 109°F
Power Budget	200 W

Power Allocation		0 W / 200 W
-------------------------	--	-------------

Port	PoE Mode	Schedule	Priority	PD Class	Current Used [mA]	Power Used [W]	Power Allocation [W]
1	Enable ▾	Profile 1 ▾	Critical ▾	--	0	0	36
2	Enable ▾	Profile 1 ▾	Critical ▾	--	0	0	36
3	Enable ▾	Profile 1 ▾	Critical ▾	--	0	0	36
4	Enable ▾	Profile 1 ▾	Critical ▾	--	0	0	36
5	Enable ▾	Profile 1 ▾	Critical ▾	--	0	0	36
6	Enable ▾	Profile 1 ▾	Critical ▾	--	0	0	36
7	Enable ▾	Profile 1 ▾	Critical ▾	--	0	0	36
8	Enable ▾	Profile 1 ▾	Critical ▾	--	0	0	36
Total					0	0	0

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 Management Mode	There are six modes for configuring how the ports/PDs may reserve power and when to shut down ports.

Object	Description
	<p>Classification mode: System reserves PoE power to PD according to PoE class level.</p> <p>Consumption mode: System offers PoE power according to PD real power consumption.</p> <p>Allocation mode: Users can assign how much PoE power for per port and the system reserves PoE power to the PD.</p>
Temperature Threshold	Allows setting over temperature protection threshold value. If the system temperature is overly high, the system will lower the total PoE power budget automatically.
PoE Temperature	Displays the PoE chip temperature
Power Budget	Sets the PoE power budget limitation.

Current power consumption

The page includes the following fields:

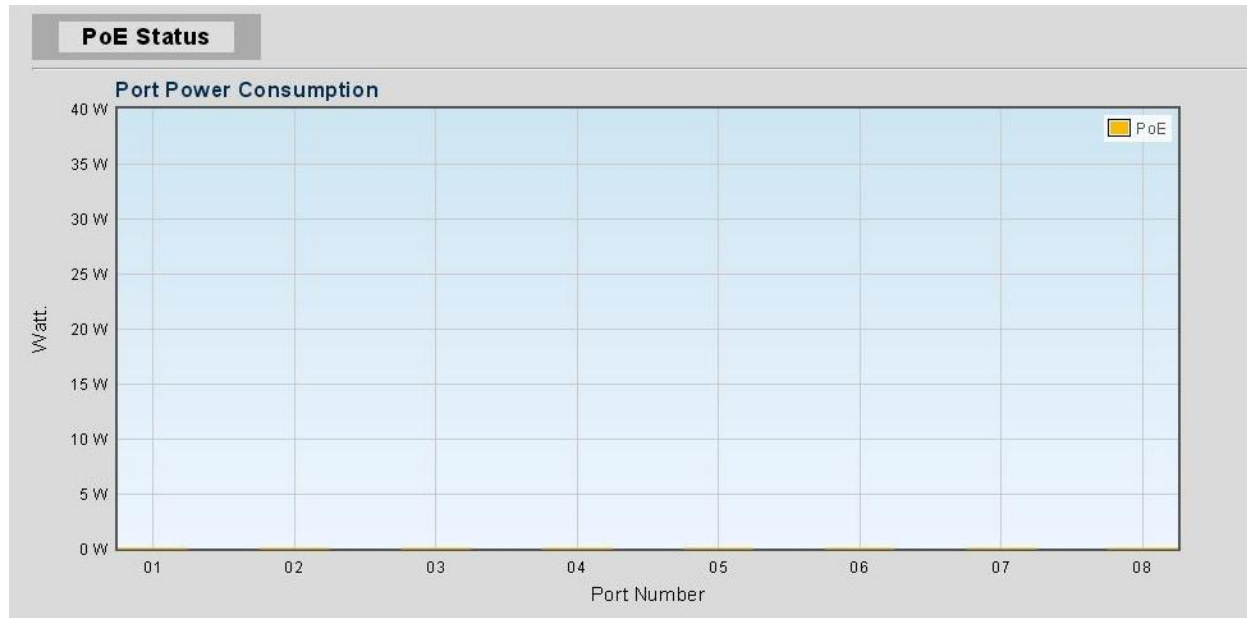
Object	Description
PoE Mode	<p>There are three PoE modes:</p> <p>Enable: Enables the PoE function.</p> <p>Disable: Disables the PoE function</p> <p>Schedule: Enables the PoE function in schedule mode</p>
Schedule	<p>Indicates the schedule profile mode. Possible profiles are:</p> <p>Profile1</p> <p>Profile2</p> <p>Profile3</p> <p>Profile4</p>
Priority	<p>Priority represents PoE port priority. There are three levels of power priority: Low, High, and Critical.</p> <p>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.</p>
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. The PD will return to Class 0 to 4 in accordance with the maximum power draw.
Current Used [mA]	The Power Used shows how much current the PD currently is using.
Power Used [W]	The Power Used shows how much power the PD currently is using.
Power Allocation	Limits the port PoE supply Watts. The per port maximum value must less than 36 W, and total port values must 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.

