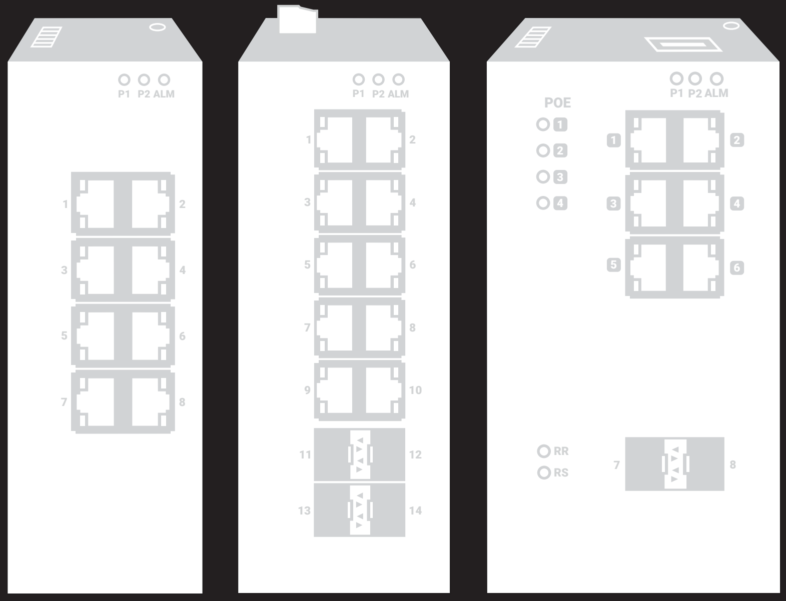
USER MANUAL

LIG1014A, LIG1080A, LIG1082A, LIE1014A, LIE1080A, LIE1082A

INDUSTRIAL ETHERNET SWITCHES

24/7 TECHNICAL SUPPORT AT 1.877.877.2269 OR VISIT BLACKBOX.COM



BLACK BOX®

TABLE OF CONTENTS

SAFETY INSTRUCTIONS

SAFETY WARNING

CAUTION: YOUR EYES MIGHT BE DAMAGED!

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.

If the equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

CHAPTER 1: SPECIFICATIONS

1.1 LIG1014A

INDUSTRIAL MANAGED GIGABIT ETHERNET SWITCH (LIG1014A)	
APPROVALS	
STANDARDS	UL508/CSA C22, EN61010-1, CE, FCC Part 15, CISPR22 (EN55022) Class A, IEC60068-2-6, -27, -32 (Vibration, Shock, Free Fall), MTBF > 25 years, IEC61000-4-2, -3, -4, -5, -6 (Level 3)
FEATURES	Web, SNMP v1/v2c, Telnet, HTTPS, SSH, Radius, TFTP/FTP, Syslog, VLAN, Diagnostic Tools, RMON 1,2,3,9, DHCP, Client/Server/Snooping/Relay/Option82, QoS, IGMP Proxy/Snooping v1/v2, Filter Features, LLDP, STP, RSTP, MSTP, LACP
FIRMWARE	
MAC ADDRESS	8000 MAC Addresses
FRAME SIZE	9000 Bytes (Jumbo frame capable)
BUFFER MEMORY	512 kbytes
HARDWARE	
CHASSIS	IP30
CONNECTORS	(10) RJ-45, 10/100/1000 Mbps speed auto-negotiation, MDI-MDI-X auto-crossover, (4) 100/1000BASE-SFP module slots, (1) RJ-45 console port
INDICATORS	(1) P1 LED, (1) P2 LED, (1) ALM LED, (10) RJ-45 Ehernet Port Link LEDs, (10) RJ-45 Ethernet Port Speed LEDs, (4) SFP Port Link LEDs, (4) SFP Port Speed LEDs
DIMENSIONS (WITHOUT DIN RAIL CLIP)	6.0"H x 2.4"W x 4.3"D (15.4 x 6 x 10.9 cm)
WEIGHT	2.4 lb. (1.1 kg)
INSTALLATION OPTIONS	DIN-rail mounting; Wallmounting
POWER	
POE	No
INPUT	Redundant input terminals, reverse power protection, 12 – 58 VDC
MAXIMUM POWER	11 Watts
ENVIRONMENTAL	
OPERATING TEMPERATURE	-40 to +167° F (-40 to +75° C), cold startup at -40° C
STORAGE TEMPERATURE	-40 to +185° F (-40 to +85° C)
HUMIDITY	5 to 95% RH (non-condensing)

1.2 LIG1080A

INDUSTRIAL MANAGED GIGABIT ETHERNET SWITCH (LIG1080A)	
APPROVALS	
STANDARDS	Agency Compliance: Vibration, shock & freefall, IEC60068-2-6, -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: 463,158 Hours
FEATURES	Web, SNMP v1/v2c, Telnet, HTTPS, SSH, Radius, TFTP/FTP, Syslog, VLAN, Diagnostic Tools, RMON 1,2,3,9, DHCP, Client/Server/Snooping/Relay/Option82, QoS, IGMP Proxy/Snooping v1/v2, Filter Features, LLDP, STP, RSTP, MSTP, LACP, v3 to SNMP, v3 to IGMP Proxy/Snooping
FIRMWARE	
MAC ADDRESS	8000 MAC Addresses
FRAME SIZE	9000 Bytes (Jumbo frame capable)
HARDWARE	
CHASSIS	IP30
CONNECTORS	(8) RJ-45, 10/100/1000 Mbps speed auto-negotiation, MDI-MDI-X auto-crossover, (1) RJ-45 console port
INDICATORS	(1) P1 LED, (1) P2 LED, (1) ALM LED, (8) RJ-45 Ehernet Port Link LEDs, (8) RJ-45 Ethernet Port Speed LEDs
DIMENSIONS (WITHOUT DIN RAIL CLIP)	6.0"H x 4.3"W x 2.4"D (15.4 x 10.9 x 6.0 cm)
WEIGHT	2.33 lbs. (1.06 kg)
INSTALLATION OPTIONS	DIN-rail mounting; Wallmounting
POWER	
POE	No
INPUT	Redundant input terminals, reverse power protection, 12 – 58 VDC
MAXIMUM POWER	10.5 Watts
ENVIRONMENTAL	
OPERATING TEMPERATURE	-40 to +167° F (-40 to +75° C), cold startup at -40° C
STORAGE TEMPERATURE	-40 to +185° F (-40 to +85° C)
HUMIDITY	5 to 95% RH (non-condensing)

CHAPTER 1: SPECIFICATIONS

1.3 LIG1082A

INDUSTRIAL MANAGED GIGABIT ETHERNET SWITCH (LIG1082A)	
APPROVALS	
STANDARDS	Agency Compliance: Vibration, shock & freefall, IEC60068-2-6, -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: 463,158 Hours
FEATURES	Web, SNMP v1/v2c, Telnet, HTTPS, SSH, Radius, TFTP/FTP, Syslog, VLAN, Diagnostic Tools, RMON 1,2,3,9, DHCP, Client/Server/Snooping/Relay/Option82, QoS, IGMP Proxy/Snooping v1/v2, Filter Features, LLDP, STP, RSTP, MSTP, LACP, v3 to SNMP, v3 to IGMP Proxy/Snooping
FIRMWARE	
MAC ADDRESS	8000 MAC Addresses
FRAME SIZE	9000 Bytes (Jumbo frame capable)
HARDWARE	
CHASSIS	IP30
CONNECTORS	(6) RJ-45, 10/100/1000 Mbps speed auto-negotiation, MDI-MDI-X auto-crossover, (2) 100/1000BASE-SFP module slots, (1) RJ-45 console port
INDICATORS	(1) P1 LED, (1) P2 LED, (1) ALM LED, (6) RJ-45 Ehernet Port Link LEDs, (6) RJ-45 Ethernet Port Speed LEDs, (2) SFP Port Link LEDs, (2) SFP Port Speed LEDs
DIMENSIONS (WITHOUT DIN RAIL CLIP)	6.0"H x 4.3"W x 2.4"D (15.4 x 10.9 x 6.0 cm)
WEIGHT	2.33 lbs. (1.06 kg)
INSTALLATION OPTIONS	DIN-rail mounting; Wallmounting
POWER	
POE	No
INPUT	Redundant input terminals, reverse power protection, 12 – 58 VDC
MAXIMUM POWER	10.5 Watts
ENVIRONMENTAL	
OPERATING TEMPERATURE	-40 to +167° F (-40 to +75° C), cold startup at -40° C
STORAGE TEMPERATURE	-40 to +185° F (-40 to +85° C)
HUMIDITY	5 to 95% RH (non-condensing)

1.4 LIE1014A

INDUSTRIAL MANAGED POE GIGABIT ETHERNET SWITCH (LIE1014A)	
APPROVALS	
STANDARDS	UL508/CSA C22, EN61010-1, CE, FCC Part 15, CISPR22 (EN55022) Class A, IEC60068-2-6, -27, -32 (Vibration, Shock, Free Fall), MTBF > 25 years, IEC61000-4-2, -3, -4, -5, -6 (Level 3)
FEATURES	Web, SNMP v1/v2c, Telnet, HTTPS, SSH, Radius, TFTP/FTP, Syslog, VLAN, Diagnostic Tools, RMON 1,2,3,9, DHCP, Client/Server/Snooping/Relay/Option82, QoS, IGMP Proxy/Snooping v1/v2, Filter Features, LLDP, STP, RSTP, MSTP, LACP
FIRMWARE	
MAC ADDRESS	8000 MAC Addresses
FRAME SIZE	9000 Bytes (Jumbo frame capable)
BUFFER MEMORY	512 kbytes
HARDWARE	
CHASSIS	IP30
CONNECTORS	(8) RJ-45, IEEE 802.3at PoE PSE ports, 10/100/1000 Mbps speed auto-negotiation, MDI-MDI-X auto-crossover; (4) 100/1000BASE-SFP module slot, (1) RJ-45 console port
INDICATORS	(1) P1 LED, (1) P2 LED, (1) ALM LED, (8) RJ-45 Ehernet Port Link LEDs, (8) RJ-45 Ethernet Port Speed LEDs, (4) SFP Port Link LEDs, (4) SFP Port Speed LEDs, (8) PoE Port LEDs
DIMENSIONS (WITHOUT DIN RAIL CLIP)	6.1”H x 3.0”W x 5.0”D (15.4 x 7.7 x 12.8 cm)
WEIGHT	3.1 lb. (1.4 kg)
INSTALLATION OPTIONS	DIN-rail mounting; Wallmounting
POWER	
POE	Yes
INPUT	Redundant input terminals, reverse power protection, 12 –58 VDC, 54–58 VDC for PoE+, 48–58 VDC for PoE
MAXIMUM POWER	Without PoE: 14 Watts, With PoE: 265 Watts
ENVIRONMENTAL	
OPERATING TEMPERATURE	-40 to +167° F (-40 to +75° C), cold startup at -40° C
STORAGE TEMPERATURE	-40 to +185° F (-40 to +85° C)
HUMIDITY	5 to 95% RH (non-condensing)

CHAPTER 1: SPECIFICATIONS

1.5 LIE1080A

INDUSTRIAL MANAGED POE GIGABIT ETHERNET SWITCH (LIE1080A)	
APPROVALS	
STANDARDS	Agency Compliance: Vibration, shock & freefall, IEC60068-2-6, -27, -32 Certification compliance: CE/FCC; EN 50121-4, NEMA TS-2 Electrical safety: CSA C22, UL60905, CE EMC: FCC Part 15, CISPR 22 (EN55022) Class , IEC61000-4-2, -3, -4, -5, -6 RoHS and WEEE: RoHS (Pb free) and WEEE compliant MTBF: > 25 years
FEATURES	Web, SNMP v1/v2c, Telnet, HTTPS, SSH, Radius, TFTP/FTP, Syslog, VLAN, Diagnostic Tools, RMON 1,2,3,9, DHCP, Client/Server/Snooping/Relay/Option82, QoS, IGMP Proxy/Snooping v1/v2, Filter Features, LLDP, STP, RSTP, MSTP, LACP, v3 to SNMP, v3 to IGMP Proxy/Snooping
FIRMWARE	
MAC ADDRESS	8000 MAC Addresses
FRAME SIZE	9000 Bytes (Jumbo frame capable)
HARDWARE	
CHASSIS	IP30
CONNECTORS	(8) RJ-45, 10/100/1000 Mbps speed auto-negotiation, MDI-MDI-X auto-crossover, (1) RJ-45 console port
INDICATORS	(1) P1 LED, (1) P2 LED, (1) ALM LED, (8) RJ-45 Ehernet Port Link LEDs, (8) RJ-45 Ethernet Port Speed LEDs, (10) PoE Port LEDs
DIMENSIONS (WITHOUT DIN RAIL CLIP)	6.1"H x 3.0"W x 5.0"D (15.4 x 7.7 x 12.8 cm)
WEIGHT	3.1 lb. (1.4 kg)
INSTALLATION OPTIONS	DIN-rail mounting; Wallmounting
POWER	
POE	Yes
INPUT	Redundant input terminals, reverse power protection, 12 –58 VDC, 54–58 VDC for PoE+, 48–58 VDC for PoE
MAXIMUM POWER	Without PoE: 14 Watts, With PoE: 265 Watts
ENVIRONMENTAL	
OPERATING TEMPERATURE	-40 to +167° F (-40 to +75° C), cold startup at -40° C
STORAGE TEMPERATURE	-40 to +185° F (-40 to +85° C)
HUMIDITY	5 to 95% RH (non-condensing)

CHAPTER 1: SPECIFICATIONS

1.6 LIE1082A

INDUSTRIAL MANAGED POE GIGABIT ETHERNET SWITCH (LIE1082A)	
APPROVALS	
STANDARDS	Agency Compliance: Vibration, shock & freefall, IEC60068-2-6, -27, -32 Certification compliance: CE/FCC; EN 50121-4, NEMA TS-2 Electrical safety: CSA C22, UL60905, 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 yrs
FEATURES	Web, SNMP v1/v2c, Telnet, HTTPS, SSH, Radius, TFTP/FTP, Syslog, VLAN, Diagnostic Tools, RMON 1,2,3,9, DHCP, Client/Server/Snooping/Relay/Option82, QoS, IGMP Proxy/Snooping v1/v2, Filter Features, LLDP, STP, RSTP, MSTP, LACP, v3 to SNMP, v3 to IGMP Proxy/Snooping
FIRMWARE	
MAC ADDRESS	8000 MAC Addresses
FRAME SIZE	9000 Bytes (Jumbo frame capable)
HARDWARE	
CHASSIS	IP30
CONNECTORS	(6) RJ-45, 10/100/1000 Mbps speed auto-negotiation, MDI-MDI-X auto-crossover, (2) 100/1000BASE-SFP module slot, (1) RJ-45 console port
INDICATORS	(1) P1 LED, (1) P2 LED, (1) ALM LED, (6) RJ-45 Ehernet Port Link LEDs, (6) RJ-45 Ethernet Port Speed LEDs, (2) SFP Port Link LEDs, (2) SFP Port Speed LEDs, (6) PoE Port LEDs
DIMENSIONS (WITHOUT DIN RAIL CLIP)	6.1”H x 3.0”W x 5.0”D (15.4 x 7.7 x 12.8 cm)
WEIGHT	3.1 lb. (1.4 kg)
INSTALLATION OPTIONS	DIN-rail mounting; Wallmounting
POWER	
POE	Yes
INPUT	Redundant input terminals, reverse power protection, 12 –58 VDC, 54–58 VDC for PoE+, 48–58 VDC for PoE
MAXIMUM POWER	Without PoE: 14 Watts, With PoE: 265 Watts
ENVIRONMENTAL	
OPERATING TEMPERATURE	-40 to +167° F (-40 to +75° C), cold startup at -40° C
STORAGE TEMPERATURE	-40 to +185° F (-40 to +85° C)
HUMIDITY	5 to 95% RH (non-condensing)

CHAPTER 1: SPECIFICATIONS

1.7 SYSTEM STATISTICS

SYSTEM STATISTICS	
FUNCTION NAME	**SYSTEM MAXI-MUM VALUE**
VLAN ID	4096
VLAN LIMITATION	1024
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
RADIUS SERVER	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
IGMP GROUP	256

CHAPTER 2: OVERVIEW

2.1 INTRODUCTION

The Industrial Managed and Unmanaged Gigabit Ethernet Switches include unmanaged switches that provide four (4) copper RJ-45 or RJ-45 PoE ports and one (1) multi-rate SFP slot and managed switches that provide six (6), eight (8) or ten (10) copper RJ-45 or RJ-45 PoE ports and two (2) or four (4) multi-rate SFP slots.

Power over Ethernet

The LIE401A, LIE1014A, LIE1080A and LIE1082A switches support Power over Ethernet compliant to the IEEE 802.3af and IEEE 802.3at standard on all copper ports. Thus these switches can be used to power standard PoE PD devices with up to 30 watts per port along with the Ethernet data on standard Ethernet Cabling.

Multi-rate SFP slots

The benefit of having multi-rate SFP slots is to be able to use 100-Mbps and 1-Gbps SFP Modules for either multi- or single-mode in a mix and match as needed. If requirements change, just replace the SFP module and protect your switch investment.

Power

The switches are powered from 12- to 58-VDC. The PoE models need 48 VDC for 802.3af and a minimum of 53 VDC for 802.3at.

Extended temperature range

All models are tested and released for operating temperatures from -40° up to +75° Celsius. They passed shock, vibration and freefall test and comply with the IEC600068-2-6, -27 and -32 standards.

Management

The switches offer powerful features including Layer 3 routing and management with all advanced filter and multicast algorithms needed today to easily prioritize, partition, and organize a reliable high-speed network.

2.2 AVAILABLE MODELS

Six models of the Industrial Gigabit Ethernet Switches are available:

- Industrial Gigabit Ethernet Switch - Managed, Extreme Temperature, (10) RJ-45, (4) SFP (LIG1014A)
- Industrial Gigabit Ethernet Managed L2+ Switch - Extreme Temperature, (8) RJ-45 (LIG1080A)
- Industrial Gigabit Ethernet Managed L2+ Switch - Extreme Temperature, (6) RJ-45, (2) SFP (LIG1082A)
- Industrial Gigabit Ethernet PoE+ Switch - Managed, (8) RJ-45, (4) SFP (LIE1014A)
- Industrial Gigabit Ethernet Managed L2+ Switch - PoE+, Extreme Temperature, (8) RJ-45 (LIE1080A)
- Industrial Gigabit Ethernet Managed L2+ Switch - PoE+, Extreme Temperature, (6) RJ-45, (2) SFP (LIE1082A)

SPECIFICATION COMPARISON CHART

	LIE1014A	LIE1080A	LIE1082A	LIG1014A	LIG1080A	LIG1082A
RJ-45 POE PORTS	8	8	6	—	—	—
RJ-45 PORTS	—	—	—	10	8	6
SFP PORTS	4	NONE	2	4	NONE	2
P1 LED	1	NONE	1	1	NONE	2
P2 LED	1	1	1	1	1	1
ALM LED	1	1	1	1	1	1
ETHERNET PORT LINK LED	8	8	6	10	8	6
ETHERNET PORT SPEED LED	8	8	6	10	8	6
SFP PORT LINK LED	4	NONE	2	4	NONE	2
SFP PORT SPEED LED	4	NONE	2	4	NONE	2
MANAGED	YES	YES	YES	YES	YES	YES

CHAPTER 2: OVERVIEW

2.3 FEATURES

- CATx models reach distance up to 426 feet (130 m)
- Unmanaged models (LIE401A and LIG401A) offer (4) 10/100/1000 plus (1) multi-rate SFP
- Managed models (LIE1014A, LIE1080A, LIE1082A, LIG1014A, LIG1080A and LIG1082A) provide (6), (8) or (10) 10/100/1000 plus (2) or (4) multi-rate SFPs
- Models with Power over Ethernet Plus deliver 30 watts power per port to remote PD devices
- Extended temperature range: -40° to +75°C
- L2 wire speed switching
- 12 to 58V DC dual input, reverse polarity
- IP30 industrial design
- DIN-rail mountable
- Shock, vibration and freefall test to IEC60068-2-6, -27, -32
- EMC approval acc. to IEC61000-4-2, -3, -4, -5, -6 (Level 3)

2.4 WHAT'S INCLUDED

LIG1014A:

- (1) Industrial Managed Gigabit Ethernet Switch
- (2) Wallmount plates
- (1) DIN rail clip
- (1) DC power terminal block
- (10) RJ-45 port dust covers
- (4) SFP port dust covers
- (1) quick start guide

LIG1080A:

- (1) Industrial Managed Gigabit Ethernet Switch
- (2) Wallmount plates
- (1) DIN rail clip
- (1) DC power terminal block
- (8) RJ-45 port dust covers
- (1) quick start guide

LIG1082A:

- (1) Industrial Managed Gigabit Ethernet Switch
- (2) Wallmount plates
- (1) DIN rail clip
- (1) DC power terminal block
- (6) RJ-45 port dust covers
- (2) SFP PORT DUST COVERS
- (1) quick start guide

LIE1014A:

- (1) Industrial Managed Gigabit POE Ethernet Switch
- (2) Wallmount plates
- (1) DIN rail clip
- (1) DC power terminal block
- (8) RJ-45 port dust covers
- (4) SFP port dust covers
- (1) quick start guide

LIE1080A:

- (1) Industrial Managed Gigabit POE Ethernet Switch
- (2) Wallmount plates
- (1) DIN rail clip
- (1) DC power terminal block
- (8) RJ-45 port dust covers
- (1) quick start guide

LIE1082A:

- (1) Industrial Managed Gigabit POE Ethernet Switch
- (2) Wallmount plates
- (1) DIN rail clip
- (1) DC power terminal block
- (6) RJ-45 port dust covers
- (2) SFP port dust covers
- (1) quick start guide

2.5 HARDWARE DESCRIPTION

2.5.1 LIG1014A

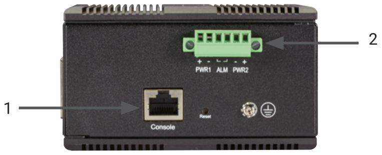


FIGURE 2-1. LIG1014A TOP PANEL

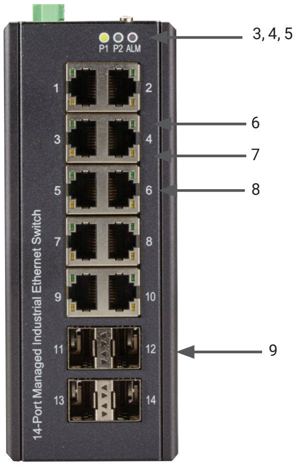


FIGURE 2-2. LIG1014A FRONT PANEL

TABLE 2-1. LIG1014A COMPONENTS

NUMBER IN FIGURES 2-1 AND 2-2	COMPONENT	DESCRIPTION
1	(1) RJ-45 connector	Links to console for management
2	(1) 6-pin terminal block	Power 1, Power 2 and Alarm connections
3	(1) P1 LED	Lights when power to Power Supply 1 is ON
4	(1) P2 LED	Lights when power to Power Supply 2 is ON
5	(1) Alarm LED	Lights to indicate an alarm
6	(10) Link/Activity LEDs	Lights when there is activity on the respective port
7	(10) Speed LEDs	Lights when port is operating at 100 Mbps
8	(10) RJ-45 connectors	Connect to devices
9	(4) SFP module cages	Connect to fiber optic uplinks

2.5.2 LIG1080A

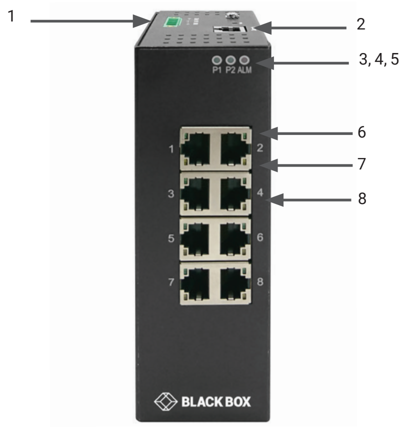


FIGURE 2-3. LIG1080A TOP AND FRONT PANELS

TABLE 2-2. LIG1080A COMPONENTS

NUMBER IN FIGURE 2-3	COMPONENT	DESCRIPTION
1	(1) 6-pin terminal block	Power 1, Power 2 and Alarm connections
2	(1) RJ-45 connector	Links to console for management
3	(1) P1 LED	Lights when power to Power Supply 1 is ON
4	(1) P2 LED	Lights when power to Power Supply 2 is ON
5	(1) Alarm LED	Lights to indicate an alarm
6	(8) Link/Activity LEDs	Lights when there is activity on the respective port
7	(8) Speed LEDs	Lights when port is operating at 100 Mbps
8	(8) RJ-45 connectors	Connect to devices

2.5.3 LIG1082A

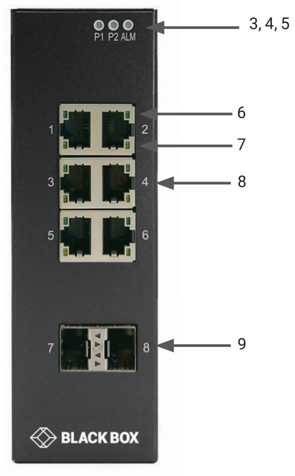


FIGURE 2-4. LIG1082A FRONT PANEL

TABLE 2-3. LIG1082A COMPONENTS

NUMBER IN FIGURES 2-4	COMPONENT	DESCRIPTION
1 (not shown)	(1) RJ-45 connector	Links to console for management
2 (not shown)	(1) 6-pin terminal block	Power 1, Power 2 and Alarm connections
3	(1) P1 LED	Lights when power to Power Supply 1 is ON
4	(1) P2 LED	Lights when power to Power Supply 2 is ON
5	(1) Alarm LED	Lights to indicate an alarm
6	(6) Link/Activity LEDs	Lights when there is activity on the respective port
7	(6) Speed LEDs	Lights when port is operating at 100 Mbps
8	(6) RJ-45 connectors	Connect to devices
9	(2) SFP module cages	Connect to fiber optic uplinks

2.5.4 LIE1014A

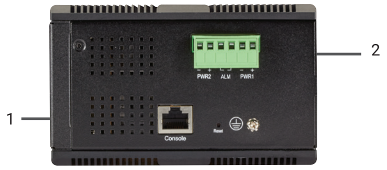


FIGURE 2-5. LIE1014A TOP PANEL

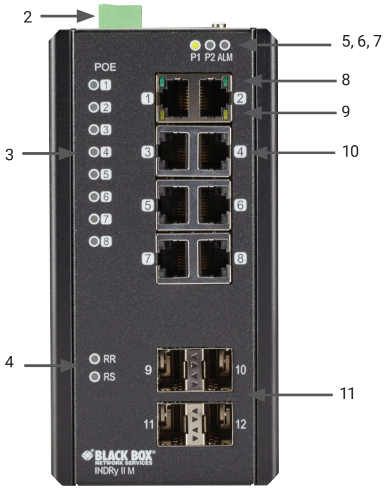


FIGURE 2-6. LIE1014A FRONT PANEL

TABLE 2-4. LIE1014A COMPONENTS

NUMBER IN FIGURES 2-5 AND 2-6	COMPONENT	DESCRIPTION
1	(1) RJ-45 connector	Links to console for management
2	(1) 6-pin terminal block	Power 1, Power 2 and Alarm connections
3	(8) PoE LEDs	Light when port is using Power over Ethernet (PoE)
4	(1) RR LED, (1) RS LED	Ring Role, Ring Status (see Table 3-2 in Section 3.14)
5	(1) P1 LED	Lights when power to Power Supply 1 is ON
6	(1) P2 LED	Lights when power to Power Supply 2 is ON
7	(1) Alarm LED	Lights to indicate an alarm
8	(8) Link/Activity LEDs	Lights when there is activity on the respective port
9	(8) Speed LEDs	Lights when port is operating at 100 Mbps
10	(8) RJ-45 PoE connectors	Connect to PoE devices
11	(4) SFP module cages	Connect to fiber optic uplinks

2.5.5 LIE1080A

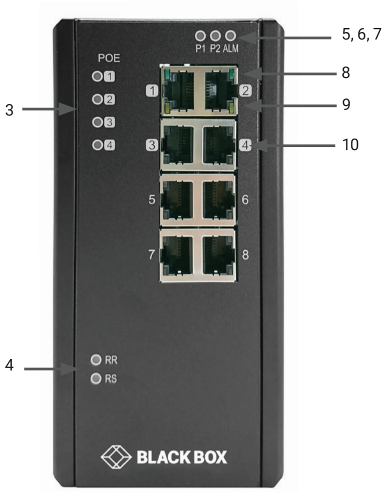


FIGURE 2-7. LIE1080A FRONT PANEL

TABLE 2-5. LIE1080A COMPONENTS

NUMBER IN FIGURE 2-7	COMPONENT	DESCRIPTION
1 (not shown)	(1) RJ-45 connector	Links to console for management
2 (not shown)	(1) 6-pin terminal block	Power 1, Power 2 and Alarm connections
3	(8) PoE LEDs	Light when port is using Power over Ethernet (PoE)
4	(1) RR LED, (1) RS LED	Ring Role, Ring Status (see Table 3-2 in Section 3.14)
5	(1) P1 LED	Lights when power to Power Supply 1 is ON
6	(1) P2 LED	Lights when power to Power Supply 2 is ON
7	(1) Alarm LED	Lights to indicate an alarm
8	(8) Link/Activity LEDs	Lights when there is activity on the respective port
9	(8) Speed LEDs	Lights when port is operating at 100 Mbps
10	(8) RJ-45 PoE connectors	Connect to PoE devices

2.5.6 LIE1082A

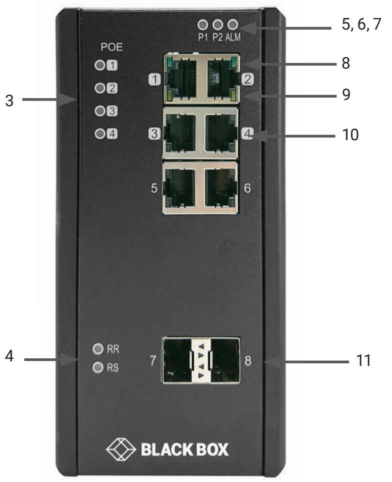


FIGURE 2-8. LIE1082A FRONT PANEL

TABLE 2-6. LIE1082A COMPONENTS

NUMBER IN FIGURE 2-7	COMPONENT	DESCRIPTION
1 (not shown)	(1) RJ-45 connector	Links to console for management
2 (not shown)	(1) 6-pin terminal block	Power 1, Power 2 and Alarm connections
3	(6) PoE LEDs	Light when port is using Power over Ethernet (PoE)
4	(1) RR LED, (1) RS LED	Ring Role, Ring Status (see Table 3-2 in Section 3.14)
5	(1) P1 LED	Lights when power to Power Supply 1 is ON
6	(1) P2 LED	Lights when power to Power Supply 2 is ON
7	(1) Alarm LED	Lights to indicate an alarm
8	(6) Link/Activity LEDs	Lights when there is activity on the respective port
9	(6) Speed LEDs	Lights when port is operating at 100 Mbps
10	(6) RJ-45 PoE connectors	Connect to PoE devices
11	(2) SFP module cages	Link to fiber optic SFP modules

3.1 DIN RAIL MOUNTING

Follow these steps to mount the switch on a DIN rail.

