



ISW Series Managed Industrial Ethernet Switch Hardware Installation & User Guide

ISW 4-10/100P, 2-10/100T, 2-SFP

ISW 4GbP, 2GbT, 2-SFP

ISW 8-10/100P, 4-SFP

ISW 8GbP, 4-SFP

9034965-02 Rev AB
April 2022



Copyright © 2022 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: <https://www.extremenetworks.com/support/policies/open-source-declaration/>



Table of Contents

Preface.....	5
Text Conventions.....	5
Documentation and Training.....	6
Getting Help.....	7
Subscribe to Service Notifications.....	7
Providing Feedback.....	7
Industrial Series Switch Overview.....	9
Safety Instructions.....	9
Faceplate and Panels.....	10
LED Status Indicators.....	12
Technical Specifications.....	14
System Statistics.....	17
Installing Industrial Switches.....	18
Mounting the ISW (DIN-Rail).....	18
Mounting the ISW (Wall).....	19
Connecting the Ethernet Interface (RJ45 Ethernet).....	20
Connecting the Ethernet Interface (Fiber).....	21
Connecting the Power Terminal Block.....	23
Alarm Relay and Ground Connection.....	23
Console Connection.....	24
System Reset.....	25
Connecting & Logging in to the Switch.....	26
Web Browser Support.....	26
Monitoring the Ethernet Interface.....	27
Upgrading and Downgrading Software.....	27
Resetting Configuration Defaults via CLI Command.....	27
Resetting Configuration Defaults via Web UI.....	28
ISW Application Guides.....	29
VLAN Application Guide.....	29
Example 1: Default VLAN Settings.....	29
Example 2: Port-based VLANs.....	30
Example 3: IEEE 802.1Q Tagging.....	32
Security Application Guide.....	34
Case 1: ACL for MAC Address.....	35
Case 2: ACL for IP address.....	48
Case 3: ACL for L4 Port.....	48
Case 4: ACL for ToS.....	48
Ring Version 2 Application Guide.....	49
Ring Version 2 Features.....	49
Configuring RingV2 (Web UI).....	54

Configuring RingV2 (Console).....	62
RingV2 with ERPS.....	63
QoS Application Guide.....	63
SP/SPWRR.....	63
Application Examples.....	64
IGMP Application Guide.....	69
Example 1.....	69
Example 2.....	71
Example 3.....	73
802.1x Authentication Application Guide.....	74
802.1x Configuration Overview.....	74
802.1x Timer Parameters.....	77
Enable 802.1x and MAC Authentication on the Same Port.....	78
Power over Ethernet (PoE) Application Guide.....	80
Reserved Power Determination.....	81
Power Management Mode.....	82
Other PoE Parameters.....	83
PoE Power Scheduling & Reset.....	84
Regulatory and Compliance Information.....	88
Federal Communications Commission (FCC) Notice.....	88
Industry Canada Notice CAN ICES-3 (A)/NMB-3(A).....	88
Product Safety.....	88
Electromagnetic Compatibility (EMC).....	89
Korea EMC Statement (KCC).....	89
BSMI EMC Statement - Taiwan.....	89
Glossary.....	90



Preface

This section describes the text conventions used in this document, where you can find additional information, and how you can provide feedback to us.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings






Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
screen displays	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words <i>enter</i> and <i>type</i>	When you see the word <i>enter</i> in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says <i>type</i> .
Key names	Key names are written in boldface, for example Ctrl or Esc . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
<i>italic</i> text	Italic text indicates variable content.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member</i> [<i>member</i> ...].
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware and software compatibility](#) for Extreme Networks products

[Extreme Optics Compatibility](#)

[Other resources](#) such as white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit www.extremenetworks.com/education/.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form (all fields are required).
3. Select the products for which you would like to receive notifications.



Note

You can modify your product selections or unsubscribe at any time.

4. Select **Submit**.

Providing Feedback

The Information Development team at Extreme Networks has made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help

you work better, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information in the document.
- Broken links or usability issues.

If you would like to provide feedback, you can do so in three ways:

- In a web browser, select the feedback icon and complete the online feedback form.
- Access the feedback form at <https://www.extremenetworks.com/documentation-feedback/>.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.



Industrial Series Switch Overview

[Safety Instructions](#) on page 9

[Faceplate and Panels](#) on page 10

[LED Status Indicators](#) on page 12

[Technical Specifications](#) on page 14

ISW-Series Managed Industrial Ethernet Switch deliver high quality, wide operation temperature range, extended power input range, and advanced VLAN (Virtual LAN) & QoS (Quality of Service) features. It's ideal for harsh environments and mission-critical applications.

The Managed Ethernet Switch solutions are designed for supporting standard industrial applications. Managed switches are easier to prioritize, partition, and organize user's network, providing a more reliable and better quality services.

This guide covers installation for the following Industrial Switches:

- ISW 4-10/100P,2-10/100T,2-SFP
- ISW 8-10/100P,4-SFP
- ISW 4GBP,2GBT,2-SFP
- ISW 8GBP,4-SFP

Safety Instructions

When a connector is removed during installation, testing, or servicing, or when an energized fiber is broken, a risk of ocular exposure to optical energy that may be potentially hazardous occurs, depending on the laser output power.

The primary hazards of exposure to laser radiation from an optical-fiber communication system are:

- Damage to the eye by accidental exposure to a beam emitted by a laser source.
- Damage to the eye from viewing a connector attached to a broken fiber or an energized fiber.

Faceplate and Panels

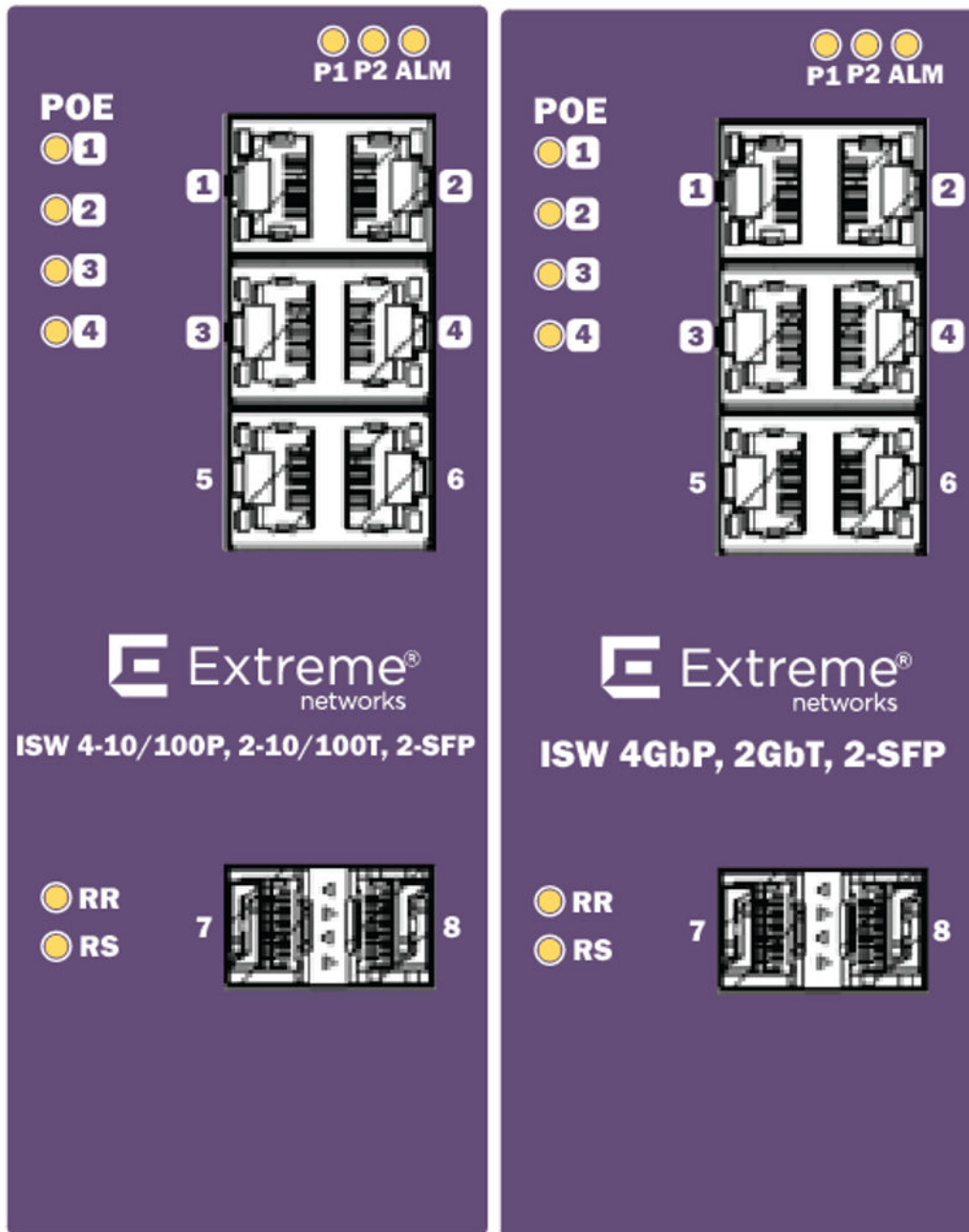


Figure 1: 4-Port PoE Series Faceplate

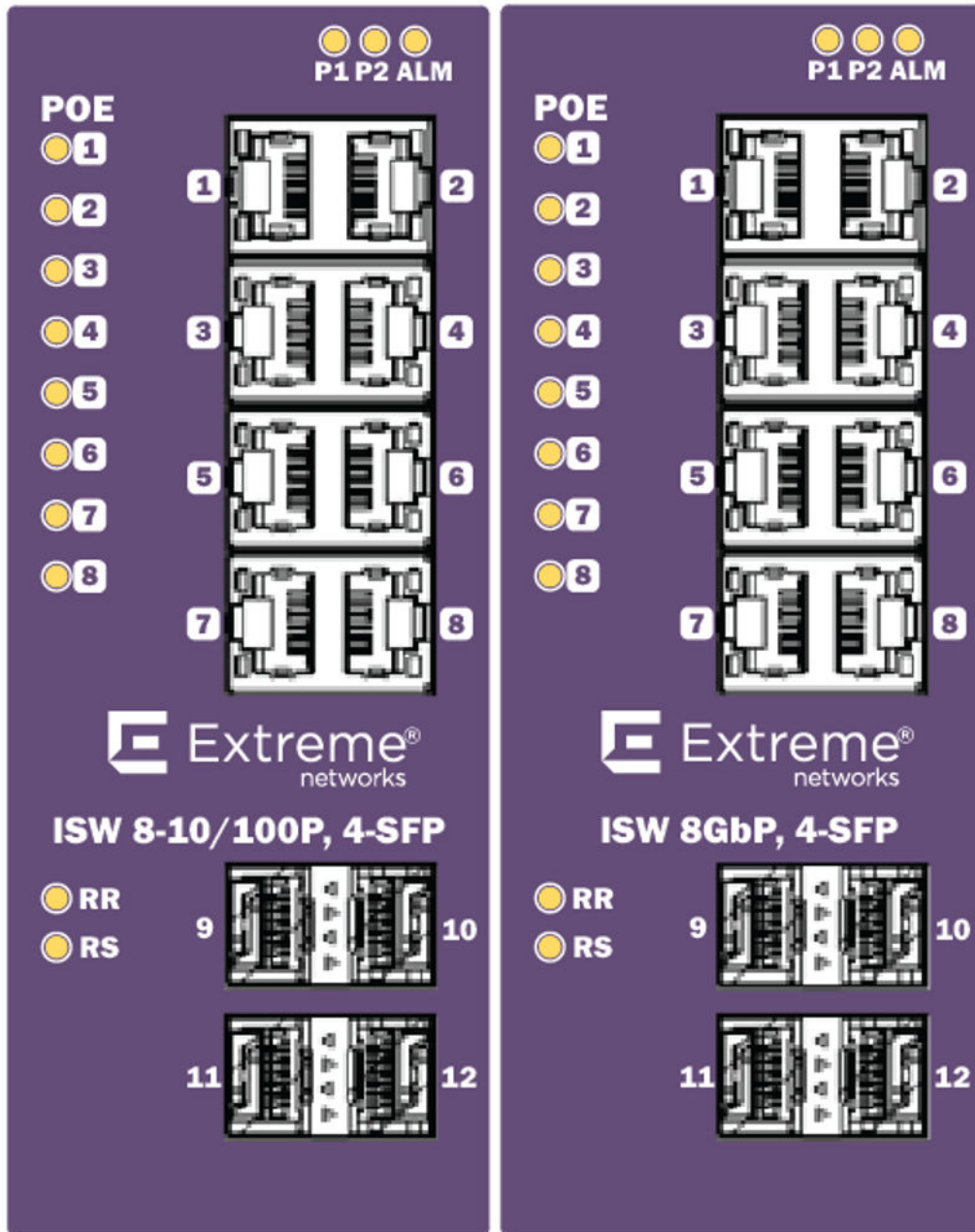


Figure 2: 8-Port PoE Series Faceplate

Front Panel	
System Status LED	P1, P2 and Alarm
Gigabit Ethernet Copper Ports	RJ45
Gigabit Ethernet SFP ports	SFP Slots
POE LED	POE port status
RR/RS LED	Device info/status



Figure 3: Top Panel

Top Panel	
Power Input (Dual)	6P Terminal Block
Console (RS232)	RJ45
Reset	Push Button

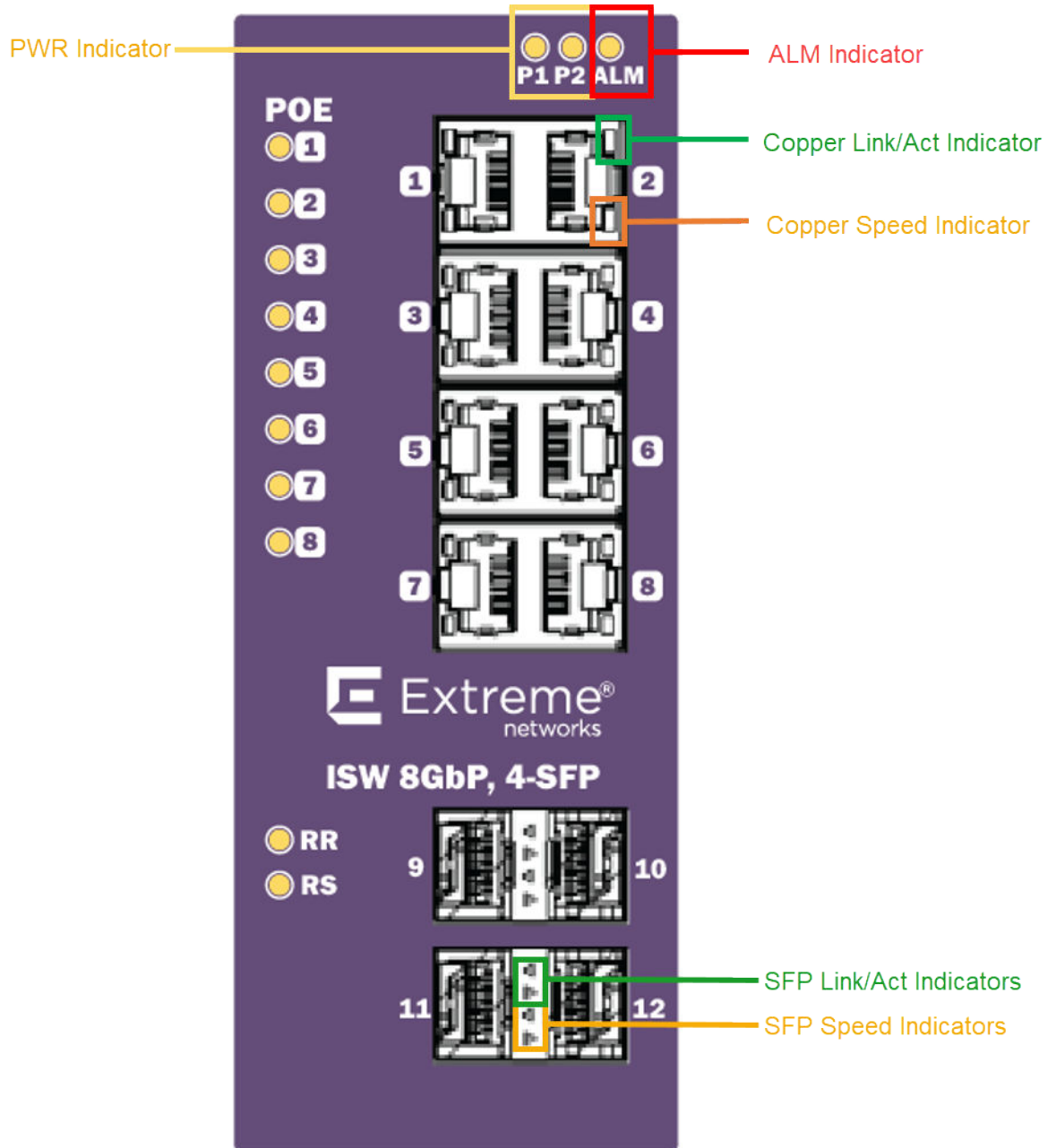
LED Status Indicators

Table 4: LED Status Indicators

LED	State	Description
P1	On Green	P1 power line has power
	Off	P1 power line disconnect or does not have supply power
P2	On Green	P2 power line has power
	Off	P2 power line disconnect or does not have supply power
Alarm	On Red	Alarm event occurs
	Off	No alarm
Copper ports Link/Act	On Green	Ethernet link up but no traffic is detected
	Flashing Green	Ethernet link up and there is traffic detected
	Off	Ethernet link down
Copper ports Speed	On Amber	A 100 Mbps or a 1000 Mbps connection is detected
	Off	No link or a 10 Mbps connection is detected

Table 4: LED Status Indicators (continued)

LED	State	Description
SFP port Link/Act	On Green	Ethernet link up
	Off	Ethernet link down
SFP port Speed	On Amber	SFP port speed 1000 Mbps connection is detected.
	Off	No link or a SFP port speed 100Mbps connection is detected
RR (Redundant Role)	On	Redundant Master (Ring Master, Ring Coupling Backup, Dual Homing, Chain Head, Balancing Chain Central Block) is enabled in the system.
	Off	No Redundant Master is enabled in the system.
RS (Redundant Status)	On	<ol style="list-style-type: none"> 1. If any Ring port links are down, the RS LED will be ON. 2. If the device has any of Redundant Master (Ring Master, Ring Coupling Backup, Dual Homing, Chain Head, Balancing Chain Central Block) and detects a Ring/Coupling/Dual Homing/Chain/Balancing Chain failure (any node is link down), and then RS LED will be ON.
	Off	All of the Ring ports are link up or Ring/Coupling/Dual Homing/Chain/Balancing Chain is healthy.