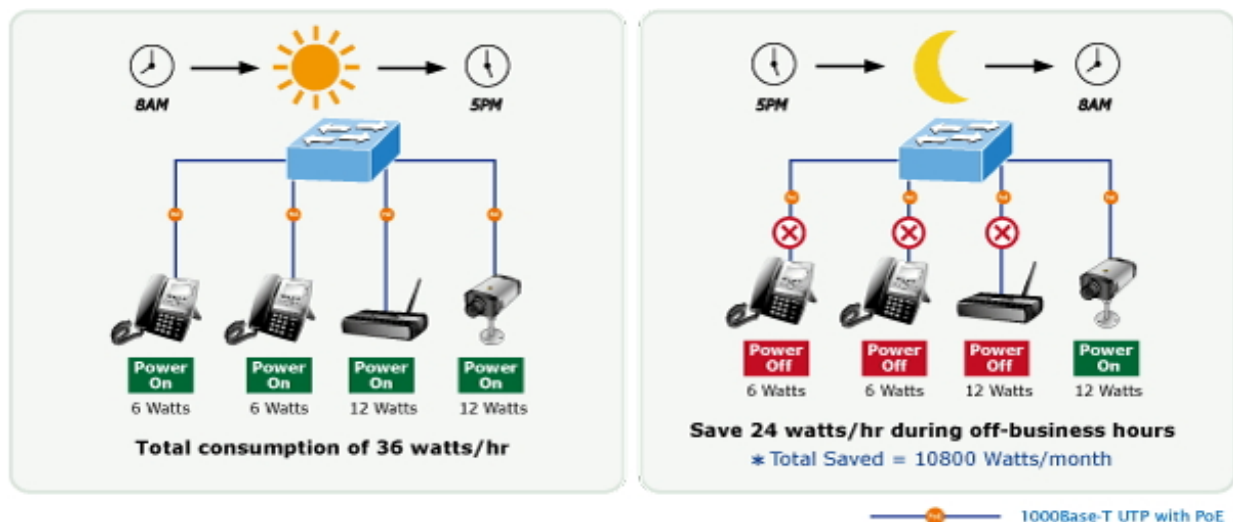
PoE status

Inspect the current status for all PoE ports on the PoE Status page.



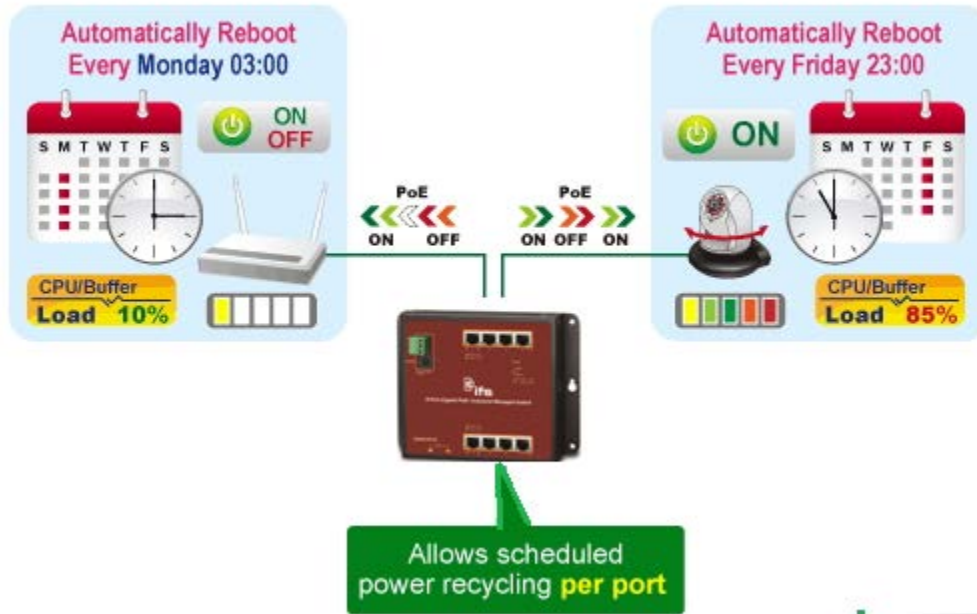
PoE schedule

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.