1. Screw the DIN-Rail bracket on with the bracket and screws in the accessory kit.

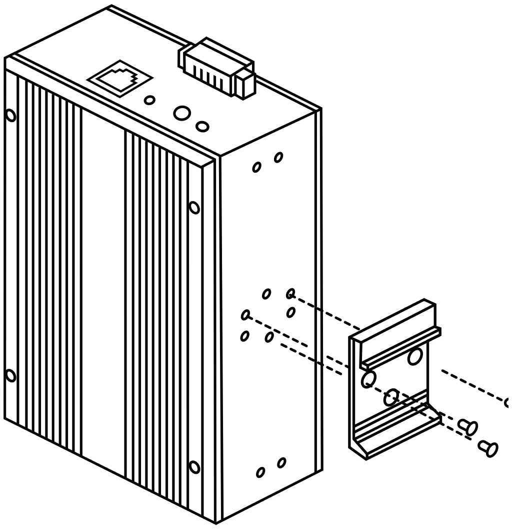


FIGURE 3-1. DIN RAIL MOUNTING STEP 1

2. Hook the unit over the DIN rail.

3. Push the bottom of the unit towards the DIN Rail until it snaps into place.

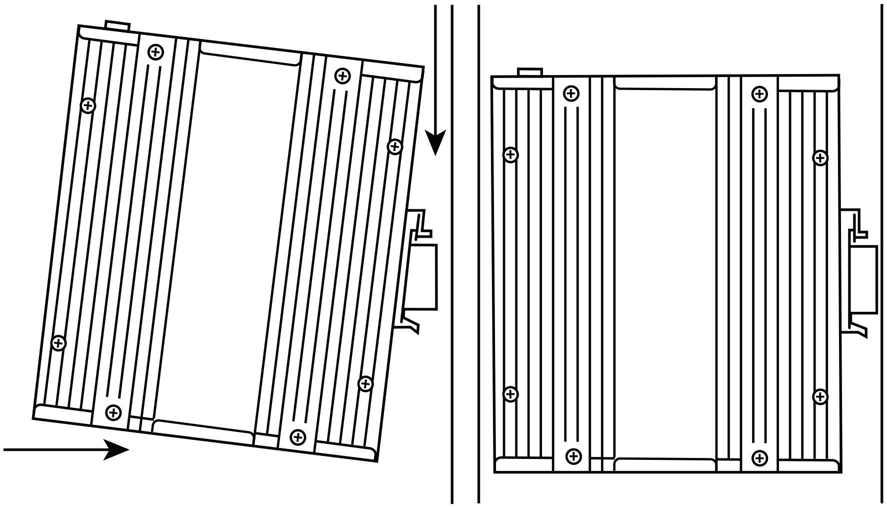


FIGURE 3-2. DIN RAIL MOUNTING STEPS 2 AND 3

3.2 WALLMOUNTING

Follow these steps to mount the switch on a wall.

1. Screw the wall-mount brackets on with screws in the accessory kit.

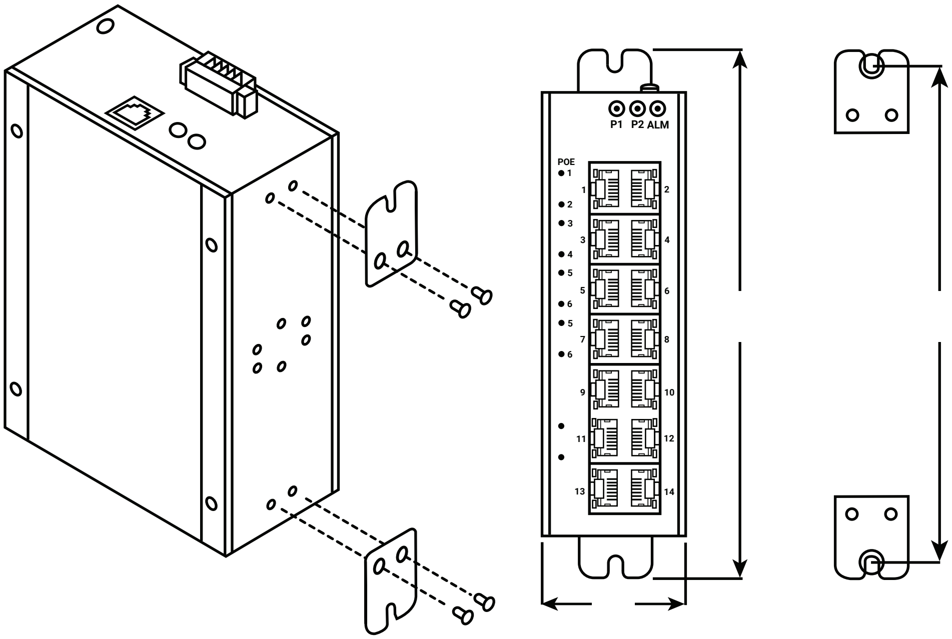


FIGURE 3-3. MOUNTING THE SWITCH ON A WALL

3.3 ALARM RELAY AND GROUND

The alarm relay output contacts are in the middle of the DC terminal block connector as shown in the next figure.

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

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

The switch must be properly grounded for optimum system performance.

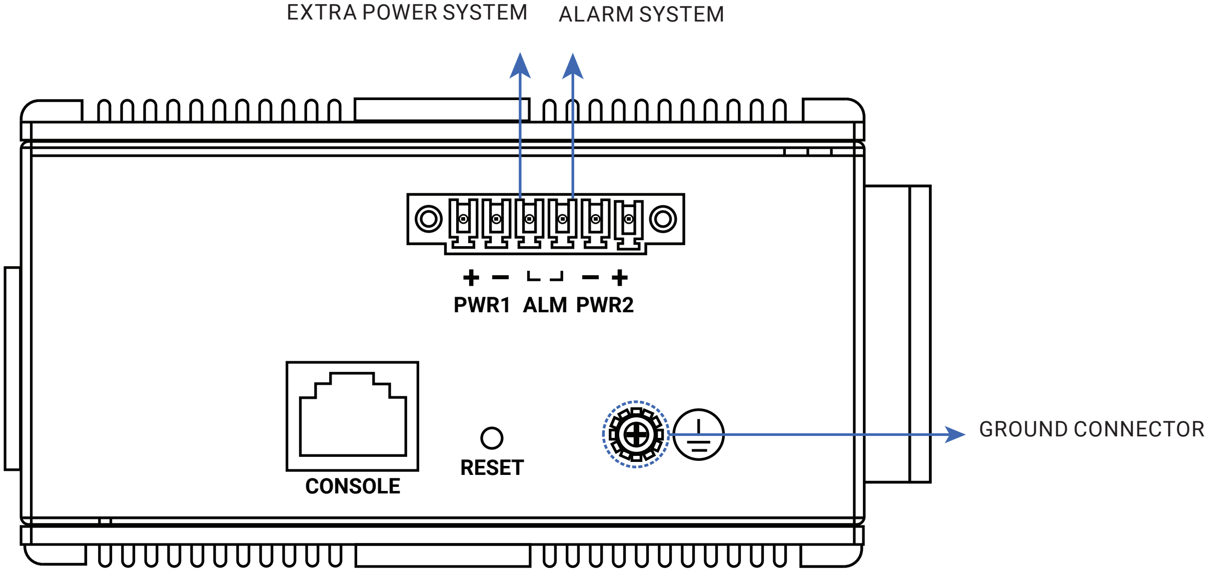


FIGURE 3-4. ALARM RELAY AND GROUND

3.4 CONNECTING THE ETHERNET INTERFACE (RJ-45 ETHERNET)

The switch provides two types of Ethernet interfaces: electrical (RJ-45) and optical (SFP) interfaces.

Connecting the Ethernet interface via RJ45:

To connect the switch to a PC, use straight-through or cross-over Ethernet cables,

To connect the switch to an Ethernet device, use UTP (Unshielded Twisted Pair) or STP (Shielded Twisted Pair) Ethernet cables.

The pin assignment of RJ-45 connector is shown in the following figure and table.

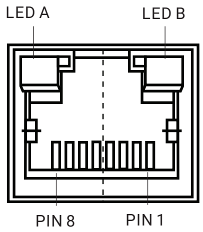


TABLE 3-1. RJ-45 PINOUT

PIN	ASSIGNMENT	POE ASSIGNMENT (FOR POE MANAGED SERIES ONLY)
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

3.5 CONNECTING THE ETHERNET INTERFACE (FIBER, SFP)

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.

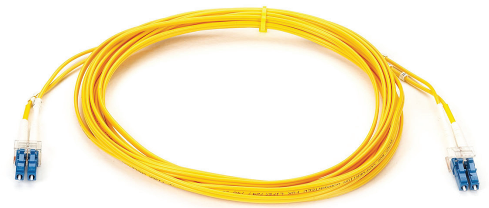


FIGURE 3-5. FIBER OPTICS CABLE WITH LC DUPLEX CONNECTOR

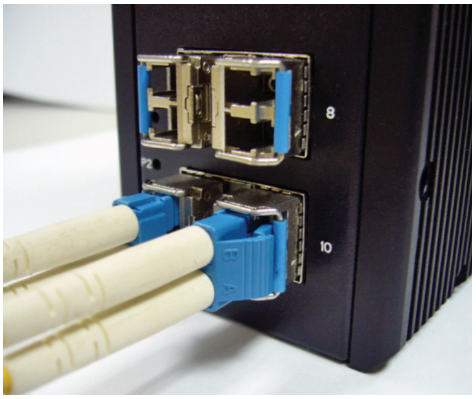


FIGURE 3-6. CONNECT THE OPTICAL FIBER TO THE SFP SOCKET

⚠ **DANGER:**

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.

3.6 POWER CONNECTION

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.

MANAGED SERIES

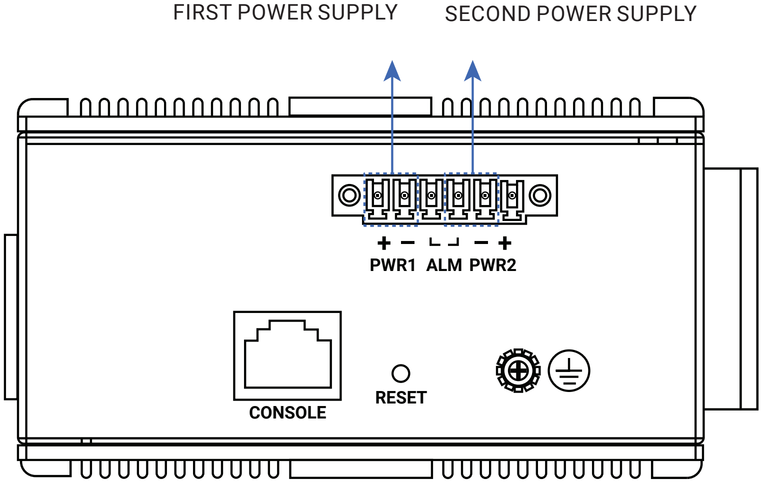


FIGURE 3-7. MANAGED SERIES

POE MANAGED SERIES

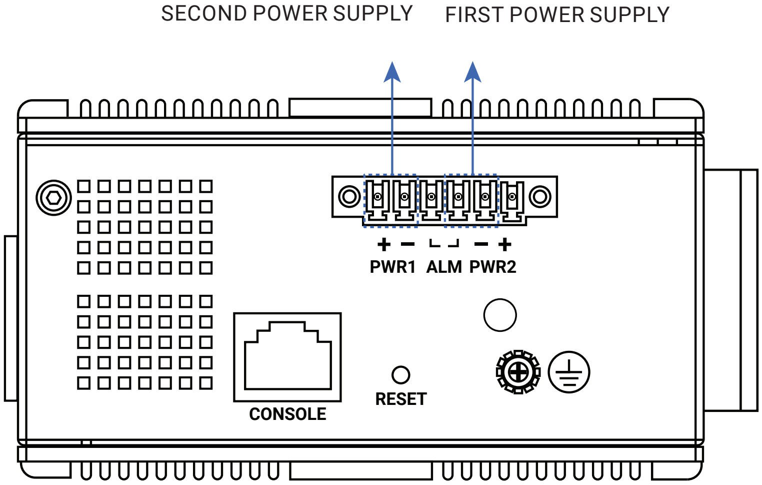


FIGURE 3-8. POE MANAGED SERIES

3.7 ALARM RELAY AND GROUND

The alarm relay output contacts are in the middle of the DC terminal block connector as shown in the figure below.

The alarm relay out is "Normal Open," and it will be closed when the switch detects any predefined failure such as power failures or Ethernet link failures.

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

The switch must be properly grounded for optimum system performance.

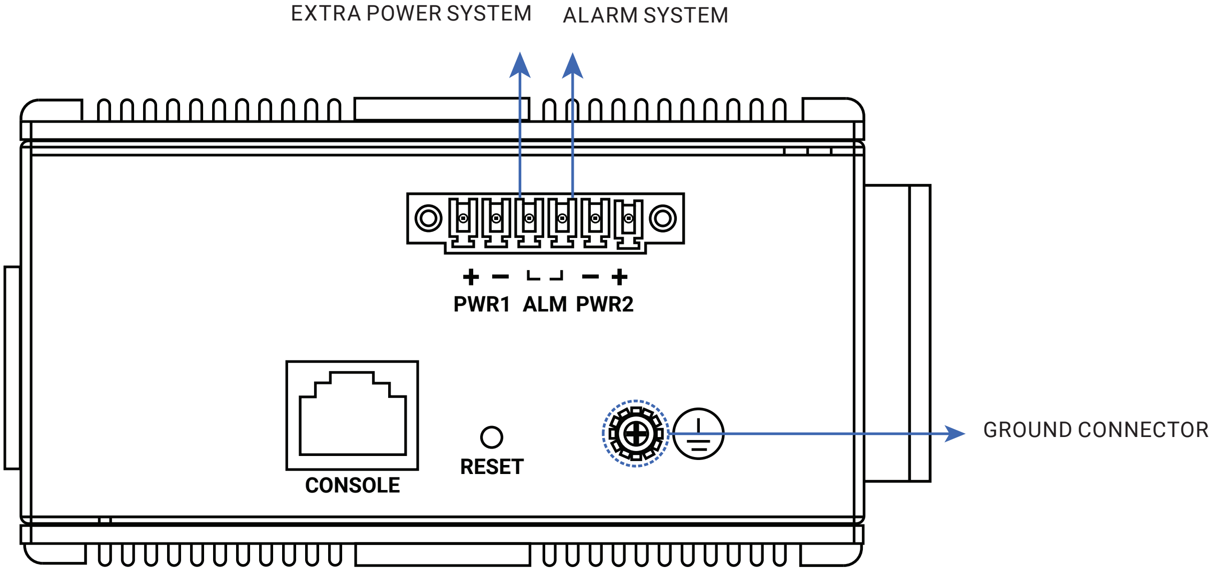


FIGURE 3-9. ALARM RELAY AND GROUND

3.8 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 switch may not respond; then you may need to push the Reset button.

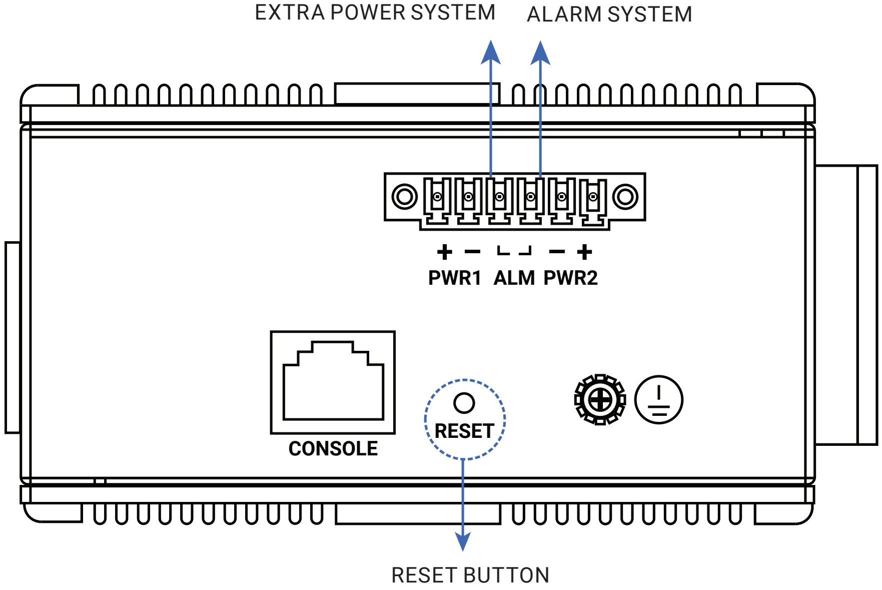


FIGURE 3-10. RESET BUTTON

3.9 CONSOLE CONNECTION

The Console port is for local management by using a terminal emulator or a computer with terminal emulation software. The DB9 connector connects to the computer's COM port.

- Baud rate = 115200 bps
- 8 data bits, 1 stop bit
- Priority = None
- Flow control = None

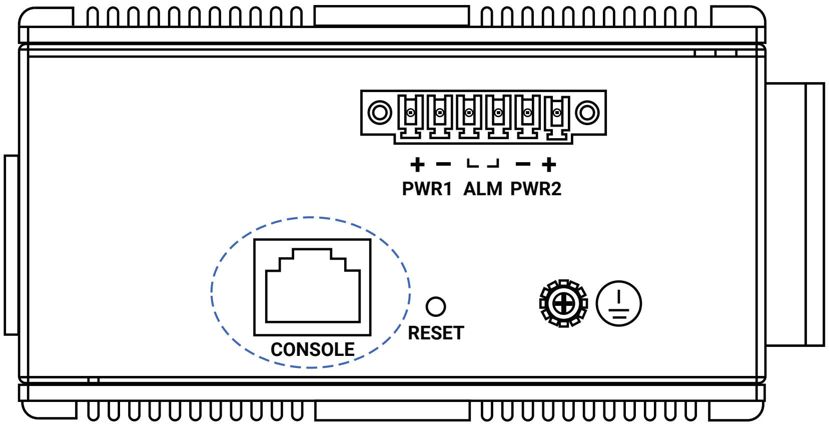


FIGURE 3-11. CONSOLE CONNECTOR

To connect the host PC to the Console port, an RJ-45 (male) connector-to-RS232 DB9 (female) connector cable is required. The RJ-45 connector of the cable is connected to the Console port of the switch; the DB9 connector of the cable is connected to the PC COM port. The pin assignment of the Console cable is shown below:

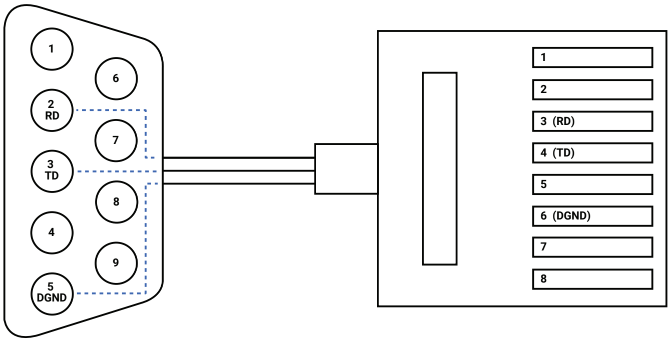


FIGURE 3-12. CONSOLE CABLE

3.10 WEB INTERFACE INITIALIZATION (OPTIONAL)

WEB BROWSER SUPPORT

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

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

Firefox with the following default settings is recommended:

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

Google Chrome with the following default settings is recommended:

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

CONNECT AND LOGIN

Connecting to the RJ-45 Ethernet port.

Factory default IP: 192.0.2.1

Login with default account and password.
Username: admin

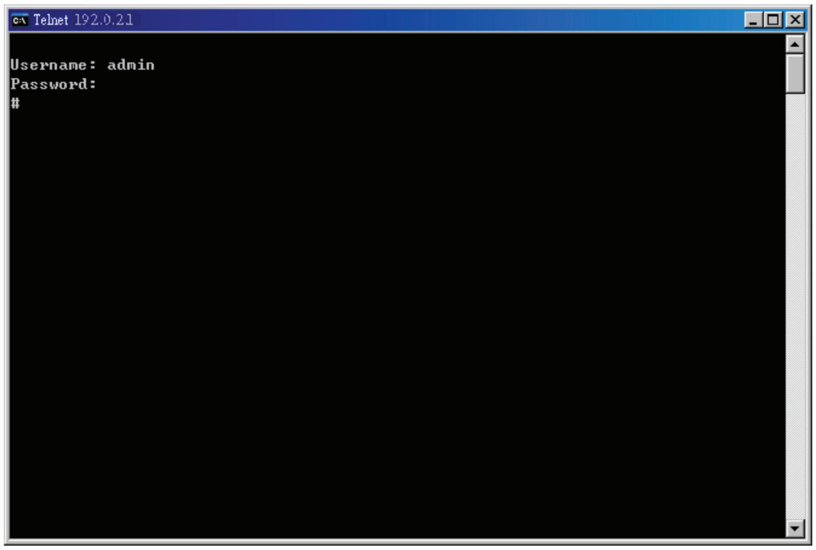
Password: (none)

3.11 CLI INITIALIZATION AND CONFIGURATION (OPTIONAL)

1. Connect to the RJ-45 Ethernet port.
2. Type in the command under Telnet: telnet 192.0.2.1
3. Login with default account and password.

Username: admin

Password: (none)



```
Username: admin
Password:
#
```

FIGURE 3-13. LOGIN TO COMMAND LINE INTERFACE (CLI)

4. Change the IP with the commands listed below:

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

FIGURE 3-14. CLI COMMAND

3.12 UPGRADE/DOWNGRADE SOFTWARE

1. In the Web UI, go to the Maintenance —> Software —> Upload page.
2. Select software file and click the Upload button.

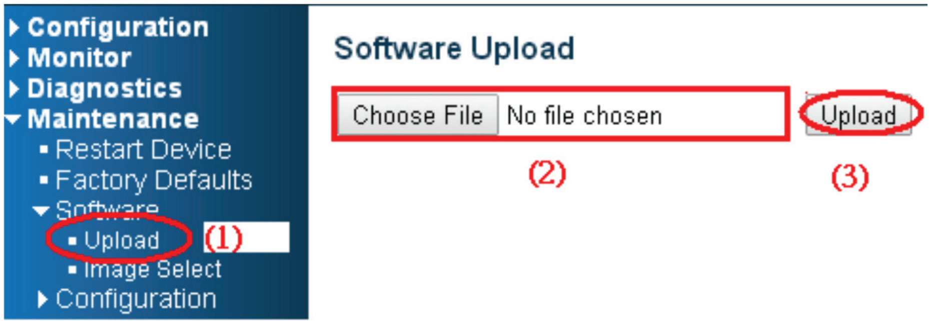
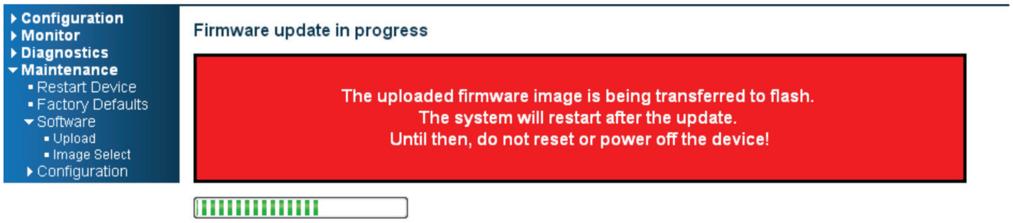


FIGURE 3-15. SOFTWARE UPLOAD BUTTON

3. After starting to upload the software to the device, do not restart the device; wait until it auto reboots and the upgrade finishes.



Firmware update in progress

The uploaded firmware image is being transferred to flash.
The system will restart after the update.
Until then, do not reset or power off the device!