Technical Specifications

Ethernet	
Operating mode	Store and forward, L2 wire-speed/non-blocking switching engine
MAC addresses	8K
Jumbo frames	9K Bytes
Copper RJ45 Ports	
Speed	10/100/1000 Mbps

MDI/MDIX Auto-crossover	Support straight or cross wired cables
Auto-negotiating	10/100/1000 Mbps speed auto-negotiation; Full and half duplex
Ethernet isolation	1500 VRMS 1 minute
SFP (pluggable) Ports	
Port types supported	SFP (pluggable) Ports 100/1000Base SFP slot Support 100/1000BaseT SFP transceiver
Fiber port connector	LC typically for fiber (depends on module)
Optimal fiber cable	Typical 50 or 62.5/125 μm for multimode (mm); Typical 8 or 9/125 μm for single mode (sm)
Network Redundancy	
Fast failover protection rings	Single & Multiple rings supported
Spanning Tree Protocol	IEEE 802.1D STP, IEEE 802.1w RSTP, IEEE 802.1s MSTP
Port Trunk with LACP	Static trunk or Dynamic via LACP
Bridge, VLANs & Protocols	
Flow control	IEEE 802.3x (Full Duplex) and Back-Pressure(Half Duplex)
<u>VLAN</u> Types	Port-based VLANs IEEE 802.1Q tag-based VLANs IEEE 802.1ad Double Tagging (Q in Q)
Multicast protocols	<u>IGMP (Internet Group Management Protocol)</u> v1, v2 IGMP snooping and querying Immediate leave and leave proxy Throttling and filtering
<u>LLDP (Link Layer Discovery Protocol)</u>	IEEE 802.1ab LLDP
Traffic management & QoS	
Priority	IEEE 802.1p <u>QoS</u>
Number of queues per port	8
Scheduling schemes	SPQ, WRR
Traffic Shaper	Port-based shaping
Security	
Port security	IP and MAC-based access control IEEE 802.1X authentication Network Access Control
Power	
Power input	Redundant Input Terminals
Input voltage range Max. power consumption	Non-POE mode: 12–58 VDC 802.3af POE mode 46–58 VDC 802.3at POE mode 50–58 VDC Power Consumption: 15 Watts without POE PD loading
Reverse power protection	Yes
Total PoE output power budget PoE PSE port output power management	120W (ISW 16801) / 240W (ISW 16803) Scheduling; power control; PoE PD power consumption monitoring

Transient protection	15,000 watts peak
Indicators	
Power Status indication	Indication of power input status
Ethernet port indication	Link & Speed
Management	
User Management interfaces	<ul style="list-style-type: none"> • CLI • Web-based Management • <u>SNMP (Simple Network Management Protocol) v1, v2c</u> • Telnet (5 sessions)
Management Security	HTTPS, SSH Radius Client for Management
Upgrade & Restore	Configuration Import/Export Firmware Upgrade
Diagnostic	Syslog Per-VLAN mirroring SFP with DDM (Digital Diagnostic Monitoring)
MIBs	RMON 1,2,3,9; Q-Bridge MIB, RFC 1213 MIB-II, RFC 4188 Bridge MIB
<u>DHCP (Dynamic Host Configuration Protocol)</u>	Client, Server, Relay, Snooping, Option 82
<u>NTP/SNTP (Simple Network Time Protocol)</u>	Yes
Environmental & Compliances	
Operating temperature range	-40 to +75°C (cold startup at -40°C)
Storage temperature range	-40 to +85°C
Humidity (non-condensing)	5 to 95% RH
Vibration, shock & freefall	IEC68-2-6, -27, -32
Certification compliance	CE/FCC; EN-50121-4
Electrical safety	CSA C22, EN61010-1, CE
EMC	FCC Part 15, CISPR 22 (EN55022) Class A IEC61000-4-2, -3, -4, -5, -6
RoHS and WEEE	RoHS (Pb free) and WEEE compliant
MTBF	> 25 years
Mechanical	
Ingress protection	IP30
Installation option Dimension Weight	DIN-Rail mounting, Wall mounting 77mm W x 154mm H x 128mm D (3 in. W x 6 in. H x 5 in. D) Unpackaged:1.49kg (3.3 lb.); Packaged: 1.99kg (4.4 lb.)

System Statistics

Function Name	System Max Value
<u>VLAN ID</u>	4096
VLAN Limitation	2048
Privilege Level of User	15
RMON Statistic Entry	65535
RMON Alarm Entry	65
RMON Event Entry	65535
IPMC Profile	64
IPMC Rule / Address Entry	128
ACE	256
ICMP Type / Code	255
<u>RADIUS (Remote Authentication Dial In User Service) Server</u>	5
TACACS+ Server	5
MAC-based VLAN Entry	256
IP subnet-based VLAN Entry	128
Protocol-based VLAN Group	125
Voice VLAN OUI	16
QCE	256
IP Interface	8
IP Route	32
Security Access Management	16
MVR VLAN	4
MAC Learning table address	8k
<u>IGMP Group</u>	1000



Installing Industrial Switches

- [Mounting the ISW \(DIN-Rail\) on page 18](#)
- [Mounting the ISW \(Wall\) on page 19](#)
- [Connecting the Ethernet Interface \(RJ45 Ethernet\) on page 20](#)
- [Connecting the Ethernet Interface \(Fiber\) on page 21](#)
- [Connecting the Power Terminal Block on page 23](#)
- [Alarm Relay and Ground Connection on page 23](#)
- [Console Connection on page 24](#)
- [System Reset on page 25](#)
- [Connecting & Logging in to the Switch on page 26](#)
- [Monitoring the Ethernet Interface on page 27](#)
- [Upgrading and Downgrading Software on page 27](#)
- [Resetting Configuration Defaults via CLI Command on page 27](#)
- [Resetting Configuration Defaults via Web UI on page 28](#)

Mounting the ISW (DIN-Rail)

Mounting steps:

1. Screw the DIN-Rail bracket on with the bracket and screws in the accessory kit.
2. Hook the unit over the DIN rail.
3. Push the bottom of the unit towards the DIN Rail until it snaps into place.

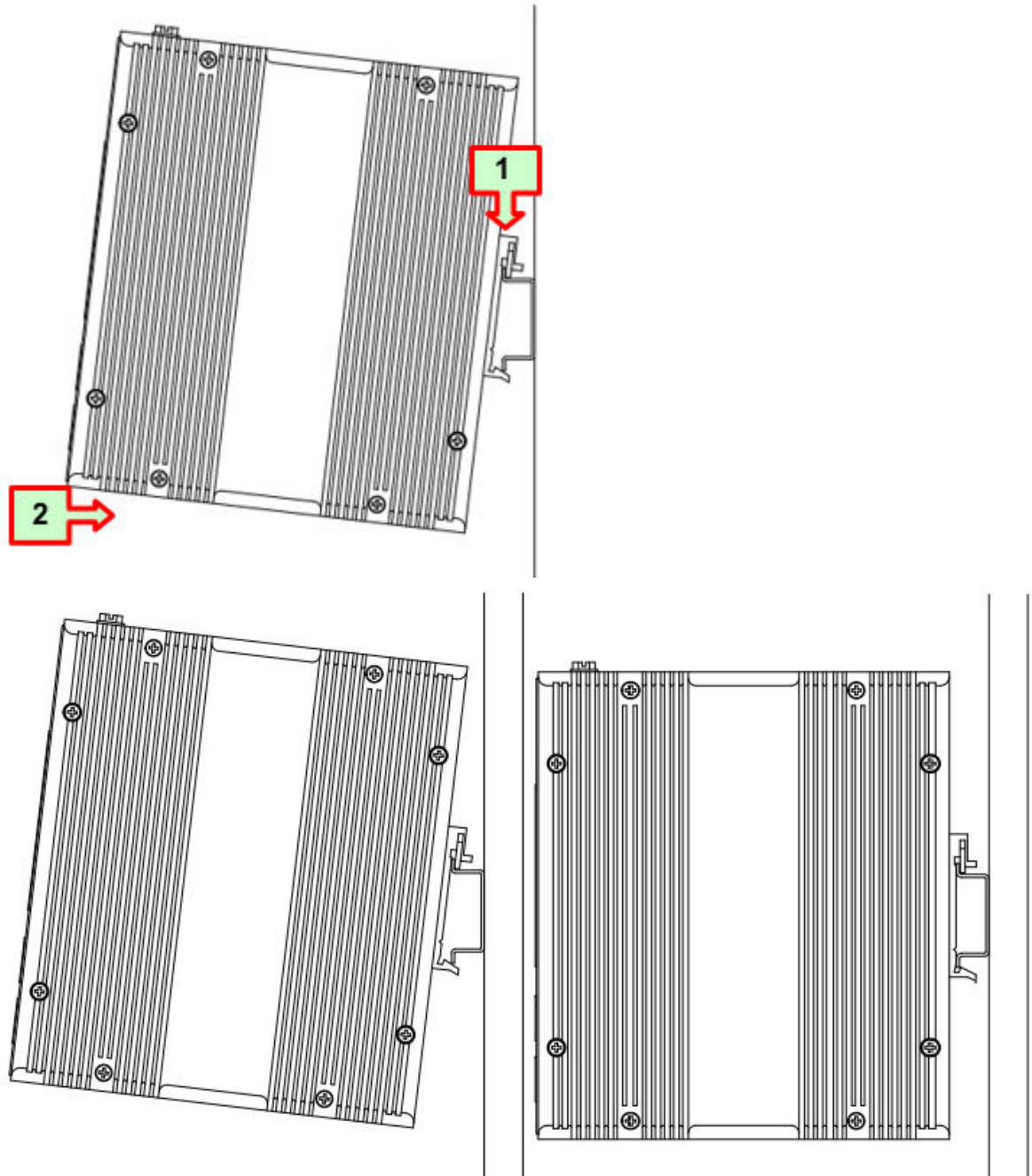
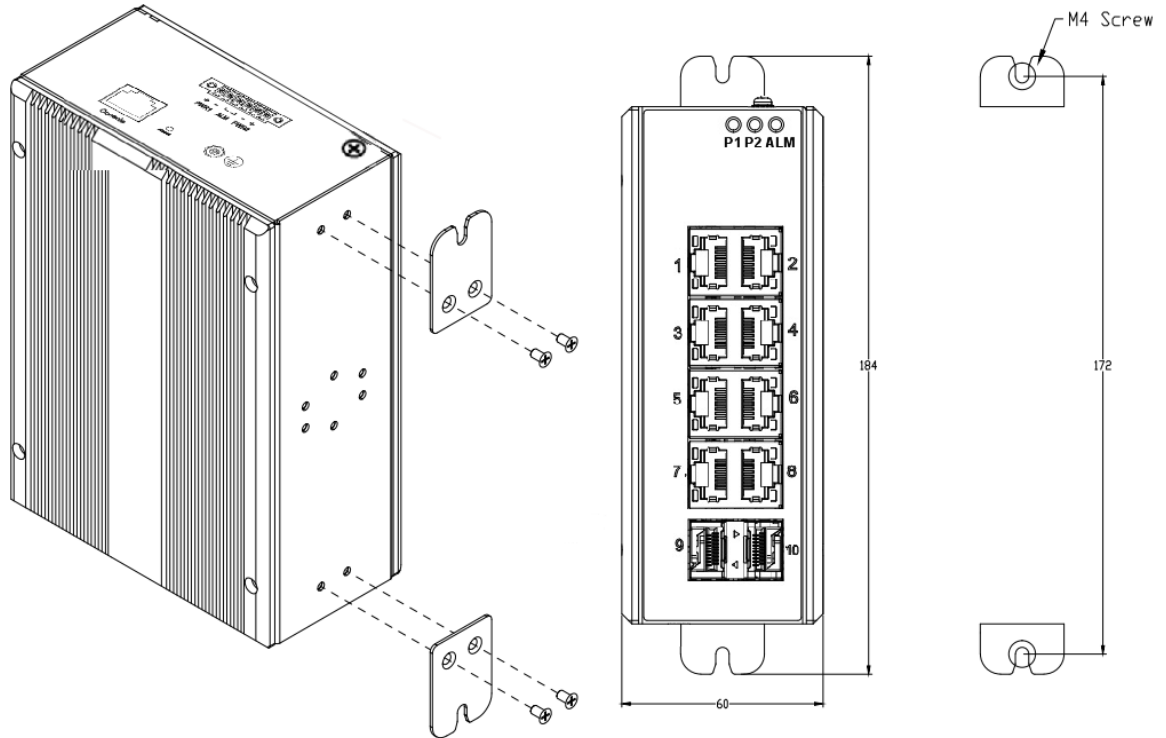


Figure 4: DIN-Rail Mounting

Mounting the ISW (Wall)

Attach the wall-mounting plates with the screws provided in the accessory kit.



Connecting the Ethernet Interface (RJ45 Ethernet)

ISW provides two types of electrical (RJ45) and optical (mini-GBIC) interfaces.

- To connect to a PC, use a straight-through or a cross-over Ethernet cable.
- To connect the ISW copper port to an Ethernet device, use UTP (Unshielded Twisted Pair) or STP (Shielded Twisted Pair) Ethernet cables.



The pin assignment of RJ45 connector is shown in [Figure 5](#) and [Table 5](#)

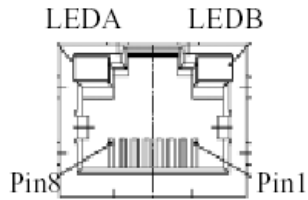


Figure 5: RJ45 Connector Pins

Table 5: RJ45 Connector Pin Assignment

Pin	Assignment	PoE Assignment
1, 2	T/Rx+, T/Rx-	Positive VPort
3, 6	T/Rx+, T/Rx-	Negative VPort
4, 5	T/Rx+, T/Rx-	X
7, 8	T/Rx+, T/Rx-	X

Connecting the Ethernet Interface (Fiber)

For both 100/1000 Mbps fiber speed connections, the SFP slots are available. The SFP slot accepts the fiber transceivers that typically have an LC connector.

The fiber transceivers have options of multimode, single mode, long-haul, or special-application transceivers.

Prepare a proper SFP module and install it into the optical port. Then you can connect fiber optics cabling that uses LC connectors or SC connectors (with the use of an optional SC-to-LC adapter) to the fiber optics connector.

Refer to [LED Status Indicators](#) on page 12 for the normal operational LED status.

Figure 6: Fiber optics cable with LC duplex connector



Figure 7: Connect the optical fiber to the SFP socket



Warning

Never attempt to view optical connectors that might be emitting laser energy. Do not power up the laser product without connecting the laser to the optical fiber and putting the cover in position, as laser outputs will emit infrared laser light at this point.

Connecting the Power Terminal Block

The DC power interface is a 6-pin terminal block with polarity signs on the top panel. The ISW can be powered from two power supply (input range 12V – 58V). The DC power connector is a 6-pin terminal block; there is alarm contact on the middle terminal block.

The switch can be powered from two power supplies (input range 12V – 58V). Insert the positive and negative wires into V+ and V- contacts on the terminal block respectively and tighten the wire-clamp screws to prevent the wires from being loosened.



Note

The DC power should be connected to a well-fused power supply.

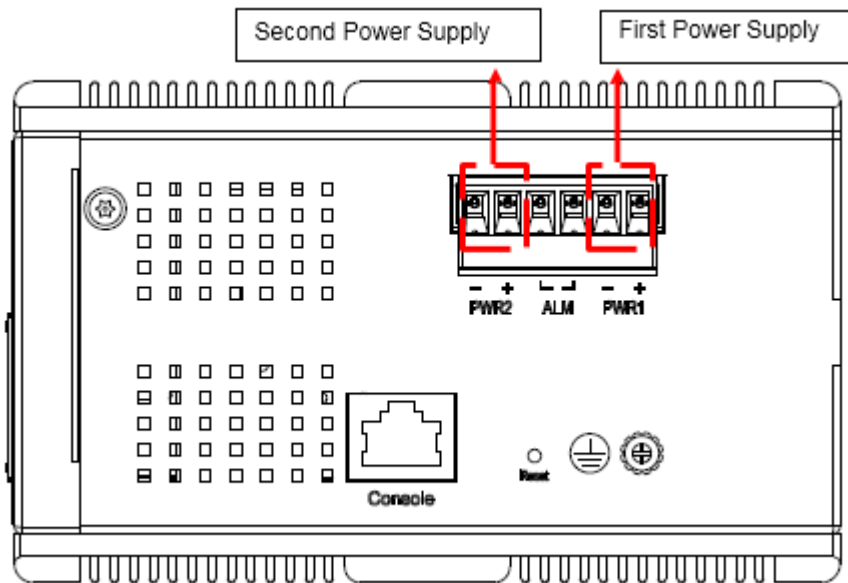


Figure 8: Power Supplies

Power Connector (6P Terminal Block)	
Input	DC 12-58V
PWR1 +/-	Power Input 1 +/-
PWR2 +/-	Power Input 2 +/-
ALM	Alarm relay output

Alarm Relay and Ground Connection

The alarm relay output contacts are in the middle of the DC terminal block connector as shown in [Figure 9](#).

The alarm relay out is “Normal Open,” and it will be closed when detected any predefined failure such as power failures or Ethernet link failures.

The relay output with current carrying capacity of 0.5A @ 24 VDC.

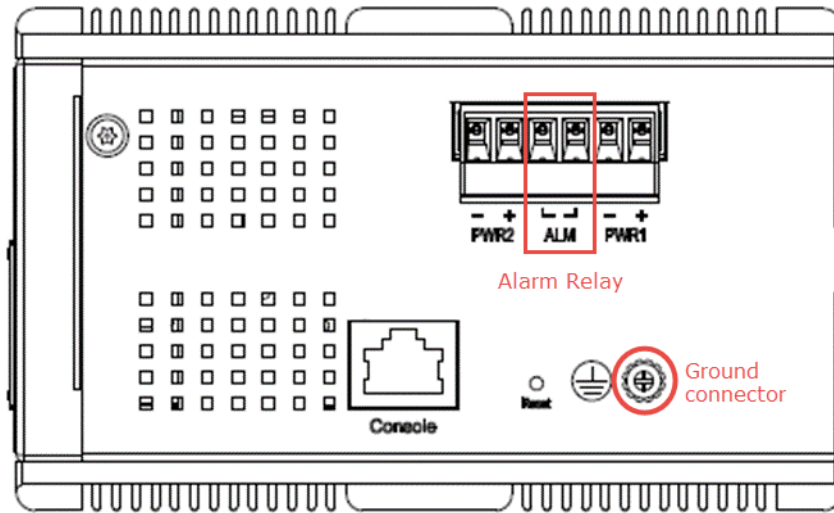


Figure 9: Alarm Relay and Ground Connector

Console Connection

The Console port is for local management by using a terminal emulator or a computer with terminal emulation software.

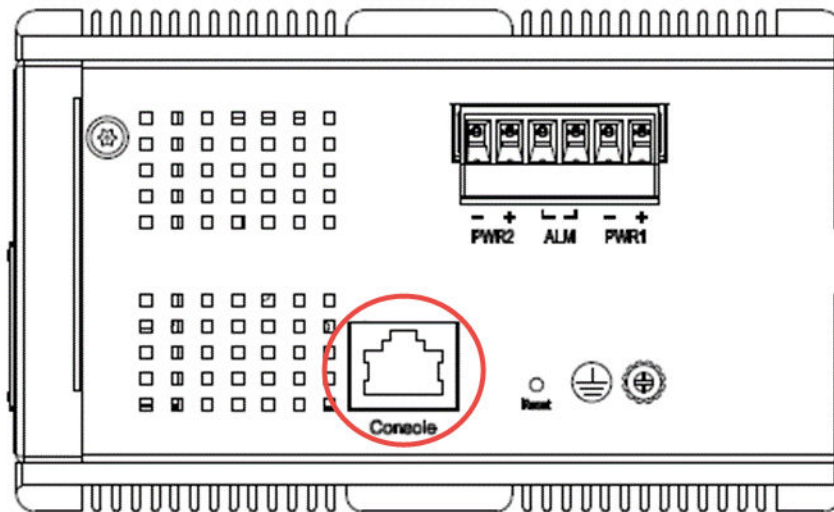


Figure 10: ISW Console Port

To connect the host PC to the switch, use the supplied RJ45 (male) connector-to-RS232 DB9 (female) connector. Connect the RJ45 connector to the switch’s Console port shown in [Figure 10](#), and then connect the DB9 connector to the PC COM port.



Important

Using a different cable than the one provided with the switch may cause bootup issues.

Once the host PC is connected to the switch, enter the following terminal settings:

- **Speed (baud rate):** 115200 bps
- **Data bits:** 8
- **Stop bits:** 1
- **Parity:** None
- **Flow control:** None

The pin assignment of the Console cable is shown in [Figure 11](#).

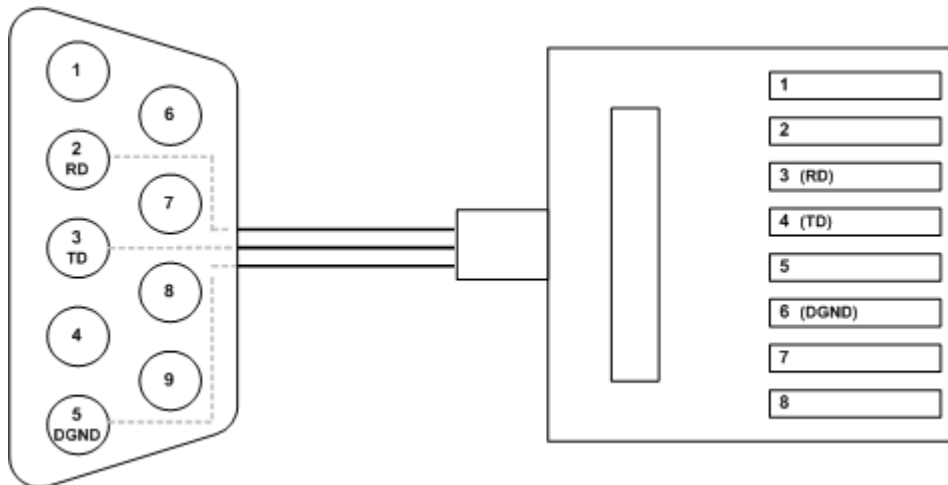
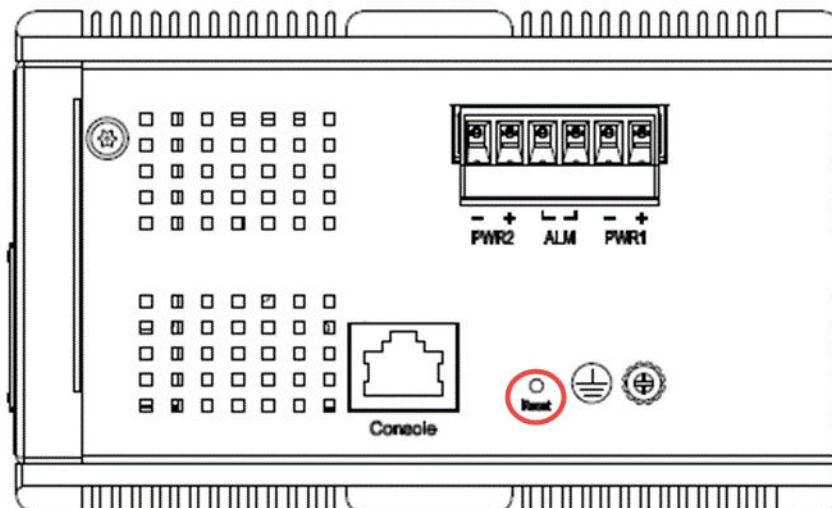


Figure 11: Console Cable Pin Assignment

System Reset

The **Reset** button is provided to reboot the system without the need to remove power. Under normal circumstances, you will not have to use it. However, on rare occasions, the ISW may not respond and you may need to push the **Reset** button.