PoE Schedule

PoE Schedule Configuration

Profile: Profile 1 ▼

Delete	Week Day	Start Hour	Start Min	End Hour	End Min	Reboot Enable	Reboot Only	Reboot Hour	Reboot Min
<div style="display: flex; justify-content: space-around; margin-top: 10px;"> Add New Rule Apply </div>									

Sta																									
Fri																									
Thu																									
Wed																									
Tue																									
Mon																									
Sun																									
	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

■ PoE Schedule
■ PoE Reboot

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 menu, and the profile number from the Schedule drop-down menu, for each port to which you want to apply the schedule profile.

The page includes the following fields:

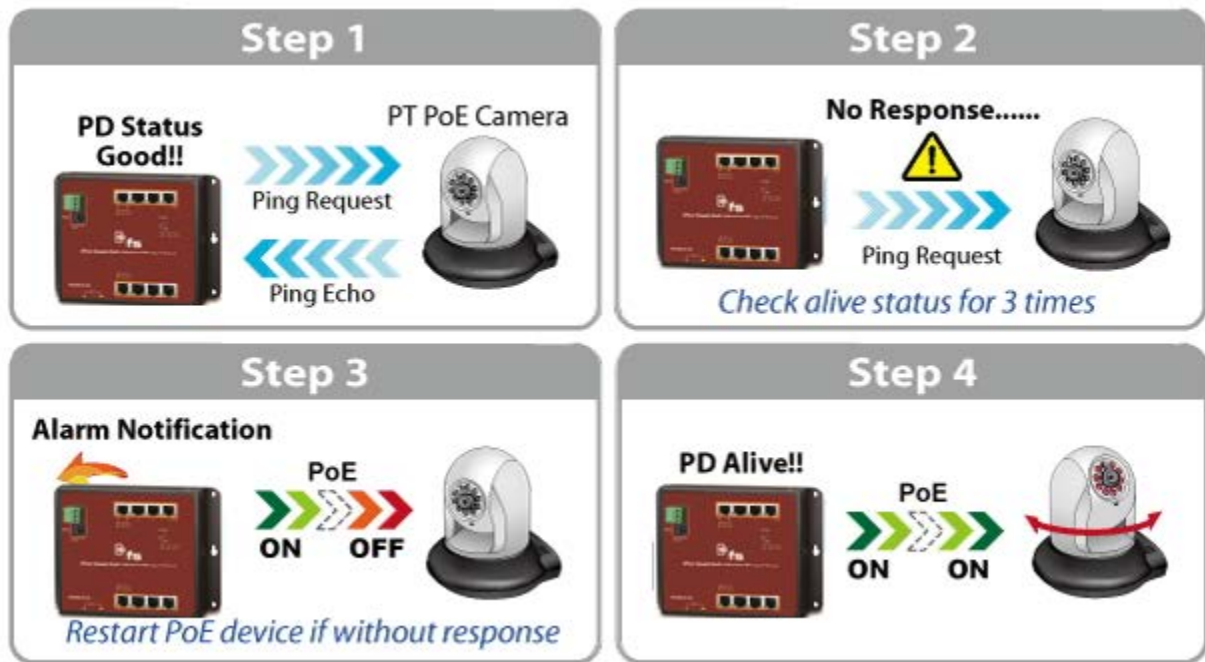
Object	Description
Profile	Set the schedule profile mode. Possible profiles are: Profile1 Profile2 Profile3 Profile4
Week Day	Set the weekday for enabling the PoE function.
Start Hour	Set the hour for enabling the PoE function.
Start Min	Set the minute for enabling the PoE function.
End Hour	Set the 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.
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.

PoE alive check configuration

The IFS PoE managed switch can be configured to monitor connected PD status in real-time via ping action. Once the PD stops working and does not respond, the PoE switch restarts PoE port power, and restores the PD to a working state. This increases reliability and reduces administrator management problems.