FIGURE 3-16. UPGRADE IN PROCESS SCREEN

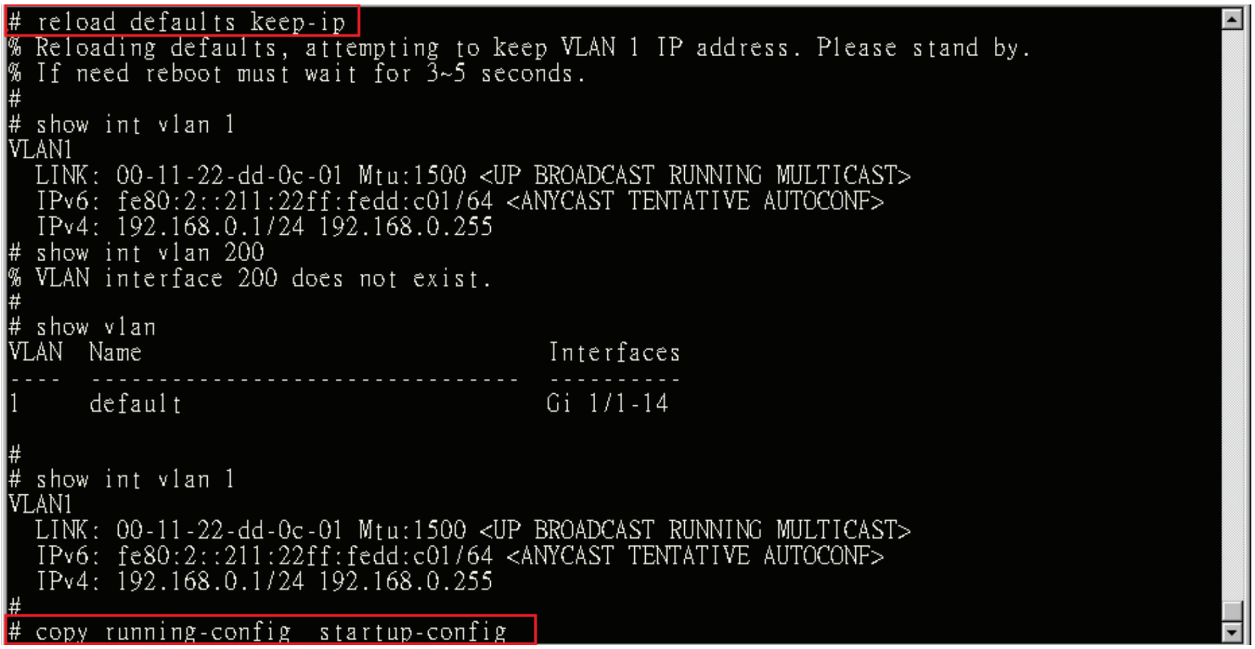
3.13 RESET TO DEFAULT AND SAVE CONFIGURATION

CONFIGURATION VIA CLI COMMAND

To see what the current interface and IP address is and if the manager wants to reset the configuration to default but keep the management IP setting:

1. Execute this command: reload defaults keep-ip
2. Check the interface VLAN and IP address, confirm only if the management IP setting is kept.
3. Execute this command: copy running-config startup-config

CHAPTER 3: INSTALLATION

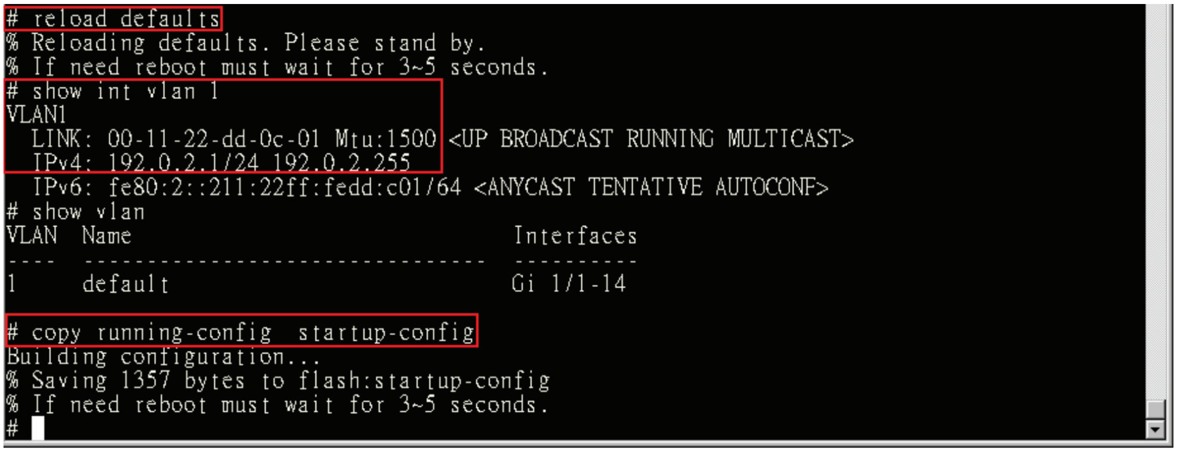


```
# reload defaults keep-ip
% Reloading defaults, attempting to keep VLAN 1 IP address. Please stand by.
% If need reboot must wait for 3~5 seconds.
#
# show int vlan 1
VLAN1
  LINK: 00-11-22-dd-0c-01 Mtu:1500 <UP BROADCAST RUNNING MULTICAST>
  IPv6: fe80:2::211:22ff:fedd:c01/64 <ANYCAST TENTATIVE 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
```

FIGURE 3-17. RESET CONFIGURATION BUT KEEP MANAGEMENT IP SETTING

To reset all configurations to default:

1. Execute this command: reload defaults
2. Check the interface VLAN and IP address, confirm that they all changed to the default setting.
3. Execute this command: copy running-config startup-config



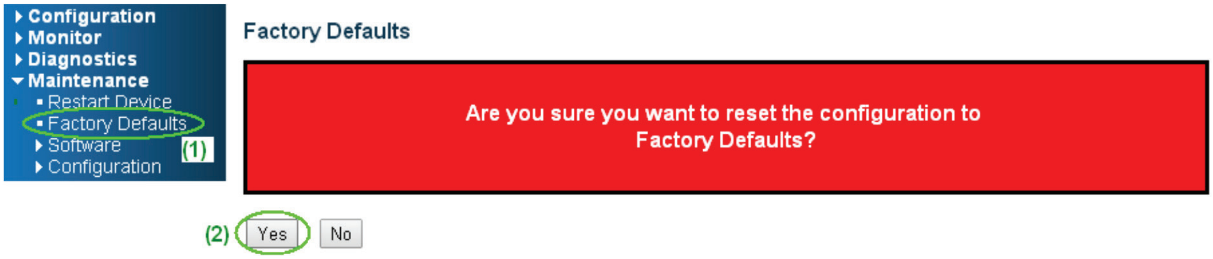
```
# reload defaults
% Reloading defaults. Please stand by.
% If need reboot must wait for 3~5 seconds.
# show int vlan 1
VLAN1
  LINK: 00-11-22-dd-0c-01 Mtu:1500 <UP BROADCAST RUNNING MULTICAST>
  IPv4: 192.0.2.1/24 192.0.2.255
  IPv6: fe80:2::211:22ff:fedd:c01/64 <ANYCAST TENTATIVE AUTOCONF>
# show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

FIGURE 3-18. RESET ALL CONFIGURATIONS

CONFIGURATION VIA WEB UI

If the manager wants to reset the configuration to default but keep the management IP setting:

1. Go to Maintenance —> Factory Defaults page and click the Yes button.

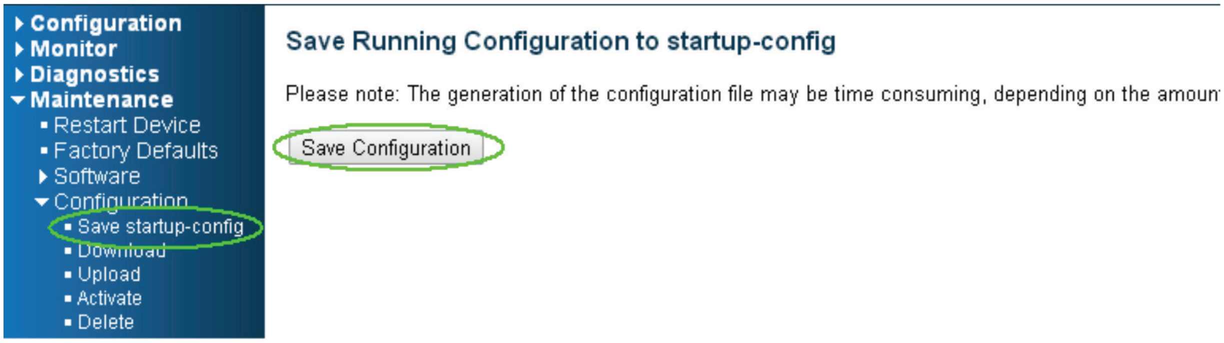


Factory Defaults

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

FIGURE 3-19. RESET TO FACTORY DEFAULTS SCREEN

2. Go to Maintenance —> Configuration —> Save startup-config pagination, then click the Save Configuration button, then reset.



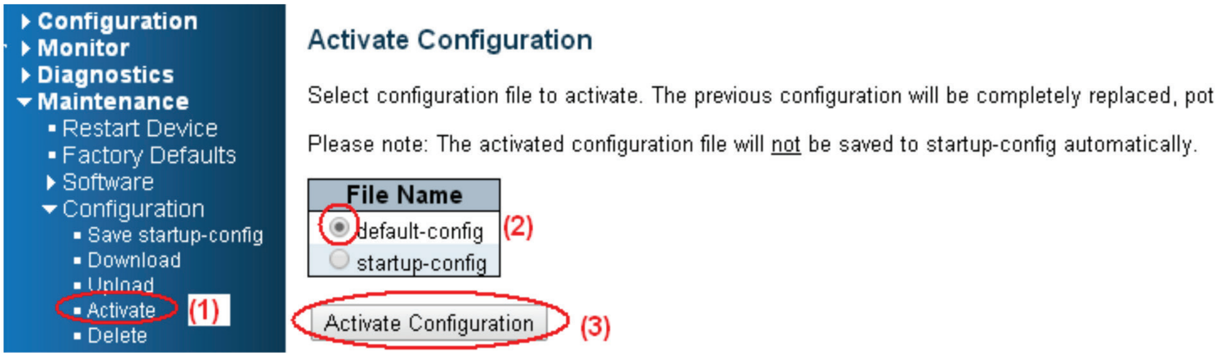
Save Running Configuration to startup-config

Please note: The generation of the configuration file may be time consuming, depending on the amoun

FIGURE 3-20. SAVE CONFIGURATION SCREEN

To reset all configurations to defaults:

1. Go to the Maintenance —> Configuration —> Activate page, select default-config, then click the Activate Configuration button.



Activate Configuration

Select configuration file to activate. The previous configuration will be completely replaced, pot

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

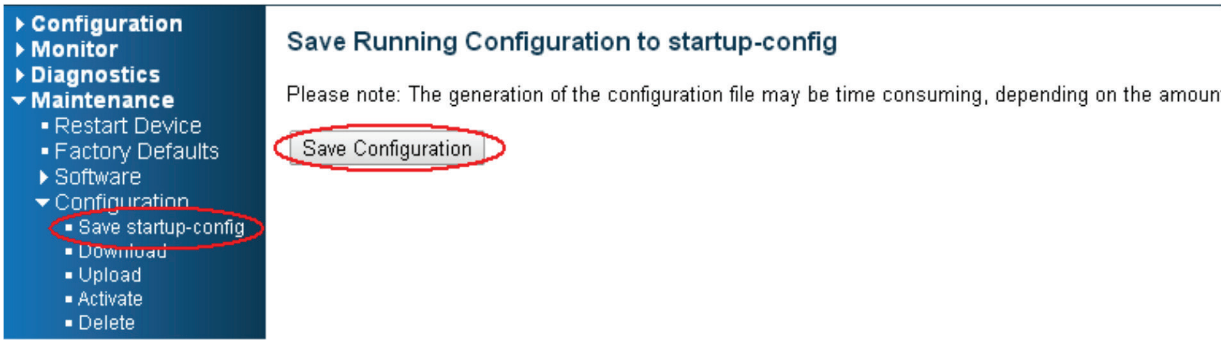
File Name
● default-config
○ startup-config

FIGURE 3-21. ACTIVATE CONFIGURATION SCREEN

2. Change the PC’s IP address to an address in the 192.0.2.X network.

3. Change the Web’s IP to 192.0.2.1 (default IP).

4. Go to the Maintenance —> Configuration —> Save startup-config page, then click the Save Configuration button to reset.



Save Running Configuration to startup-config

Please note: The generation of the configuration file may be time consuming, depending on the amoun

FIGURE 3-22. SAVE CONFIGURATION SCREEN

3.14 LED STATUS INDICATORS

TABLE 3-2. LED STATUS INDICATORS

LED NAME	INDICATOR /COLOR	CONDITION
P1	On Green	P1 power line has power
	Off	P1 power line is disconnected or does not have supply power
P2	On Green	P2 power line has power
	Off	P2 power line is disconnected or does not have supply power
Alarm	On Red	Alarm event occurs
	Off	No alarm
Copper port 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 port Speed	On Yellow	A 100 Mbps or a 1000 Mbps connection is detected
	Off	No link or a 10 Mbps connection is detected
SFP port Link/Act	On Green	Ethernet link up
	Off	Ethernet link down
SFP port Speed	On Yellow	SFP port speed 1000 Mbps connection is detected.
	Off	No link or a SFP port speed 100 Mbps connection is detected
POE MANAGED SERIES ONLY		
RR (Ring Role)	On Green	One of 3 Ring group is enabled and is Master role.
	Off	Ring is slave role
RS (Ring Status)	On Green	Ring fail is detected
	Off	No ring fail detected
PoE	On Yellow	PoE is detected
	Off	No link

CHAPTER 4: VLAN APPLICATION

This chapter describes how to configure Virtual LANs (VLANs) in the switch. The switch 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.

4.1 EXAMPLE 1: DEFAULT VLAN SETTINGS

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

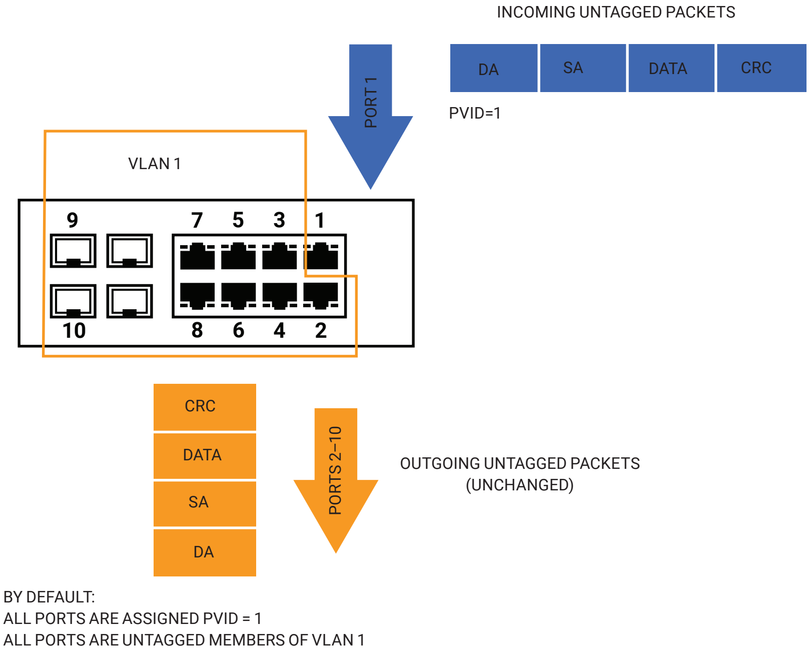

INCOMING UNTAGGED PACKETS
PORT 1
DA
SA
DATA
CRC
PVID=1
VLAN 1
9
7
5
3
1
10
8
6
4
2
CRC
DATA
SA
DA
PORTS 2–10
OUTGOING UNTAGGED PACKETS
(UNCHANGED)
BY DEFAULT:
ALL PORTS ARE ASSIGNED PVID = 1
ALL PORTS ARE UNTAGGED MEMBERS OF VLAN 1

FIGURE 4-1. VLAN EXAMPLE 1

4.2 EXAMPLE 2: PORT-BASED VLANS

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

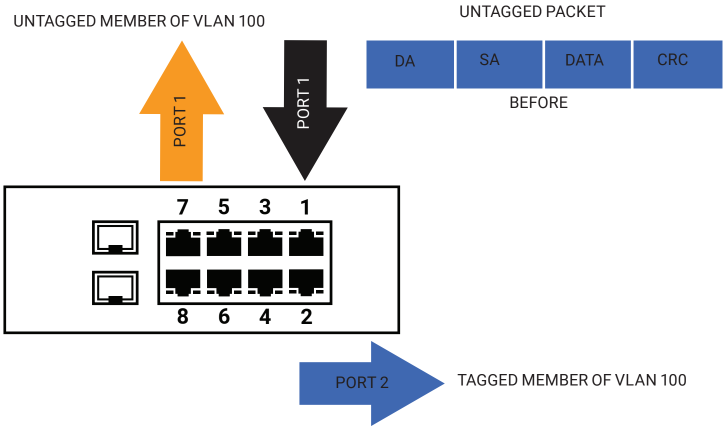
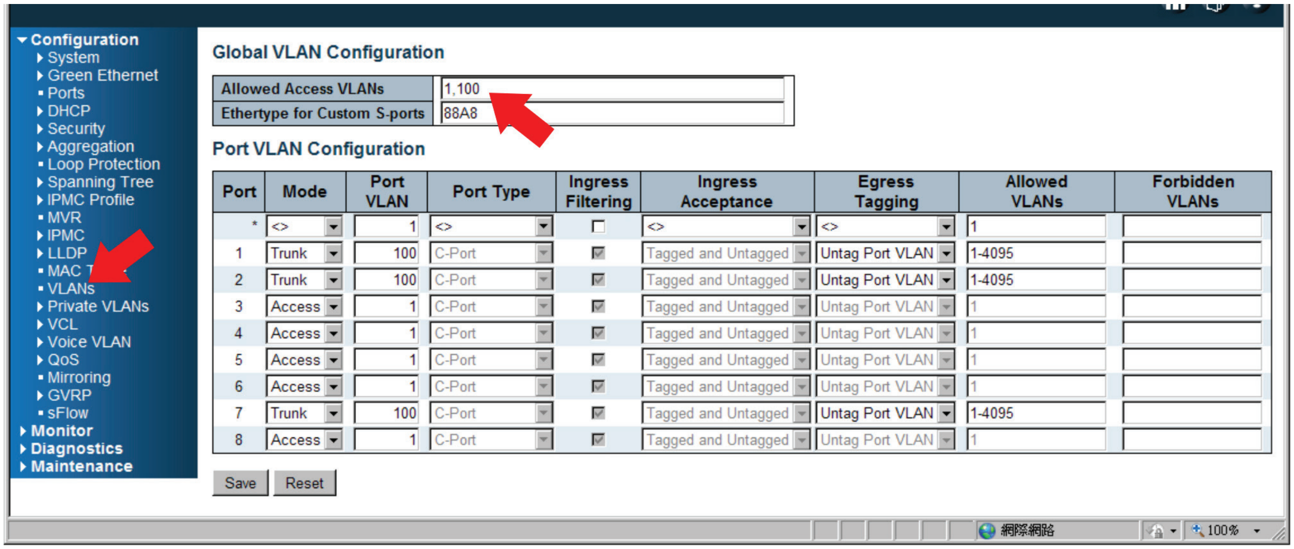


FIGURE 4-2. VLAN EXAMPLE 2

CONFIGURATION

STEP 1: Go to Configuration -> VLANs -> Port VLAN configuration 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	<>	□	<>	<>	1	
1	Trunk	100	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
2	Trunk	100	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
7	Trunk	100	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1-4095	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

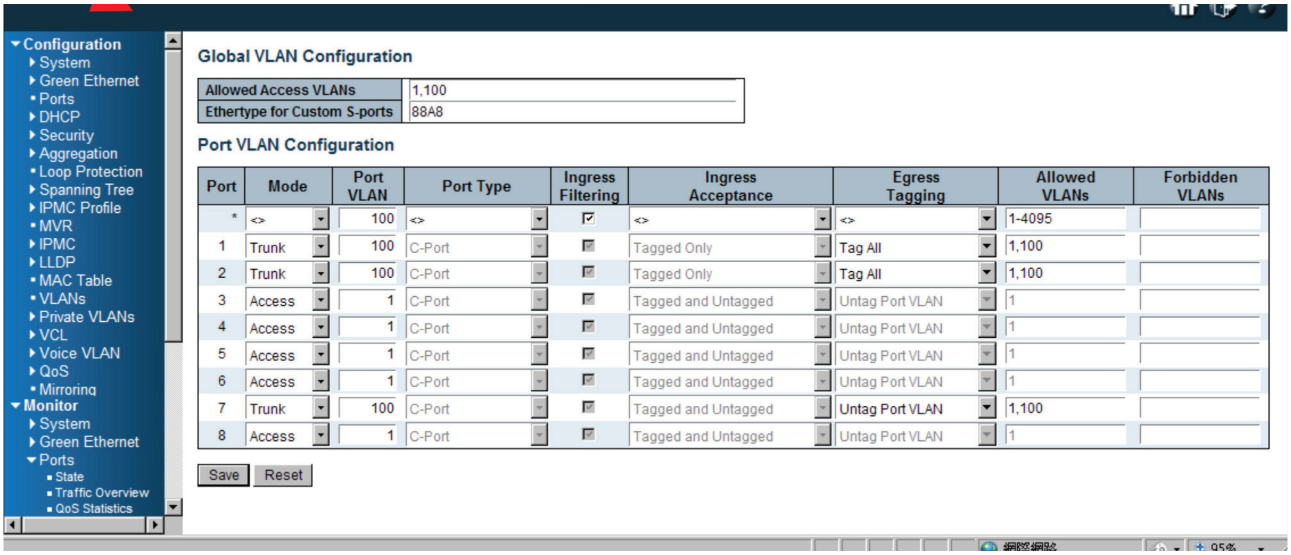
FIGURE 4-3. PORT-BASED VLAN CONFIGURATION

STEP 2: Select Configuration -> VLAN -> Static VLAN. Create a VLAN with VLAN ID 100. Enter a VLAN name in the Name field.

STEP 3: Assign VLAN tag setting to or remove it from a port by toggling the check box under an 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.

Here we set tagged VLAN100 on Port 1 and Port 2, untagged VLAN100 on Port7.



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
*	<>	100	<>	☑	<>	<>	1-4095	
1	Trunk	100	C-Port	☑	Tagged Only	Tag All	1,100	
2	Trunk	100	C-Port	☑	Tagged Only	Tag All	1,100	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
7	Trunk	100	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1,100	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

FIGURE 4-4. SET TAGGED AND UNTAGGED VLANS

STEP 4: Transmit untagged unicast packets from Port 1 to Port 2 and Port 7. The switch 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.

STEP 5: Transmit untagged unicast packets from Port 2 to Port 1 and Port 7. The switch 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.

STEP 6: Transmit untagged unicast packets from Port 7 to Port 1 and Port 2. The switch 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.

STEP 7: Repeat step 4 using broadcast and multicast packets.

CLI COMMAND

```
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
```

4.3 EXAMPLE 3: IEEE 802.1Q TAGGING

The switch is able to construct a 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. Hosts in different VLANs cannot communicate with each other directly.

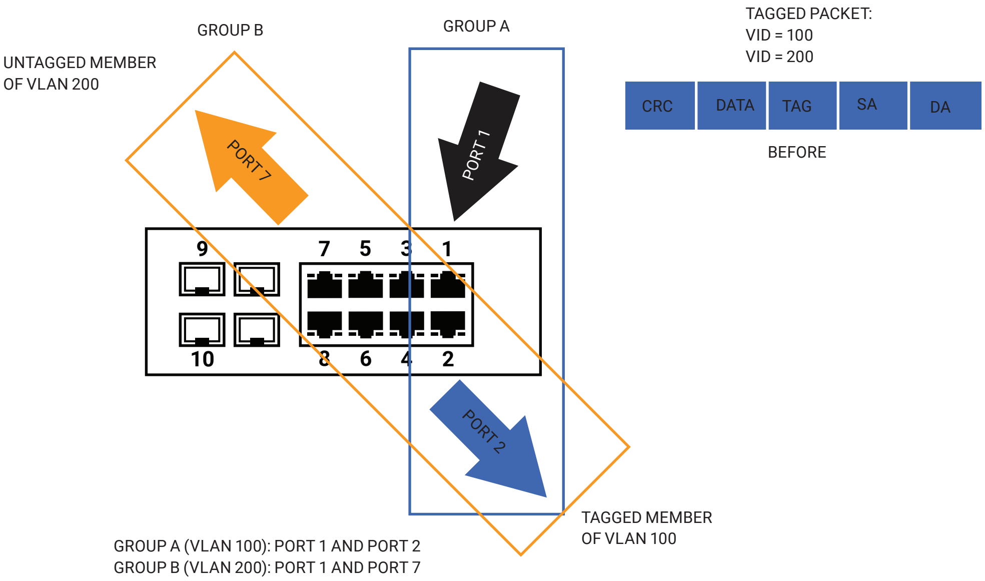


FIGURE 4-5. IEEE 802.1Q TAGGING EXAMPLE

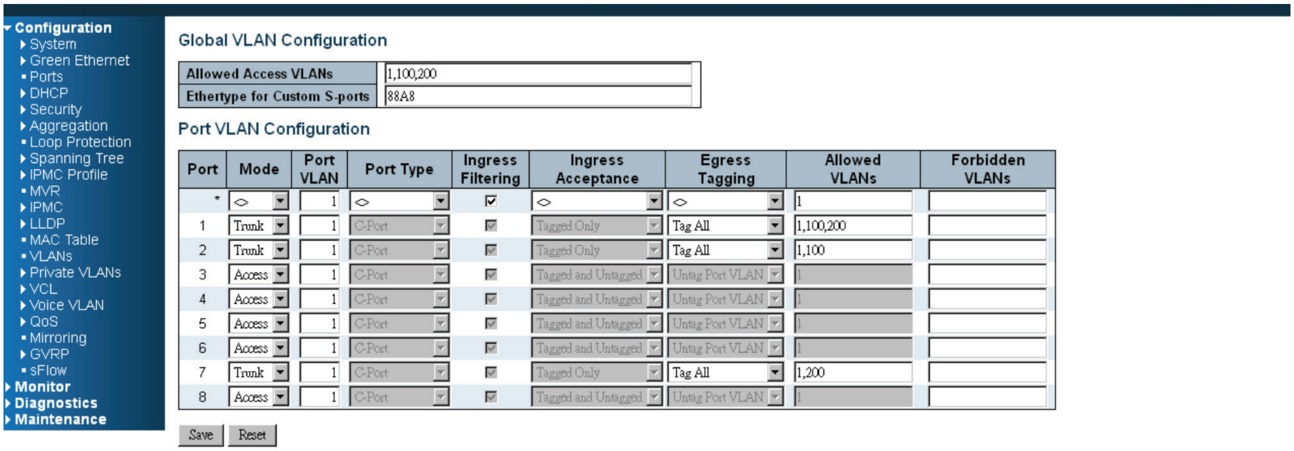
In this case:

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.
4. Both the Group A and Group B can go to Internet through the switch.

CHAPTER 4: VLAN APPLICATION

CONFIGURATION

STEP 1: Go to C configuration -> VLANs -> Port VLAN configuration page specify the VLAN membership as follows:



Global VLAN Configuration

Allowed Access VLANs	1,100,200
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	<>	☑	<>	<>	1	
1	Trunk	1	C-Port	☑	Tagged Only	Tag All	1,100,200	
2	Trunk	1	C-Port	☑	Tagged Only	Tag All	1,100	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
7	Trunk	1	C-Port	☑	Tagged Only	Tag All	1,200	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

FIGURE 4-6. EXAMPLE 3 CONFIGURATION SCREEN

STEP 2: Transmit unicast packets with VLAN tag 100 from Port 1 to Port 2 and Port 7. The switch should tag it with VID 100. The packet only has access to Port 2. For Port 2, the outgoing packet leaves as a tagged packet with VID 100.

STEP 3: Transmit unicast packets with VLAN tag 200 from Port 1 to Port 2 and Port 7. The switch should tag it with VID 200. The packet only has access to Port 7. The outgoing packet on Port 7 is stripped of its tag as an untagged packet.

STEP 4: Transmit unicast packets with VLAN tag 100 from Port 2 to Port 1 and Port 7. The switch 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.

STEP 5: Transmit unicast packets with VLAN tag 200 from Port 7 to Port 1 and Port 2. The switch 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.

STEP 6: Repeat the above steps using broadcast and multicast packets.

CLI COMMAND