Connecting & Logging in to the Switch

1. Connect to ISW Ethernet port (RJ45 Ethernet port) using factory default IP: 192.0.2.1.
2. Log in with default account and password (admin / [none])
3. (Optional) Change the IP with commands listed below:

```
enable
configure terminal
interface vlan 1
ip address xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx
exit
```

4. To log in to the web interface, enter your switch's IP address in a web browser.
Refer to [Web Browser Support](#) on page 26 to ensure your browser is supported.
5. Enter the account name and password.
6. Click **Sign in**.

For information on configuring and monitoring the switch through the web interface, see the [ISW-Series Managed Industrial Ethernet Switch Web Configuration Guide](#).

Web Browser Support

Internet Explorer

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

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

Firefox

Firefox with the following default settings is recommended:

Web page font	Times New Roman
Encoding	Unicode (UTF-8)
Text size	16

Chrome

Google Chrome with the following default settings is recommended:

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

Monitoring the Ethernet Interface

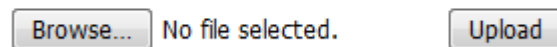
By RJ45 Ethernet: See the figures in [Industrial Series Switch Overview](#) on page 9 for monitoring 8 Gigabit Ethernet with copper connector (RJ45). Also refer to [Table 4](#) on page 12 for the normal operational LED status.

By SFP: See the figures in [Industrial Series Switch Overview](#) on page 9 for monitoring 4 Gigabit Ethernet with SFP connector. Also refer to [Table 4](#) on page 12 for the normal operational LED status.

Upgrading and Downgrading Software

1. From the web UI, go to **Maintenance** > > **Software** > > **Upload** page.
2. Select the software file, and click **Upload**.

Software Upload



3. After beginning the upload process, do not cold/warm start device. Instead, wait for auto-reboot, and then the upgrade can complete.

Resetting Configuration Defaults via CLI Command

If you want to reset the configuration to default, but keep management IP settings, do the following:

1. Execute the command: `reload defaults keep-ip`
2. Check interface *VLAN (Virtual LAN)* and IP address, and confirm only management IP setting is kept.
3. Execute the command: `copy running-config startup-config`

```

COM1:115200baud - Tera Term VT
File Edit Setup Control Window Help
# reload defaults keep-ip
% Reloading defaults, attempting to keep VLAN 1 IP address. Please stand by.
% If need reboot must wait for 3~5 seconds.
#
# show int vlan 1
VLAN1
  LINK: 00-11-22-dd-0c-01 Mtu:1500 <UP BROADCAST RUNNING MULTICAST>
  IPv6: fe80:2::211:22ff:fedd:c01/64 <ANYCAST TENTATIVE AUTOCONF>
  IPv4: 192.168.0.1/24 192.168.0.255
# show int vlan 200
% VLAN interface 200 does not exist.
#
# show vlan
VLAN  Name                               Interfaces
-----
1     default                               Gi 1/1-14
#
# show int vlan 1
VLAN1
  LINK: 00-11-22-dd-0c-01 Mtu:1500 <UP BROADCAST RUNNING MULTICAST>
  IPv6: fe80:2::211:22ff:fedd:c01/64 <ANYCAST TENTATIVE AUTOCONF>
  IPv4: 192.168.0.1/24 192.168.0.255
#
# copy running-config startup-config

```

If you want to reset all configurations to the default:

4. Execute the command: `reload defaults`
5. Check interface VLAN and IP address, and confirm they all change to default settings.

- Execute the command: `copy running-config startup-config`

```
# reload defaults
% Reloading defaults. Please stand by.
% If need reboot must wait for 3~5 seconds.
# show int vlan 1
VLAN1
  LINK: 00-11-22-dd-0c-01 Mtu:1500 <UP BROADCAST RUNNING MULTICAST>
  IPv4: 192.0.2.1/24 192.0.2.255
  IPv6: fe80:2::211:22ff:fedd:c01/64 <ANYCAST TENTATIVE AUTOCONF>
# show vlan
VLAN Name                Interfaces
-----
1    default                Gi 1/1-14

# copy running-config startup-config
Building configuration...
% Saving 1357 bytes to flash:startup-config
% If need reboot must wait for 3~5 seconds.
#
```

Resetting Configuration Defaults via Web UI

If you want to reset the configuration to default, but keep management IP settings, do the following:

- Go to **Maintenance > Factory Default** and click **Yes**.

Factory Defaults

**Are you sure you want to reset the configuration to
Factory Defaults?**

- Go to **Maintenance > Configuration > Save startup-config** and click **Save Configuration**.

Save Running Configuration to startup-config

Please note: The generation of the configuration file may be time consuming, depending on the amount of non-default configuration.

If you want to reset all configurations to the default:

- Go to **Maintenance > Configuration > Activate**.
- Select **default-config** and then click **Activate Configuration**.

Activate Configuration

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

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

File Name

default-config
 startup-config

- Change PC's IP address belong to 192.0.2.X networks.
- Change web's IP be 192.0.2.1 (default IP) to login DUT's Web UI.
- Go to **Maintenance > Configuration > Save startup config** and then click **Save Configuration**.



ISW Application Guides

[VLAN Application Guide on page 29](#)

[Security Application Guide on page 34](#)

[Ring Version 2 Application Guide on page 49](#)

[QoS Application Guide on page 63](#)

[IGMP Application Guide on page 69](#)

[802.1x Authentication Application Guide on page 74](#)

[Power over Ethernet \(PoE\) Application Guide on page 80](#)

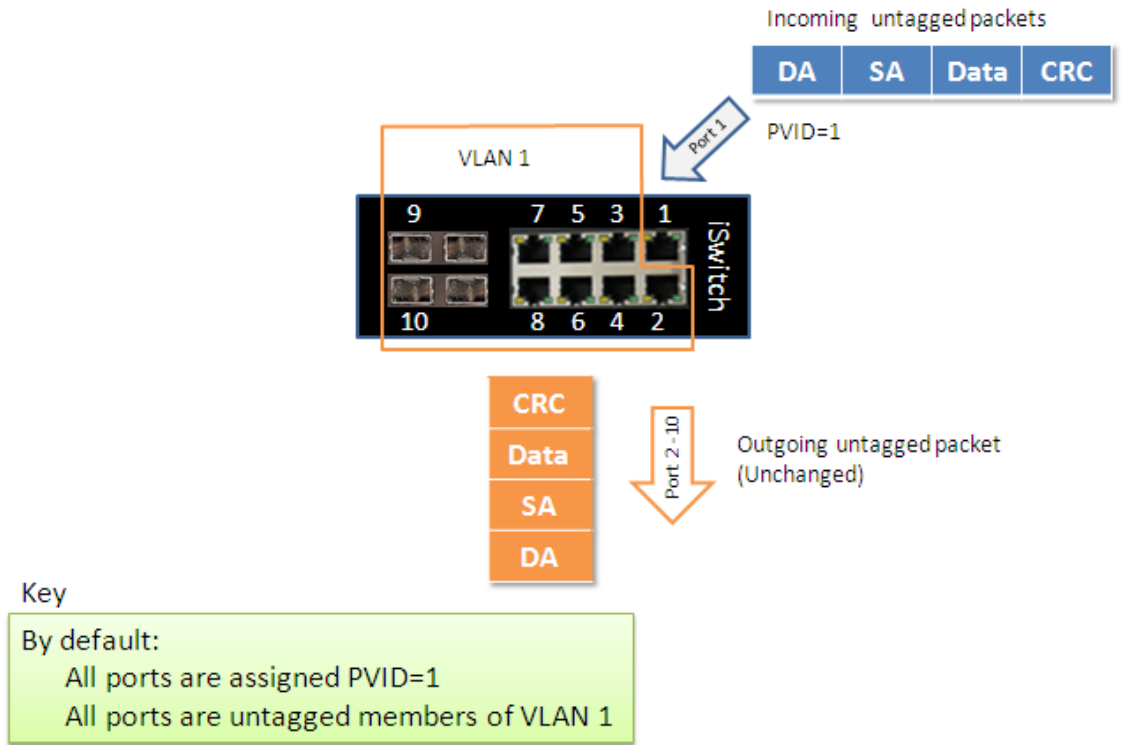
This chapter describes how to configure VLAN (Virtual LAN)s in ISW. The ISW supports up to 2048 VLANs. Ports are grouped into broadcast domains by assigning them to the same VLAN. Frames received in on VLAN can only be forwarded within that VLAN, and multicast frames and unknown unicast frames are flooded only to ports in the same VLAN.

VLAN Application Guide

Example 1: Default VLAN Settings

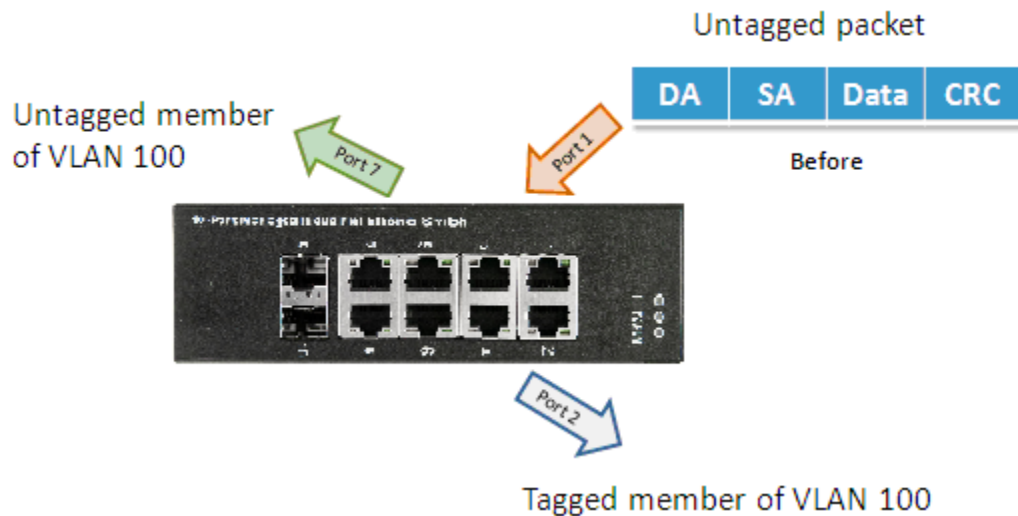
Each port in the ISW has a configurable default VLAN number, known as its PVID. This places all ports on the same VLAN initially, although each port PVID is configurable to any VLAN number between 1 and 4094.

The default configuration settings for ISW have all ports set as untagged members of VLAN 1 with all ports configured as PVID=1. In default configuration example shown in the following figure, all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID=1).



Example 2: Port-based VLANs

When the ISW receives an untagged VLAN packet, it will add a VLAN tag to the frame according to the PVID setting on a port. As shown in the following figure, the untagged packet is marked (tagged) as it leaves the ISW through Port 2, which is configured as a tagged member of VLAN100. The untagged packet remains unchanged as it leaves the ISW through Port 7, which is configured as an untagged member of VLAN100.



Configuring Port-based VLANs from the Web UI

- Go to **Configuration > VLANs > Port VLAN** configuration table and configure PVID 100 on Port 1, Port 2, and Port 7.

Global VLAN Configuration

Allowed Access VLANs	1,100
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Trunk	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1-4095	
2	Trunk	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
7	Trunk	100	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1-4095	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
9	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
10	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
11	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
12	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	

Save Reset

- Select **Configuration > VLAN > Static > VLAN**.
- Create a VLAN with VLAN ID 100.
- Enter a VLAN name in the Name field.
- Assign VLAN tag setting to or remove it from a port by toggling the check box under the individual port number.

The tag settings determine if packets that are transmitted from the port tagged or untagged with the VLAN ID. The possible tag settings are:

Tag All	Specifies that the egress packet is tagged for the port.
Untag port VLAN	Specifies that the egress packet is untagged for the port.
Untag All	Specifies that all frames, whether classified to the Port VLAN or not, are transmitted without a tag.

- Transmit untagged unicast packets from Port 1 to Port 2 and Port 7.
The ISW should tag it with VID 100. The packet has access to Port2 and Port 7. The outgoing packet is stripped of its tag to leave Port 7 as an untagged packet. For Port 2, the outgoing packet leaves as a tagged packet with VID 100.
- Transmit untagged unicast packets from Port 2 to Port 1 and Port 7.
The ISW should tag it with VID 100. The packet has access to Port1 and Port 7. The outgoing packet is stripped of its tag to leave Port 7 as an untagged packet. For Port 1, the outgoing packet leaves as a tagged packet with VID 100.
- Transmit untagged unicast packets from Port 7 to Port 1 and Port 2.
The ISW should tag it with VID 100. The packet has access to Port1 and Port 2. For Port 1 and Port 2, the outgoing packet leaves as a tagged packet with VID 100.
- Repeat step 6 on page 31 using broadcast and multicast packets.

Configuring Port-based VLANs from the CLI

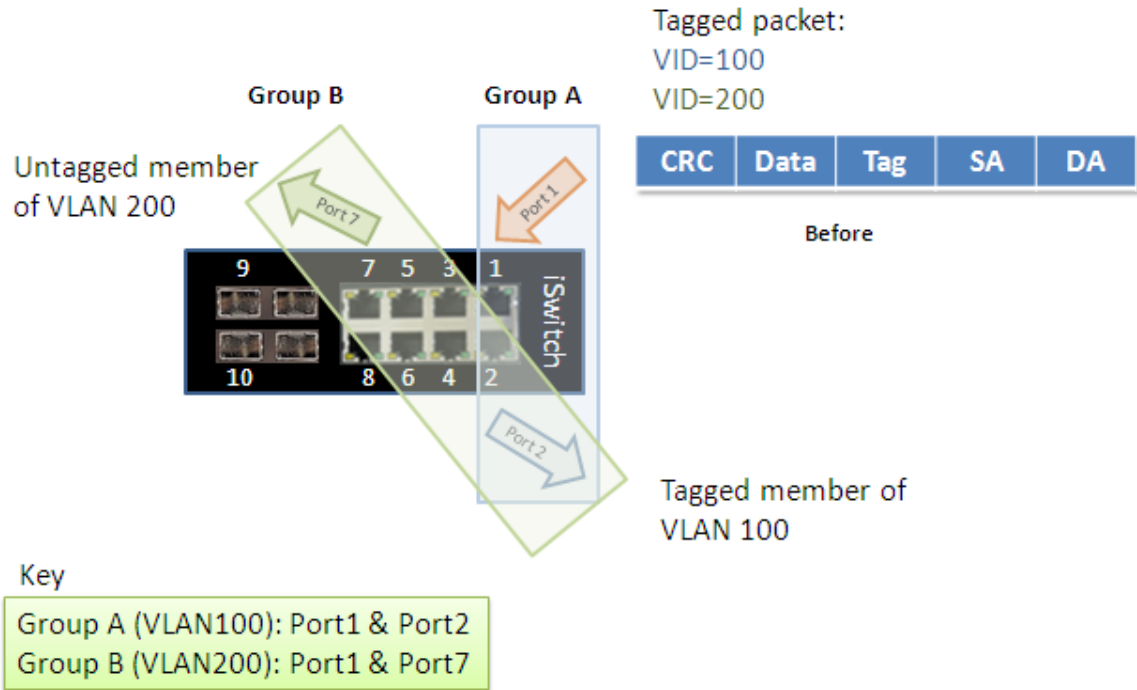
To configure VLANs from the CLI, execute the following commands:

```
vlan 1
vlan 100
interface GigabitEthernet 1/1
switchport access vlan 100
switchport trunk native vlan 100
switchport trunk allowed vlan 1,100
switchport trunk vlan tag native
switchport mode trunk
exit
interface GigabitEthernet 1/2
switchport access vlan 100
switchport trunk native vlan 100
switchport trunk allowed vlan 1,100
switchport trunk vlan tag native
switchport mode trunk
exit
interface GigabitEthernet 1/7
switchport access vlan 100
switchport trunk native vlan 100
switchport trunk allowed vlan 1,100
switchport mode trunk
exit
```

Example 3: IEEE 802.1Q Tagging

ISW is able to construct Layer-2 broadcast domain by identifying VLAN ID specified by IEEE 802.1Q. It forwards a frame between bridge ports assigned to the same VLAN ID and can set multiple VLANs on each bridge port.

In the following figure, the tagged incoming packets are assigned directly to VLAN 100 and VLAN 200 because of the tag assignment in the packet. Port 2 is configured as a tagged member of VLAN 100, and Port 7 is configured as an untagged member of VLAN 200. Hosts in the same VLAN communicate with each other as if they in a LAN. However, hosts in different VLANs cannot communicate with each other directly.



In this case:

1. The hosts from Group A can communicate with each other.
2. The hosts from Group B can communicate with each other.
3. The hosts of Group A and Group B can't communicate with each other.

Configuring 802.1Q Tagging from the Web UI

Go to **Configuration** > > **VLANS** > **Port VLAN** configuration table and specify the VLAN membership:

- a. Transmit unicast packets with VLAN tag 100 from Port 1 to Port 2 and Port 7.
The ISW should tag it with VID 100. The packet only has access to Port2. For Port 2, the outgoing packet leaves as a tagged packet with VID 100.
- b. Transmit unicast packets with VLAN tag 200 from Port 1 to Port 2 and Port 7.
The ISW should tag it with VID 200. The packet only has access to Port7. The outgoing packet on Port 7 is stripped of its tag as an untagged packet.
- c. Transmit unicast packets with VLAN tag 100 from Port 2 to Port 1 and Port 7.
The ISW should tag it with VID 100. The packet only has access to Port1. For Port 1, the outgoing packet leaves as a tagged packet with VID 100.
- d. Transmit unicast packets with VLAN tag 200 from Port 7 to Port 1 and Port 2.
The ISW should tag it with VID 200. The packet only has access to Port1. The outgoing packet on Port 1 will leave as a tagged packet with VID 200.
- e. Repeat the above steps using broadcast and multicast packets.

Global VLAN Configuration

Allowed Access VLANs	1,100
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Trunk	1	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	1,100,200	
2	Trunk	1	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	1,100	
3	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
7	Trunk	1	C-Port	<input checked="" type="checkbox"/>	Tagged Only	Tag All	1,200	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
9	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
10	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
11	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
12	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	

Configuring 802.1Q Tagging from the CLI

```
vlan 100
vlan 200
interface GigabitEthernet 1/1
switchport access vlan 100
switchport trunk allowed vlan 1,100,200
switchport trunk vlan tag native
switchport mode trunk
exit
interface GigabitEthernet 1/1
switchport access vlan 100
switchport trunk allowed vlan 1,100
switchport trunk vlan tag native
switchport mode trunk
exit
interface GigabitEthernet 1/7
switchport access vlan 100
switchport trunk allowed vlan 1,200
switchport trunk vlan tag native
switchport mode trunk
exit
```

Security Application Guide

ACL (Access Control List) function supports access control security for MAC address, IP address, Layer4 Port, and Type of Service. Each has five actions: Deny, Permit, Queue Mapping, CoS (Class of Service) Marking, and Copy Frame. You can set the default ACL rule to Permit or Deny.

To get more clearly for these ACL function, see following table.