PD Alive Check

PD Alive Check

Port Select	Mode	Interval Time (10~300s)	Retry Count (1~5)	Action	Reboot Time (30~180s)
Select Ports	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	30	2	None	90

Apply

The page includes the following fields:

Object	Description
Mode	Enable or disable the per port PD Alive Check function. By default, all ports are disabled.
Ping PD IP Address	This column permits the user to set a PoE device IP address for pinging the PoE device. Note: the PD's IP address must be set to the same network segment as the PoE switch.
Interval Time (10~300s)	This column permits the user to set how long the system should issue a ping request to a PD to detect if the PD is alive or dead. Interval time range is from 10 to 300 seconds.
Retry Count (1~5)	This column permits the user to set the number of times the system retries pinging the PD. For example, if the count is set to 2, and the system retries pinging the PD and the PD doesn't respond continuously, the PoE port will be reset.
Action	Permits the user to set the action applied if the PD does not respond. The PoE switch can perform the following three actions: PD Reboot: The system will reset the PoE port that is connected to the PD. PD Reboot & Alarm: The system will reset the PoE port and issue an alarm

Object	Description
	message via Syslog. Alarm: The system will issue an alarm message via Syslog.
Reboot Time (30~180s)	This column permits the user to set the PoE device rebooting time. The PD Alive-check is not a defining standard, so a PoE device doesn't report reboot information to the PoE switch. Therefore, the user must determine how long the PD will take to finish booting, and then set the time value in this column. The system checks the PD again according to the reboot time. If you are not sure of the precise booting time, we suggest setting it to a longer time period.

Buttons

- Click **Apply** to apply changes.
- Click **Edit** to edit the entry.

Maintenance

Use the Maintenance menu items to display and configure basic configurations of the managed switch. Under Maintenance, the following topics are provided to back up, upgrade, save, and restore the configuration. This section has the following items:

- **Factory Default:** Reset the configuration of the switch on this page.
- **Reboot Switch:** Restart the switch on this page. After restart, the switch will boot normally.
- **Backup Manager:** Back up the switch configuration.
- **Upgrade Manager:** Upgrade the switch configuration.
- **Dual Image:** Select active or backup image on this page.

Factory default

Reset the configuration of the switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary. Click **Restore** to reset the configuration to factory default.



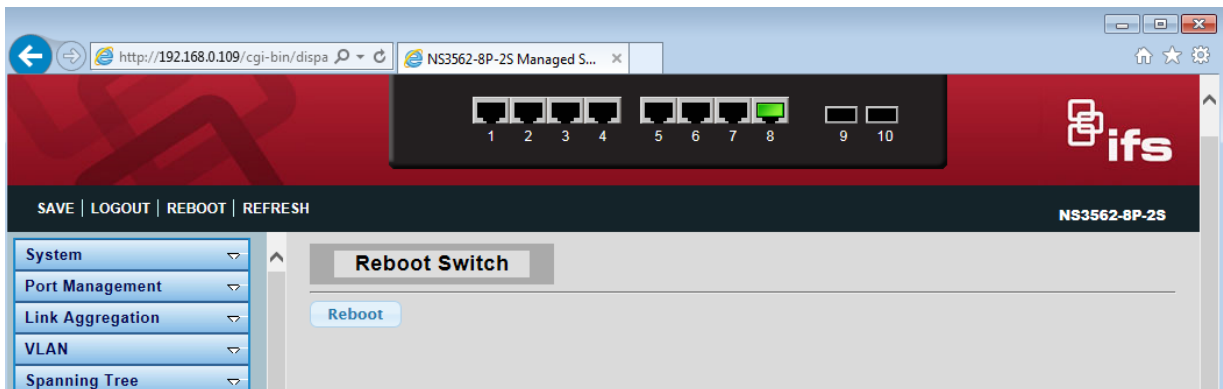
The system loads the default IP settings as follows:

- Default IP address: 192.168.0.100
- Subnet mask: 255.255.255.0
- Default Gateway: 192.168.0.254
- The other setting value is back to disable or none.

To reset the managed switch to the factory default setting, you can also press the hardware reset button at the front panel for 10 seconds. After the device reboots, you can log in to the management web interface within the same subnet of 192.168.0.xx.