```
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
```

CHAPTER 5: SECURITY APPLICATION

ACL 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 Marking, and Copy Frame. The user can set the default ACL rule to Permit or Deny.

TABLE 5-1. ACL FUNCTIONS

DEFAULT ACL RULE	ACTIONS				
	DENY	PERMIT	QUEUE MAPPING	COS MARKING	COPY FRAME
Permit	(a)	(b)	(c)	(d)	(e)
Deny	(f)	(g)	(h)	(i)	(j)

Brief descriptions of the table above:

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

(b): Permit all frames.

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

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

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

(f): Deny all frames.

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

(h): Deny all frames.

(i): Deny all frames.

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

5.1 CASE 1: ACL FOR MAC ADDRESS

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

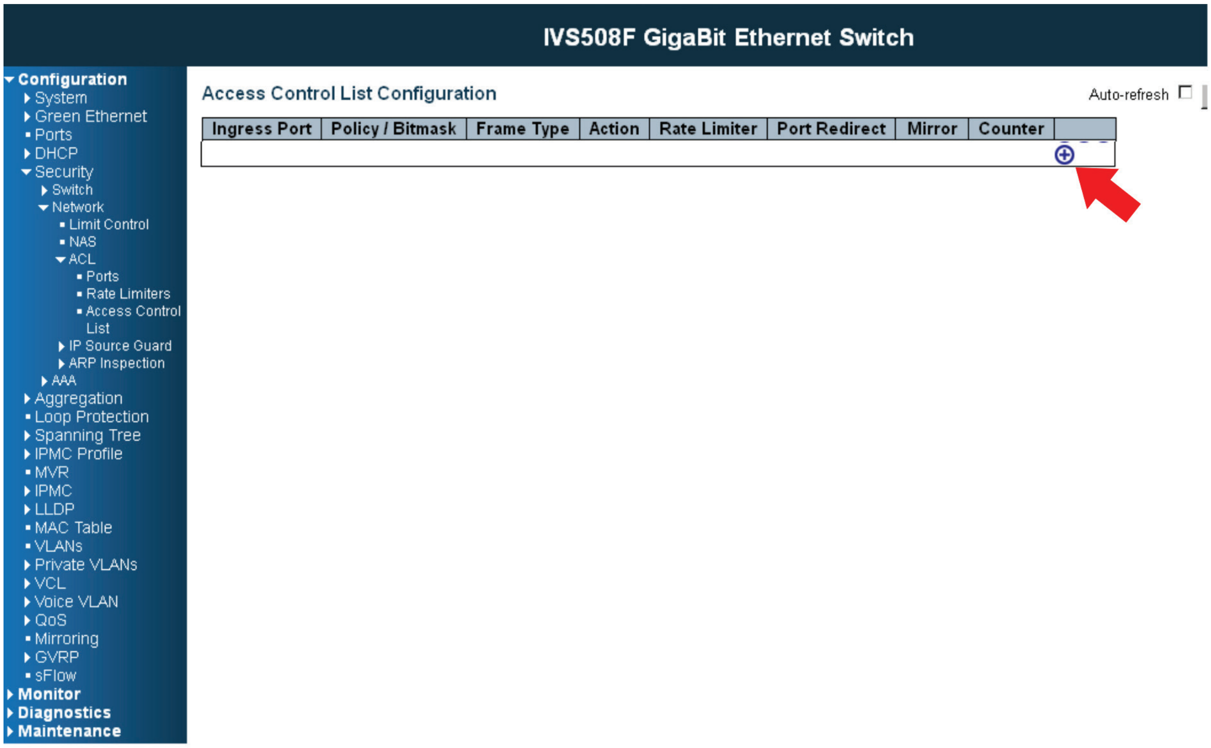
To filter only one directional MAC address, set the other MAC address to all zeroes. Besides MAC address, the switch also supports VLAN and Ether type for filter additionally. Certain VLAN or Ether type under these MAC address will take effect. If the user doesn’t care if the switch uses VLAN or Ether type, he can just set to zero values. Following are examples:

CASE 1A

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

One directional MAC address with one VLAN deny filtering.

STEP 1: Create a new ACL Profile. (Profile Name: DenySomeMac)



Access Control List Configuration

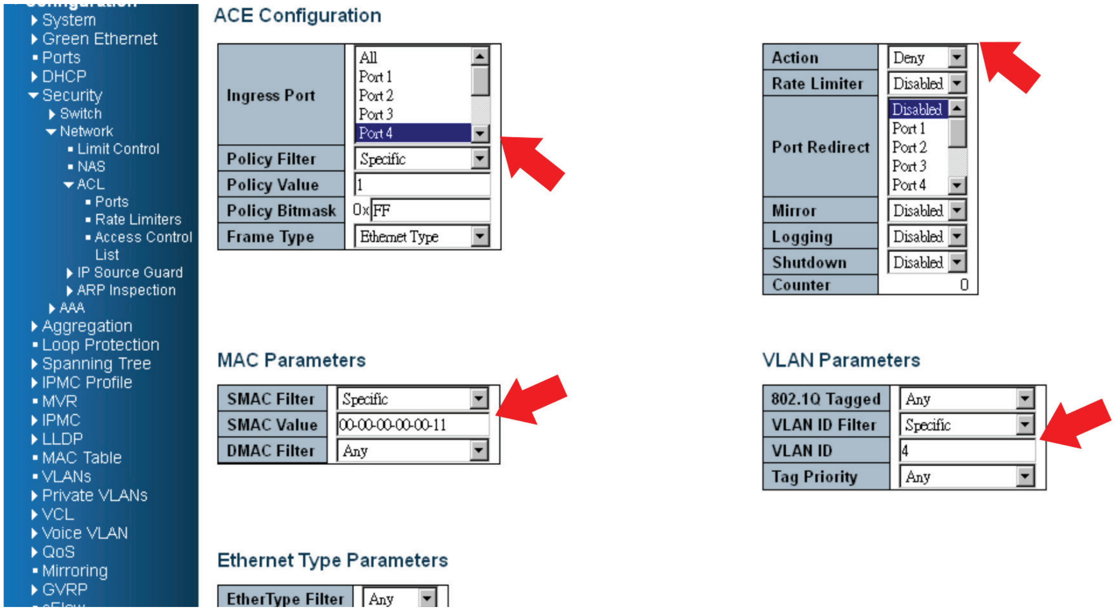
Auto-refresh □

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

FIGURE 5-1. CREATE A NEW ACL PROFILE SCREEN

STEP 2: Create a new ACL Entry rule under this ACL profile. (Deny MAC: 11 and VLAN: 4)

STEP 3: Bind this ACL profile to a GE port. (PORT-4)



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

FIGURE 5-2. BIND ACL PROFILE SCREEN

STEP 4: Send frames between PORT-3 and PORT-4, and see the test result.

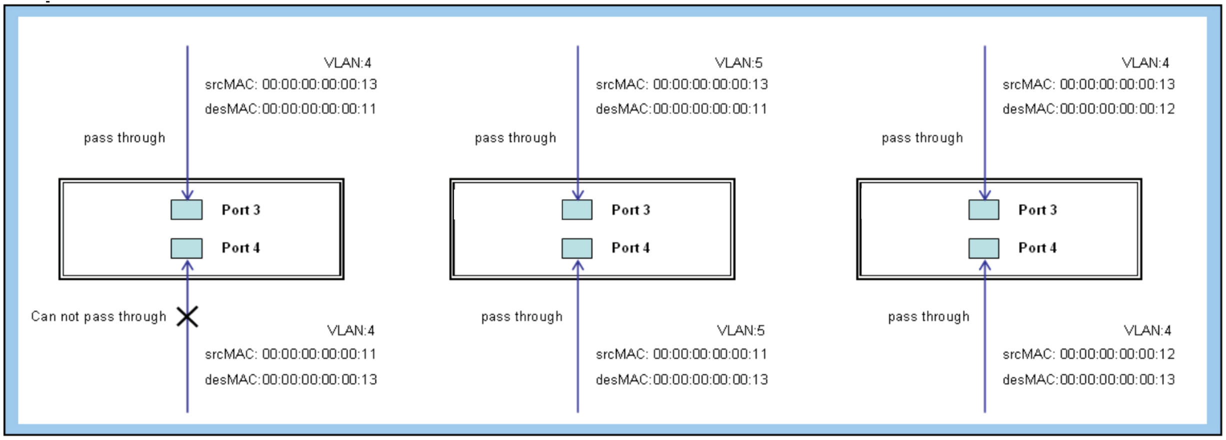


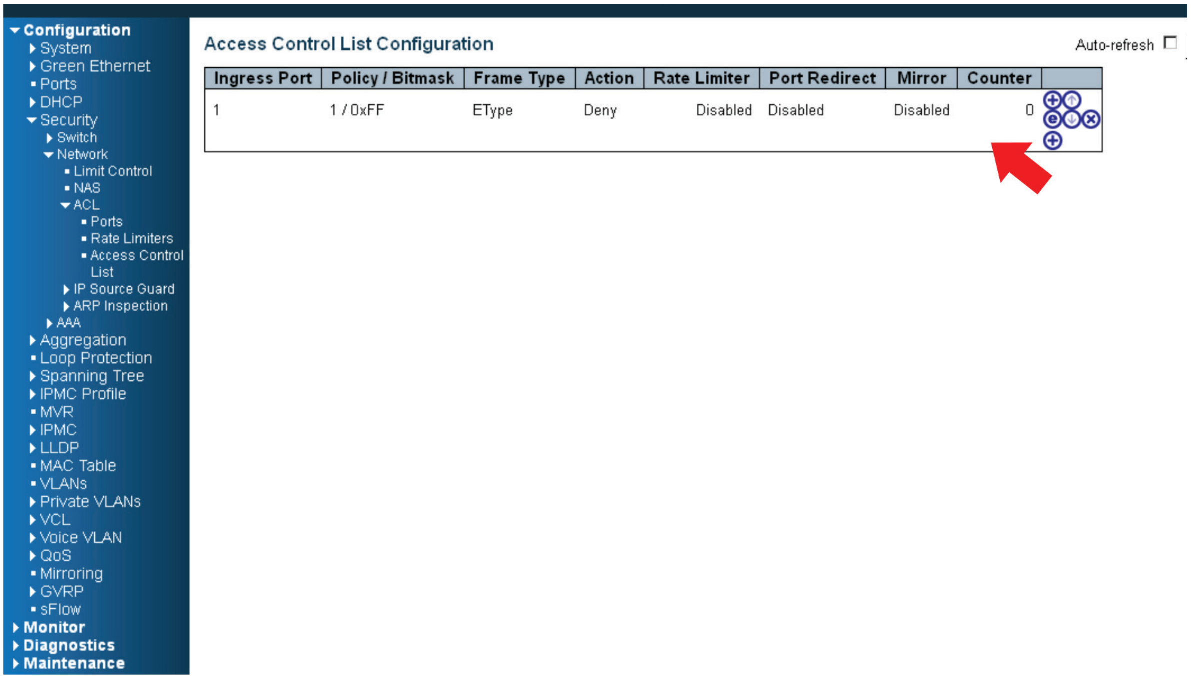
FIGURE 5-3. TEST RESULT SCREEN

CLI COMMAND

```
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
```

Two directional MAC address with all VLANs denying filtering.

STEP 1: Create a new ACL Profile. (Profile Name: DenySomeMac)



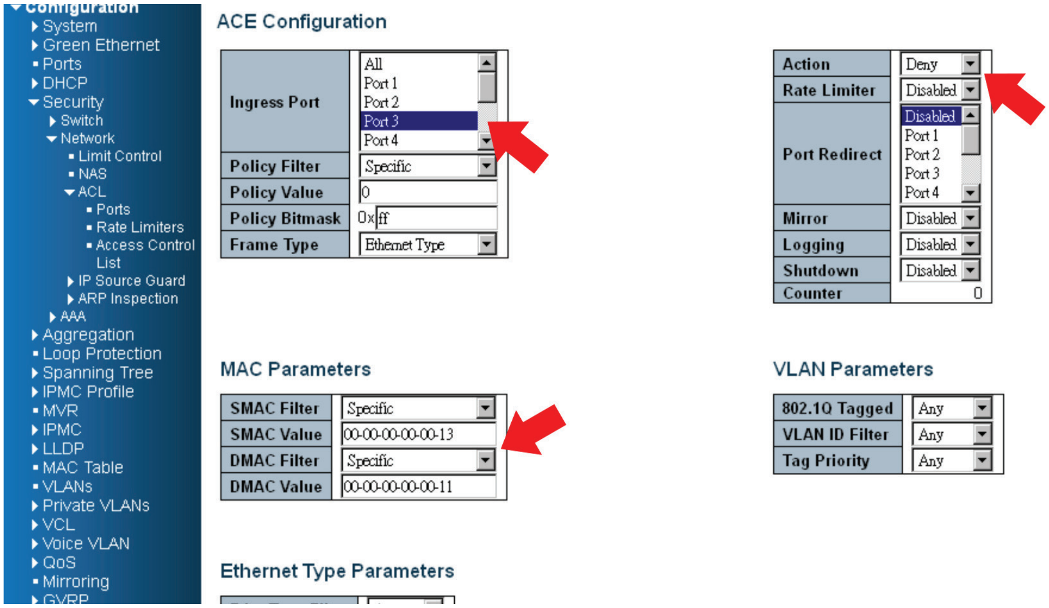
Access Control List Configuration

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

FIGURE 5-4. ACL CONFIGURATION SCREEN

STEP 2: Create a new ACL Entry rule under this ACL profile. (Deny SrcMAC: 13 and DesMAC: 11)

STEP 3: Bind this ACL profile to a GE port. (PORT-3)



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

FIGURE 5-5. BIND ACL PROFILE TO GE PORT SCREEN

Step 4: Send frames between PORT-3 and PORT-4, and see test result.

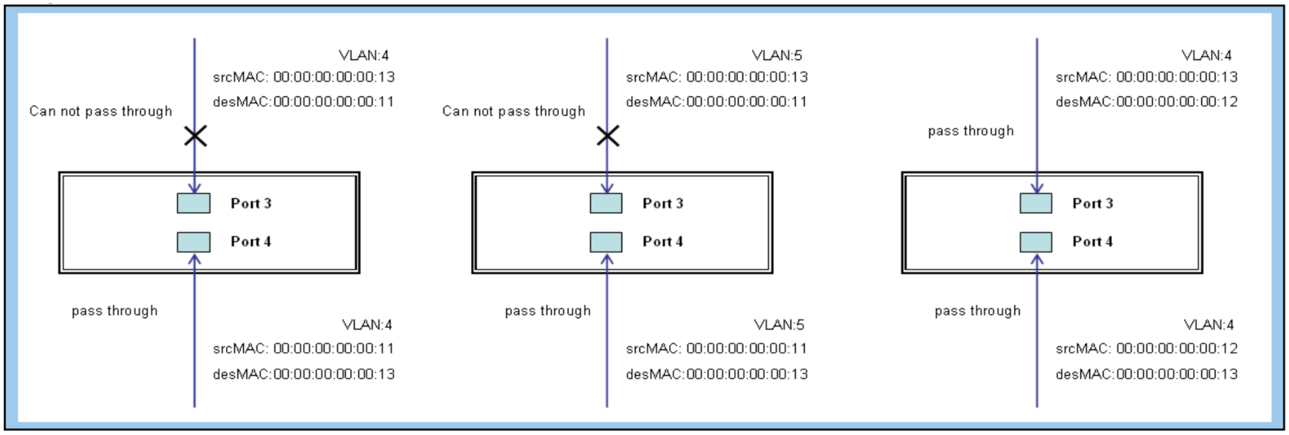


FIGURE 5-6. TEST RESULT

CLI COMMAND

```
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
```

CASE 1B

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

CASE 1C

User can set the default ACL Rule of GE port as “Permit”, then 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 1D

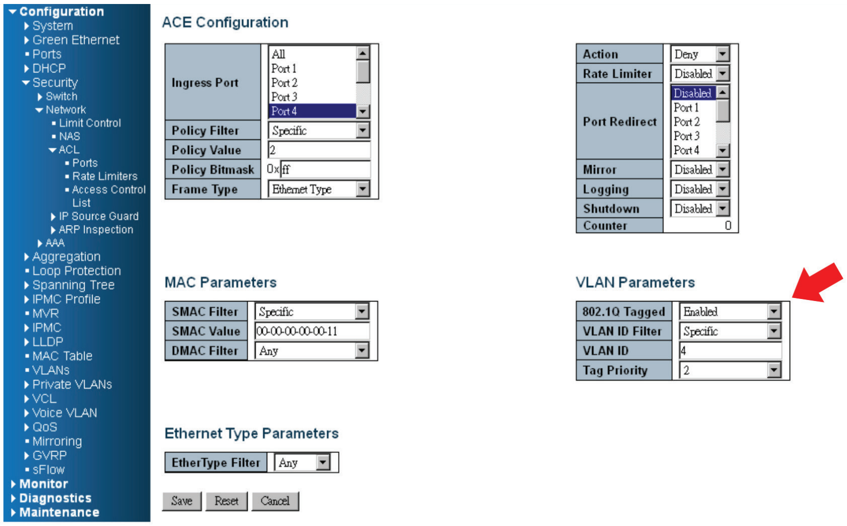
User can set default ACL Rule of GE port as “Permit”, then bind a suitable profile with “CoS Marking” action for some ACL function. It means the GE port can remark CoS of the VLAN frame received from this port.

One directional MAC address with CoS Marking action. (one VLAN, and don’t care Ether Type)

STEP 1: Create a new ACL Profile. (Profile Name: CoSMarkingTest)

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

STEP 3: Bind this ACL profile to a GE port. (PORT-4)



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

FIGURE 5-7. CASE 1D SCREEN

STEP 4: Send frames between PORT-3 and PORT-4, and see the test result.

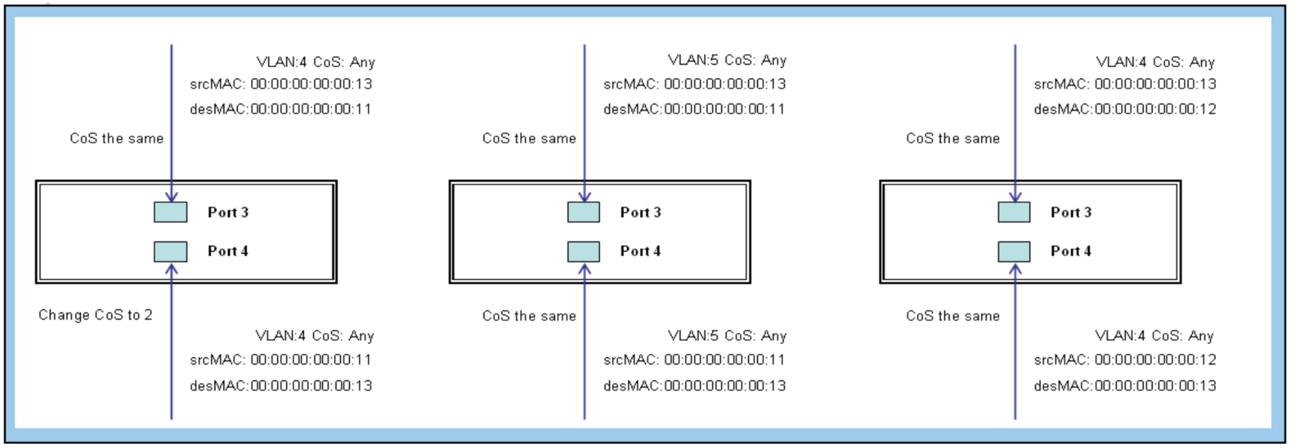


FIGURE 5-8. TEST RESULT

CLI COMMAND

```
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
```

CASE 1E

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

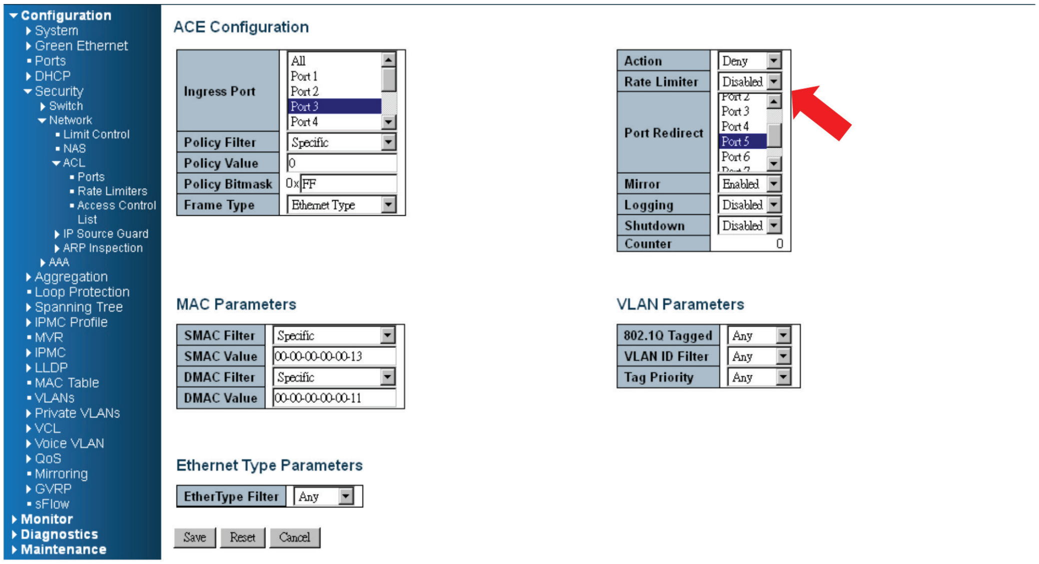
Two directional MAC address with Copy Frame action. (Don’t care VLAN ID, Ether Type)

STEP 1: Create a new ACL Profile. (Profile Name: CopyFrameTest)

STEP 2: Create a new ACL Entry rule under this ACL profile. (SrcMAC: 13 and DesMAC: 11)

STEP 3: Set analyzer port to enable and mirror analyzer port.

STEP 4: Bind this ACL profile to a GE port. (PORT-3)



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 2 Port 3 Port 4 Port 5 Port 6 Port 7
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

FIGURE 5-9. CASE 1E SCREEN

STEP 5: Send frames between PORT-3 and PORT-4, and see test result.

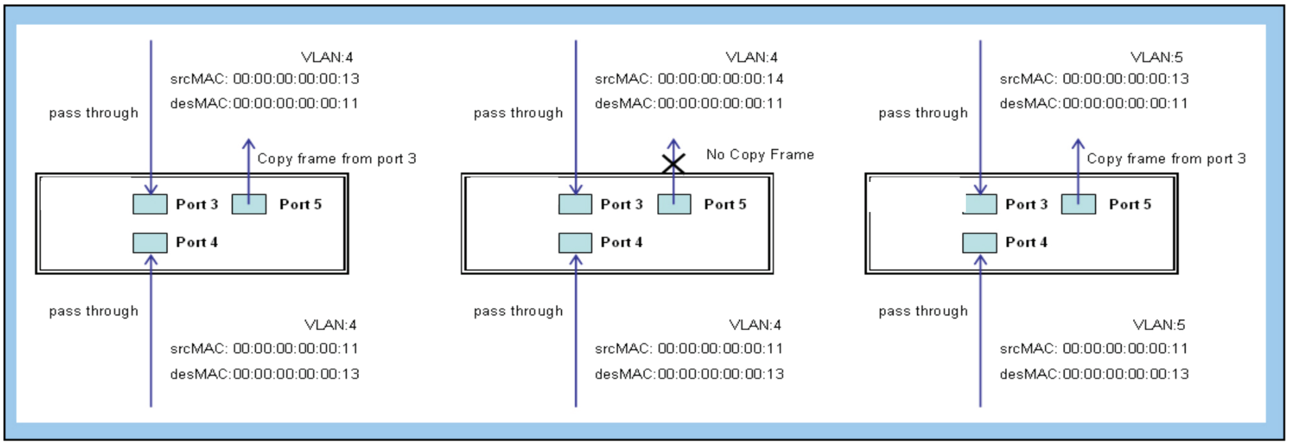


FIGURE 5-10. TEST RESULT

CLI COMMAND

```
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
```

CASE 1F

This case means all frames will not pass through.

CASE 1G

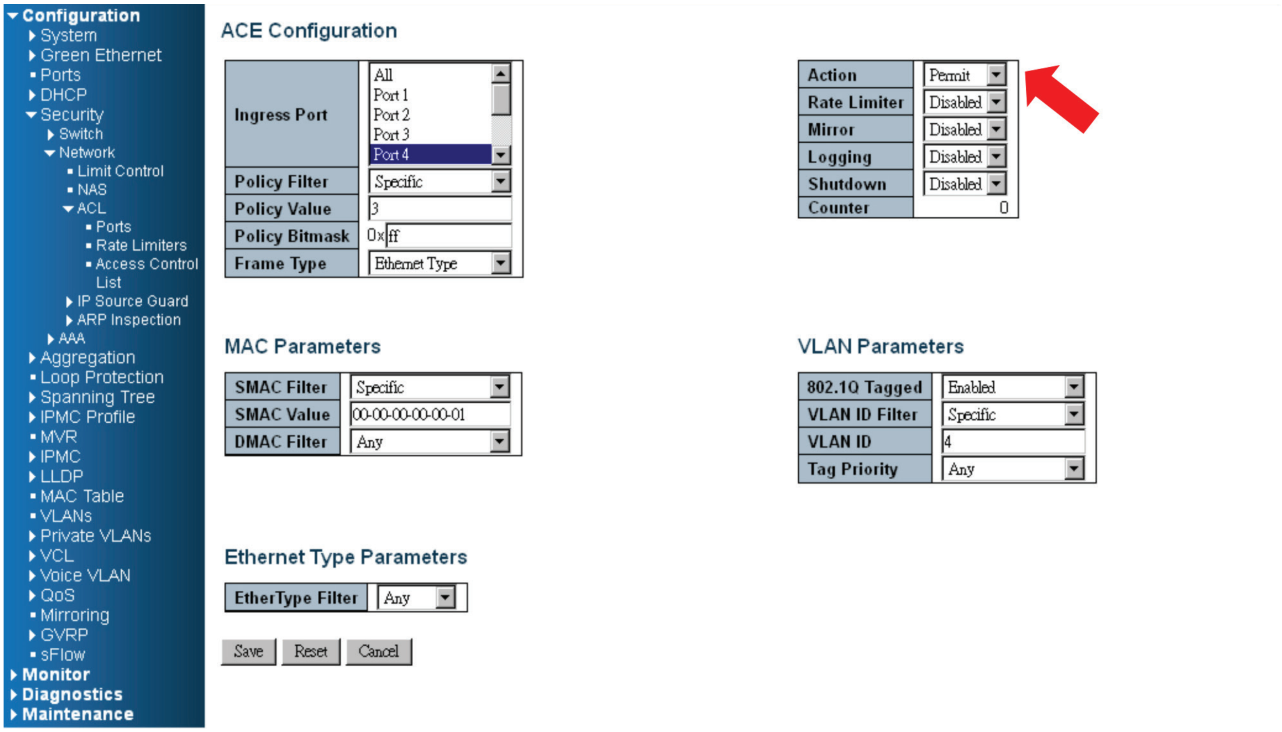
User can set default ACL Rule of GE port as “Deny”, then bind a suitable profile with “Permit” action for ACL. It means the GE port cannot pass through all packets but the ACL entry of the profile binding.

One directional MAC address with one VLAN permit filtering.

STEP 1: Create a new ACL Profile. (Profile Name: AllowSomeMac)

STEP 2: Create a new ACL Entry rule under this ACL profile. (Allow MAC: 11 and VLAN: 4)

STEP 3: Bind this ACL profile to a GE port. (PORT-4)



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

FIGURE 5-11. ACL PROFILE BINDING

STEP 4: Send frames between PORT-3 and PORT-4, and see test result.

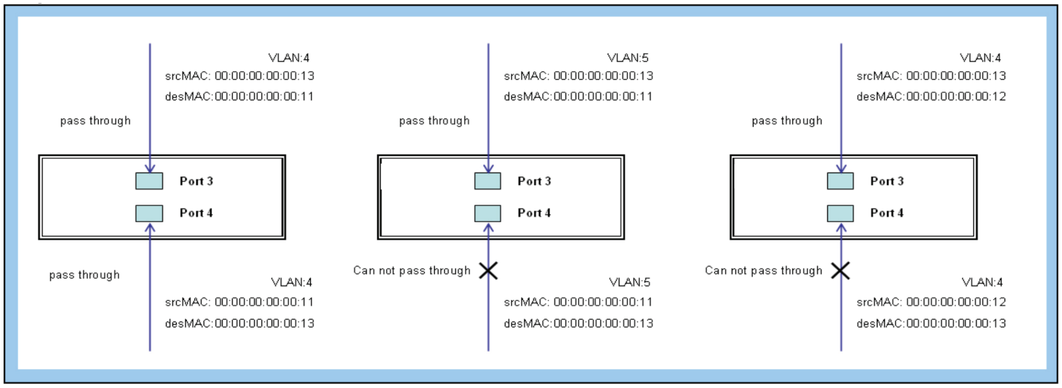


FIGURE 5-12. TEST RESULT

CLI COMMAND

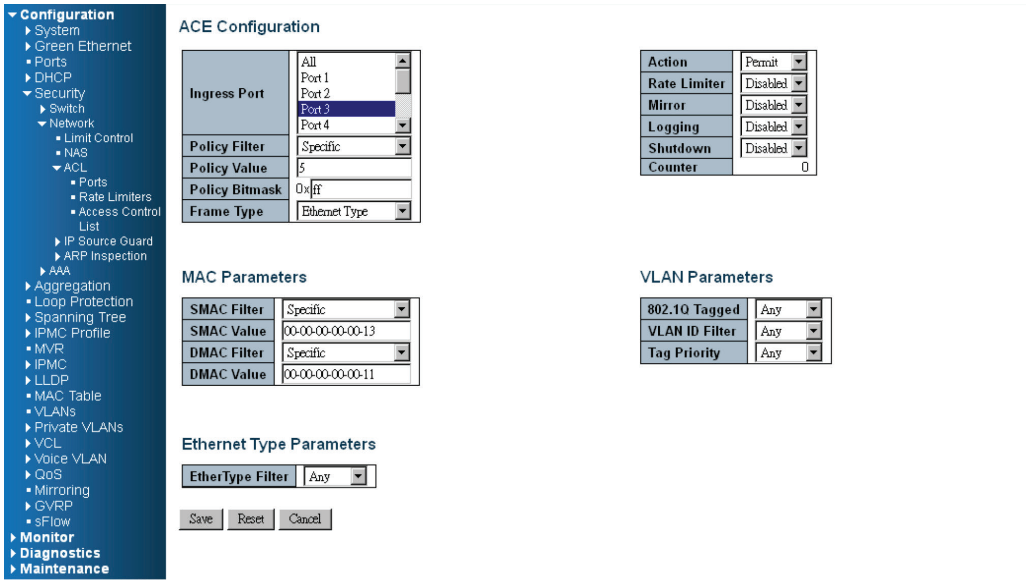
```
access-list ace 4 ingress interface GigabitEthernet 1/4 policy 3 tag tagged vid 4 frametype etype smac 00-00-00-00-00-11
exit
 interface GigabitEthernet 1/3
 switchport trunk allowed vlan 4,5
 switchport trunk vlan tag native
!
interface GigabitEthernet 1/4
 switchport trunk allowed vlan 4,5
 switchport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

Two directional MAC address with all VLAN permit filtering.