Default ACL Rule	Actions				
	Permit	Queue Mapping	CoS Marking	Copy Frame	
Permit	(a)	(b)	(c)	(d)	(e)
Deny	(f)	(g)	(h)	(i)	(j)

Brief descriptions of the above table:

(a): Permit all frames, but deny frames set in ACL entry.

(b): Permit all frames.

(c): Permit all frames, and to do queue mapping of the transmitting frames.

(d): Permit all frames, and to change CoS value of the transmitting frames.

(e): Permit all frames, and to copy frame which set in ACL entry to a defined GE port.

(f): Deny all frames.

(g): Deny all frames, but permit frames set in ACL entry.

(h): Deny all frames.

(i): Deny all frames.

(j): Deny all frames, but to copy frame which set in ACL entry to a defined GE port.

Case 1: ACL for MAC Address

For MAC address ACL, it can filter on source MAC address, destination MAC address, or both. When it filters on both MAC address, packets coincident with both rules will take effect. In other words, it does not do filter if it only coincident with one rule.

If you want to filter only one directional MAC address, the other MAC address just set to all zero. It means “don’t care” portion. Besides MAC address, it also supports VLAN and Ether type for filter additionally. Certain VLAN or Ether type under these MAC address will take effect. If you don’t care VLAN or Ether type, you can just set to zero values.

Following are examples about the above table:

Case 1: (a)

You can set default ACL Rule of GE port as “Permit”, then to bind a suitable profile with “deny” action for ACL. It means GE port can pass through all packets but not ACL entry of the profile binding.

Case 1: (b)

This case acts as no ACL function. It means all frames will pass through.

Case 1: (c)

You can set default ACL Rule of GE port as “Permit”, then to bind a suitable profile with “Queue Mapping” action for some ACL function. It means GE port can do queue mapping 0-7 of the frame received from this port.

Case 1: (d)

You can set default ACL Rule of GE port as “Permit”, then to bind a suitable profile with “CoS Marking” action for some ACL function. It means GE port can remark CoS of the VLAN frame received from this port.

Case 1: (e)

You can set default ACL Rule of GE port as “Permit”, then to bind a suitable profile with “Copy Frame” action for mirror analyzer used. It means the system will copy frames from binding GE Port to analyzer port.

Case 1: (f)

This case means all frames will not pass through.

Case 1: (g)

You can set default ACL Rule of GE port as “Deny”, then to bind a suitable profile with “Permit” action for ACL. It means GE port can not pass through all packets but ACL entry of the profile binding.

Case 1: (h)

Because the default ACL Rule of GE port is “Deny”, Queue Mapping action has no sense. We do not do this case.

Case 1: (i)

Because the default ACL Rule of GE port is “Deny”, CoS Marking action has no sense. We do not do this case.

Case 1: (j)


You can set default ACL Rule of GE port as “Deny”, then to bind a suitable profile with “Copy Frame” action for mirror analyzer used. It means the system will copy frames from binding GE Port to analyzer port. There is no frame received from the denied GE port but the mirror analyzer port.

Configuring One-directional MAC Address with One VLAN Deny Filtering (Web UI)

1. Navigate to **Configuration > Security > Network > ACL > Access Control List**.

Access Control List Configuration

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

2. Click  to create a new ACL Profile (profile name: DenySomeMac).
3. Create a new ACL Entry rule under this ACL profile. (Deny MAC: 11 and VLAN: 4)
4. Bind this ACL profile to a GE port (PORT4).

5. Send frames between PORT3 and PORT4, and see test result.

ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Specific
Policy Value	1
Policy Bitmask	0x FF
Frame Type	Ethernet Type

Action	Deny
Rate Limiter	Disabled
Port Redirect	Disabled Port 1 Port 2 Port 3 Port 4
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

MAC Parameters

SMAC Filter	Specific
SMAC Value	00-00-00-00-00-11
DMAC Filter	Any

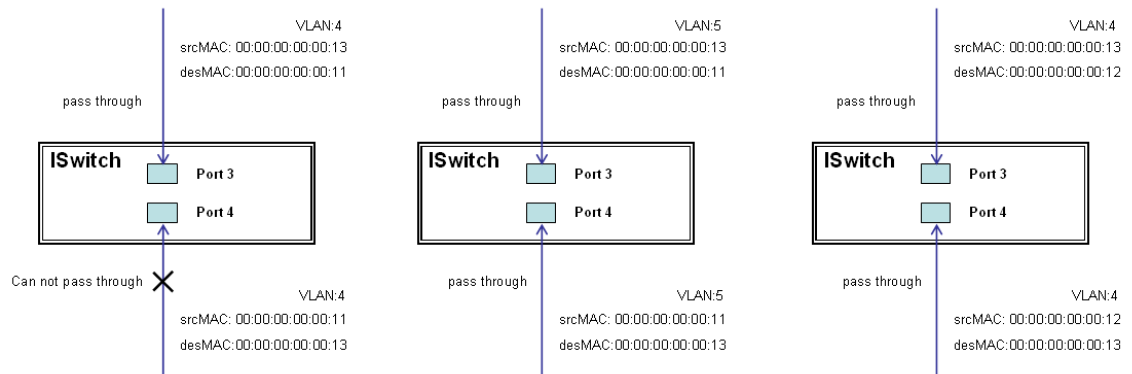
VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Specific
VLAN ID	4
Tag Priority	Any

Ethernet Type Parameters

EtherType Filter	Any
-------------------------	-----

Save Reset Cancel



Configuring One-directional MAC Address with One VLAN Deny Filtering (CLI Commands)

```
access-list ace 1 ingress interface GigabitEthernet 1/4 policy 1 vid 4 frametype etype
smac 00-00-00-00-00-11 action deny
exit
interface GigabitEthernet 1/3
switchport trunk allowed vlan 4,5
switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
switchport trunk allowed vlan 4,5
```


```
switchport trunk vlan tag nativevlan 4
exit
```

Configuring Two-directional MAC Address with all VLAN Deny Filtering (Web UI)

1. Navigate to **Configuration > Security > Network > ACL > Access Control List**.

Access Control List Configuration

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

2. Click the second  to create a new ACL Profile after the first one (profile name: DenySomeMac).

Access Control List Configuration

Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter
4	1 / 0xFF	EType	Deny	Disabled	Disabled	Disabled	0

3. Create a new ACL Entry rule under this ACL profile (Deny SrcMAC: 13 and DesMAC: 11).
4. Bind this ACL profile to a GE port (PORT3).
5. Send frames between PORT3 and PORT4, and see test result.

ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Specific
Policy Value	0
Policy Bitmask	0x ff
Frame Type	Ethernet Type

Action	Deny
Rate Limiter	Disabled
Port Redirect	Disabled Port 1 Port 2 Port 3 Port 4
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

MAC Parameters

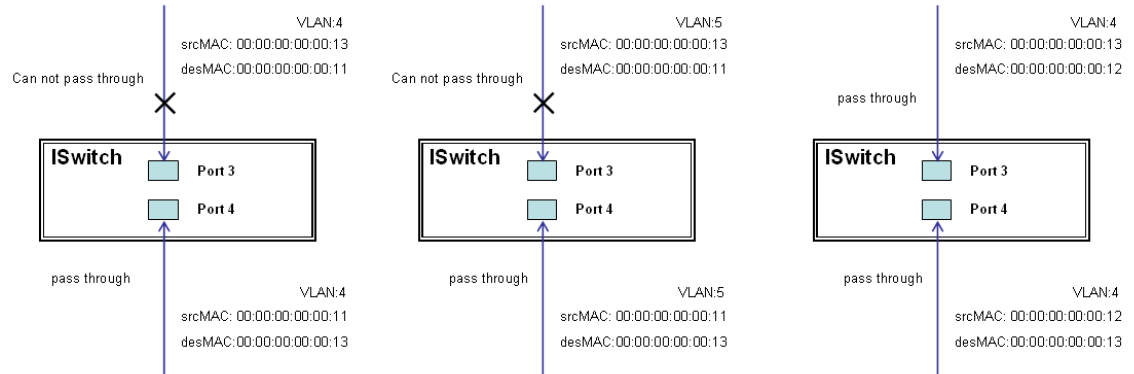
SMAC Filter	Specific
SMAC Value	00-00-00-00-00-13
DMAC Filter	Specific
DMAC Value	00-00-00-00-00-11

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Ethernet Type Parameters

EtherType Filter	Any
-------------------------	-----



Configuring Two-directional MAC Address with all VLAN Deny Filtering (CLI Commands)

```
access-list ace 2 ingress interface GigabitEthernet 1/3 policy 0 frametype etype smac
00-00-00-00-00-13 dmac 00-00-00-00-00-11 action deny
exit
interface GigabitEthernet 1/3
switchport trunk allowed vlan 4,5
switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
switchport trunk allowed vlan 4,5
switchport trunk vlan tag nativevlan 4
exit
```

Configuring One-directional MAC Address with CoS Marking Action (one VLAN, and don't care Ether Type) - Web UI

1. Navigate to **Configuration > Security > Network > ACL > Access Control List**.

Access Control List Configuration

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

2. Create a new ACL Profile (profile name: CoSMarkingTest).
3. Create a new ACL Entry rule under this ACL profile (Filter SrcMAC: 11 and VLAN ID: 4 frame to CoS: 2).

- Bind this ACL profile to a GE port (PORT4).

ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Specific
Policy Value	2
Policy Bitmask	0x ff
Frame Type	Ethernet Type

Action	Deny
Rate Limiter	Disabled
Port Redirect	Disabled Port 1 Port 2 Port 3 Port 4
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

MAC Parameters

SMAC Filter	Specific
SMAC Value	00-00-00-00-00-11
DMAC Filter	Any

VLAN Parameters

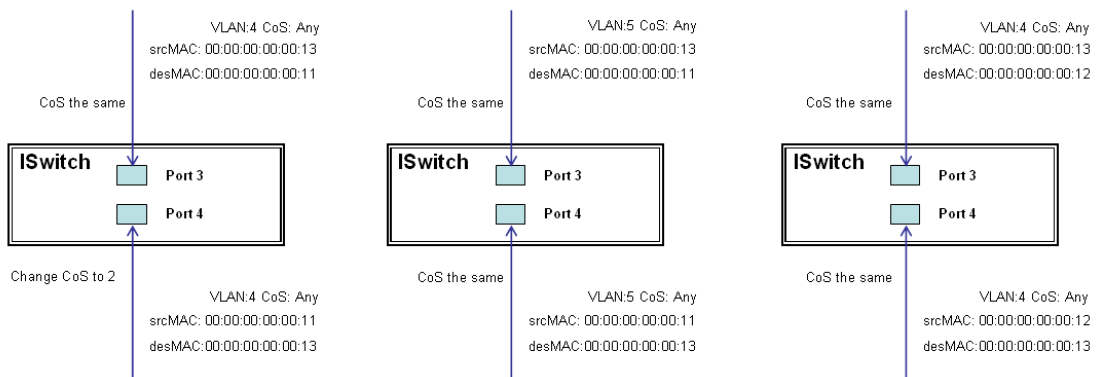
802.1Q Tagged	Enabled
VLAN ID Filter	Specific
VLAN ID	4
Tag Priority	2

Ethernet Type Parameters

EtherType Filter	Any
-------------------------	-----

Save Reset Cancel

- Send frames between PORT3 and PORT4, and see test result.



Configuring One-directional MAC Address with CoS Marking Action (one VLAN, and don't care Ether Type) - CLI Commands

```

access-list ace 1 next 2 ingress interface GigabitEthernet 1/4 policy 1 vid 4 frametype
etype smac 00-00-00-00-00-11 action deny
exit
interface GigabitEthernet 1/3
 switchport trunk allowed vlan 4,5
 switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
    
```



```
switchport trunk allowed vlan 4,5
switchport trunk vlan tag native
exit
```

Configuring Two-directional MAC Address with Copy Frame action (Don't care VLAN ID, Ether Type) – Web UI

1. Navigate to **Configuration > Security > Network > ACL > Access Control List**.

Access Control List Configuration

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

2. Create a new ACL Profile (profile name: CopyFrameTest).
3. Create a new ACL Entry rule under this ACL profile (SrcMAC: 13 and DesMAC: 11).
4. Set analyzer port to enable and mirror analyzer port.
5. Bind this ACL profile to a GE port (PORT3).

ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Specific
Policy Value	0
Policy Bitmask	0x FF
Frame Type	Ethernet Type

Action	Deny
Rate Limiter	Disabled
Port Redirect	Port 3 Port 4 Port 5 Port 6 Port 7
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

MAC Parameters

SMAC Filter	Specific
SMAC Value	00-00-00-00-00-13
DMAC Filter	Specific
DMAC Value	00-00-00-00-00-11

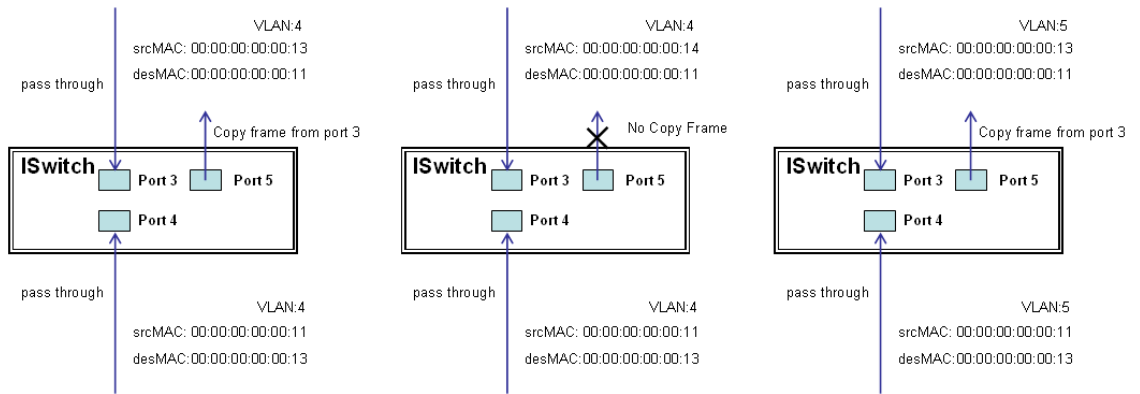
VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Ethernet Type Parameters

EtherType Filter	Any
-------------------------	-----

6. Send frames between PORT3 and PORT4, and see test result.



Configuring Two-directional MAC Address with Copy Frame action (Don't care VLAN ID, Ether Type) - CLI Commands

```
access-list ace 2 next 3 ingress interface GigabitEthernet 1/3 policy 0 frametype etype
smac 00-00-00-00-00-13 dmac 00-00-00-00-00-11 action deny mirror redirect interface
GigabitEthernet 1/5
exit
interface GigabitEthernet 1/3
switchport trunk allowed vlan 4,5
switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
switchport trunk allowed vlan 4,5
switchport trunk vlan tag native
exit
```

Configuring One-directional MAC Address with One VLAN Permit Filtering (Web UI)

1. Navigate to **Configuration > Security > Network > ACL > Access Control List**.

Access Control List Configuration

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

2. Create a new ACL Profile (profile name: AllowSomeMac).
3. Create a new ACL Entry rule under this ACL profile (allow MAC: 11 and VLAN: 4).
4. Bind this ACL profile to a GE port (PORT4.)

5. Send frames between PORT3 and PORT4, and see test result.

ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Specific
Policy Value	3
Policy Bitmask	0x ff
Frame Type	Ethernet Type

Action	Permit
Rate Limiter	Disabled
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

MAC Parameters

SMAC Filter	Specific
SMAC Value	00-00-00-00-00-01
DMAC Filter	Any

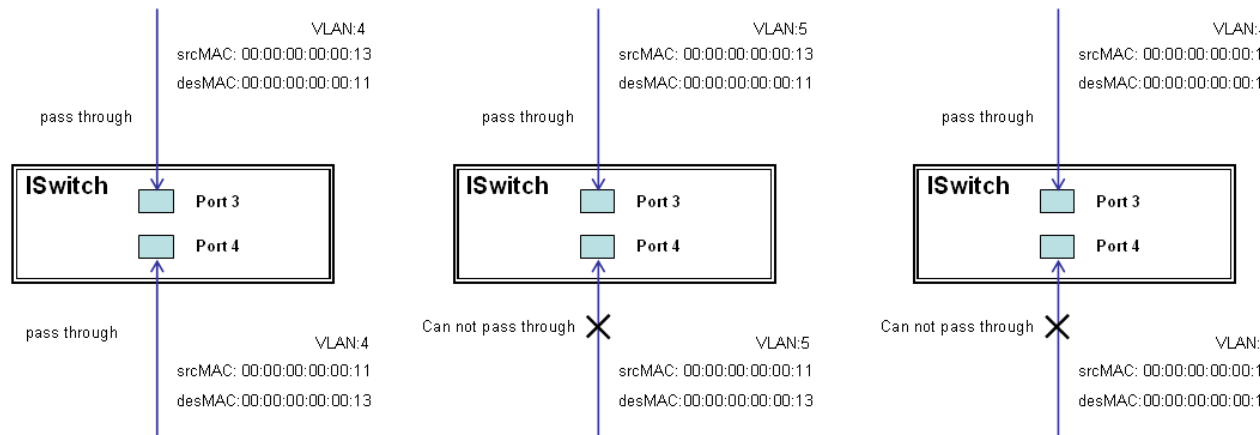
VLAN Parameters

802.1Q Tagged	Enabled
VLAN ID Filter	Specific
VLAN ID	4
Tag Priority	Any

Ethernet Type Parameters

EtherType Filter	Any
-------------------------	-----

Save Reset Cancel



Configuring One-directional MAC Address with One VLAN Permit Filtering (CLI Commands)

```
access-list ace 4 ingress interface GigabitEthernet 1/4 policy 3 tag tagged vid 4
frametype etype smac 00-00-00-00-00-11
exit
interface GigabitEthernet 1/3
switchport trunk allowed vlan 4,5
switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
switchport trunk allowed vlan 4,5
```

```
switchport trunk vlan tag native
exit
```

Configuring Two-directional MAC Address with All VLAN Permit Filtering (Web UI)

1. Navigate to **Configuration > Security > Network > ACL > Access Control List**.

Access Control List Configuration

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

2. Create a new ACL Profile (profile name: AllowSomeMac).
3. Create a new ACL Entry rule under this ACL profile (allow SrcMAC: 13 and DesMAC: 11).
4. Bind this ACL profile to a GE port (PORT3).

ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Specific
Policy Value	5
Policy Bitmask	0x ff
Frame Type	Ethernet Type

Action	Permit
Rate Limiter	Disabled
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

MAC Parameters

SMAC Filter	Specific
SMAC Value	00-00-00-00-00-13
DMAC Filter	Specific
DMAC Value	00-00-00-00-00-11

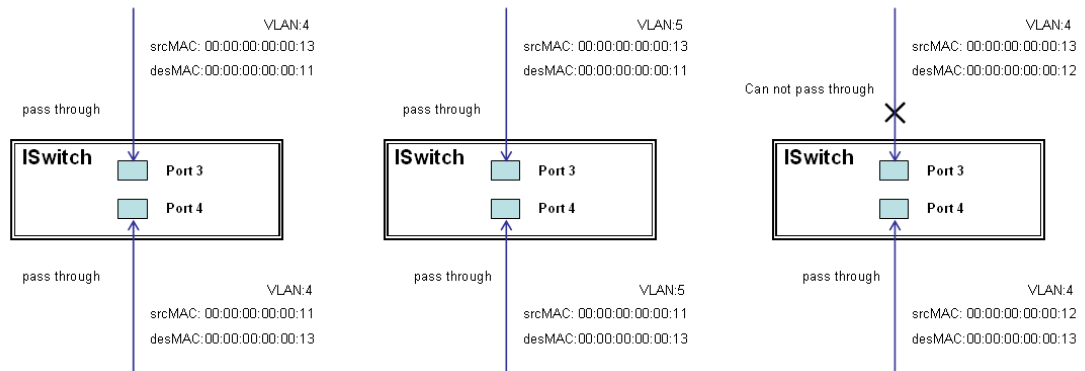
VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Ethernet Type Parameters

EtherType Filter	Any
-------------------------	-----

5. Send frames between PORT3 and PORT4 (see test result below).



Configuring Two-directional MAC Address with All VLAN Permit Filtering (CLI Commands)

```
access-list ace 5 ingress interface GigabitEthernet 1/3 policy 5 frametype etype smac
00-00-00-00-00-13 dmac 00-00-00-00-00-11
exit
interface GigabitEthernet 1/3
switchport trunk allowed vlan 4,5
switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
switchport trunk allowed vlan 4,5
switchport trunk vlan tag native
exit
```

Configuring One-directional MAC Address with Copy Frame Action (don't care VLAN, Ether Type) - Web UI

1. Navigate to **Configuration > Security > Network > ACL > Access Control List**.

Access Control List Configuration

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

2. Create a new ACL Profile (profile name: CopyFrameTest).

3. Create a new ACL Entry rule under this ACL profile (SrcMAC: 13 and DesMAC: 11).

ACE Configuration

Ingress Port	<ul style="list-style-type: none"> Port 1 Port 2 <li style="background-color: #007bff; color: white;">Port 3 Port 4 Port 5
Policy Filter	Specific
Policy Value	4
Policy Bitmask	0x ff
Frame Type	Ethernet Type

Action	Permit
Rate Limiter	Disabled
Mirror	Enabled
Logging	Disabled
Shutdown	Disabled
Counter	0

MAC Parameters

SMAC Filter	Specific
SMAC Value	00-00-00-00-00-13
DMAC Filter	Specific
DMAC Value	00-00-00-00-00-11

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Ethernet Type Parameters

EtherType Filter	Any
-------------------------	-----

4. Bind this ACL profile to a GE port (PORT3).
5. Save the entry.

6. From **Configuration > Mirroring**, set the analyzer port to enable and mirror analyzer port.

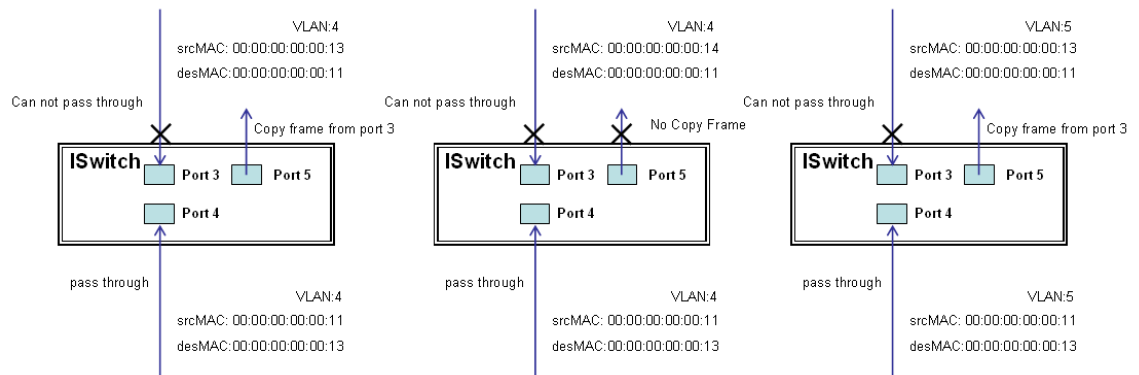
Mirror Configuration

Port to mirror to

Mirror Port Configuration

Port	Mode
*	<>
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
CPU	Enabled

7. Send frames between PORT3 and PORT4, see test result.



Configuring One-directional MAC Address with Copy Frame Action (don't care VLAN, Ether Type) - CLI Commands

```
access-list ace 5 next 6 ingress interface GigabitEthernet 1/3 policy 5 frametype etype
smac 00-00-00-00-00-13 dmac 00-00-00-00-00-11
Exit
```

```

monitor destination interface GigabitEthernet 1/5
monitor source cpu both
exit
interface GigabitEthernet 1/3
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
  switchport trunk allowed vlan 4,5
  switchport trunk vlan tag native
exit

```

Case 2: ACL for IP address

For IP address ACL, it can filter on source IP address, destination IP address, or both. It also supports to set IP range ACL. When it filters on both IP address, packets coincident with both rules will take effect. In other words, it does not do filter if it only coincident with one rule.

If you want to filter only one directional IP address, the other IP address just set to all zero. It means don't care portion. Besides IP address, it also supports Protocol for filter additionally. (TCP=6, UDP=17, etc.) Certain Protocol under these IP addresses will take effect. If you use doesn't care Protocol, you can just set to zero value. The detail testing (refer to MAC ACL above).

Case 3: ACL for L4 Port

For Layer4 port ACL, it can filter on (1) source IP address, (2) source L4 port, (3) destination IP address, (4) destination L4 port, and (5) UDP or TCP Protocol. You can select to filter on (1)-(4) for all or some specific values, but it should select exact one Protocol from UDP or TCP.

When it filters on both directional IP address and L4 port, packets coincident with both rules will take effect. In other words, it does not do filter if it only coincident with one rule.

If you want to filter only one directional IP address or L4 port, the other IP address and L4 port must be set to all zeroes. It means don't care portion. The detail testing (refer to MAC ACL above).

Case 4: ACL for ToS

For Type of Service (ToS) ACL, it can filter on (1) source IP address with ToS type, or (2) destination IP address with ToS type, or (3) both, or (4) both not (just filter ToS). When it filters on both IP address, packets coincident with both rules will take effect. In other words, it does not do filter if it only coincident with one rule.

If you want to filter only one directional IP address, the other IP address must be set to all zeroes. It means don't care portion. The detail testing, please refer to case 1 MAC ACL above.

Valid Values: Precedence: 0-7, ToS: 0-15, DSCP: 0-63

0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Precedence				Type of Service				DS field				ECN field			

Value 7 is reserved and set to 0.

Examples:

- Pre (001) means 1
- Pre (100) means 4
- ToS (00010) means 1
- ToS (10000) means 8
- DSCP (000001) means 1
- DSCP (100000) means 32

Ring Version 2 Application Guide

Having a reliable network is very important to Ethernet applications, especially in an Industrial domain. ISW-Series Managed Industrial Ethernet Switch provide fast failover ring protection, ensuring seamless network operation in the event of a link loss or a network device error. It can be applied by Ethernet cable and fiber.

Ring Version 2 Features

You can configure ISW switches for the following RingV2 topologies:

- [Single Ring Topology](#) on page 49
- [Coupling and Dual Homing Topologies](#) on page 50
- [Chain and Balancing Chain Topologies](#) on page 52
- [Dual Ring Topologies](#) on page 53

When setting up a RingV2 configuration, follow these guidelines:



Note

- Enable single ring before configuring coupling or dual homing.
- When single ring, coupling, or dual homing is enabled, any chain or balancing chain configuration is inactive.
- When chain or balancing chain is enabled, any configurations for single-ring, coupling, or dual homing are inactive.
- Dual ring topologies can be single ring, chain, or balancing chain.

Single Ring Topology

[Figure 12](#) shows a single ring topology with normal data flow, data flowing in two directions from the ring master when a link is broken, and the restoration of normal data flow after the link comes back online.

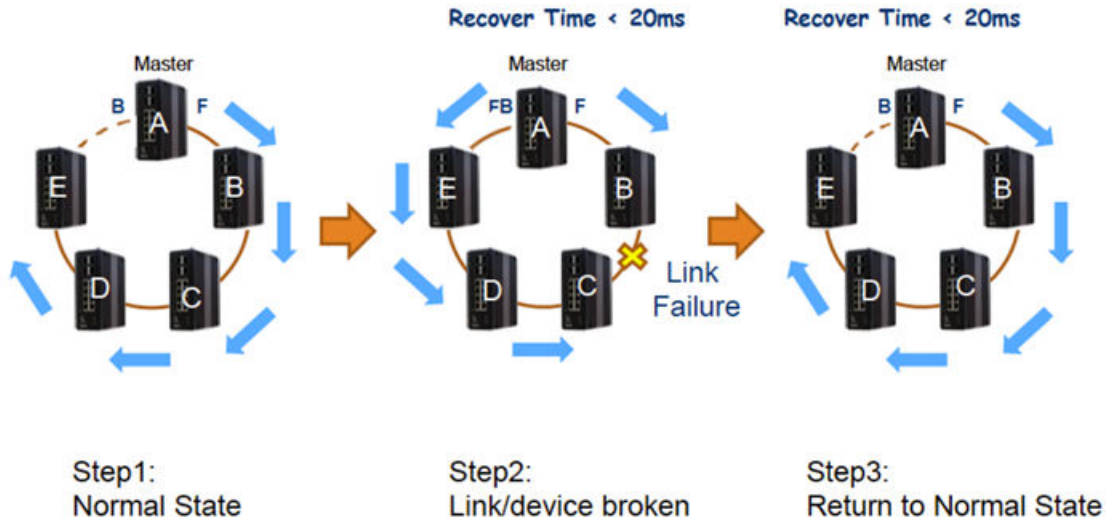


Figure 12: Single ring topology

The single ring topology supports **ring-master** and **ring-slave** options.

Ring - Each switch can be master or slave.

- When the switch’s role is ring master, one ring port is the forward port and another is the block port. The block port is a redundant port. In normal state, it is blocked.
- When the switch’s role is ring slave, both ring ports are forward ports.

Coupling and Dual Homing Topologies

Figure 13 shows a coupling topology, in which adjacent rings share two switches in common. A primary port is on one switch, and a backup port is on another switch.

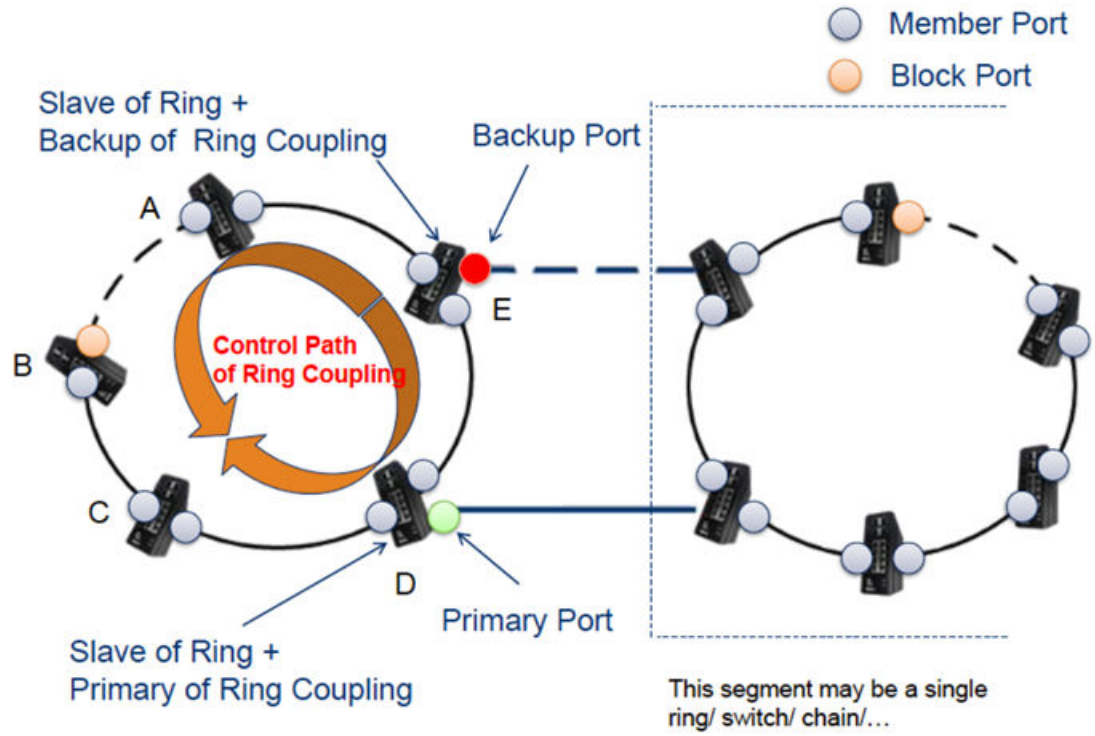


Figure 13: Coupling topology

Figure 14 shows a dual homing topology, in which adjacent rings share a single switch in common. Both primary port and backup port are on the shared switch.

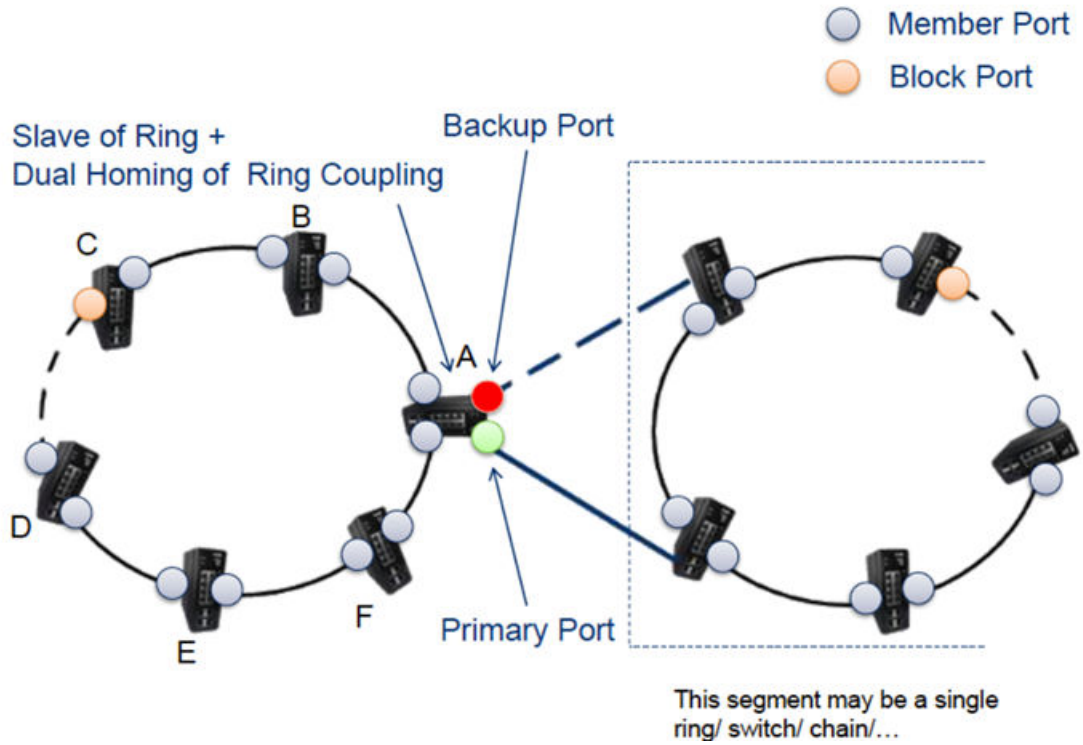


Figure 14: Dual homing topology

Ring - Each switch can be master or slave.

Coupling and dual homing - Each switch can be primary, backup, or both.

- When the switch's role is coupling/primary, only one ring port, the primary port, needs to be configured.
- When the switch's role is coupling/backup, only one ring port, the backup port, needs to be configured. The backup port is a redundant port. In normal state, it is blocked.
- When the switch's role is dual-homing, one ring port is the primary port and another is the backup port. The backup port is a redundant port. In normal state, it is blocked.

Chain and Balancing Chain Topologies

Chain Topology

Figure 15 shows a chain topology in which data flows through the head port to all switches in the chain. When a connection within the chain is broken, data flows through both the head and tail ports to reach all switches in the chain.

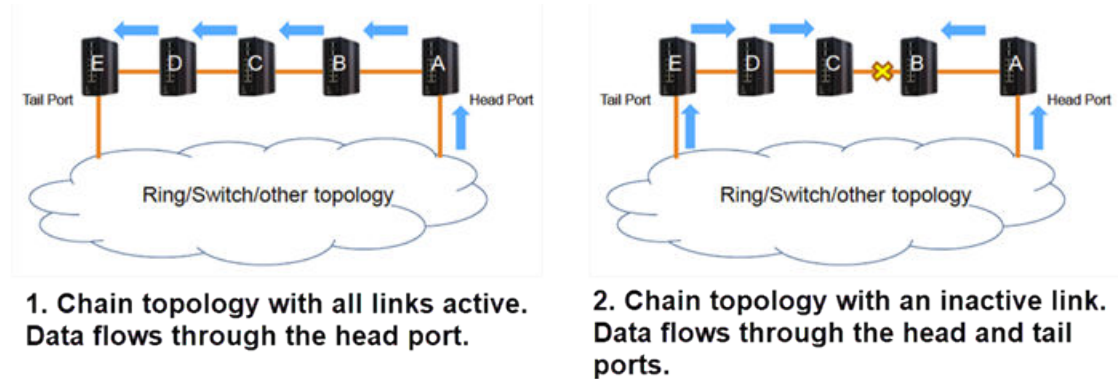


Figure 15: Chain topology

Chain - Each switch can be head, tail or member.

- When the role is chain/head, one ring port is the head port and another is the member port. In normal state, both ring ports are forwarded.
- When the role is chain/tail, one ring port is the tail port and another is the member port. The tail port is a redundant port. In normal state, the tail port is blocked.
- When the role is chain/member, both ring ports are member ports. In normal state, both ring ports are forwarded.

Balancing Chain Topology

Figure 16 shows a chain topology in which data flows through terminal ports at both ends to the central block in the chain. When a connection within the chain is broken, data flows along the chain to reach all switches in the chain.

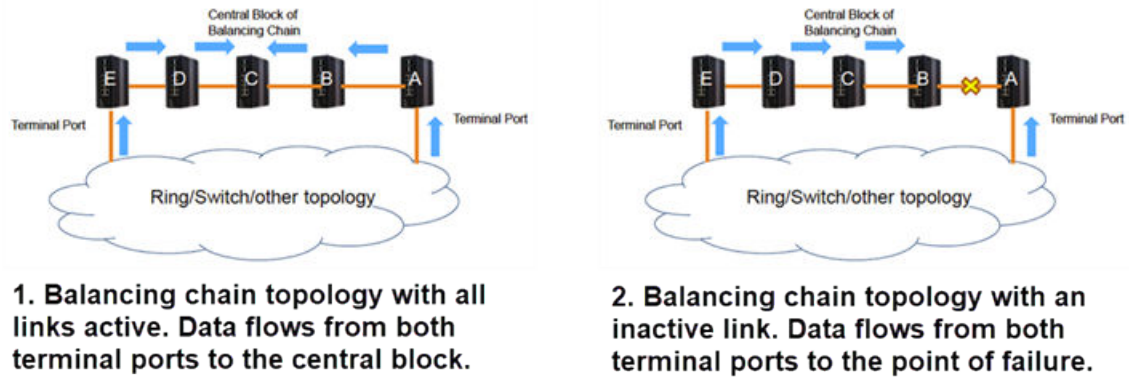


Figure 16: Balancing chain topology

Balancing Chain - Each switch can be central-block, terminal-1/2 or member.

- When the role is balancing-chain/central-block, one ring port is the member port and another is the block port. The block port is a redundant port. In normal state, the block port is blocked.
- When the role is balancing-chain/terminal-1/2, one ring port is the terminal port and another is the member port. In normal state, both ring ports are forwarded.
- When the role is balancing-chain/member, both ring ports are member ports. In normal state, both ring ports are forwarded.

Topology Change Notification (TCN)

When an ISW chain or balancing chain is restored after an interruption, the ISW switches at the end of the chain generate a TCN BPDU packet. The packet is processed by the VSP switches that are connected to the ISW chain, resulting in fast (less than 100ms) network redundancy recovery time.

This feature provides the following benefits:

- Fast recovery time.
- When the chain topology changes, the VSP switches will fast age MAC addresses learned on the VLANs extended into the ISW chains.
- VSP switches connected to the same chain no longer need to share a virtual interswitch trunk (vIST) to keep MAC addresses synchronized across both switches.

This feature is present in firmware version v01.01.03.0013 or later. No configuration steps are required to activate it on the ISW switches, and it works even though Spanning Tree Protocol (STP) has been disabled on the ISWs in order to activate the RingV2 chain..



Note

On the VSP switches, Spanning Tree must be enabled on the ports that connect to the ISW switches.

NEW! Dual Ring Topologies

In ISW, dual ring configurations support the following topologies. For each topology, a sample configuration is shown.