Reboot switch

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



Backup manager

This function allows backup of the current image or configuration of the managed switch to the local management station.

Backup Manager	
Backup Method	TFTP
Server IP	<input type="text"/> (IPv4 or IPv6 Address)
Backup Type	<input checked="" type="radio"/> Image <input type="radio"/> Running configuration <input type="radio"/> Startup configuration <input type="radio"/> Backup configuration <input type="radio"/> Flash log <input type="radio"/> Buffered log
Image	<input checked="" type="radio"/> vmlinux_poe_test.bix (Active) <input type="radio"/> vmlinux_poe_test.bix (Backup)

The page includes the following fields:

Object	Description
Backup Method	Select a backup method from this drop-down menu.
Server IP	Type in the TFTP server IP address.
Backup Type	Select the backup type.
Image	Select the active or backup image.

Buttons

- Click **Backup** to back up the image, configuration, or log.

Upgrade manager

This function permits reloading the managed switch's current image or configuration to the local management station.

Upgrade Manager	
Upgrade Method	TFTP
Server IP	<input type="text"/> (IPv4 or IPv6 Address)
File Name	<input type="text"/>
Upgrade Type	<input checked="" type="radio"/> Image <input type="radio"/> Startup Configuration <input type="radio"/> Backup Configuration <input type="radio"/> Running Configuration
Image	<input type="radio"/> (Active) <input checked="" type="radio"/> (Backup)

The page includes the following fields:

Object	Description
Upgrade Method	Select an upgrade method from this drop-down menu.
Server IP	Type in the TFTP server IP address.
File Name	The name of the firmware image or configuration.
Backup Type	Select the upgrade type.
Image	Select the active or backup image.

Buttons

- Click **Upgrade** to upgrade the image or configuration.

Dual image

This page provides information about the active and backup firmware images in the device, and permits reversion to the backup image. The page displays two tables with information about the active and backup firmware images.

Dual Image Configuration	
Active Image	<input checked="" type="radio"/> v1.0b140225.bix(Active) <input type="radio"/> v1.0b140225.bix(Backup)

The page includes the following fields:

Object	Description
Image	Select the active or backup image.

Buttons

- Click **Apply** to apply the active image.

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.

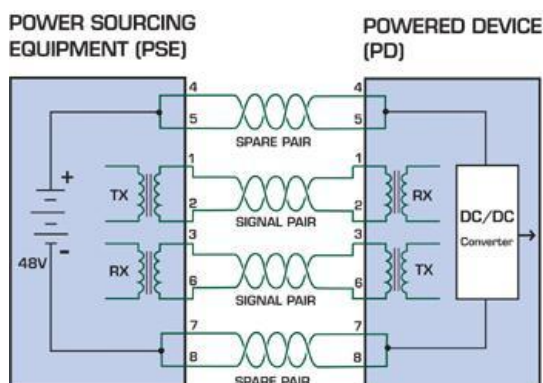
Powered Device (PD)

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.

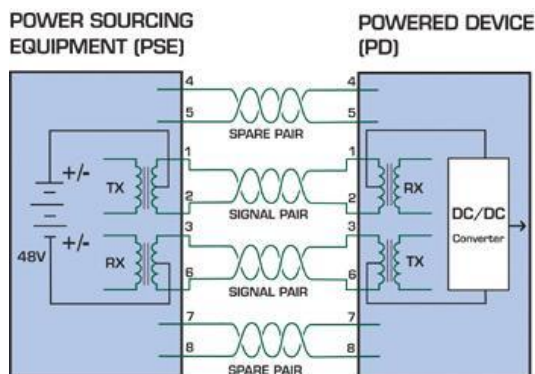
How power is transferred through the cable

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

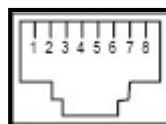
This chapter contains information to help you solve issues. If the industrial managed switch is not functioning properly, ensure that it was set up according to the instructions in this manual.