STEP 1: Create a new ACL Profile. (Profile Name: AllowSomeMac)

STEP 2: Create a new ACL Entry rule under this ACL profile. (Allow SrcMAC: 13 and DesMAC: 11)

STEP 3: Bind this ACL profile to a GE port. (PORT-3)



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

FIGURE 5-13.

STEP 4: Send frames between PORT-3 and PORT-4, see test result.

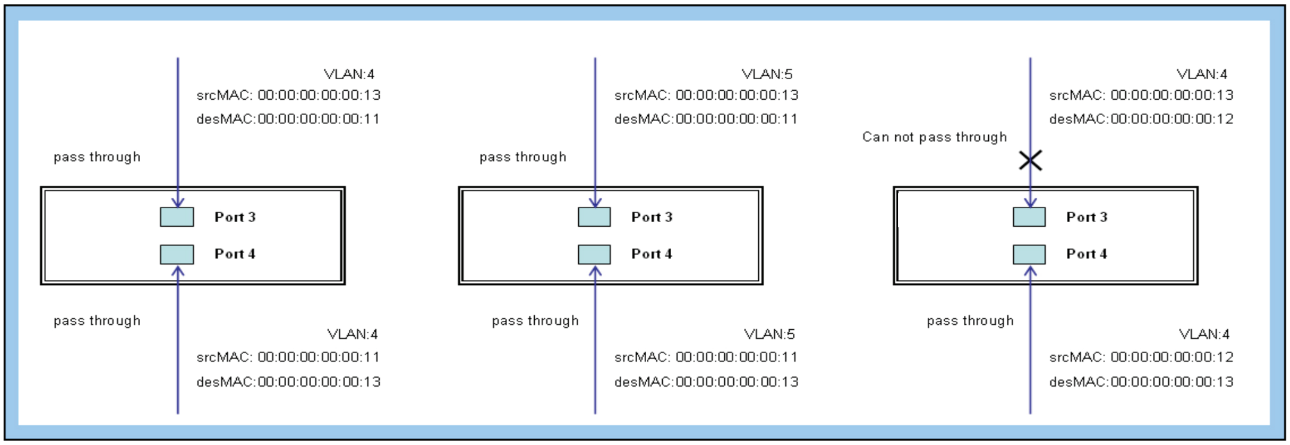


FIGURE 5-14.

CLI COMMAND

```
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
```

CASE 1H

Because the default ACL Rule of GE port is “Deny”, Queue Mapping action does not apply. We do not do this case.

CASE 1I

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

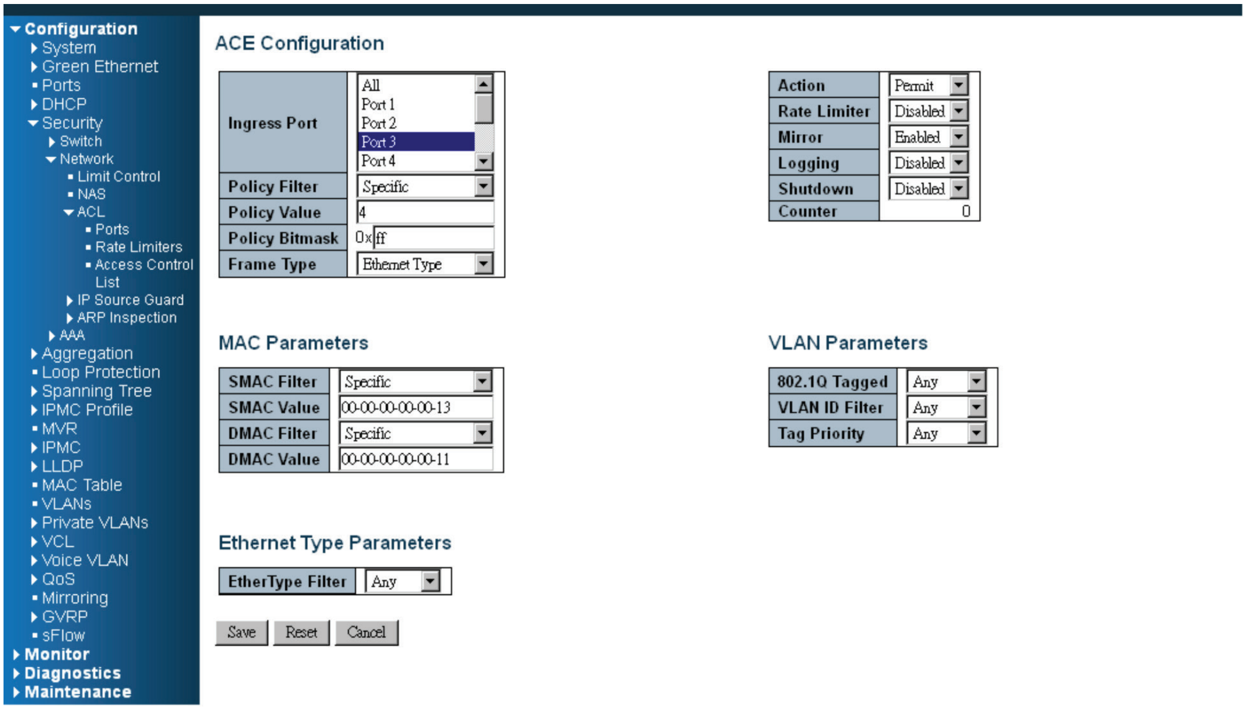
CASE 1J

User can set default ACL Rule of GE port as "Deny", then bind a suitable profile with "Copy Frame" action for mirror analyzer used. It means the system will copy frames from the binding GE Port to the analyzer port. No frames are received from the denied GE port but the mirror analyzer port.

One directional MAC address with Copy Frame action. (Don't case VLAN, Ether Type)

STEP 1: Create a new ACL Profile. (Profile Name: CopyFrameTest)

STEP 2: Create a new ACL Entry rule under this ACL profile. (SrcMAC: 13 and DesMAC: 11)



ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
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

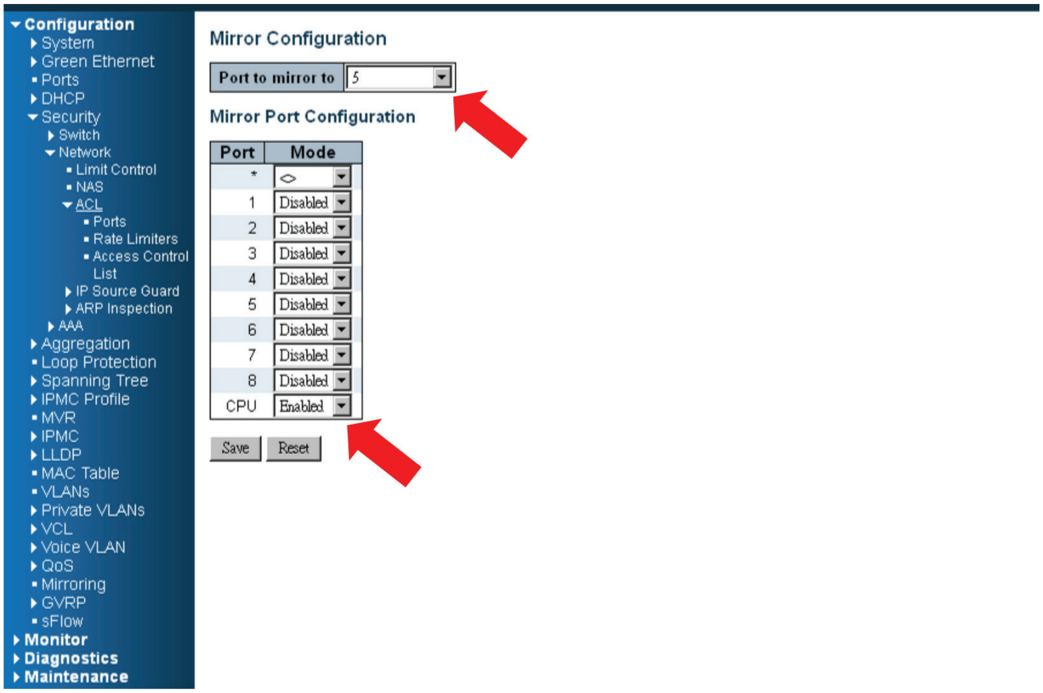
Ethernet Type Parameters

EtherType Filter	Any

FIGURE 5-15.

STEP 3: Bind this ACL profile to a GE port. (PORT-3)

STEP 4: Set the analyzer port to enable and mirror analyzer port.



Mirror Configuration

Port to mirror to: 5

Mirror Port Configuration

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

FIGURE 5-16.

STEP 5: Send frames between PORT-3 and PORT-4, see test result.

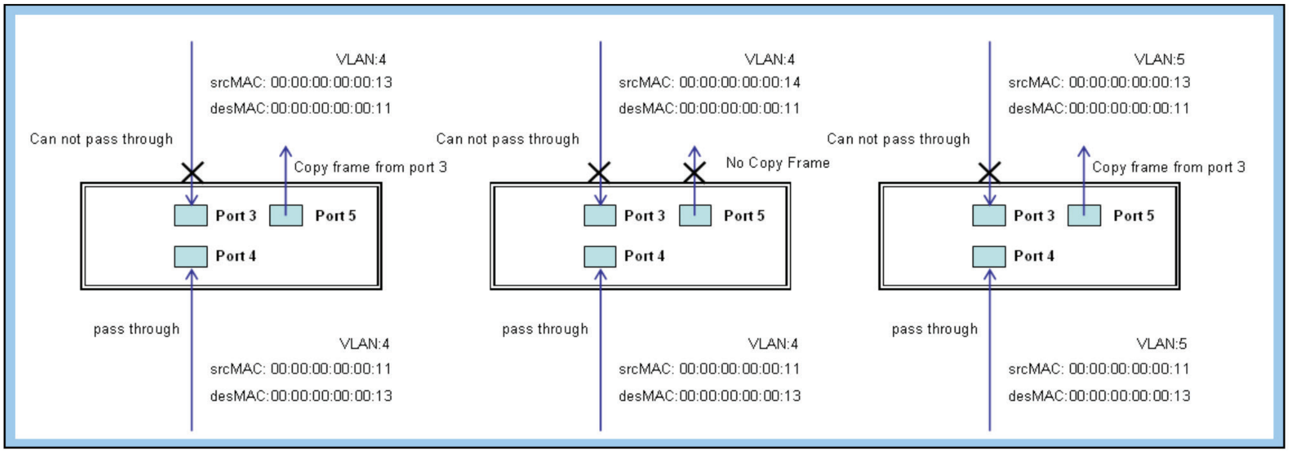


FIGURE 5-17. TEST RESULT

CLI COMMAND

```
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
```

5.2 CASE 2: ACL FOR IP ADDRESS

For IP address ACL, the switch can filter on source IP address, destination IP address, or both. It also supports setting the IP range ACL. When it filters on both IP address, packets that coincide with both rules will take effect. In other words, it does not filter if it only coincides with one rule.

To filter only one directional IP address, set the other IP address to all zero. This means don't care. In addtion to IP address, the switch also supports Protocol filtering. (TCP=6, UDP=17, etc.) Certain Protocols under these IP addresses will take effect. If the user prefers doesn't care Protocol, he can just set this valueto zero. The detailed testing, refer to MAC ACL.

5.3 CASE 3: ACL FOR L4 PORT

For Layer4 port ACL, the switch 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. Users can select to filter on (1)~(4) for all or some specific values, but you should select exactly one Protocol from UDP or TCP.

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

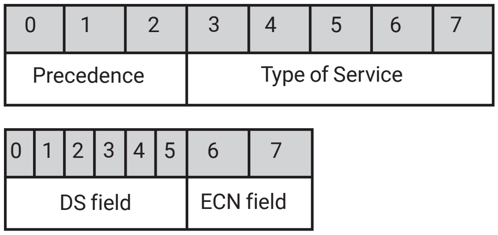
If user wants to filter only one directional IP address or L4 port, set the other IP address and L4 port to all zeroes. This means don't care. For detailed testing, refer to MAC ACL.

5.4 CASE 3: ACL FOR TOS

For Type of Service (ToS) ACL, the switch 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 that coincide with both rules will take effect. In other words, it does not filter if it only coincides with one rule.

To filter only one directional IP address, set the other IP address to all zeroes. It means don't care. For detailed testing, refer to case 1 MAC ACL.

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



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

0	1	2	3	4	5	6	7
DS field						ECN field	

The value (7) is reserved and set to 0.
Ex: Pre (001) means 1
Pre (100) means 4
ToS (00010) means 1
ToS (10000) means 8
DSCP (000001) means 1
DSCP (100000) means 32

FIGURE 5-18. TYPE OF SERVICE ACL

CHAPTER 6: RING VERSION2 APPLICATION

For a reliable network industrial Ethernet applications, the switch provides a mini-second grade failover ring protection; this feature offers a seamless working network even if encountering some issues with connections. This works with twisted-pair and fiber cable.

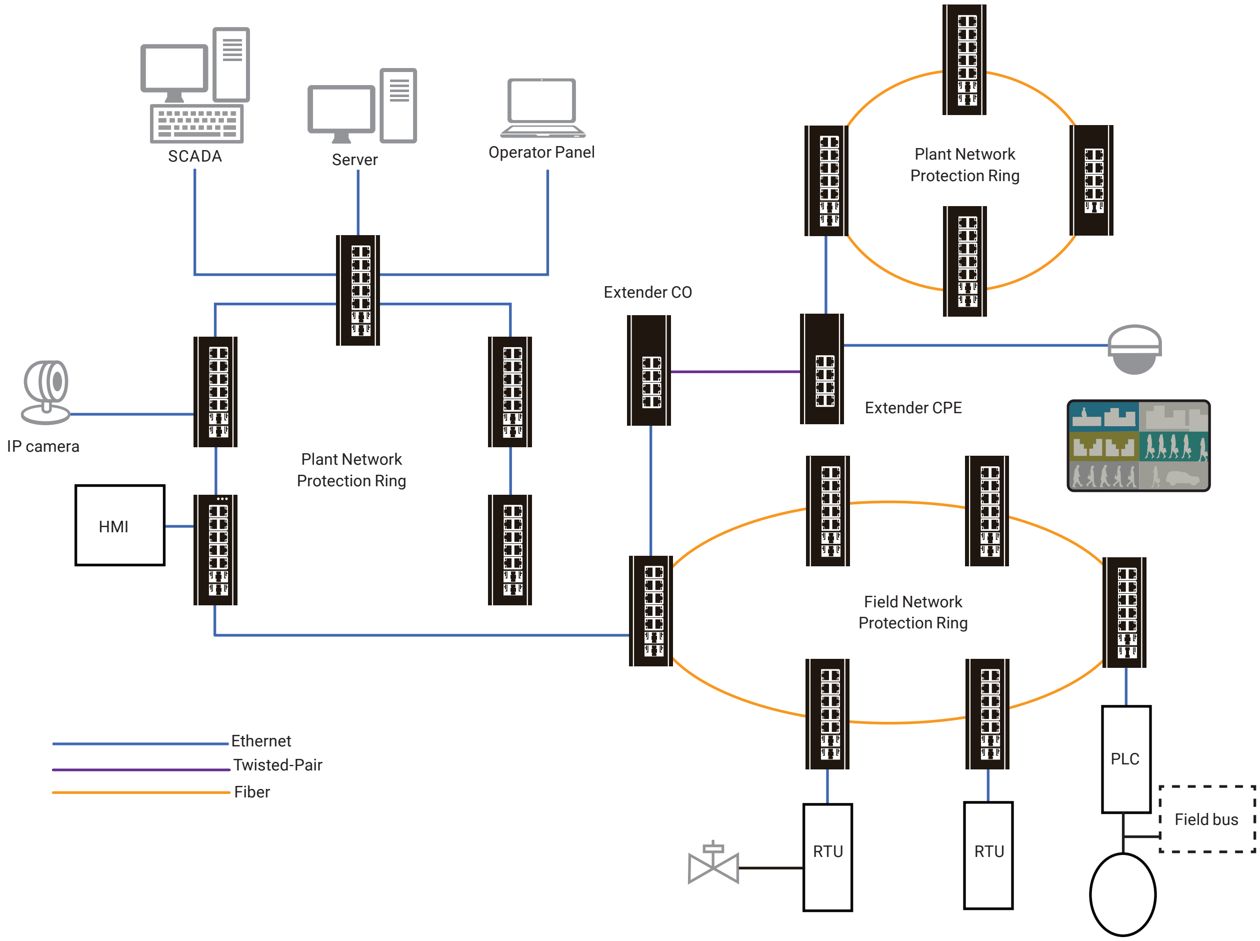


FIGURE 6-1.

6.1 RING VERSION2 FEATURE

Group 1 - This supports the option of ring-master and ring-slave.

- Ring - This could be master or slave.
- When the role is ring master, one ring port is forward port and another is block port. The block port is a redundant port. It is blocked in normal state.
- When the role is ring/slave, both ring ports are forward port.

CHAPTER 6: RING VERSION2 APPLICATION

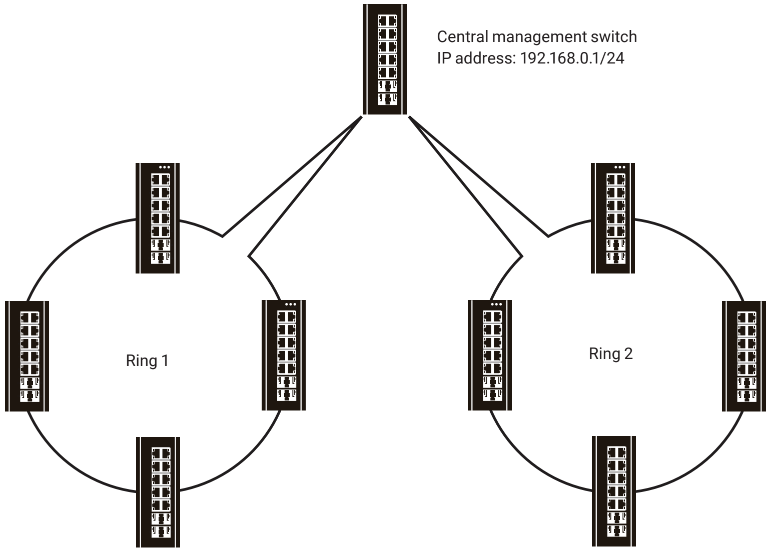


FIGURE 6-2. RING MASTER AND RING SLAVE SUPPORTED

Group 2 - This supports configuration of the ring, coupling and dual-homing.

- Ring - It could be master or slave.
- Coupling - It could be primary and backup.

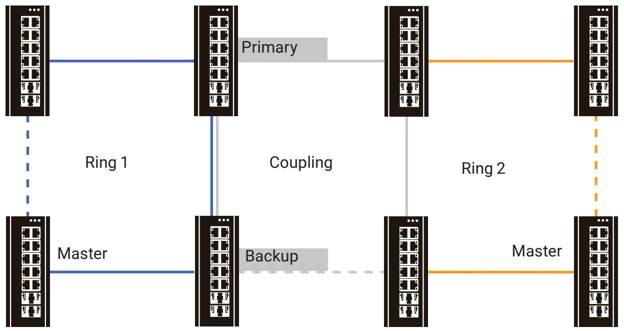


FIGURE 6-3. RING CONFIGURATOI, COUPLING AND DUAL HOMING SUPPORTED

- When role is coupling/primary, only one ring port named primary port is configured.
- When role is coupling/backup, only one ring port named backup port is configured. This backup port is a redundant port. In a normal state, it is blocked.

Dual-Homing

When the role is dual-homing, one ring port is the primary port and another is the backup port. This backup port is a redundant port. In normal state, it is blocked.

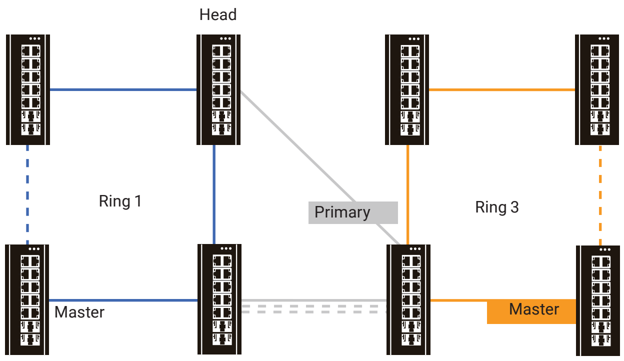


FIGURE 6-4. DUAL HOMING

Group 3 - This supports configuration of the chain and balancing-chain.

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

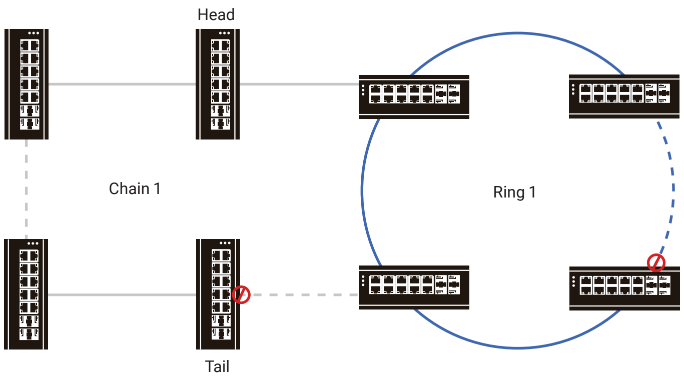


FIGURE 6-5. CHAIN CONFIGURATION

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

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

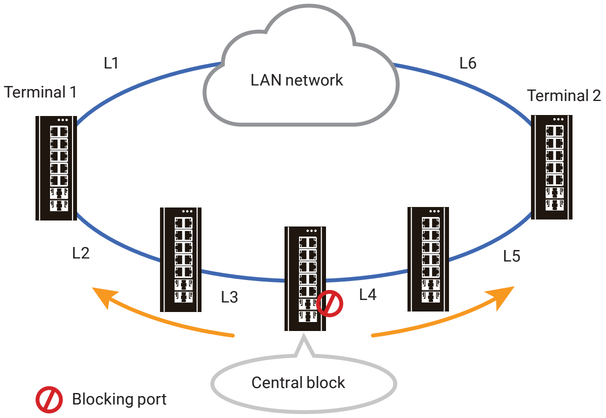


FIGURE 6-6. BALANCING CHAIN

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

NOTE 1: It must enable group1 before configure group2 as coupling.

NOTE 2: When group1 or group2 is enabled, the configuration of group3 is invisible.

NOTE 3: When group3 is enabled, the configuration of group1 and group3 is invisible.

6.2 HOW TO CONFIGURE RINGV2

CONFIGURATION (CONSOLE)

To configure the ring protection in the switch:

1. Log in as “admin” account in the console.
2. Go to Configure mode by ”configure terminal.”
3. Go to configure ring protection group by command “ringv2 protect group1.”
4. Before configuring, disable ring protection status using the “mode disable” command.
5. Set all necessary parameters:

- Node 1 and Node 2, choose the ports to connect to the other switch.
- For example, choose PORT-1 and PORT-2 to connect to the other switch.
- Then choose one of the ring connection devices to be “Master” on which the “Node 2 port” can be a blocking port.

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

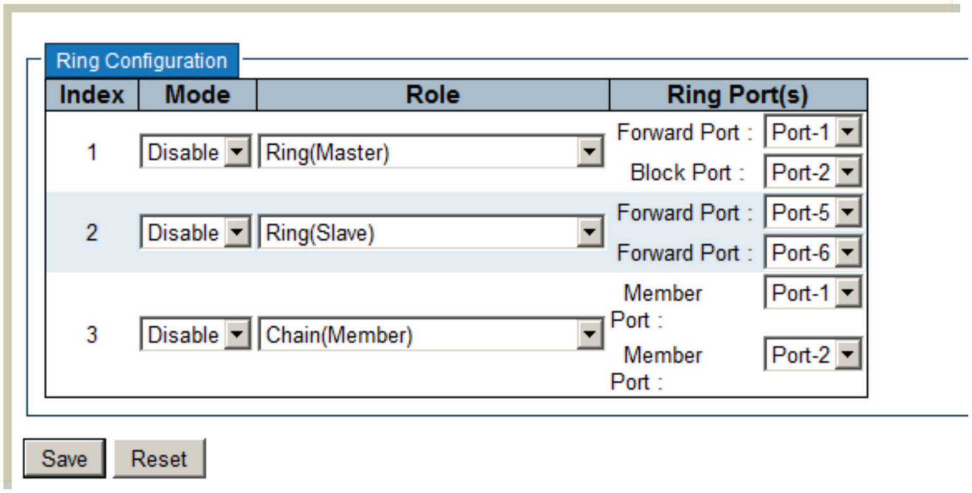
To finish the configuration, enable ring protection status using the “mode enable” command.