- Ring with LAG

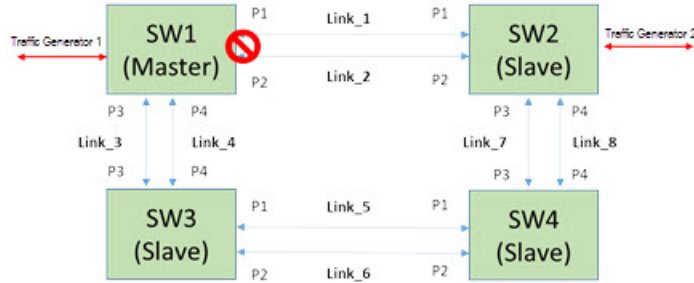


Figure 17: Ring with LAG

- Chain with LAG

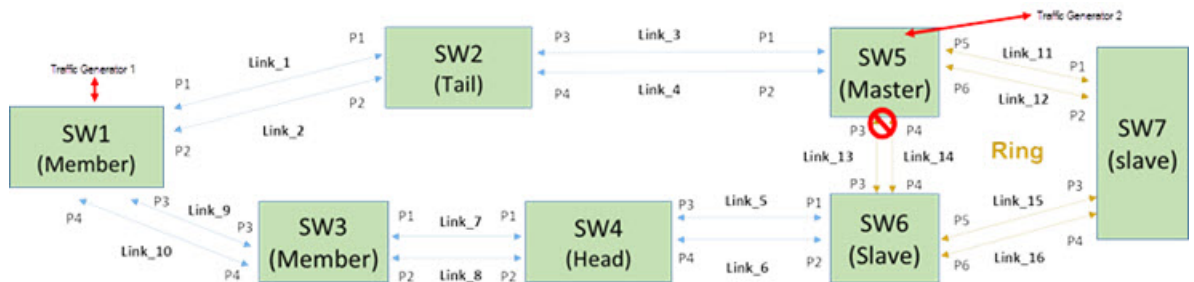


Figure 18: Chain with LAG

- Balancing chain with LAG

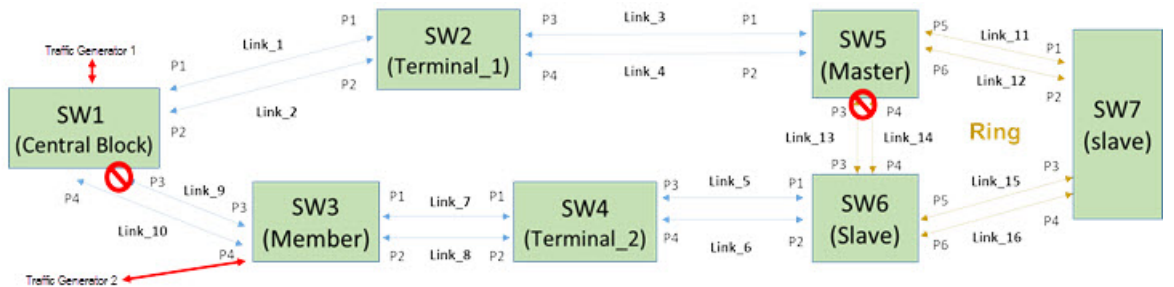


Figure 19: Balancing with LAG

Configuring RingV2 (Web UI)

In the current ISW-Series design, one device supports a three-ring index, including Ring & Chain (single ring, dual ring, coupling, dual-homing, chain, and balancing-chain.)

RingV2 Configuration

Ring Configuration

Index	Mode	Role	Ring Port(s)
1	Disable ▾	Ring(Slave) ▾	Forward Port : Port-1 ▾ Forward Port : Port-2 ▾
2	Disable ▾	Ring(Slave) ▾	Forward Port : Port-3 ▾ Forward Port : Port-4 ▾
3	Disable ▾	Chain(Member) ▾	Member Port : Port-1 ▾ Member Port : Port-2 ▾

When setting up a RingV2 configuration, follow these guidelines:



Note

- Enable single ring before configuring coupling or dual homing.
- When single ring, coupling, or dual homing is enabled, any chain or balancing chain configuration is inactive.
- When chain or balancing chain is enabled, any configurations for single-ring, coupling, or dual homing are inactive.
- Dual ring topologies can be single ring, chain, or balancing chain.

1. Disable RSTP on all ring ports by navigating to **Configuration > Spanning Tree > CIST ports**.
2. Clear **STP Enabled** on the desired ring ports.
3. Select **Save**.

STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
						Role	TCN		
-	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-point
						Role	TCN		
*	<input checked="" type="checkbox"/>	<>	<>	<>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
5	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
7	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
8	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
9	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
10	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
11	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
12	<input checked="" type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Save Reset

Configuring the Ring Master

1. Navigate to **Configuration > RingV2**.
2. Enable Index1, and select role as **Ring(Master)**.
3. Select one port as a Forward Port, and another as Block Port.

RingV2 Configuration

Ring Configuration

Index	Mode	Role	Ring Port(s)
1	Enable	Ring(Master)	Forward Port : Port-1 Block Port : Port-2
2	Disable	Ring(Slave)	Forward Port : Port-3 Forward Port : Port-4
3	Disable	Chain(Member)	Member Port : Port-1 Terminal Port : Port-2

Save Reset

Configuring the Ring Slave

1. Navigate to **Configuration > RingV2**.
2. Enable Index1, and select role as **Ring(Slave)**.
3. Select two ports as Forward Ports.

RingV2 Configuration

Ring Configuration			
Index	Mode	Role	Ring Port(s)
1	Enable	Ring(Slave)	Forward Port : Port-1 Forward Port : Port-2
2	Disable	Ring(Slave)	Forward Port : Port-3 Forward Port : Port-4
3	Disable	Chain(Member)	Member Port : Port-1 Terminal Port : Port-2

Save Reset

NEW! Web Configuration for Dual Ring

In the following example, LAGs can be configured as ring ports.

RingV2 Configuration

Ring Configuration			
Index	Mode	Role	Ring Port(s)
1	Enable	Ring(Master)	Forward Port : Aggr-1 Block Port : Aggr-2
2	Enable	Ring(Slave)	Forward Port : Aggr-3 Forward Port : Aggr-4
3	Disable	Chain(Member)	Member Port : Port-1 Member Port : Port-2

Configuring the Coupling Primary

1. Navigate to **Configuration > RingV2**.
2. Enable Index1, and select role as **Ring(Slave)**.
3. Select two ports as Forward Ports.
4. Enable Index2, and select role as **Coupling(Primary)**.
5. Select one port as a Primary Port.

RingV2 Configuration

Ring Configuration

Index	Mode	Role	Ring Port(s)
1	Enable ▾	Ring(Slave) ▾	Forward Port : Port-1 ▾ Forward Port : Port-2 ▾
2	Enable ▾	Coupling(Primary) ▾	Primary Port : Port-3 ▾
3	Disable ▾	Chain(Member) ▾	Member Port : Port-1 ▾ Terminal Port : Port-2 ▾

Save
Reset

Configuring the Coupling Backup

1. Navigate to **Configuration > RingV2**.
2. Enable Index1, and select role as **Ring(Slave)**.
3. Select two ports as Forward Ports.
4. Enable Index2, and select role as **Coupling(Backup)**.
5. Select one port as a Backup Port.

RingV2 Configuration

Ring Configuration

Index	Mode	Role	Ring Port(s)
1	Enable ▾	Ring(Slave) ▾	Forward Port : Port-1 ▾ Forward Port : Port-2 ▾
2	Enable ▾	Coupling(Backup) ▾	Backup Port : Port-3 ▾
3	Disable ▾	Chain(Member) ▾	Member Port : Port-1 ▾ Terminal Port : Port-2 ▾

Save
Reset

Configuring Dual-Homing

1. Navigate to **Configuration > RingV2**.
2. Enable Index1, and select role as **Ring(Slave)**.
3. Select two ports as Forward Ports.
4. Enable Index2, and select role as **Dual Homing**.

5. Select one port as a Primary Port, and the other as Backup Port.

RingV2 Configuration

Ring Configuration			
Index	Mode	Role	Ring Port(s)
1	Enable ▾	Ring(Master) ▾	Forward Port : Port-3 ▾ Block Port : Port-4 ▾
2	Enable ▾	Dual Homing ▾	Primary Port : Port-5 ▾ Backup Port : Port-6 ▾
3	Disable ▾	Chain(Member) ▾	Member Port : Port-1 ▾ Block Port : Port-2 ▾

Configuring Chain Member

1. Navigate to **Configuration > RingV2**.
2. Disable Index1 and Index2, and then enable Index3.
3. Select role as **Chain(Member)**.
4. Select two member ports for this chain member switch.

RingV2 Configuration

Ring Configuration			
Index	Mode	Role	Ring Port(s)
1	Disable ▾	Ring(Slave) ▾	Forward Port : Port-1 ▾ Block Port : Port-2 ▾
2	Disable ▾	Ring(Slave) ▾	Forward Port : Port-3 ▾ Forward Port : Port-4 ▾
3	Enable ▾	Chain(Member) ▾	Member Port : Port-1 ▾ Member Port : Port-2 ▾

Save Reset

Configuring Chain Head

1. Navigate to **Configuration > RingV2**.
2. Disable Index1 and Index2, and then enable Index3.
3. Select role as **Chain(Head)**.
4. Select a member port and a head port for this chain head switch.

RingV2 Configuration

Ring Configuration

Index	Mode	Role	Ring Port(s)
1	Disable ▾	Ring(Slave) ▾	Forward Port : Port-1 ▾ Block Port : Port-2 ▾
2	Disable ▾	Ring(Slave) ▾	Forward Port : Port-3 ▾ Forward Port : Port-4 ▾
3	Enable ▾	Chain(Head) ▾	Member Port : Port-1 ▾ Head Port : Port-2 ▾

Save
Reset

Configuring Chain Tail

1. Navigate to **Configuration > RingV2**.
2. Disable Index1 and Index2, and then enable Index3.
3. Select role as **Chain(Tail)**.
4. Select a member port and a tail port for this chain tail switch.

RingV2 Configuration

Ring Configuration

Index	Mode	Role	Ring Port(s)
1	Disable ▾	Ring(Slave) ▾	Forward Port : Port-1 ▾ Block Port : Port-2 ▾
2	Disable ▾	Ring(Slave) ▾	Forward Port : Port-3 ▾ Forward Port : Port-4 ▾
3	Enable ▾	Chain(Tail) ▾	Member Port : Port-1 ▾ Tail Port : Port-2 ▾

Configuring Balancing Chain – Central Block

1. Navigate to **Configuration > RingV2**.
2. Disable Index1 and Index2, and then enable Index3.
3. Select role as **Balancing Chain(Central Block)**.
4. Select a member port and a block port for this central block switch.

RingV2 Configuration

Ring Configuration

Index	Mode	Role	Ring Port(s)
1	Disable ▾	Ring(Slave) ▾	Forward Port : Port-1 ▾ Block Port : Port-2 ▾
2	Disable ▾	Ring(Slave) ▾	Forward Port : Port-3 ▾ Forward Port : Port-4 ▾
3	Enable ▾	Balancing Chain(Central Block) ▾	Member Port : Port-1 ▾ Block Port : Port-2 ▾

Configuring Balancing Chain (Terminal-1 or -2)

1. Navigate to **Configuration > RingV2**.

2. Disable Index1 and Index2, and then enable Index3.
3. Select role as **Balancing Chain(Terminal-1 or -2)**.
4. Select a member port and a terminal port for this balancing chain terminal switch.

RingV2 Configuration

Ring Configuration

Index	Mode	Role	Ring Port(s)
1	Disable ▾	Ring(Slave) ▾	Forward Port : Port-1 ▾ Block Port : Port-2 ▾
2	Disable ▾	Ring(Slave) ▾	Forward Port : Port-3 ▾ Forward Port : Port-4 ▾
3	Enable ▾	Balancing Chain(Terminal-1) ▾	Member Port : Port-1 ▾ Terminal Port : Port-2 ▾

Save
Reset

- Chain(Member)
- Chain(Head)
- Chain(Tail)
- Balancing Chain(Central Block)
- Balancing Chain(Terminal-1)
- Balancing Chain(Terminal-2)
- Balancing Chain(Member)

Configuring RingV2 (Console)

To configure the ring protection using the ISW-Series management switch:

1. Log in to the console with the admin account.
2. Go to Configure mode by executing: **configure terminal**
3. Go to configure ring protection group by executing: **ringv2 protect group1**
4. Before configuring the ring, you must disable ring protection status by executing: **mode disable**
5. Set all necessary parameters:

For Node 1 and Node 2, choose the ports that you connect with other switch. For example, choose PORT-1 and PORT-2 that means PORT-1 is one of the ports connected with other switch, so is PORT-2. Then choose one of ring connection devices be "Master" that can accept the "Node 2 port" and be the blocking port.

```
node1 interface GigabitEthernet 1/1
node2 interface GigabitEthernet 1/2
role ring-master
```

6. To finish, enable ring protection status by executing command: **mode enable**



Important

Note the status of Previous Command Result after every action.

```
configure terminal
ring protect group1
mode disable
node1 interface GigabitEthernet 1/1
node2 interface GigabitEthernet 1/2
role ring-master
mode enable
exit
```

In the following example of a dual-ring topology, the support LAG ports are configured for ring node1 and node2.

```
(config-ringv2-group1)#
(config-ringv2-group1)#node1 aggregation group <LAG group ID>
(config-ringv2-group1)#node2 aggregation group <LAG group ID>
```

NEW! RingV2 with ERPS

Although RingV2 cannot be used concurrently with Ethernet Ring Protection Switching (ERPS), you might need to configure ERPS if your ISW ring will interact with rings on other platforms. ExtremeXOS (EXOS) switches can run with ERPS, for example, and so can some switches from other manufacturers.

When configuring a RingV2 ISW switch to interact with an EXOS switch running ERPS, keep the following principles in mind:

- The key to connecting RingV2 rings with ERPS rings is ensuring that configuration parameters align in both systems.
- ISW default values for some timings (associated with recovery of the ring) do not match EXOS defaults.
- Some ISW variables have a different accepted variable length than the equivalent variables in EXOS.
- Carefully test your configuration, using logs and other troubleshooting tools to understand ways in which the settings interact with each other.

For details about configuring ERPS on an ISW switch, see:

- "ERPS" in *ISW Series Managed Industrial Ethernet Switch Web Configuration Guide*
- "Configuring ERPS from the CLI" in *ISW Series Managed Industrial Ethernet Switch Command Reference Guide*

QoS Application Guide

QoS (Quality of Service) features allow you to allocate network resources to mission-critical applications at the expense of applications that are less sensitive to such factors as time delays or network congestion. You can configure your network to prioritize specific types of traffic, ensuring that each type receives the appropriate QoS level.

SP/SPWRR

The KGS can be configured to have 8 output CoS queues (Q0-Q7) per port, into which each packet is placed. Q0 is the highest priority Queue. Each packet's 802.1p priority determines its CoS queue. You

need to bind VLAN priority/queue mapping profile to each port, for every VLAN priority need assign a traffic descriptor for it. The traffic descriptor defines the shape parameter on every VLAN priority for Ethernet interface. Currently KGS supports Strict Priority and SP+WRR (Weighted Round Robin) scheduling methods on each port. Please find the detail reference on ISW user manual.

Default Priority and Queue mapping is as follows:

Priority0	Priority1	Priority2	Priority3	Priority4	Priority5	Priority6	Priority7
Queue0	Queue1	Queue2	Queue3	Queue4	Queue5	Queue6	Queue7
SPQ	SPQ	SPQ	SPQ	SPQ	SPQ	SPQ	SPQ

Application Examples

Following we provide several examples for various QoS combinations and you can configure QoS using the web-based management system, CLI or SNMP (*Simple Network Management Protocol*).

Example 1: SPQ without Shaping (Default profile)

We send 2 Streams (Stream0, Stream1) from PORT-1 to PORT-2. Both 2 Streams each have 100Mbps. Stream0 includes VLAN Priority0, Stream1 includes VLAN Priority7. Set PORT-2 link speed to 100Mbps.

Expected Result

We expect PORT-2 only can receive 100Mbps of Stream1, and Stream0 will be discarded. This case will help you to understand how SPQ works on the ISW.

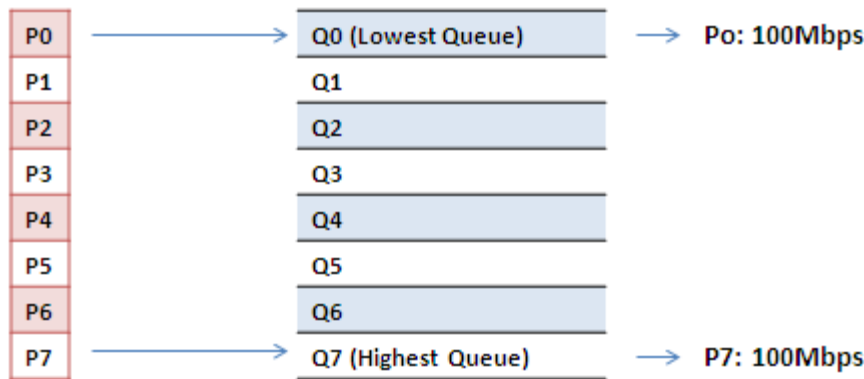
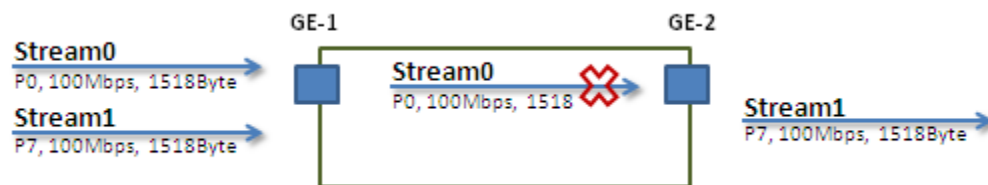


Figure 20: Gigabit port VLAN Priority & Queue Mapping



Stream0:

- Dst Mac : 00:00:00:00:20:01
- Src Mac : 00:00:00:00:10:01
- Vlan : 100
- Vlan prio : 0
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream1:

- Dst Mac : 00:00:00:00:20:02
- Src Mac : 00:00:00:00:10:02
- Vlan : 100
- Vlan prio : 7
- Send rate : 100Mbps
- Packet length: 1518bytes

Web Management

1. Navigate to **Configuration > Ports**.
2. Set port 2 link speed to **100Mbps full duplex**.

Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode
		Current	Configured	Current Rx	Current Tx	Configured		
*			<>			<input type="checkbox"/>	9600	<>
1	● Down	Auto	Auto	✗	✗	<input type="checkbox"/>	9600	Discard
2	● 100fdx	10Mbps FDX	10Mbps FDX	✗	✗	<input type="checkbox"/>	9600	Discard
3	● Down	Auto	Auto	✗	✗	<input type="checkbox"/>	9600	Discard
4	● Down	Auto	Auto	✗	✗	<input type="checkbox"/>	9600	Discard
5	● Down	Auto	Auto	✗	✗	<input type="checkbox"/>	9600	Discard
6	● Down	Auto	Auto	✗	✗	<input type="checkbox"/>	9600	Discard
7	● Down	Auto	Auto	✗	✗	<input type="checkbox"/>	9600	Discard
8	● Down	Auto	Auto	✗	✗	<input type="checkbox"/>	9600	Discard
9	● Down	Auto	Auto	✗	✗	<input type="checkbox"/>	9600	
10	● Down	Auto	Auto	✗	✗	<input type="checkbox"/>	9600	
11	● Down	Auto	Auto	✗	✗	<input type="checkbox"/>	9600	
12	● Down	Auto	Auto	✗	✗	<input type="checkbox"/>	9600	

Save

Reset

3. Select **Configuration > VLANs** and create a VLAN with VLAN ID 100.
4. Enter a VLAN name in the **Name** field. In this example, we set tagged VLAN100 on PORT1 and PORT2.

CLI Configuration

```
interface GigabitEthernet 1/1
switchport trunk native vlan 100
switchport trunk allowed vlan 1,100
switchport trunk vlan tag native
switchport mode trunk
!
```

```
interface GigabitEthernet 1/2
  switchport trunk native vlan 100
  switchport trunk allowed vlan 1,100
  switchport trunk vlan tag native
  switchport mode trunk
```

Example 2: SPQ with Shaping

We send two Streams (Stream0, Stream1) from port1 to port-2. Both streams each have 100 Mbps. Stream0 includes VLAN Priority0, Stream1 includes VLAN Priority7. Stream3 and Stream4 only for learning which make sure the traffic are not flooding.

Expected Result

We expect PORT-2 only can receive 20Mbps of Stream1, and 80Mbps of Stream0. This case will help you to understand how SPQ works on the ISW.