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 managed switch doesn't connect to the network	<ol style="list-style-type: none">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 managed switch does not power up.	<ol style="list-style-type: none">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-

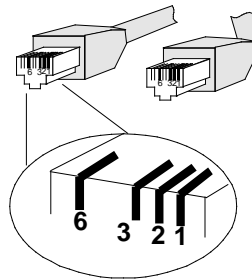
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

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	<p>Access Control Entry. It describes access permission associated with a particular ACE ID.</p> <p>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.</p>
ACL	<p>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.</p> <p>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.</p>

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 you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc.) for each ingress port. They will only apply if the frame gets past the ACE matching without 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 802.11 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	<p>Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.</p> <p>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.</p>
DHCP	<p>Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.</p> <p>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.</p> <p>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.</p> <p>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.</p>

DHCP Relay	<p>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.</p> <p>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 (option 2). 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.</p> <p>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.</p> <p>The Remote ID is 6 bytes in length, and the value is equal to the DHCP relay agent's MAC address.</p>
------------	--

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	<p>Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.</p> <p>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.</p>
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	<p>Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).</p> <p>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.</p> <p>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.</p>
------	--

HTTPS	<p>Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection.</p> <p>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.</p> <p>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.</p>
-------	---

I

ICMP	<p>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.</p>
------	--

IEEE 802.1X	<p>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.</p>
-------------	---

IGMP	<p>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.</p>
------	---

IGMP Querier	<p>A router sends IGMP query messages onto a particular link. This router is called the Querier.</p>
--------------	--

IMAP	<p>Internet Message Access Protocol. It is a protocol for email clients to retrieve email messages from a mail server.</p> <p>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.</p> <p>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.</p>
------	---

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 extensdion 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	<p>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.</p> <p>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.</p>
MEP	<p>MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).</p>
MD5	<p>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.</p>
Mirroring	<p>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.</p> <p>Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port</p>
MLD	<p>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.</p>
MVR	<p>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.</p> <p>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.</p>

N

NAS	<p>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.</p>
-----	---

NetBIOS	<p>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).</p> <p>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.</p>
NFS	<p>Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.</p> <p>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.</p>
NTP	<p>Network Time Protocol. A network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as the transport layer.</p>

O

OAM	<p>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.</p>
Optional TLVs	<p>A LLDP frame contains multiple TLVs</p> <p>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.</p>
OUI	<p>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>

P

PCP	<p>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.</p>
PD	<p>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.</p>
PHY	<p>Physical Interface Transceiver. It is the device that implements the Ethernet physical layer (IEEE-802.3).</p>

Ping	<p>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.</p> <p>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.</p>
Policer	<p>A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.</p>
POP3	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
PPPoE	<p>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.</p>
Private VLAN	<p>In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.</p>
PTP	<p>Precision Time Protocol. A network protocol for synchronizing the clocks of computer systems.</p>

Q

QCE	<p>QoS Control Entry. It describes the QoS class associated with a particular QCE ID.</p> <p>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.</p>
-----	--

QCL	<p>QoS Control List. It is the list table of QCEs, containing QoS control entries that classify a specific QoS class on specific traffic objects.</p> <p>Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.</p>
QL	<p>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.</p>
QoS	<p>Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.</p> <p>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.</p>
QoS Class	<p>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.</p>

R

RARP	<p>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.</p>
RADIUS	<p>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.</p>
RDI	<p>Remote Defect Indication. It is a OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP.</p>
Router Port	<p>A router port is a port on the Ethernet switch that connects it to the Layer 3 multicast device.</p>
RSTP	<p>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.</p>

S

SAMBA	<p>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.</p> <p>Samba can be installed on a variety of operating system platforms, including Linux and most common Unix platforms.</p> <p>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".</p>
SHA	<p>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.</p>
Shaper	<p>A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.</p>
SMTP	<p>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.</p>
SNAP	<p>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.</p>
SNMP	<p>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.</p>
SNTP	<p>Simple Network Time Protocol. A network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as a transport layer.</p>
SPROUT	<p>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.</p>

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 obsolete 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	<p>Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange messages between computers.</p> <p>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.</p> <p>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.</p> <p>Common network applications that use TCP include the World Wide Web (WWW), email, and File Transfer Protocol (FTP).</p>

TELNET	<p>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.</p> <p>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.</p>
TFTP	<p>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.</p>
ToS	<p>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).</p>
TLV	<p>Type Length Value. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as a TLV.</p>
TKIP	<p>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.</p>

U

UDP	<p>User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.</p> <p>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.</p> <p>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.</p> <p>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).</p>
-----	---

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	<p>Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:</p> <p>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.</p> <p>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.</p> <p>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.</p>
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	<p>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).</p>
WPA-PSK	<p>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.</p>
WPA-Radius	<p>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.</p>
WPS	<p>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.</p>
WRED	<p>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.</p>
WTR	<p>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.</p>