NOTE: Please pay attention to 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
```

CONFIGURATION (WEB UI)

In the switch’s current Ringv2 design, one device supports 3 ring indexes, including Ring & Chain (single ring, dual ring, coupling, dual-homing, chain, and balancing-chain.)



Ring Configuration

Index	Mode	Role	Ring Port(s)	
1	Disable	Ring(Master)	Forward Port : Block Port :	Port-1 Port-2
2	Disable	Ring(Slave)	Forward Port : Forward Port :	Port-5 Port-6
3	Disable	Chain(Member)	Member Port : Member Port :	Port-1 Port-2

FIGURE 6-7. RING CONFIGURATION SCREEN

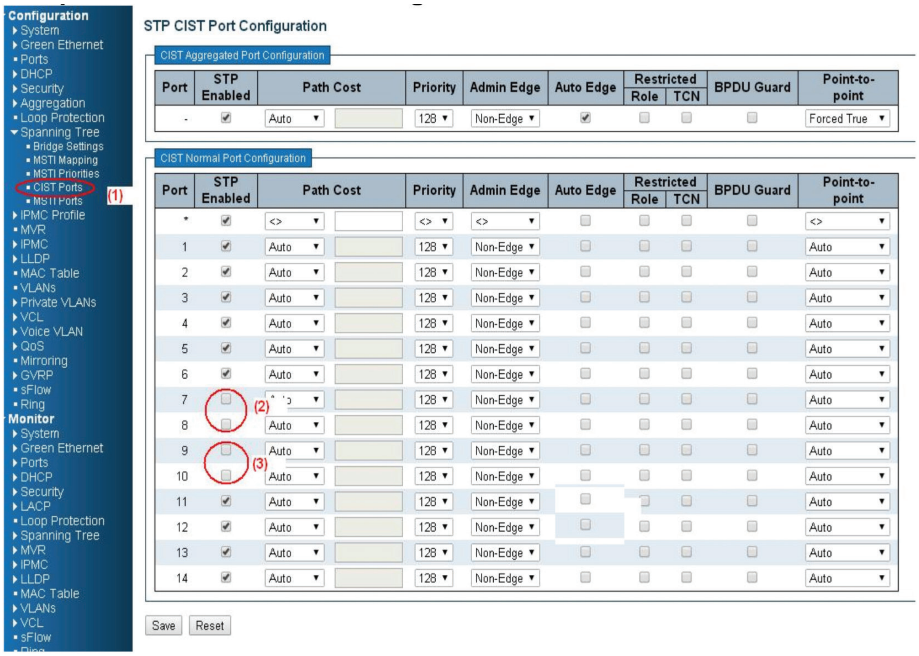
NOTE 1: You must enable group1 before configuring group2 as coupling.

NOTE 2: When group1 or group2 is enabled, the configuration of group3 is invisible.

NOTE 3: When group3 is enabled, the configuration of group1 and group3 is invisible.

STEP 1: Disable RSTP on All Ring Ports

1. Go to “Configuration —> Spanning Tree —> CIST ports” Web page.



STP CIST Port Configuration

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted Role	Restricted TCN	BPDU Guard	Point-to-point
-	☑	Auto ▼		128 ▼	Non-Edge ▼	☑	□	□	□	Forced True ▼

CIST Normal Port Configuration

Port	STP Enabled	Path Cost		Priority	Admin Edge	Auto Edge	Restricted Role	Restricted TCN	BPDU Guard	Point-to-point
*	☑	<> ▼		<> ▼	<> ▼	□	□	□	□	<> ▼
1	☑	Auto ▼		128 ▼	Non-Edge ▼	□	□	□	□	Auto ▼
2	☑	Auto ▼		128 ▼	Non-Edge ▼	□	□	□	□	Auto ▼
3	☑	Auto ▼		128 ▼	Non-Edge ▼	□	□	□	□	Auto ▼
4	☑	Auto ▼		128 ▼	Non-Edge ▼	□	□	□	□	Auto ▼
5	☑	Auto ▼		128 ▼	Non-Edge ▼	□	□	□	□	Auto ▼
6	☑	Auto ▼		128 ▼	Non-Edge ▼	□	□	□	□	Auto ▼
7	□	Auto ▼		128 ▼	Non-Edge ▼	□	□	□	□	Auto ▼
8	□	Auto ▼		128 ▼	Non-Edge ▼	□	□	□	□	Auto ▼
9	□	Auto ▼		128 ▼	Non-Edge ▼	□	□	□	□	Auto ▼
10	□	Auto ▼		128 ▼	Non-Edge ▼	□	□	□	□	Auto ▼
11	☑	Auto ▼		128 ▼	Non-Edge ▼	□	□	□	□	Auto ▼
12	☑	Auto ▼		128 ▼	Non-Edge ▼	□	□	□	□	Auto ▼
13	☑	Auto ▼		128 ▼	Non-Edge ▼	□	□	□	□	Auto ▼
14	☑	Auto ▼		128 ▼	Non-Edge ▼	□	□	□	□	Auto ▼

FIGURE 6-8. STP CIST PORT CONFIGURATION SCREEN

2. Do not enable STP global.

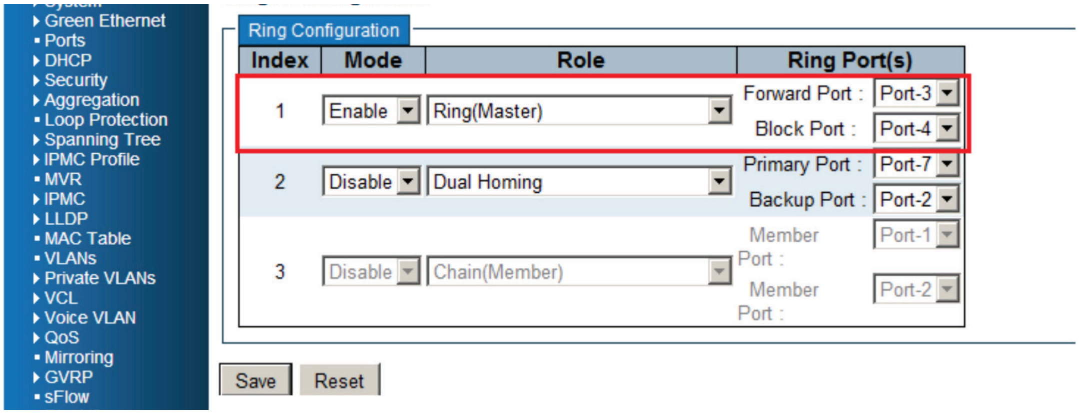
3. Click the “Save” button.

RING MASTER

1. Go to “Configuration —> RingV2” Web page.

2. Enable Index1, and Select Role as Ring(Master).

3. Select one port as a “Forward Port”, another as “Block Port.”



Ring Configuration

Index	Mode	Role	Ring Port(s)
1	Enable ▼	Ring(Master) ▼	Forward Port : Port-3 ▼ Block Port : Port-4 ▼
2	Disable ▼	Dual Homing ▼	Primary Port : Port-7 ▼ Backup Port : Port-2 ▼
3	Disable ▼	Chain(Member) ▼	Member Port : Port-1 ▼ Member Port : Port-2 ▼

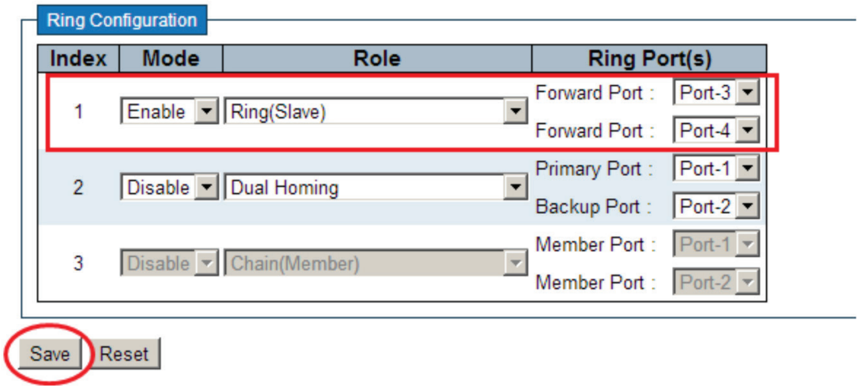
FIGURE 6-9. RING MASTER CONFIGURATION SCREEN

RING SLAVE

1. Go to “Configuration —> “RingV2” Web page.

2. Enable Index1, and Select Role as Ring(Slave)

3. Select two ports as “Forward Port.”



Index	Mode	Role	Ring Port(s)
1	Enable	Ring(Slave)	Forward Port : Port-3 Forward Port : Port-4
2	Disable	Dual Homing	Primary Port : Port-1 Backup Port : Port-2
3	Disable	Chain(Member)	Member Port : Port-1 Member Port : Port-2

FIGURE 6-10. RING SLAVE CONFIGURATION SCREEN

COUPLING PRIMARY

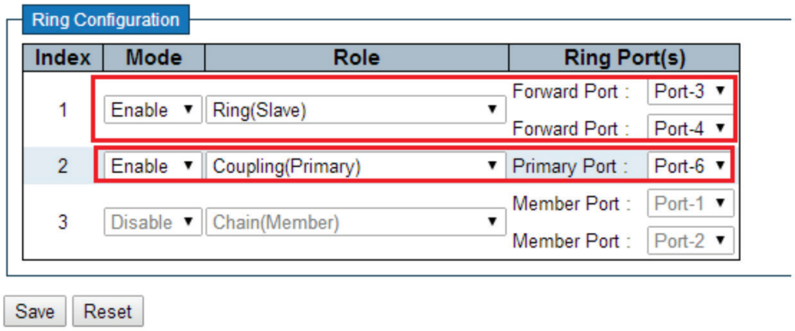
1. Go to “Configuration —> “RingV2” Web page.

2. Enable Index1, and Select Role as Ring(Slave).

3. Select two ports as “Forward Port.”

4. Enable Index2, and Select Role as “Coupling(Primary).”

5. Select one port as a “Primary Port.”



Index	Mode	Role	Ring Port(s)
1	Enable	Ring(Slave)	Forward Port : Port-3 Forward Port : Port-4
2	Enable	Coupling(Primary)	Primary Port : Port-6
3	Disable	Chain(Member)	Member Port : Port-1 Member Port : Port-2

FIGURE 6-11. COUPLING PRIMARY CONFIGURATION SCREEN

COUPLING BACKUP

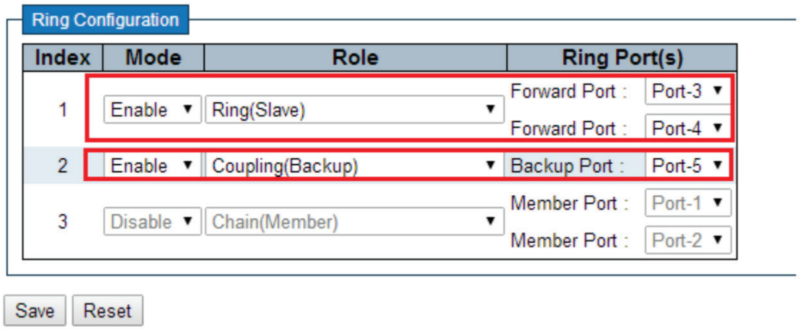
1. Go to “Configuration —> “RingV2” Web page.

2. Enable Index1, and Select Role as Ring(Slave).

3. Select two ports as a “Forward Port.”

4. Enable Index2, and Select Role as “Coupling(Backup).”

5. Select one port as a “Backup Port.”



Ring Configuration

Index	Mode	Role	Ring Port(s)
1	Enable	Ring(Slave)	Forward Port : Port-3 Forward Port : Port-4
2	Enable	Coupling(Backup)	Backup Port : Port-5
3	Disable	Chain(Member)	Member Port : Port-1 Member Port : Port-2

FIGURE 6-12. COUPLING BACKUP CONFIGURATION SCREEN

DUAL HOMING

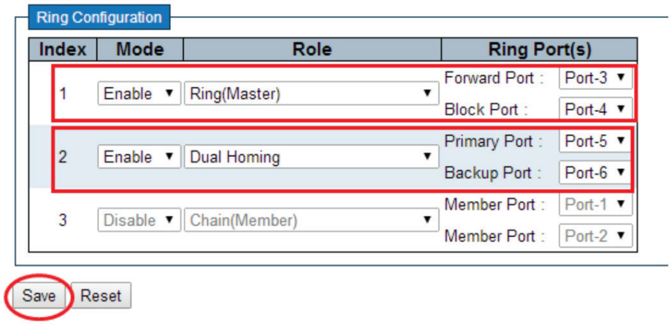
1. Go to “Configuration —> “RingV2” Web page.

2. Enable Index1, and Select Role as Ring(Slave).

3. Select two ports as a “Forward Port.”

4. Enable Index2, and Select Role as “Dual Homing.”

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



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 Member Port : Port-2

FIGURE 6-13. DUAL HOMING CONFIGURATION SCREEN

CHAIN CONFIGURATION

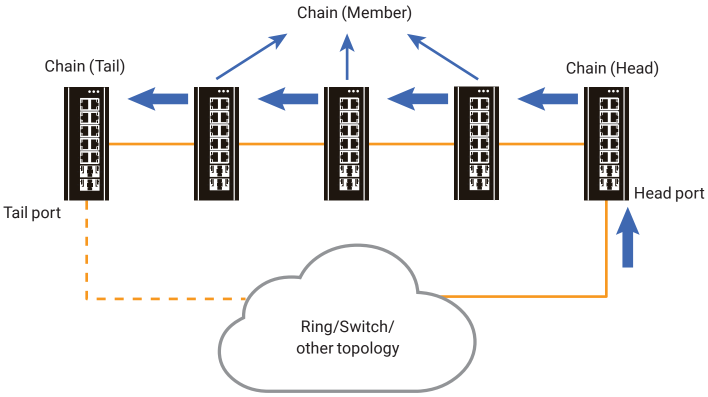


FIGURE 6-14. CHAIN CONFIGURATION

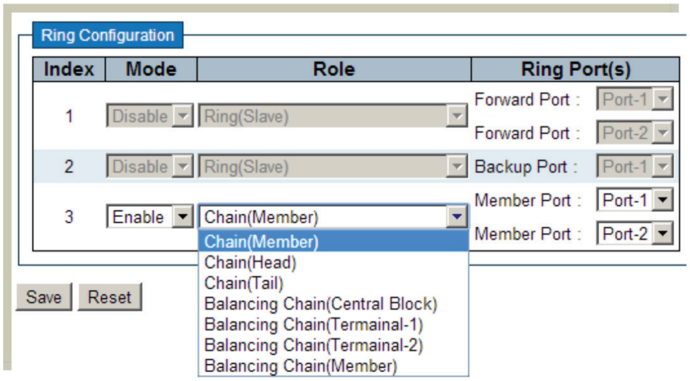
CHAIN - MEMBER

1. Go to “Configuration —> “RingV2” Web page.

2. Disable Index1 and Index2, then enable Index3.

3. Select Role to “Chain(Member).”

4. Select two member ports for this chain member switch.



Ring Configuration

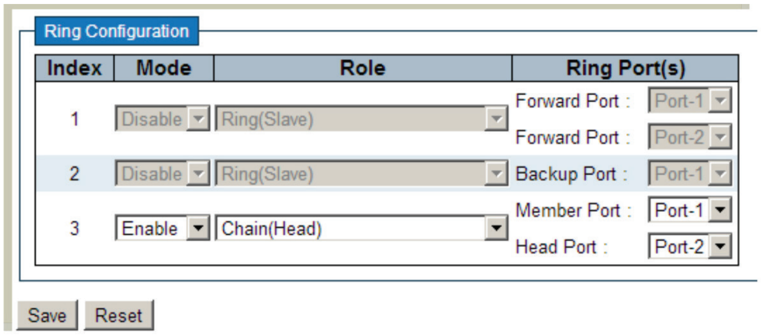
Index	Mode	Role	Ring Port(s)
1	Disable	Ring(Slave)	Forward Port : Port-1 Forward Port : Port-2
2	Disable	Ring(Slave)	Backup Port : Port-1
3	Enable	Chain(Member)	Member Port : Port-1 Member Port : Port-2

Chain(Member)
Chain(Head)
Chain(Tail)
Balancing Chain(Central Block)
Balancing Chain(Termainal-1)
Balancing Chain(Termainal-2)
Balancing Chain(Member)
Save
Reset

FIGURE 6-15. CHAIN MEMBER SCREEN

CHAIN - HEAD

1. Go to “Configuration —> “RingV2” Web page.
2. Disable Index1 and Index2, then enable Index3.
3. Select Role to “Chain(Head).”
4. Select a member port and a head port for this chain head switch.

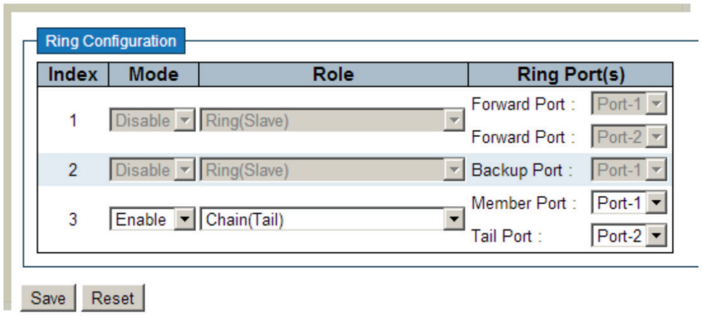


Index	Mode	Role	Ring Port(s)	
1	Disable	Ring(Slave)	Forward Port :	Port-1
			Forward Port :	Port-2
2	Disable	Ring(Slave)	Backup Port :	Port-1
3	Enable	Chain(Head)	Member Port :	Port-1
			Head Port :	Port-2

FIGURE 6-16. CHAIN HEAD SCREEN

CHAIN - TAIL

1. Go to “Configuration —> “RingV2” Web page.
2. Disable Index1 and Index2, then enable Index3.
3. Select Role to “Chain(Tail).”
4. Select a member port and a tail port for this chain tail switch.



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

FIGURE 6-17. CHAIN TAIL SCREEN

BALANCE CHAIN CONFIGURATION

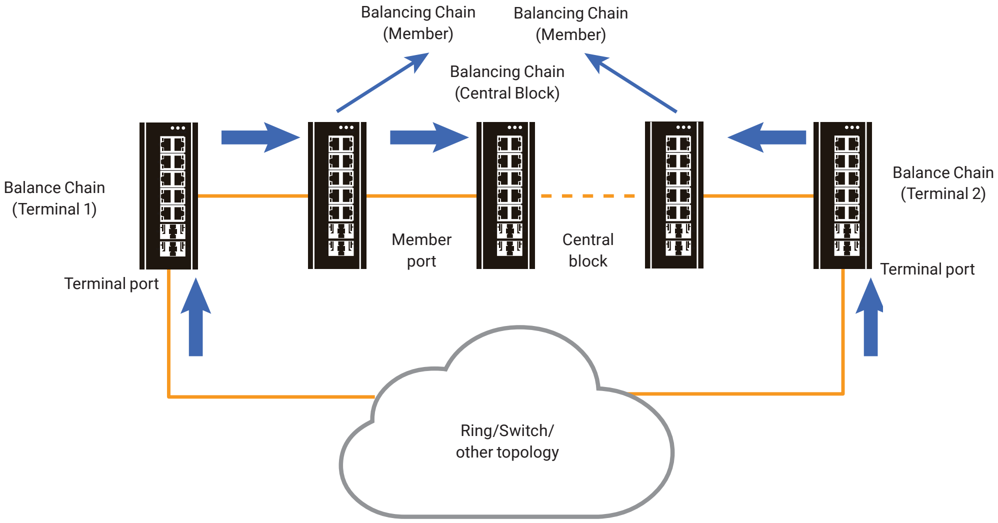
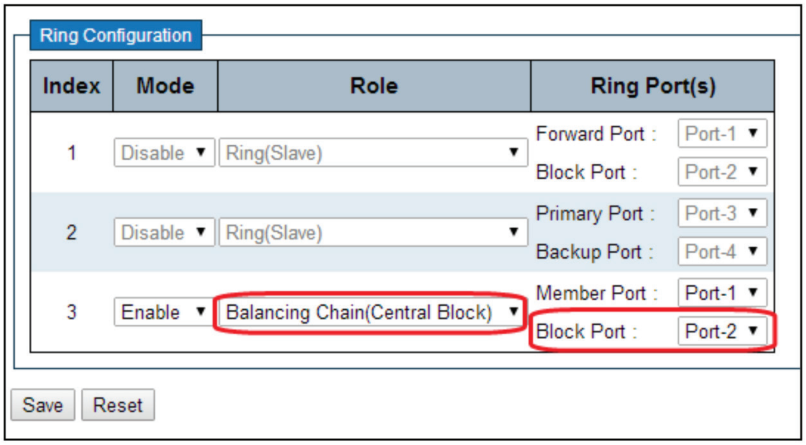


FIGURE 6-18. BALANCE CHAIN CONFIGURATION

BALANCE CHAIN - CENTRAL BLOCK

1. Go to “Configuration —> “RingV2” Web page.
2. Disable Index1 and Index2, then enable Index3.
3. Select Role to “Balancing Chain(Central Block).”
4. Select a member port and a block port for this central block switch.



Ring Configuration

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

FIGURE 6-19. BALANCE CHAIN CENTRAL BLOCK SCREEN

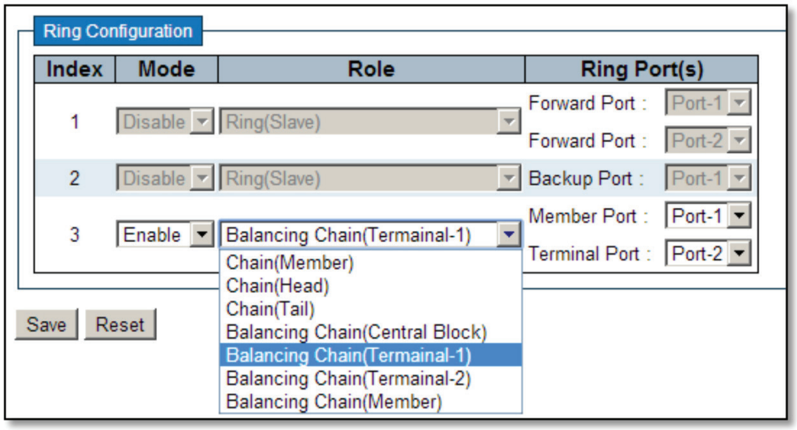
BALANCE CHAIN - TERMINAL 1 AND 2

1. Go to “Configuration —> “RingV2” Web page.

2. Disable Index1 and Index2, then enable Index3.

3. Select Role to “Balancing Chain(Terminal-1 or -2).”

4. Select a member port and a terminal port for this balancing chain terminal switch.



Ring Configuration

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

Chain(Member)
Chain(Head)
Chain(Tail)
Balancing Chain(Central Block)
Balancing Chain(Termainal-1)
Balancing Chain(Termainal-2)
Balancing Chain(Member)
Save
Reset

FIGURE 6-20. BALANCE CHAIN - TERMINAL 1 AND 2 SCREEN

CHAPTER 7: QOS APPLICATION

Quality of Service (QoS) 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 Quality of Service (QoS) level.

7.1 SP/SPWRR

The switch can be configured to have 8 output Class of Service (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. The user needs to bind VLAN priority/ queue mapping profile to each port, and for every VLAN priority the user needs to assign a traffic descriptor for it. The traffic descriptor defines the shape parameter on every VLAN priority for the Ethernet interface. Currently the switch supports Strict Priority and SP+WRR (Weighted Round Robin) scheduling methods on each port.

TABLE 7-1. DEFAULT PRIORITY AND QUEUE MAPPING VALUES

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. You can configure QoS using the Web-based management system, CLI (Command Line Interface) or SNMP.

7.2 EXAMPLE 1: SPQ WITHOUT SHAPING (DEFAULT PROFILE)

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

Expected Result:

We expect that PORT-2 only can receive 100 Mbps of Stream1, and Stream0 will be discarded. This explains how SPQ works on the switch.

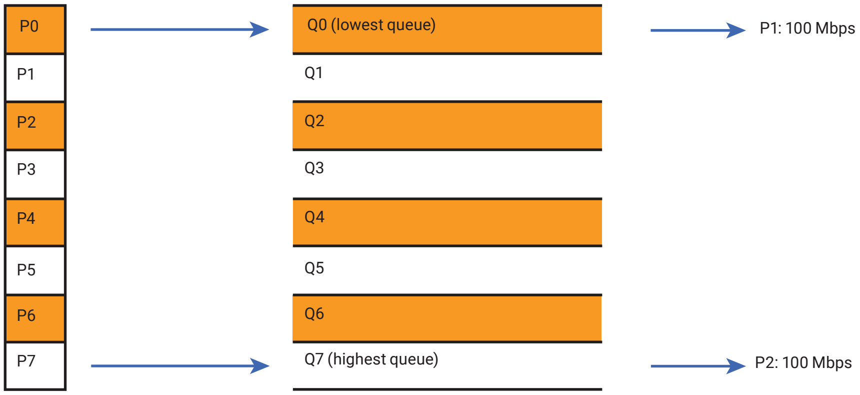


FIGURE 7-1. GIGABIT PORT VLAN PRIORITY & QUEUE MAPPING.

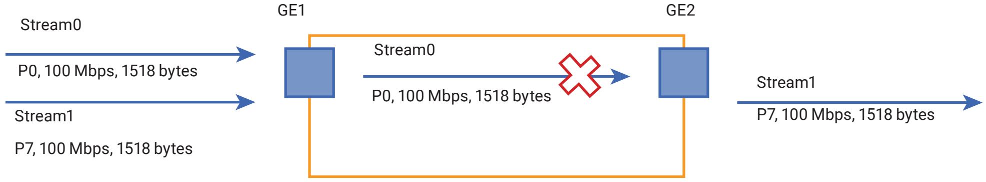


FIGURE 7-2.

- Stream0:

  Dst Mac: 00:00:00:00:20:01

  Src Mac: 00:00:00:00:10:01

  Vlan: 100

  Vlan prio: 0

  Send rate: 100 Mbps

  Packet length: 1518 bytes

- Stream1:

  Dst Mac: 00:00:00:00:20:02

  Src Mac: 00:00:00:00:10:02

  Vlan: 100

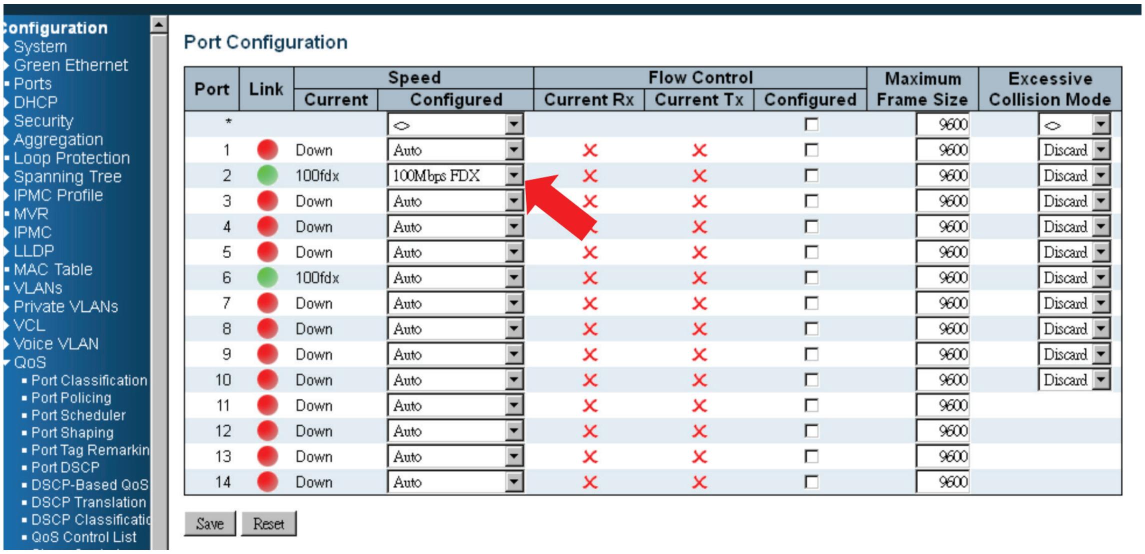
  Vlan prio: 7

  Send rate: 100 Mbps

  Packet length: 1518 bytes

WEB MANAGEMENT

STEP 1: Go to Configuration —> Ports —> set port 2 link speed to 100 Mbps full duplex.

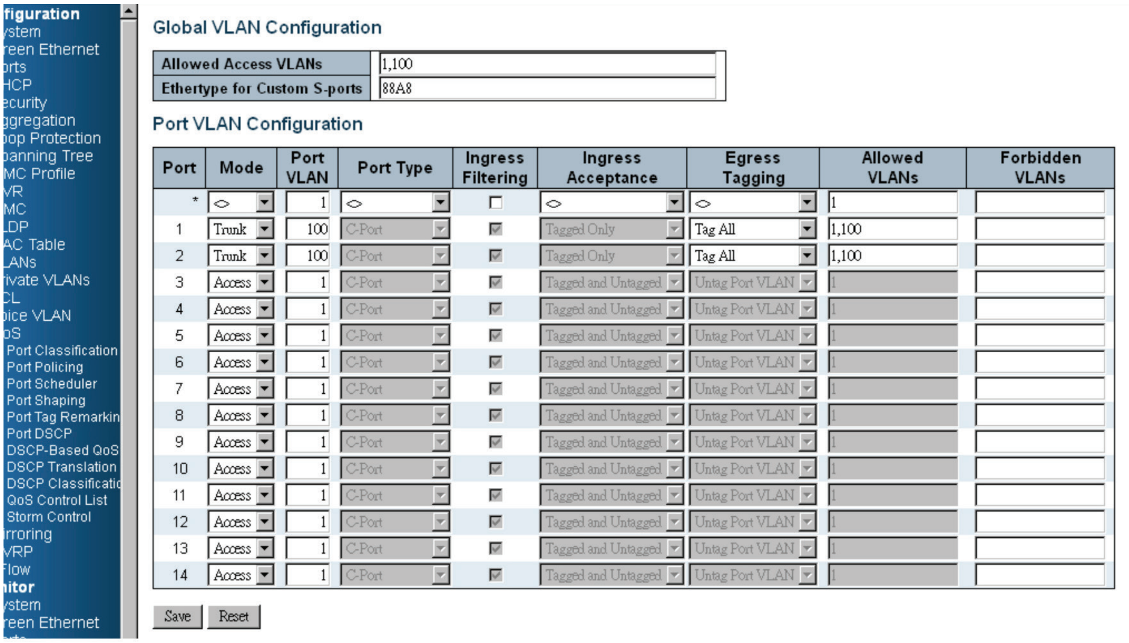


Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame Size	Excessive Collision Mode
		Current	Configured	Current Rx	Current Tx	Configured		
*			<>			□	9600	<>
1	🔴	Down	Auto	✕	✕	□	9600	Discard
2	🟢	100fdx	100Mbps FDX	✕	✕	□	9600	Discard
3	🔴	Down	Auto	✕	✕	□	9600	Discard
4	🔴	Down	Auto	✕	✕	□	9600	Discard
5	🔴	Down	Auto	✕	✕	□	9600	Discard
6	🟢	100fdx	Auto	✕	✕	□	9600	Discard
7	🔴	Down	Auto	✕	✕	□	9600	Discard
8	🔴	Down	Auto	✕	✕	□	9600	Discard
9	🔴	Down	Auto	✕	✕	□	9600	Discard
10	🔴	Down	Auto	✕	✕	□	9600	Discard
11	🔴	Down	Auto	✕	✕	□	9600	
12	🔴	Down	Auto	✕	✕	□	9600	
13	🔴	Down	Auto	✕	✕	□	9600	
14	🔴	Down	Auto	✕	✕	□	9600	

FIGURE 7-3.

STEP 2: Select Configuration —> VLANs —> Create a VLAN with VLAN ID 100. Enter a VLAN name in the Name field. Here we set tagged VLAN100 on PORT-1 and PORT-2.



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	<>	□	<>	<>	1	
1	Trunk	100	C-Port	☑	Tagged Only	Tag All	1,100	
2	Trunk	100	C-Port	☑	Tagged Only	Tag All	1,100	
3	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
7	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
8	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
9	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
10	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
11	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
12	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
13	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	
14	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLAN	1	

FIGURE 7-4.

CLI CONFIGURATION COMMAND