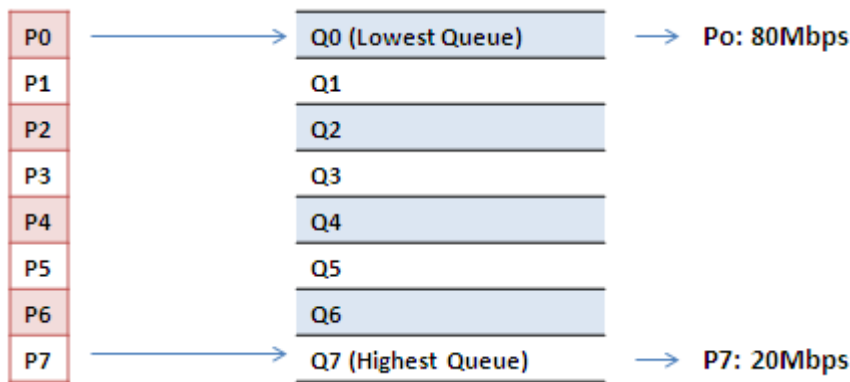


Figure 21: VDSL port VLAN Priority & Queue Mapping



Stream0:

- Dst Mac : 00:00:00:00:20:01
- Src Mac : 00:00:00:00:10:01
- Vlan : 100
- Vlan prio : 0
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream1:

- Dst Mac : 00:00:00:00:20:02
- Src Mac : 00:00:00:00:10:02

- Vlan : 100
- Vlan prio : 7
- Send rate : 100Mbps
- Packet length: 1518bytes

Stream3: (for Learning)

- Dst Mac : 00:00:00:00:10:01
- Src Mac : 00:00:00:00:20:01
- Vlan : 100
- Vlan prio : 0
- Send rate : 10Mbps
- Packet length: 1518bytes

Stream4: (for Learning)

- Dst Mac : 00:00:00:00:10:02
- Src Mac : 00:00:00:00:20:02
- Vlan : 100
- Vlan prio : 0
- Send rate : 10Mbps
- Packet length: 1518bytes

Web Management

1. Navigate to **Configuration > QoS > Port Shaping** and create a QoS profile on Port 2.

QoS Egress Port Shapers

Port	Shapers								Port	
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7		
<u>1</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
<u>2</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
<u>3</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
<u>4</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
<u>5</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
<u>6</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
<u>7</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
<u>8</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
<u>9</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
<u>10</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
<u>11</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
<u>12</u>	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

2. Select schedule mode **Strict Priority** and set shaping rate for queue 0 and queue 7 as below.

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode Strict Priority ▾

Queue Shaper				Port Shaper		
Enable	Rate	Unit	Excess	Enable	Rate	Unit
<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	<input type="checkbox"/>	500	kbps ▾
<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	<input type="checkbox"/>		

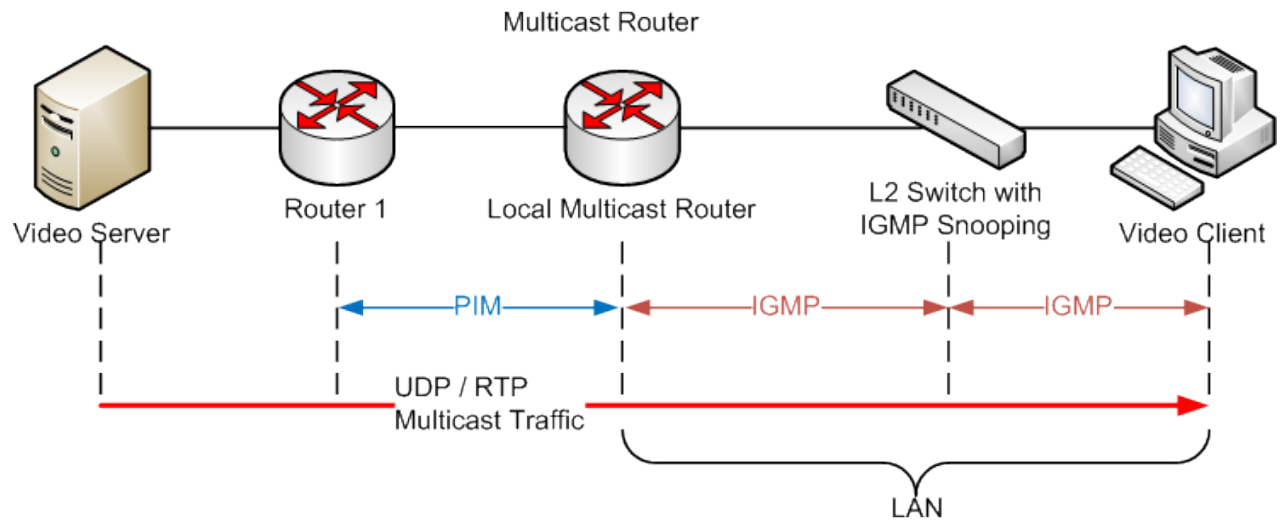
The diagram illustrates the QoS configuration for an egress port. On the left, eight queue shapers (Q0 through Q7) are shown, each with a rate of 500 kbps and an excess shaper checkbox. Arrows from each queue shaper point to a central vertical oval labeled "STRICT", representing the scheduler. An arrow from the "STRICT" scheduler points to a port shaper on the right, which is also configured with a rate of 500 kbps and an excess shaper checkbox.

Save Reset Cancel

CLI Configuration

```
interface GigabitEthernet 1/2
switchport trunk native vlan 100
switchport trunk allowed vlan 1,100
switchport trunk vlan tag native
switchport mode trunk
qos queue-shaper queue 0 80000
qos queue-shaper queue 7 20000
```

IGMP Application Guide



IGMP (Internet Group Management Protocol) 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 (Internet Control Message Protocol)* for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

Example 1

If every client should get multicast stream, navigate to **Configuration > IPMC > Basic Configuration** to select the **Snooping Enabled** check box.

IGMP Snooping Configuration

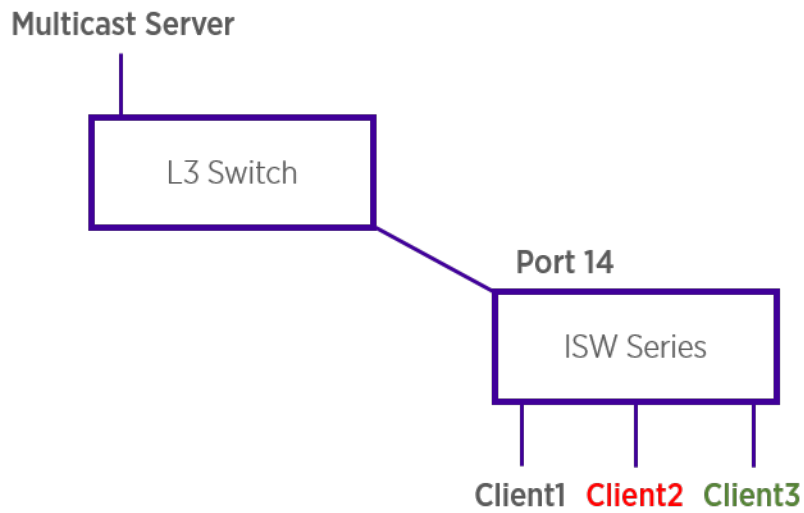
Global Configuration	
Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input checked="" type="checkbox"/>
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	<input type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<> ▾
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
11	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾
12	<input type="checkbox"/>	<input type="checkbox"/>	unlimited ▾

Save Reset

Example 2



1. Navigate to **Configuration > IPMC > Basic Configuration**,
2. Select the **Snooping Enabled** check box.
3. Clear the **Unregistered IPMCv4 Flooding Enabled** check box.
4. If Multicast stream is from L3 switch, then the uplink port must be "Router Port."

**Note**

If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.

IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	<input checked="" type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input type="checkbox"/>
IGMP SSM Range	232.0.0.0 / 8
Leave Proxy Enabled	<input type="checkbox"/>
Proxy Enabled	<input type="checkbox"/>

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
2	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
3	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
4	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
5	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
6	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
7	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
8	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
9	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
10	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
11	<input type="checkbox"/>	<input type="checkbox"/>	unlimited
12	<input checked="" type="checkbox"/>	<input type="checkbox"/>	unlimited

- Go to **Configuration > IPMC > VLAN Configuration**.
- Select the **Snooping Enabled** check box.

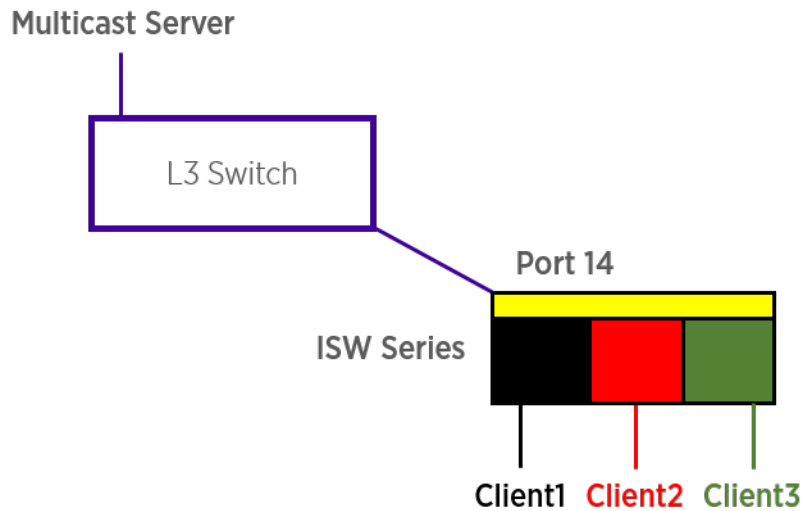
IGMP Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
Delete	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.0.1	IGMP-Auto	0	2	125	100	10	1

- Set VLAN ID of port14.

Example 3



In this scenario, these clients belong to multiple VLANs, so you have to create more one VLAN to be the agent for all client VLANs.

1. To create a VLAN, navigate to **Configuration > VLANs > Allow Access VLANs**.
2. Set port 14 be vlan200 member port.

Global VLAN Configuration

Allowed Access VLANs	1,223
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging	Allowed VLANs	Forbidden VLANs
*	<>	1	<>	<input checked="" type="checkbox"/>	<>	<>	1	
1	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
2	Hybrid	223	Unaware	<input type="checkbox"/>	Untagged Only	Untag All	223	
3	Access	223	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	223	
4	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
7	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
8	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
9	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
10	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
11	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	
12	Access	1	C-Port	<input checked="" type="checkbox"/>	Tagged and Untagged	Untag Port VLAN	1	

Save Reset

3. Navigate to **Configuration > IPMC > VLAN Configuration**.
4. Select the Snooping Enable check box.
5. Set VLAN ID of port14.
6. If there is no querier on the L3 switch, you have to select **Querier Election**, and set the **Querier Address**. The IP address is in the same network as uplink interface.

IGMP Snooping VLAN Configuration

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	RV	QI (sec)	QRI (0.1 sec)	LLQI (0.1 sec)	URI (sec)
Delete	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.0.1	IGMP-Auto	0	2	125	100	10	1

Add New IGMP VLAN

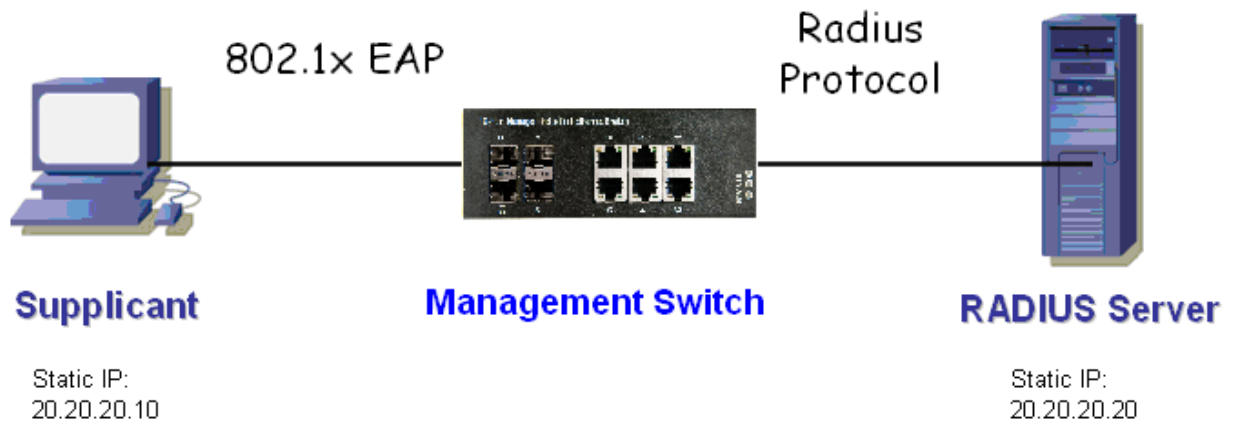
Save Reset

7. Select the *IGMP* version as **server**.

802.1x Authentication Application Guide

IEEE 802.1x derives keys which can be used to provide per-packet authentication, integrity and confidentiality. Typically use along with well-known key derivation algorithms (e.g., TLS, SRP, *MD5 (Message-Digest algorithm 5)*-Challenge, etc.). The ISW-Series supports 802.1x authentication function per port (port1-port10). You should enable 802.1x function of the system, and choose ports and type you want to apply. If you enable 802.1x authentication control for an Ethernet port, it should be authenticated before using any service from the network.

802.1x Configuration Overview



Configuring RADIUS Server

1. Prepare a Linux PC with *RADIUS (Remote Authentication Dial In User Service)* server installed.
2. Edit secret key for RADIUS server using the following settings

```
client 20.20.20.0/24 {
.....secret = a1b2c3d4
}
```



Note

The secret in the ISW should be the same as this one.

3. Edit user name and password for supplicant to authenticate with server with the following settings:

```
test123.....Cleartext-Password := "test123"
aaaa.....Cleartext-Password := "aaaa"
```

- Set a static IP address for this RADIUS Server:

Setting: 20.20.20.20

- Start the RADIUS server.

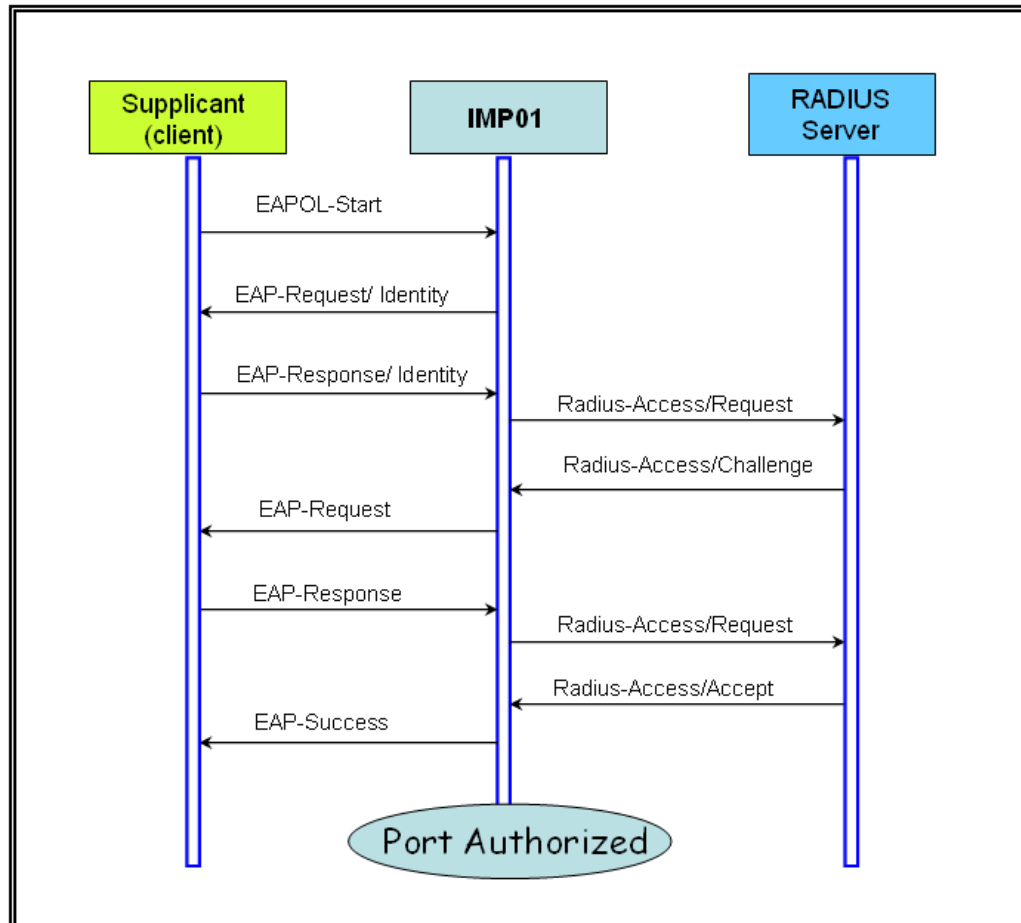
Supplicant's NIC Setting

After setting this function in NIC, supplicant should enter a correct pair of account and password in order to use this Ethernet port service from the ISW.

- Configure a static IP address 20.20.20.10 and net mask 255.255.255.0 for supplicant.
(If there is a DHCP (Dynamic Host Configuration Protocol) server to assign IP address for supplicant, this step can be ignored.)
- Select the **IEEE802.1x Authentication Enable** check box, and then set EAP type to MD5-Challenge.

Authentication Behavior

Supplicant should pass authentication process in order to use any service. After supplicant enters correct account and password which stored in RADIUS server, it can be authenticated successfully. The authentication process is as following.



Example Configuration

Below is an example 802.1x Authentication via ISW to be authenticated by RADIUS server. In this basic example, we take port 1 as a testing port, which enables 802.1x in ISW.

With default configuration, use the following web UI settings:

1. Navigate to **Configuration > Security > Network > NAS**.
2. Select **Enabled** mode to enable authentication.
3. Set port1 and port2 as **Port-based 802.1x**.

Network Access Server Configuration

System Configuration

Mode	Enabled
Reauthentication Enabled	<input type="checkbox"/>
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	<input type="checkbox"/>
RADIUS-Assigned VLAN Enabled	<input type="checkbox"/>
Guest VLAN Enabled	<input type="checkbox"/>
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	<input type="checkbox"/>

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
*	<>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
1	Port-based 802.1X	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
2	Port-based 802.1X	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
4	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
5	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
6	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
7	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
8	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
9	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
10	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
11	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize
12	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Globally Disabled	Reauthenticate Reinitialize

Save Reset

4. Navigate to **Configuration > Security > AAA > RADIUS**.

5. Click **Add New Server** and enter 20.20.20.20 as the server and a1b2c3d4 as the secret key.

RADIUS Server Configuration

Global Configuration

Timeout	5	seconds
Retransmit	3	times
Deadtime	0	minutes
Key		
NAS-IP-Address		
NAS-IPv6-Address		
NAS-Identifier		

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
Delete	20.20.20.20	1812	1813			a1b2c3d4

Add New Server

Save

Reset

6. Click **Save**.

CLI Command Configuration Example

```
configure ter
interface vlan 1
ip address 20.20.20.120 255.0.0.0
exit
exit
radius-server host 20.20.20.20 timeout 5 retransmit 3 key a1b2c3d4
dot1x re-authentication
dot1x system-auth-control
interface GigabitEthernet 1/1
dot1x port-control auto
```

802.1x Timer Parameters

Item	Parameter (sec)	Description
1	ReAuth Period	ISW will restart authentication after each Reauth-Period when authentication success and ReAuth option is enabled
2	Quiet Period	ISW will wait QuietPeriod to restart authentication process again when authentication failed in previous time.
3	Tx Period	ISW will send EAP-request to Supplicant every TxPeriod when authentication is running and Quiet Period is not running.
4	Supplicant Timeout	ISW will wait SupplicantTimeout to receive response from Supplicant.
5	Server Timeout	ISW will wait ServerTimeout to receive response from <i>RADIUS</i> server.

Enable 802.1x and MAC Authentication on the Same Port

In firmware version 1.01.04 and later, you can configure ISW switch ports to dynamically perform either 802.1x or MAC authentication.

When a connection is established and the configured port receives an authentication request, it performs the following steps, as illustrated in [Figure 22](#):

1. If EAP/EAPOL is enabled on the client, attempt to authenticate using 802.1x.
2. Otherwise, attempt to authenticate using MAC.
3. If neither attempt is successful, provide guest VLAN access.
4. If guest VLAN is not enabled, deny the authentication request.