```
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
```

7.2 EXAMPLE 2: SPQ WITH SHAPING

We send 2 Streams (Stream0, Stream1) from PORT-1 to PORT-2. Both Streams each have 100 Mbps. Stream0 includes VLAN Priority0, Stream1 includes VLAN Priority7. Stream 3 and Stream 4 are only for learning to prevent the traffic from flooding.

Expected Result:

We expect that PORT-2 only can receive 20 Mbps of Stream1 ad 80 Mps of Stream2. This explains how SPQ works on the switch.

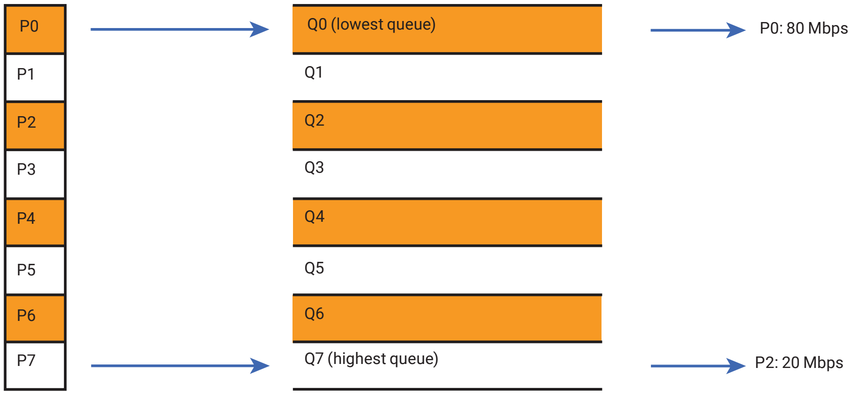


FIGURE 7-5. VDSL PORT VLAN PRIORITY AND QUEUE MAPPING

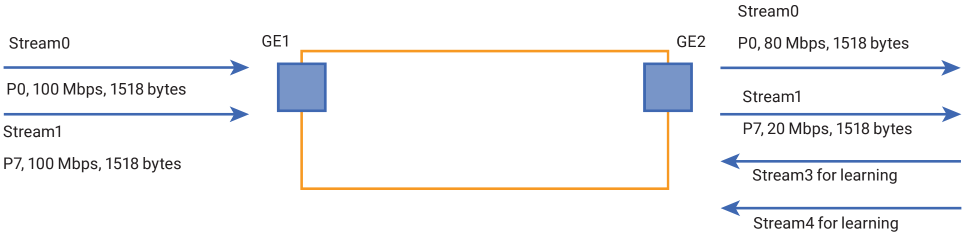


FIGURE 7-6.

- Stream0:

  Dst Mac: 00:00:00:00:20:01

  Src Mac: 00:00:00:00:10:01

  Vlan: 100

  Vlan prio: 0

  Send rate: 100 Mbps

  Packet length: 1518 bytes

- Stream1:

  Dst Mac: 00:00:00:00:20:02

  Src Mac: 00:00:00:00:10:02

  Vlan: 100

  Vlan prio: 7

  Send rate: 100 Mbps

  Packet length: 1518 bytes

- 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: 10 Mbps

  Packet length: 1518 bytes

- Stream4 (for learning):

  Dst Mac: 00:00:00:00:10:02

  Src Mac: 00:00:00:00:20:02

  Vlan: 100

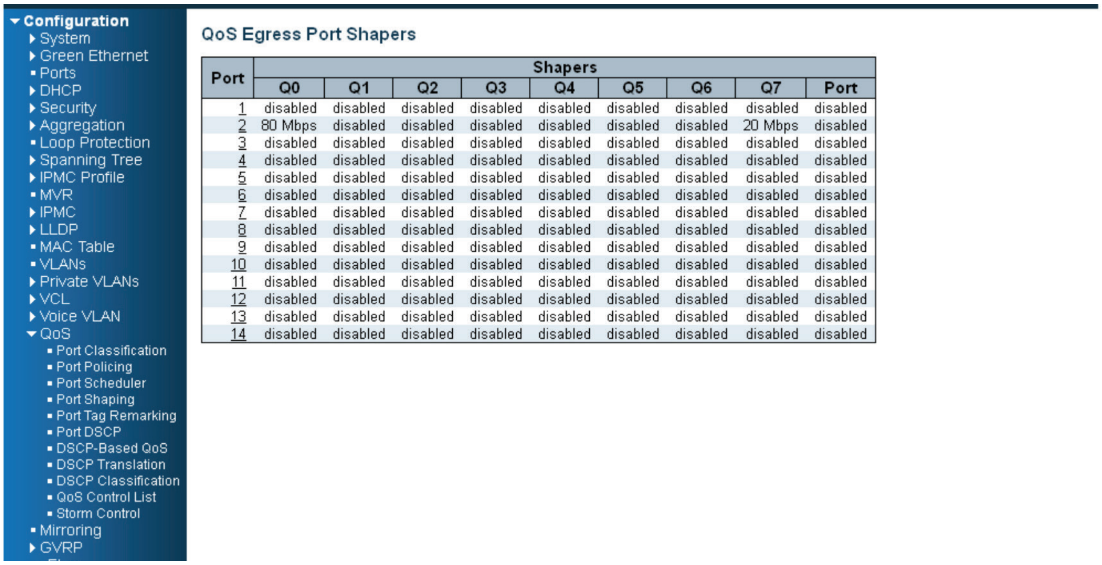
  Vlan prio: 0

  Send rate: 10 Mbps

  Packet length: 1518 bytes

WEB MANAGEMENT

STEP 1: Go to Configuration —> Qos —> Port Shaping, to create a Qos profile on Port-2.

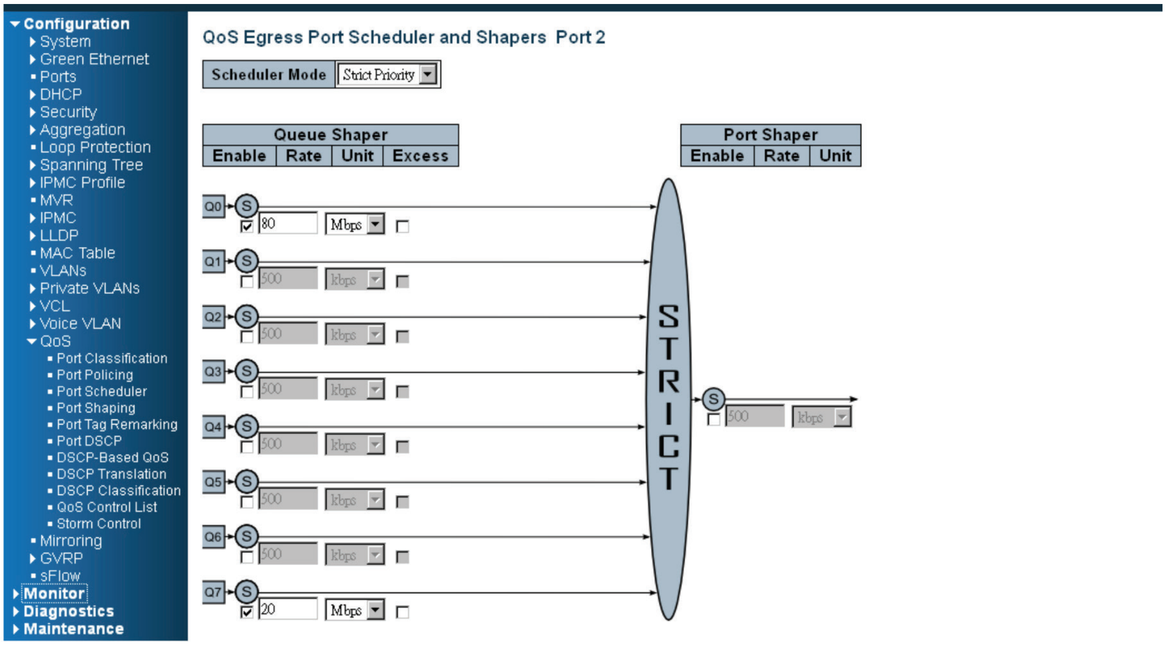


QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	80 Mbps	disabled	disabled	disabled	disabled	disabled	disabled	20 Mbps	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
10	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
11	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
12	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
13	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
14	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

FIGURE 7-7.

STEP 2: Select schedule mode to be “”Strict Priority” and set shaping rate for queue 0 and queue 7 as below.



QoS Egress Port Scheduler and Shapers Port 2

Scheduler Mode: Strict Priority

Queue	Queue Shaper			
	Enable	Rate	Unit	Excess
Q0	☑	80	Mbps	□
Q1	□	500	kbps	□
Q2	□	500	kbps	□
Q3	□	500	kbps	□
Q4	□	500	kbps	□
Q5	□	500	kbps	□
Q6	□	500	kbps	□
Q7	☑	20	Mbps	□

Port Shaper		
Enable	Rate	Unit
□	500	kbps

FIGURE 7-8.

CLI CONFIGURATION COMMAND

```
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
```

CHAPTER 8: IGMP APPLICATION

IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

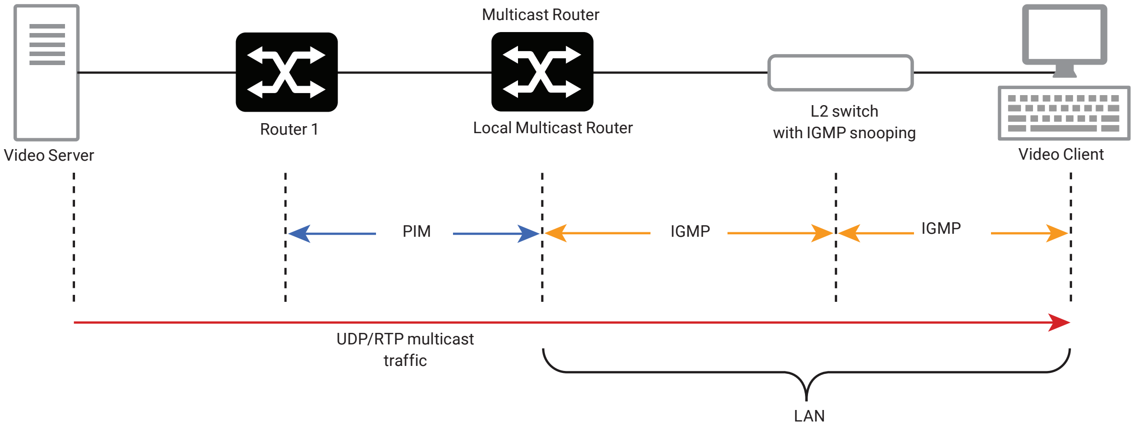
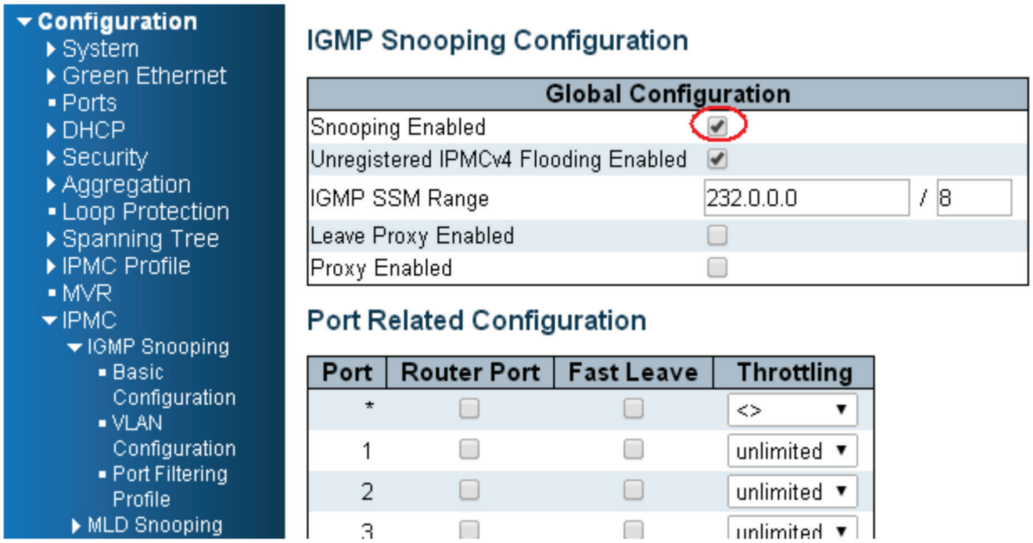


FIGURE 8-1. IGMP INSTALLATION

8.1 EXAMPLE 1

To configure every client to get a multicast stream, go to “Configuration —> IPMC —> Basic Configuration” and select the “Snooping Enable” check box.



IGMP Snooping Configuration

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

Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited

FIGURE 8-2. SNOOPING ENABLED CHECKBOX

8.2 EXAMPLE 2

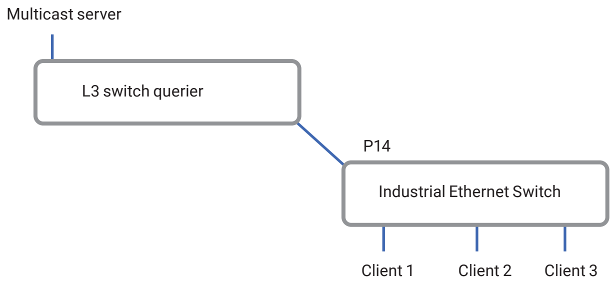


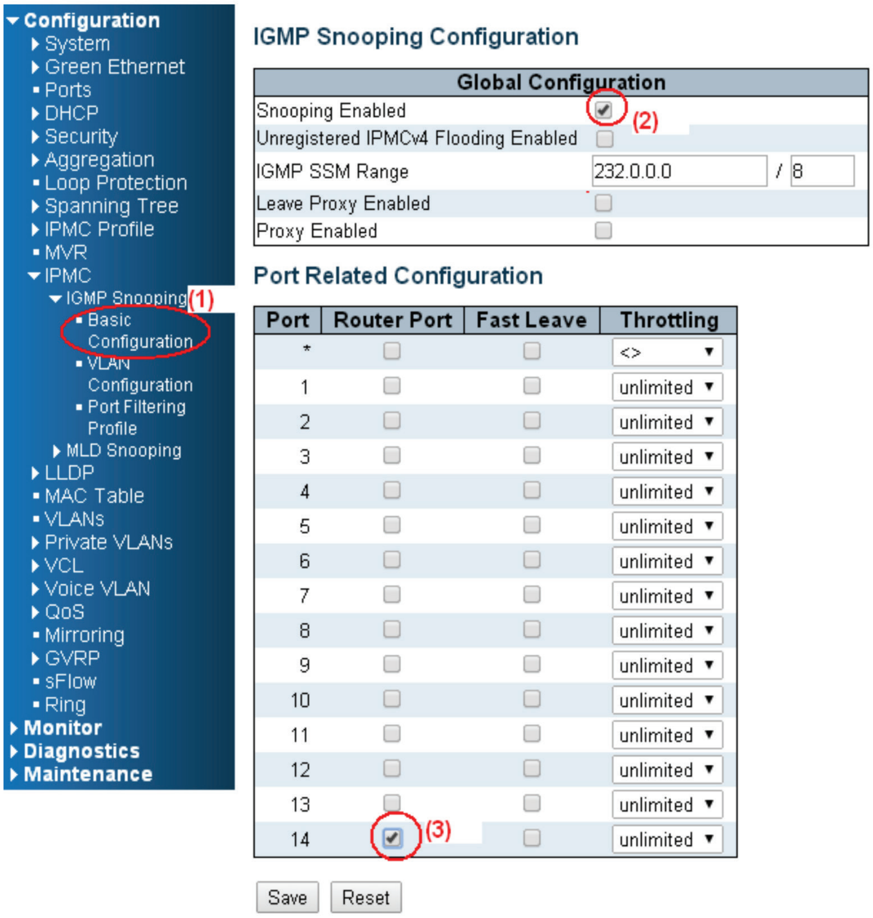
FIGURE 8-3. EXAMPLE 2

1. Go to “Configuration —> IPMC —> Basic Configuration” to select the “Snooping Enable” check box.

2. Un-select the ”Unregistered IPMCv4 Flooding Enabled” check box.

3. If Multicast stream is from an L3 switch, then the uplink port will have to be the “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	☑	
Unregistered IPMCv4 Flooding Enabled	☐	
IGMP SSM Range	232.0.0.0	/ 8
Leave Proxy Enabled	☐	
Proxy Enabled	☐	

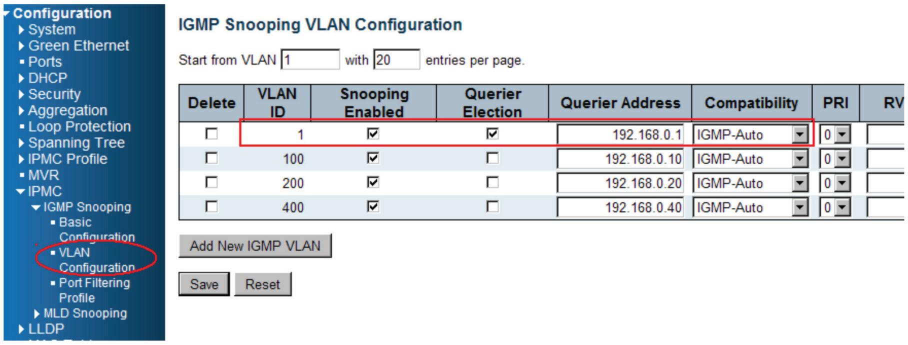
Port Related Configuration

Port	Router Port	Fast Leave	Throttling
*	☐	☐	<>
1	☐	☐	unlimited
2	☐	☐	unlimited
3	☐	☐	unlimited
4	☐	☐	unlimited
5	☐	☐	unlimited
6	☐	☐	unlimited
7	☐	☐	unlimited
8	☐	☐	unlimited
9	☐	☐	unlimited
10	☐	☐	unlimited
11	☐	☐	unlimited
12	☐	☐	unlimited
13	☐	☐	unlimited
14	☑	☐	unlimited

FIGURE 8-4.

CHAPTER 8: IGMP APPLICATION

4. Go to “Configuration —> IPMC —> VLAN Configuration” to select the “Snooping Enable” check box and set the VLAN ID of port14.



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
□	1	☑	☑	192.168.0.1	IGMP-Auto	0	
□	100	☑	□	192.168.0.10	IGMP-Auto	0	
□	200	☑	□	192.168.0.20	IGMP-Auto	0	
□	400	☑	□	192.168.0.40	IGMP-Auto	0	

FIGURE 8-5.

8.3 EXAMPLE 3

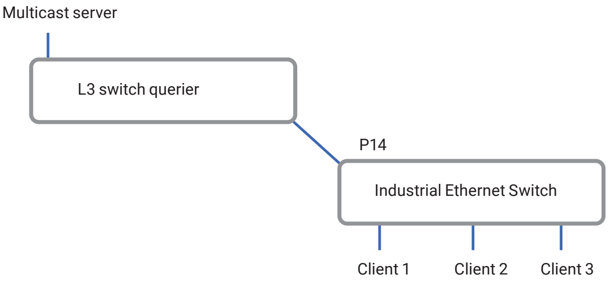
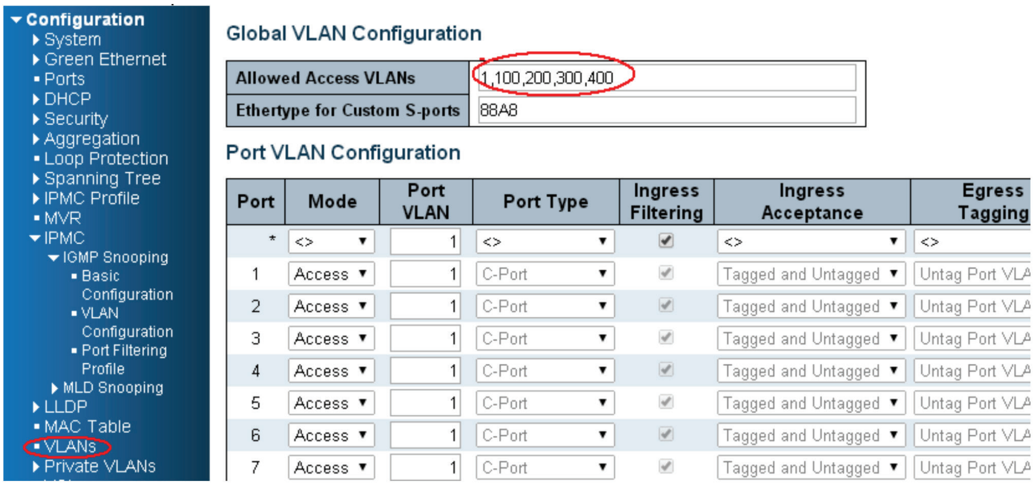


FIGURE 8-6. EXAMPLE 3

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: go to ”Configuration —> VLANs —> Allow Access VLANs”, then set port 14 to be a vlan200 member port.



Global VLAN Configuration

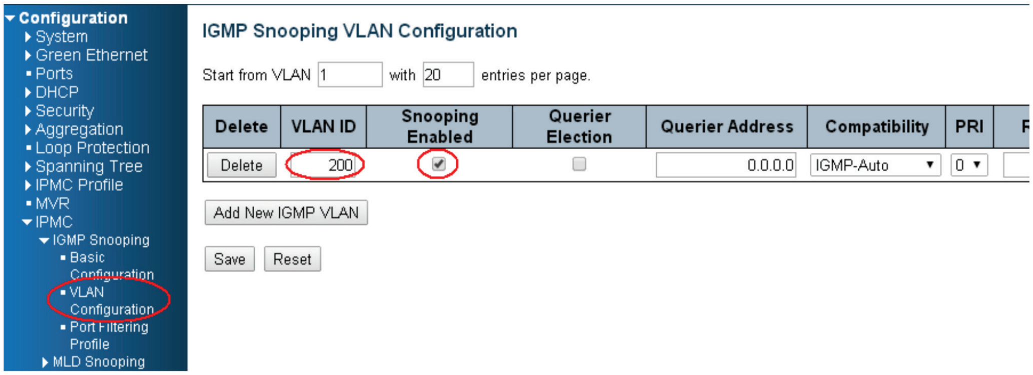
Allowed Access VLANs	1,100,200,300,400
Ethertype for Custom S-ports	88A8

Port VLAN Configuration

Port	Mode	Port VLAN	Port Type	Ingress Filtering	Ingress Acceptance	Egress Tagging
*	<>	1	<>	☑	<>	<>
1	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLA
2	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLA
3	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLA
4	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLA
5	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLA
6	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLA
7	Access	1	C-Port	☑	Tagged and Untagged	Untag Port VLA

FIGURE 8-7.

2. Go to “Configuration —> IPMC —> VLAN Configuration” to select the “Snooping Enable” check box and set the VLAN ID of port14.



IGMP Snooping VLAN Configuration

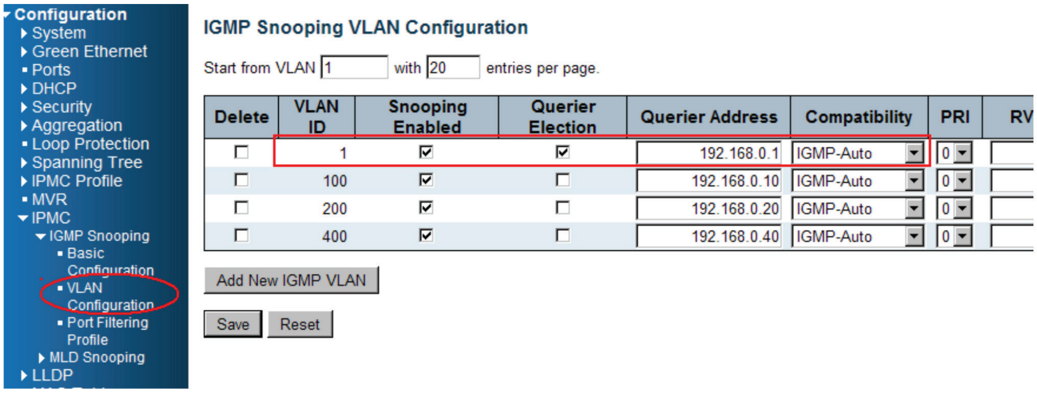
Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	Snooping Enabled	Querier Election	Querier Address	Compatibility	PRI	F
Delete	200	☑	□	0.0.0.0	IGMP-Auto	0	

FIGURE 8-8.

3. 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.

4. Select the IGMP version as server.



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
□	1	☑	☑	192.168.0.1	IGMP-Auto	0	
□	100	☑	□	192.168.0.10	IGMP-Auto	0	
□	200	☑	□	192.168.0.20	IGMP-Auto	0	
□	400	☑	□	192.168.0.40	IGMP-Auto	0	

FIGURE 8-9.

8.4 HOW TO CONFIGURE VLC

VLC CONFIGURATION ON AN IGMP SERVER

1. In the Media area of the top tool bar select “Stream.”

2. Select a video or audio file to play.

3. Confirm that the file is correct, then click “Next” twice.

4. Select the stream type as “UDP” and click the “Add” button.

5. Set the stream IP; the range is 224.0.0.1 to 239.255.255.254, and the protocol port is 1234.

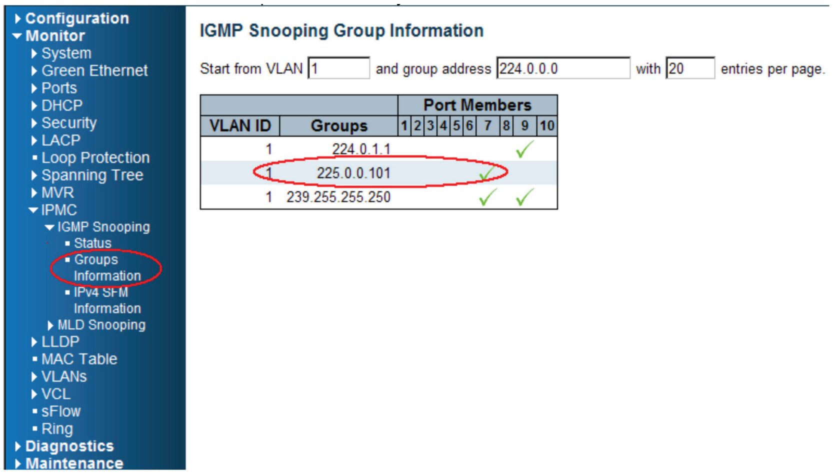
6. Select ”Sort out all stream” and click then “Stream” button, then the stream will start sending to the switch.

VLC CONFIGURATION ON AN IGMP CLIENT

1. In the Media area of the top tool bar, select open network stream.

2. Set the stream IP and protocol port to be the same as the previous setting on the server. The protocol type is "UDP."
Then click the "PLAY" button.

Return to the managed switch. Go to "Monitor —> IPMC —> Groups Information", and you will see the stream IP in the table.



IGMP Snooping Group Information

Start from VLAN 1 and group address 224.0.0.0 with 20 entries per page.

		Port Members									
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10
1	224.0.1.1									✓	
1	225.0.0.101							✓			
1	239.255.255.250							✓		✓	

FIGURE 8-10. VIEW STREAM IP IN TABLE

CHAPTER 9: 802.1X AUTHENTICATION APPLICATION

IEEE 802.1x derives keys that can be used to provide per-packet authentication, integrity and confidentially. It is typically used along with well-known key derivation algorithms (e.g. TLS, SRP, MD5-Challenge, etc.). The Industrial Ethernet Switch supports 802.1x authentication function per port (port1–port10). Enable the 802.1x function and choose the ports and type you want to apply. If you enable 802.1x authentication control for certain Ethernet port in the switch, this port should be authenticated before using any services from the network.

9.1 802.X TIMER IN THE SWITCH

TABLE 9-1. 802.X TIMER FUNCTIONS

PARAMETER	DESCRIPTION
ReAuth Period	The switch will restart authentication after each Reauth-Period when the ReAuth option is enabled
Quiet Period	The switch will wait QuietPeriod to restart the authentication process again when authentication failed.
Tx Period	The switch will send an EAP-request to Supplicant every TxPeriod when authentication is running and Quiet Period is not running.
Supplicant Timeout	The switch will wait the SupplicantTmeout to receive a response from the Supplicant.
Server Timeout	The switch will wait the ServerTimeout to receive a response from the RADIUS server.

9.2 RADIUS SERVER CONFIGURATION

STEP 1: Prepare a Linux PC with a RADIUS server installed.

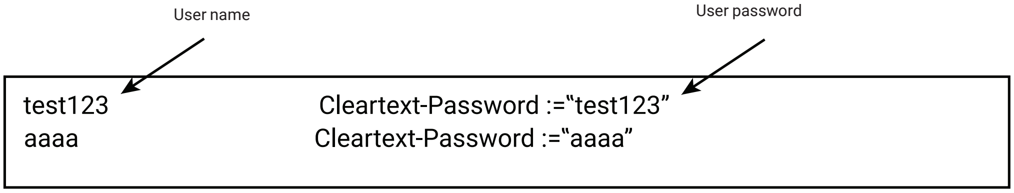
STEP 2: Edit the secret key for the RADIUS server.

Setting:

```
client 20.20.20.0/24 {
  secret = a12b3c4d
}
```

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

Setting:



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

STEP 4: Set a static IP address for this Radius Server.

Setting: 20.20.20.20

STEP 5: Start Radius Server

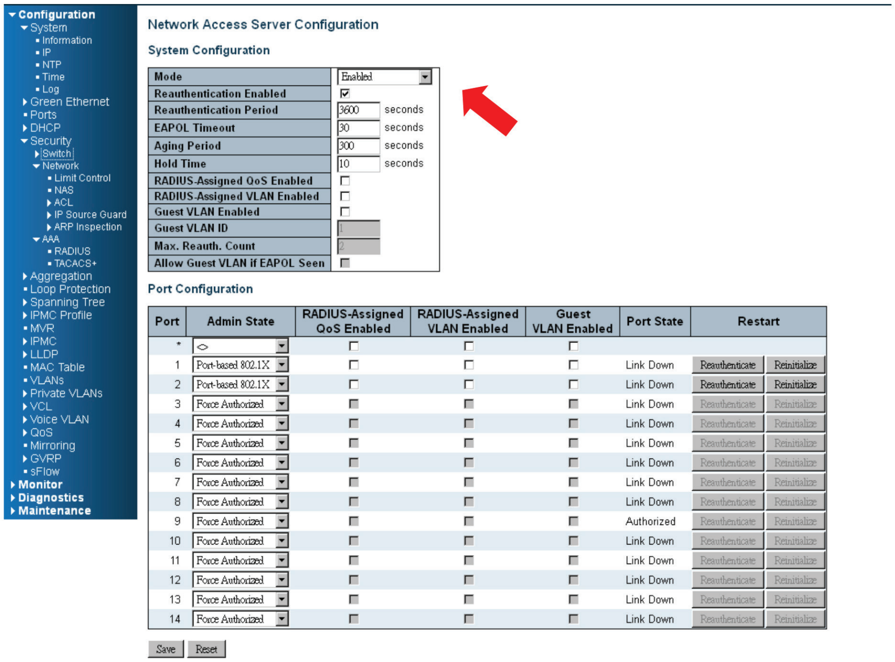
9.3 EXAMPLE

Here we take an example of 802.1x Authentication via the Industrial Ethernet Switch to be authenticated by RADIUS server. In a basic example, we take port 1 as a testing port which enables 802.1x in the switch.

With the default configuration, use the following Web UI setting .

STEP 1: Go to Configuration —> Security —> Networks —> NAS.

Select “Enable” mode to enable authentication, and set port-1, port-2 to be “Port Base 802.1x”.



Network Access Server Configuration

System Configuration

Mode	Enabled
Reauthentication Enabled	☑
Reauthentication Period	3600 seconds
EAPOL Timeout	30 seconds
Aging Period	300 seconds
Hold Time	10 seconds
RADIUS-Assigned QoS Enabled	☐
RADIUS-Assigned VLAN Enabled	☐
Guest VLAN Enabled	☐
Guest VLAN ID	1
Max. Reauth. Count	2
Allow Guest VLAN if EAPOL Seen	☐

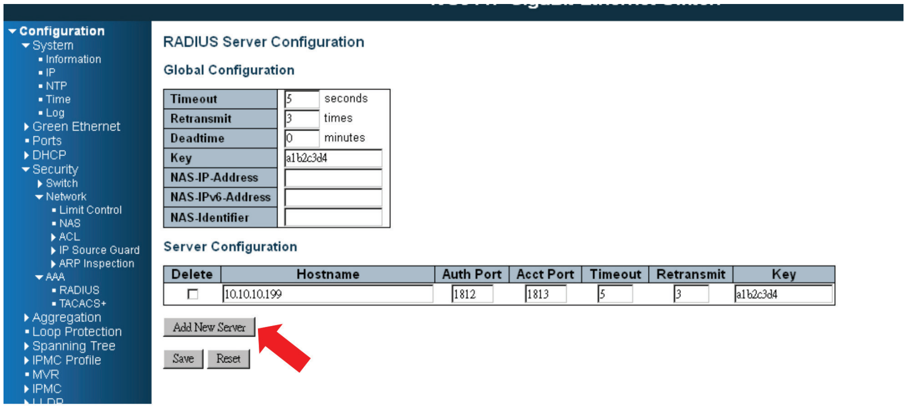
Port Configuration

Port	Admin State	RADIUS-Assigned QoS Enabled	RADIUS-Assigned VLAN Enabled	Guest VLAN Enabled	Port State	Restart
*	<>	☐	☐	☐		
1	Port-based 802.1X	☐	☐	☐	Link Down	Reauthenticate Reinitialize
2	Port-based 802.1X	☐	☐	☐	Link Down	Reauthenticate Reinitialize
3	Force Authorized	☐	☐	☐	Link Down	Reauthenticate Reinitialize
4	Force Authorized	☐	☐	☐	Link Down	Reauthenticate Reinitialize
5	Force Authorized	☐	☐	☐	Link Down	Reauthenticate Reinitialize
6	Force Authorized	☐	☐	☐	Link Down	Reauthenticate Reinitialize
7	Force Authorized	☐	☐	☐	Link Down	Reauthenticate Reinitialize
8	Force Authorized	☐	☐	☐	Link Down	Reauthenticate Reinitialize
9	Force Authorized	☐	☐	☐	Authorized	Reauthenticate Reinitialize
10	Force Authorized	☐	☐	☐	Link Down	Reauthenticate Reinitialize
11	Force Authorized	☐	☐	☐	Link Down	Reauthenticate Reinitialize
12	Force Authorized	☐	☐	☐	Link Down	Reauthenticate Reinitialize
13	Force Authorized	☐	☐	☐	Link Down	Reauthenticate Reinitialize
14	Force Authorized	☐	☐	☐	Link Down	Reauthenticate Reinitialize

FIGURE 9-1. NAS SCREEN

STEP 2: Go to Configuration —> Security —> AAA —> Radius.

Click “Add New Server,” input “20.20.20.20” for server, and “a1b2c3d4” for secret key. Then click the “Save” button.



RADIUS Server Configuration

Global Configuration

Timeout	5 seconds
Retransmit	3 times
Deadtime	0 minutes
Key	a1b2c3d4
NAS-IP-Address	
NAS-IPv6-Address	
NAS-Identifier	

Server Configuration

Delete	Hostname	Auth Port	Acct Port	Timeout	Retransmit	Key
☐	10.10.10.199	1812	1813	5	3	a1b2c3d4

FIGURE 9-2. RADIUS SCREEN

CLI COMMAND

```
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
```

CONFIGURATION

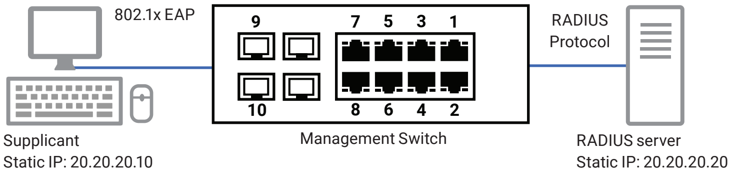


FIGURE 9-3. RADIUS SERVER CONFIGURATION

Supplicant's NIC Setting

STEP 1: Configure a static IP address 20.20.20.10 and net mask 255.255.255.0 for supplicant. (If there is a DHCP server to assign IP address for supplicant, this step can be ignored.)

STEP 2: Select the IEEE802.1x Authentication Enable check box, then configure the EAP type to MD5-Challenge.

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

Authentication Behavior

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

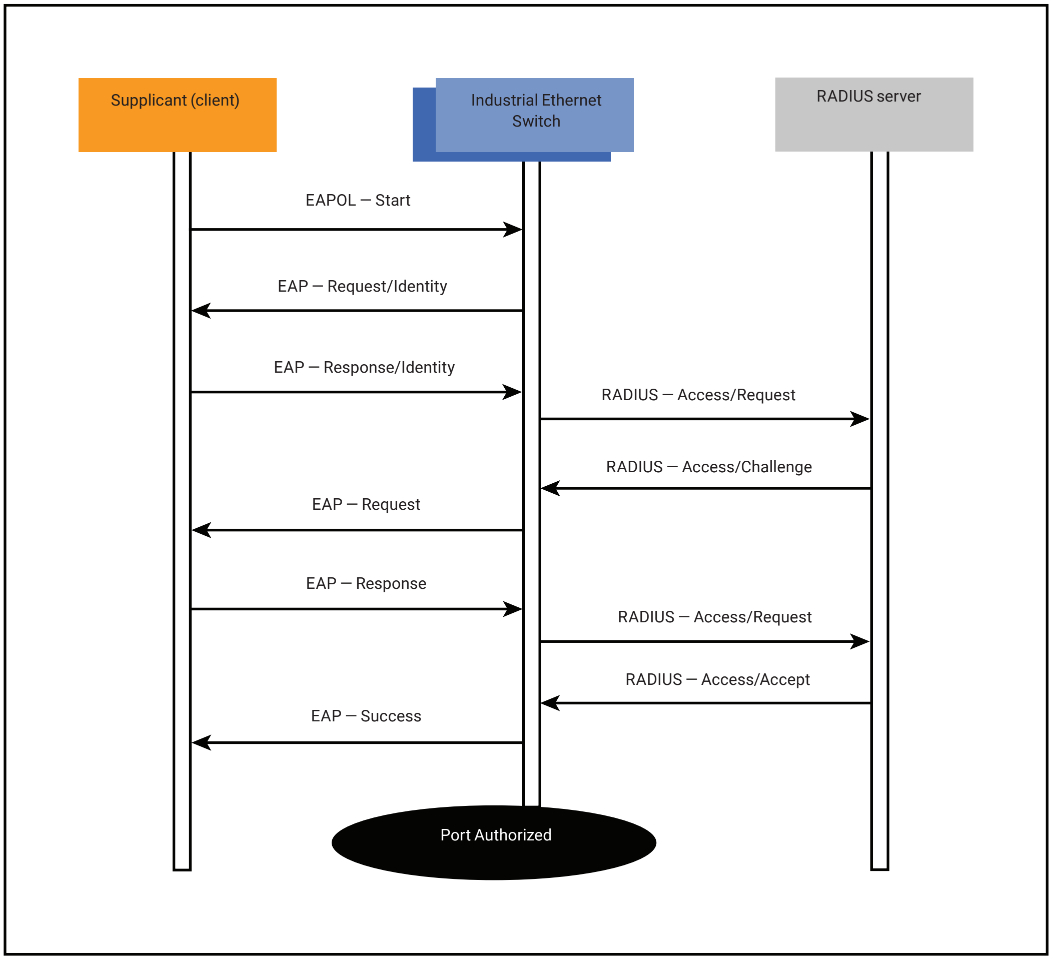


FIGURE 9-4. AUTHENTICATION PROCESS

CHAPTER 10: POWER OVER ETHERNET APPLICATION

NOTE: This chapter applies only to PoE managed models (LIE401A, LIE1014A, LIE1080A and LIE1082A).

These switches support the PoE function for connected powered devices. The operation mode contains 802.3af (15.4W), 802.3at (30W), and 802.3at with 4 pair used (60W). 60 watts only can be applied for port 1 and 2. Each port has 5 classes for selection, class 0–4. The total power budget of the system is up to 240 watts.

The PoE switches support power scheduler for each PoE port. Each time interval is 30 minutes from Sunday to Saturday. You can select which interval to set PoE on or PoE off. The switch also supports a PoE reset function to power off, then power on the PoE function on a port at certain time. A maximum of five times can be created in a week.

10.1 RESERVED POWER DETERMINATION

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

1. 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.

2. Allocated mode: In this mode, the user allocates the amount of power that each port may reserve. The allocated/reserved power for each port/PD is specified in the Maximum Power fields.

3. LLDP-MED mode: This mode is similar to the Class mode except that each port determines the amount power it reserves by exchanging PoE information using the LLDP 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.

10.2 POWER MANAGEMENT MODE

There are 2 modes for configuring when to shut down the ports:

1. 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 lower number port has higher priority.

2. 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.

10.3 OTHER SETTINGS

1. PoE Power Supply: To determine the amount of power the PD may use, you must define what amount of power a power source can deliver. Valid values are in the range 0 to 240 Watts.

2. 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.

3. 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.

4. 4 Pair: The 4 Pairs represent the 60 W power supply for the port. The option is only available when following rules are applied.

- High power switch model supports.
- Only port1 or port2 supports.
- Current operation mode is 802.3at.
- Enable: Enable 4Pairs to support 60 W.
- Disable: Disable 4Pairs to limit 30W of power.

5. PoE Priority: The Priority represents the ports 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 turn off starting from the port with the highest port number.

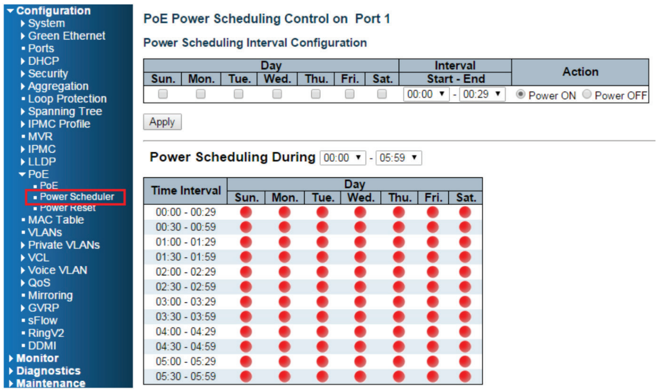
6. Maximum Power: The Maximum Power value contains a numerical value that indicates the maximum power in watts that can be delivered to a remote device.

For ports that support 4Pairs mode, the maximum allowed value is 60 W; others are 30 W.

10.4 POE POWER SCHEDULING AND RESET

The power scheduling is used to control the power alive interval on PoE port. You can 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 change 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	
□	□	□	□	□	□	□	00:00 ▾ - 00:29 ▾	● Power ON ○ Power OFF

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	🔴	🔴	🔴	🔴	🔴	🔴	🔴

FIGURE 10-1. POE SCHEDULING AND RESET

CHAPTER 10: POWER OVER ETHERNET APPLICATION

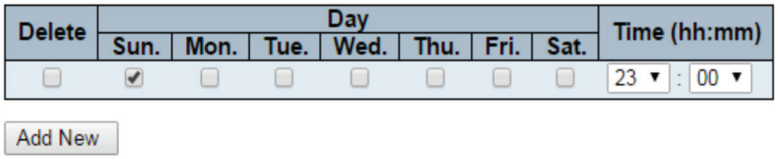
1. Day: Checkmarks indicate which day are members of the set. From Sunday to Saturday.

2. Interval: Start - Select the start hour and minute. End - Select the end hour and minute. There are 48 time intervals in one day. Each interval has 30 minutes.

3. 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.

4. PoE Power Reset: The entry is used to control the power reset time on PoE port. You can create at maximum 5 entries for each PoE port.



Delete	Day							Time (hh:mm)
	Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.	
□	☑	□	□	□	□	□	□	23 ▾ : 00 ▾

FIGURE 10-2. POE POWER RESET CONTROL ON PORT 1

10.5 EXAMPLE 1

1. Parameter Setting:

- Reserved Power determined: Class
- Power Management Mode: Actual Consumption
- Primary Power Supply: 6W

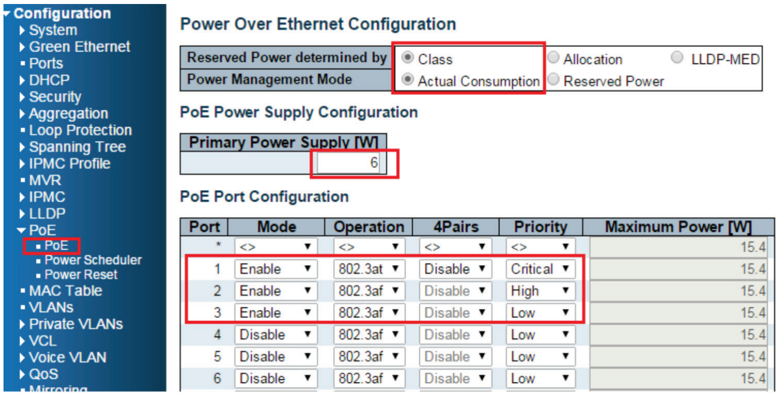
2. Test Port

- 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	● Class	○ Allocation	○ LLDP-MED
Power Management Mode	● Actual Consumption	○ Reserved Power	

PoE Power Supply Configuration

Primary Power Supply [W]
6

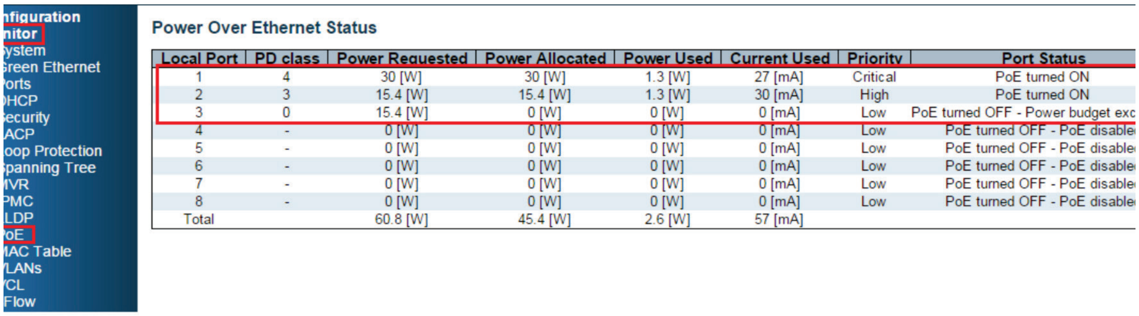
PoE Port Configuration

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

FIGURE 10-3. WEB CONFIGURATION

5. Test Result: PoE port status can be monitored by Web: Monitor —> PoE

The following table shows that if the system budget is not enough for all PoE devices, the port with higher priority port will be fed power first. The last priority port (port 3) will not be powered.



Power Over Ethernet Status

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1	4	30 [W]	30 [W]	1.3 [W]	27 [mA]	Critical	PoE turned ON
2	3	15.4 [W]	15.4 [W]	1.3 [W]	30 [mA]	High	PoE turned ON
3	0	15.4 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - Power budget exc
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disable
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disable
6	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disable
7	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disable
8	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disable
Total		60.8 [W]	45.4 [W]	2.6 [W]	57 [mA]		

FIGURE 10-4. TEST RESULT

10.6 EXAMPLE 2

1. Parameter Setting:

- Reserved Power determined: Allocation
- Power Management Mode: Reserved Power
- Primary Power Supply: 138 W (> all ports reserved power)

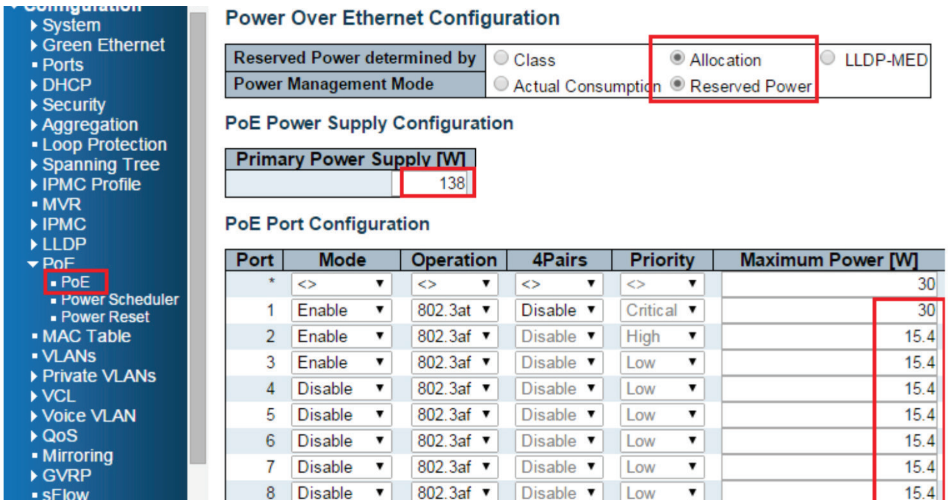
2. Port Maximum Power

- Port 1: 30 W
- Port 2– Port 8: 15.4 W
- Total: 137.8 W

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	○ Class ● Allocation ○ LLDP-MED
Power Management Mode	○ Actual Consumption ● Reserved Power

PoE Power Supply Configuration

Primary Power Supply [W]
138

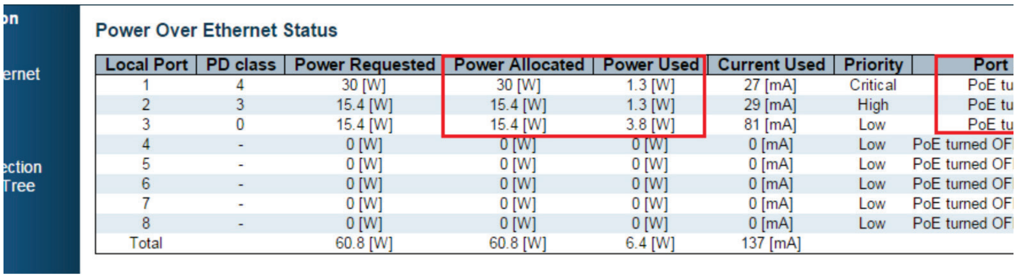
PoE Port Configuration

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

FIGURE 10-5. WEB CONFIGURATION

5. Test Result: PoE port status can be monitored by Web: Monitor —> PoE

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



Power Over Ethernet Status

Local Port	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port
1	4	30 [W]	30 [W]	1.3 [W]	27 [mA]	Critical	PoE tu
2	3	15.4 [W]	15.4 [W]	1.3 [W]	29 [mA]	High	PoE tu
3	0	15.4 [W]	15.4 [W]	3.8 [W]	81 [mA]	Low	PoE tu
4	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OF
5	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OF
6	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OF
7	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OF
8	-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OF
Total		60.8 [W]	60.8 [W]	6.4 [W]	137 [mA]		

FIGURE 10-6. TEST RESULT

APPENDIX A: REGULATORY INFORMATION

A.1 FCC STATEMENT

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

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

Shielded cables must be used with this equipment to maintain compliance with radio frequency energy emission regulations and ensure a suitably high level of immunity to electromagnetic disturbances.

All power supplies are certified to the relevant major international safety standards.

APPENDIX A: REGULATORY INFORMATION

A.2 NOM STATEMENT

1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
4. Todas las instrucciones de operación y uso deben ser seguidas.
5. El aparato eléctrico no deberá ser usado cerca del agua—por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc.
6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
8. Servicio—El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.
13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.
16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.
18. Servicio por personal calificado deberá ser provisto cuando:
    A: El cable de poder o el contacto ha sido dañado; u
    B: Objectos han caído o líquido ha sido derramado dentro del aparato; o
    C: El aparato ha sido expuesto a la lluvia; o
    D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
    E: El aparato ha sido tirado o su cubierta ha sido dañada.

APPENDIX B: DISCLAIMER/TRADEMARKS

B.1 DISCLAIMER

Black Box Corporation shall not be liable for damages of any kind, including, but not limited to, punitive, consequential or cost of cover damages, resulting from any errors in the product information or specifications set forth in this document and Black Box Corporation may revise this document at any time without notice.

B.2 TRADEMARKS USED IN THIS MANUAL

Black Box and the Black Box logo type and mark are registered trademarks of Black Box Corporation.

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

NOTES

NOTES

NOTES

NEED HELP?
LEAVE THE TECH TO US

LIVE 24/7 TECHNICAL SUPPORT

1.877.877.2269

BLACK BOX®