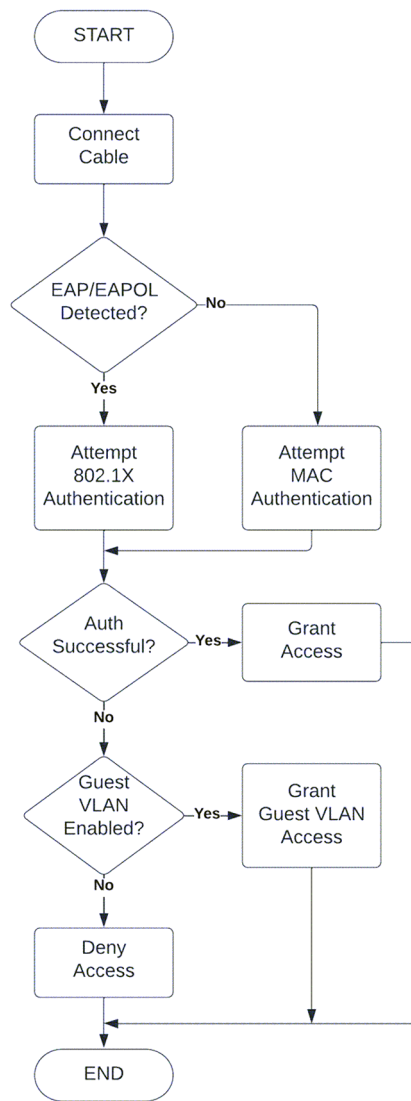


Figure 22: Flow for dynamic 802.1x and MAC authentication



Note

If you are enabling 802.1x on the end-station, a port bounce on the ISW switch will be required to perform 802.1x authentication.

See the following topics for configuration details,

NEW! *Web Configuration for 802.1x and MAC Authentication*

To enable 802.1x and MAC authentication on the same port, configure the network access server with the values highlighted in the following example:

- Select a value for **Sense Period** between 10 and 255 seconds. The default is 10 seconds.
- Specify a **Port Configuration** state of 802.1X or MAC-based sense.

- ▼ Configuration
 - ▶ System
 - ▶ Green Ethernet
 - ▶ Ports
 - ▶ DHCP
 - ▶ Security
 - ▶ Switch
 - ▶ Network
 - ▶ Limit Control
 - ▶ NAS
 - ▶ ACL
 - ▶ IP Source Guard
 - ▶ ARP Inspection
 - ▶ AAA
 - ▶ Aggregation
 - ▶ Loop Protection
 - ▶ Spanning Tree
 - ▶ IPMC Profile
 - ▶ MVR
 - ▶ IPMC
 - ▶ LLDP
 - ▶ Fabric Attach
 - ▶ PoE
 - ▶ MEP
 - ▶ ERPS
 - ▶ MAC Table
 - ▶ VLANs
 - ▶ Private VLANs
 - ▶ VCL
 - ▶ Voice VLAN
 - ▶ QoS
 - ▶ Mirroring
 - ▶ GVRP
 - ▶ sFlow
 - ▶ RingV2
 - ▶ DMI
 - ▶ Monitor
 - ▶ Diagnostics
 - ▶ Maintenance

Network Access Server Configuration

System Configuration

Mode	Enabled	▼
Reauthentication Enabled	<input type="checkbox"/>	
Reauthentication Period	3600	seconds
EAPOL Timeout	30	seconds
Aging Period	300	seconds
Hold Time	10	seconds
Sense Period	10	seconds
RADIUS-Assigned QoS Enabled	<input type="checkbox"/>	
RADIUS-Assigned VLAN Enabled	<input type="checkbox"/>	
Guest VLAN Enabled	<input checked="" type="checkbox"/>	
Guest VLAN ID	5	
Max. Reauth. Count	2	
Allow Guest VLAN if EAPOL Seen	<input checked="" type="checkbox"/>	

Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart	
* <->	▼	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
1	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate	Reinitialize
2	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate	Reinitialize
3	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate	Reinitialize
4	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate	Reinitialize
5	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate	Reinitialize
6	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate	Reinitialize
7	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Authorized	Reauthenticate	Reinitialize
8	802.1X or MAC-based sense	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Authorized	Reauthenticate	Reinitialize
9	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate	Reinitialize
10	Force Authorized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Link Down	Reauthenticate	Reinitialize

NEW! CLI Configuration for 802.1x and MAC Authentication

To enable 802.1x and MAC authentication on the same port using the command-line interface, configure the following values.

- Set the timeout sense value.

This value is used to determine whether 802.1x is enabled on the client, by checking whether the port received EAP/EAPOL packets after the port was connected. Valid values are between 10 and 255 seconds. The default is 10 seconds.

```
(config)#dot1x timeout sense-period <10-255>
```

- Specify sense on the **dot1x port-control** command.

```
(config-if)# dot1x port-control sense
```

The port is now configured to enable either 802.1x or MAC authentication.

Power over Ethernet (PoE) Application Guide

The ISW series switches support PoE function for connected powered device. The operation mode contains 802.3af (15.4W), 802.3at (30W). Each port has five classes for selection (class 0-4). Total power budget of the system is up to 240 watts.

For power management friendly use, it supports power scheduler for each PoE port. Each time interval is 30 minutes from Sunday to Saturday. Customer can select which interval to set PoE on or PoE off. It also supports PoE reset function to power off, then power on the PoE function on a port at certain time. Maximum five time can be created in a week.

Reserved Power Determination

Power Over Ethernet Configuration

Reserved Power determined by	<input checked="" type="radio"/> Class	<input type="radio"/> Allocation	<input type="radio"/> LLDP-MED
Power Management Mode	<input type="radio"/> Actual Consumption	<input checked="" type="radio"/> Reserved Power	

PoE Power Supply Configuration

Primary Power Supply [W]	240
---------------------------------	-----

PoE Port Configuration

Port	Mode	Operation	Priority	Maximum Power [W]
*	<>	<>	<>	15.4
1	Disable	802.3af	Low	15.4
2	Disable	802.3af	Low	15.4
3	Disable	802.3af	Low	15.4
4	Disable	802.3af	Low	15.4
5	Disable	802.3af	Low	15.4
6	Disable	802.3af	Low	15.4
7	Disable	802.3af	Low	15.4
8	Disable	802.3af	Low	15.4

There are three modes for configuring how the ports/PDs may reserve power:

Class 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. Five different port classes exist and one for 4, 7, 15.4 or 30 Watts.

Allocated Mode

In this mode, you allocate the amount of power that each port may reserve.

The allocated/reserved power for each port/PD is specified in the Maximum Power fields.

LLDP-MED Mode

This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the [LLDP \(Link Layer Discovery Protocol\)](#) protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode.



Note

For all modes: If a port uses more power than the reserved power for the port, the port is shut down.

Power Management Mode

Power Over Ethernet Configuration

Reserved Power determined by	<input checked="" type="radio"/> Class	<input type="radio"/> Allocation	<input type="radio"/> LLDP-MED
Power Management Mode	<input type="radio"/> Actual Consumption	<input checked="" type="radio"/> Reserved Power	

PoE Power Supply Configuration

Primary Power Supply [W]	
	240

PoE Port Configuration

Port	Mode	Operation	Priority	Maximum Power [W]
*	<>	<>	<>	15.4
1	Disable	802.3af	Low	15.4
2	Disable	802.3af	Low	15.4
3	Disable	802.3af	Low	15.4
4	Disable	802.3af	Low	15.4
5	Disable	802.3af	Low	15.4
6	Disable	802.3af	Low	15.4
7	Disable	802.3af	Low	15.4
8	Disable	802.3af	Low	15.4

There are two modes for configuring when to shut down the ports:

Actual Consumption

In this mode the ports are shut down when the actual power consumption for all ports exceeds the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shut down.

Port Priority: Critical > High > Low.

When priorities are the same, the lowest number of the port has higher priority.

Reserved Power

In this mode the ports are shut down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply.

Other PoE Parameters

Power Over Ethernet Configuration

Reserved Power determined by	<input checked="" type="radio"/> Class	<input type="radio"/> Allocation	<input type="radio"/> LLDP-MED
Power Management Mode	<input type="radio"/> Actual Consumption	<input checked="" type="radio"/> Reserved Power	

PoE Power Supply Configuration

Primary Power Supply [W]	240
---------------------------------	-----

PoE Port Configuration

Port	Mode	Operation	Priority	Maximum Power [W]
*	<>	<>	<>	15.4
1	Disable	802.3af	Low	15.4
2	Disable	802.3af	Low	15.4
3	Disable	802.3af	Low	15.4
4	Disable	802.3af	Low	15.4
5	Disable	802.3af	Low	15.4
6	Disable	802.3af	Low	15.4
7	Disable	802.3af	Low	15.4
8	Disable	802.3af	Low	15.4

PoE Power Supply

For being able to determine the amount of power the PD may use, it must be defined what amount of power a power source can deliver. Valid values are in the range 0 to 240 Watts.

PoE Mode

The PoE Mode represents the PoE operating mode for the port.

- Disable: PoE disabled for the port.
- Enable: Enables PoE for the port.
- Schedule: Enables PoE for the port by scheduling.

Operation Mode

The Operation Mode represents the PoE power operating protocol for the port.

- 802.3af : Sets PoE protocol to IEEE 802.3af.
- 802.3at : Sets PoE protocol to IEEE 802.3at.

PoE Priority

The Priority represents the port's priority. There are three levels of power priority named Low, High, and Critical.

The priority is used in the case where the remote devices require more power than the power supply

can deliver. In this case the port with the lowest priority will be turn off starting from the port with the highest port number.

Maximum Power

The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.

PoE Power Scheduling & Reset

The power scheduling is used to control the power alive interval on PoE port. It is allowed to set the specific interval to schedule power on/off in one week.

The current scheduling state is displayed graphically during the week. Green indicates the power is on and red that it is off. Directly changes checkmarks to indicate which day are members of the time interval. Check or uncheck as needed to modify the scheduling table.

PoE Power Scheduling Control on Port 1

Power Scheduling Interval Configuration

Day							Interval		Action
Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.	Start	End	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	00:00	- 00:29	<input checked="" type="radio"/> Power ON <input type="radio"/> Power OFF

Apply

Power Scheduling During 00:00 - 05:59

Time Interval	Day						
	Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.
00:00 - 00:29	●	●	●	●	●	●	●
00:30 - 00:59	●	●	●	●	●	●	●
01:00 - 01:29	●	●	●	●	●	●	●
01:30 - 01:59	●	●	●	●	●	●	●
02:00 - 02:29	●	●	●	●	●	●	●
02:30 - 02:59	●	●	●	●	●	●	●
03:00 - 03:29	●	●	●	●	●	●	●
03:30 - 03:59	●	●	●	●	●	●	●
04:00 - 04:29	●	●	●	●	●	●	●
04:30 - 04:59	●	●	●	●	●	●	●
05:00 - 05:29	●	●	●	●	●	●	●
05:30 - 05:59	●	●	●	●	●	●	●

Save

Reset

Day

Checkmarks indicate which day are members of the set. From Sunday to Saturday.

Interval

There are 48 time interval one day. Each interval has 30 minutes.

- Start - Select the start hour and minute.

- End - Select the end hour and minute.

Action

- Power On - Select the radio button to apply power on during the interval.
- Power Off - Select the radio button to apply power off during the interval.

PoE Power Reset

The entry is used to control the power reset time on PoE port.
It is allowed to create at maximum five entries for each PoE port.

PoE Power Reset Control on Port 1

Delete	Day							Time (hh:mm)
	Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.	
Delete	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	00 ▾ : 00 ▾

Add New

Save

Reset

PoE Example 1

1. Parameter Setting:
 - Reserved Power determined: Class
 - Power Management Mode: Actual Consumption
 - Primary Power Supply: 6W
2. Test Port
 - Port 1: 802.3at with critical priority
 - Port 2: 802.3af with high priority
 - Port 3: 802.3af with low priority
3. PD Power Consumption
 - Port 1: 1.3 watt (PoE Splitter)
 - Port 2: 1.3 watt (PoE VoIP Phone)
 - Port 3: 3.8 watt (PoE WiFi AP)
4. Web Configuration

Power Over Ethernet Configuration

Reserved Power determined by	<input checked="" type="radio"/> Class	<input type="radio"/> Allocation	<input type="radio"/> LLDP-MED
Power Management Mode	<input checked="" type="radio"/> Actual Consumption	<input type="radio"/> Reserved Power	

PoE Power Supply Configuration

Primary Power Supply [W]	6
--------------------------	---

PoE Port Configuration

Port	Mode	Operation	Priority	Maximum Power [W]
*	<>	<>	<>	15.4
1	Enable	802.3af	Critical	15.4
2	Enable	802.3af	High	15.4
3	Enable	802.3af	Low	15.4
4	Disable	802.3af	Low	15.4
5	Disable	802.3af	Low	15.4
6	Disable	802.3af	Low	15.4
7	Disable	802.3af	Low	15.4
8	Disable	802.3af	Low	15.4

5. Test Result:

PoE port status can be monitored from the **Monitor > PoE** menu.

If system budget is not enough for all PoE devices, the port with higher priority port will get power first. The last priority port (Port 3) will not be powered.

PoE Example 2

- Parameter Setting:
 - Reserved Power determined: Allocation
 - Power Management Mode: Reserved Power
 - Primary Power Supply: 138 W (> all port reserved power)
- Port Maximum Power
 - Port 1: 30 W
 - Port 2- Port8: 15.4 W
 - Total: 137.8 W
- PD Power Consumption
 - Port 1: 1.3 watt (PoE Splitter) Port 2: 1.3 watt (PoE VoIP Phone)
 - Port 3: 3.8 watt (PoE WiFi AP)

4. Web Configuration

Power Over Ethernet Configuration

Reserved Power determined by	<input type="radio"/> Class	<input checked="" type="radio"/> Allocation	<input type="radio"/> LLDP-MED
Power Management Mode	<input type="radio"/> Actual Consumption	<input checked="" type="radio"/> Reserved Power	

PoE Power Supply Configuration

Primary Power Supply [W]	
	138

PoE Port Configuration

Port	Mode	Operation	Priority	Maximum Power [W]
*	<>	<>	<>	30
1	Enable	802.3af	Low	30
2	Enable	802.3af	Low	15.4
3	Enable	802.3af	Low	15.4
4	Disable	802.3af	Low	15.4
5	Disable	802.3af	Low	15.4
6	Disable	802.3af	Low	15.4
7	Disable	802.3af	Low	15.4
8	Disable	802.3af	Low	15.4

<input type="button" value="Save"/>	<input type="button" value="Reset"/>
-------------------------------------	--------------------------------------

5. Test Result

PoE port status can be monitored by web: **Monitor > PoE**.

Because power has reserved for each port in advance, each powered device can use power budget of its corresponding port without exceeding its maximum power.



Regulatory and Compliance Information

Federal Communications Commission (FCC) Notice

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.



Note

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 uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.



Warning

Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Industry Canada Notice CAN ICES-3 (A)/NMB-3(A)

This digital apparatus does not exceed the class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la class A prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

Product Safety

This product complies with the following international safety standards:

- UL 60950-1 2nd edition, A2:2014
- CAN/CSA-C22.2 No.60950-1-07 2nd Ed. 2014-10
- IEC 60950-1:2005 2nd+A1:2009+A2:2013
- EN 60950-1:2006+A11+A1+A12+A2
- 2014/35/EU (2006/95/EC will be invalid by 20 April 2016)

Electromagnetic Compatibility (EMC)

This product complies with the following:

FCC 47 CFR Part 15 Subpart B Class A (US), ICES-003 (Canada)
 EN 55022 (ITE Emissions), EN 55024 (ITE Immunity)
 2014/30/EU (EMC Directive), EN 50121-1: 2017, EN 50121-4: 2016, EN 55011(ISM)
 EN 61000-6-2 (Ind. Immunity), EN61000-6-4 Ind. Emissions)
 EN 61000-3-2: 2014, EN 61000-3-3: 2013
 RCM (Australia), MSIP KCC (Korea), BSMI (Taiwan)

Korea EMC Statement (KCC)

이 기기는 업무용(A급) 전자파적합기기로서 판매자
 또는 사용자는 이 점을 주의하시기 바라며, 가정
 외의 지역에서 사용하는 것을 목적으로 합니다.

BSMI EMC Statement - Taiwan

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.

警告使用者：
 此為甲類資訊技術設備，於居住環境中使用時，可能會造成射頻
 擾動，在此種情況下，使用者會被要求採取某些適當的對策。



Glossary

ACL

An Access Control List is a mechanism for filtering packets at the hardware level. Packets can be classified by characteristics such as the source or destination MAC, IP address, IP type, or QoS queue. Once classified, the packets can be forwarded, counted, queued, or dropped.

ad hoc mode

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an AP.

ARP

Address Resolution Protocol is part of the TCP/IP suite used to dynamically associate a device's physical address (MAC address) with its logical address (IP address). The system broadcasts an ARP request, containing the IP address, and the device with that IP address sends back its MAC address so that traffic can be transmitted.

ATM

Asynchronous Transmission Mode is a start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

BSS

Basic Service Set is a wireless topology consisting of one access point connected to a wired network and a set of wireless devices. Also called an infrastructure network. See also [IBSS \(Independent Basic Service Set\)](#).

CHAP

Challenge-Handshake Authentication Protocol is one of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.

CoS

Class of Service specifies the service level for the classified traffic type.

DHCP

Dynamic Host Configuration Protocol allows network administrators to centrally manage and automate the assignment of IP addresses on the corporate network. DHCP sends a new IP address when a computer is plugged into a different place in the network. The protocol supports static or dynamic IP addresses and can dynamically reconfigure networks in which there are more computers than there are available IP addresses.

DoS attack

Denial of Service attacks occur when a critical network or computing resource is overwhelmed so that legitimate requests for service cannot succeed. In its simplest form, a DoS attack is indistinguishable from normal heavy traffic. ExtremeXOS software has configurable parameters that allow you to defeat DoS attacks.

DSSS

Direct-Sequence Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare with *FHSS (Frequency-Hopping Spread Spectrum)*.)

EAP-TLS/EAP-TTLS

EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards.

IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.

In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication.

EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.

EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.

(See also *PEAP (Protected Extensible Authentication Protocol)*.)

ESRP

Extreme Standby Router Protocol is an Extreme Networks-proprietary protocol that provides redundant Layer 2 and routing services to users.

FHSS

Frequency-Hopping Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that 'hops' in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare with *DSSS (Direct-Sequence Spread Spectrum)*.)

IBSS

An IBSS is the 802.11 term for an ad hoc network. See *ad hoc mode*.

ICMP

Internet Control Message Protocol is the part of the TCP/IP protocol that allows generation of error messages, test packets, and operating messages. For example, the ping command allows you to send ICMP echo messages to a remote IP device to test for connectivity. ICMP also supports traceroute, which identifies intermediate hops between a given source and destination.

IGMP

Hosts use Internet Group Management Protocol to inform local routers of their membership in multicast groups. Multicasting allows one computer on the Internet to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content. When all hosts leave a group, the router no longer forwards packets that arrive for the multicast group.

LLDP

Link Layer Discovery Protocol conforms to IEEE 802.1ab and is a neighbor discovery protocol. Each LLDP-enabled device transmits information to its neighbors, including chassis and port identification, system name and description, VLAN names, and other selected networking information. The protocol also specifies timing intervals in order to ensure current information is being transmitted and received.

MD5

Message-Digest algorithm is a hash function that is commonly used to generate 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.

MIC

Message Integrity Check (or Code), also called 'Michael', is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte ICV appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks.

Both integrity check mechanisms are calculated by the receiver and compared against the values sent by the sender in the frame. If the values match, there is assurance that the message has not been tampered with.

netmask

A netmask is a string of 0s and 1s that mask, or screen out, the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the netmask allows the specific host computer address to be visible.

PEAP

Protected Extensible Authentication Protocol is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (See also [EAP-TLS/EAP-TTLS](#).)

QoS

Quality of Service is a technique that is used to manage network resources and guarantee a bandwidth relationship between individual applications or protocols. A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-

time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services. Achieving the required QoS becomes the secret to a successful end-to-end business solution.

RADIUS

RADIUS is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. With RADIUS, you can track usage for billing and for keeping network statistics.

SNMP

Simple Network Management Protocol is a standard that uses a common software agent to remotely monitor and set network configuration and runtime parameters. SNMP operates in a multivendor environment, and the agent uses MIBs, which define what information is available from any manageable network device. You can also set traps using SNMP, which send notifications of network events to the system log.

SNTP

Simple Network Time Protocol is used to synchronize the system clocks throughout the network. An extension of NTP, SNTP can usually operate with a single server and allows for IPv6 addressing.

SSL

Secure Socket Layer is a protocol for transmitting private documents using the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. SSL uses the public-and-private key encryption system, which includes the use of a digital certificate.

syslog

A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.

syslog uses the UDP as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC 3164)

VLAN

The term VLAN is used to refer to a collection of devices that communicate as if they are on the same physical LAN. Any set of ports (including all ports on the switch) is considered a VLAN. LAN segments are not restricted by the hardware that physically connects them. The segments are defined by flexible user groups you create with the CLI.