

GE-DSH-73/DSH-82/DSH-82-PoE User Manual



Copyright	© 2010 GE Security, Inc. This document may not be copied in whole or in part or otherwise reproduced without prior written consent from GE Security, Inc., except where specifically permitted under US and international copyright law.
Disclaimer	The information in this document is subject to change without notice. GE Security, Inc. ("GE Security") assumes no responsibility for inaccuracies or omissions and specifically disclaims any liabilities, losses, or risks, personal or otherwise, incurred as a consequence, directly or indirectly, of the use or application of any of the contents of this document. For the latest documentation, contact your local supplier or visit us online at www.gesecurity.com. This publication may contain examples of screen captures and reports used in daily operations. Examples may include fictitious names of individuals and companies. Any similarity to names and addresses of actual businesses or persons is entirely coincidental.
Trademarks and patents	GE and the GE monogram are trademarks of General Electric Company. Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.
Intended use	Use this product only for the purpose it was designed for; refer to the data sheet and user documentation for details. For the latest product information, contact your local supplier or visit us online at www.gesecurity.com. This product is intended to be supplied by a UL Listed Direct Plug-In Power Unit marked "Class 2" or "LPS" and output rated 48 VDC, 380 mA minimum.
FCC compliance	This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. You are cautioned that any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
Regulatory information	
Manufacturer	GE Security, Inc. HQ and regulatory responsibility: GE Security, Inc., 8985 Town Center Parkway, Bradenton, FL 34202, USA EU authorized manufacturing representative: GE Security B.V., Kelvinstraat 7, 6003 DH Weert, The Netherlands
European Union directives	 2002/96/EC (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.
Contact information	For contact information see our Web site: www.gesecurity.com. For contact information see our Web site: www.gesecurity.eu.

Content

Chapter 1 Introduction 1

Package Contents 2

Chapter 2 Installation 11

Hardware Description 11

Installing the Switch 23

Chapter 3 Network Application 33

Chapter 4 Console Management 37

Chapter 5 Web-Based Management 43

About Web-based Management 43

Requirements 44

Logging on the Switch 44

System 46

Port Management 65

Protocol 76

Security 118

Digital Input/Output (GE-DSH-73) 129

Power Over Ethernet (GE-DSH-82-PoE) 131

Factory Default 135

Save Configuration 135

System Reboot 136

Chapter 6 Command Sets 137

System Commands Set 137

Port Commands Set 140

Trunk Commands Set 142

VLAN Commands Set 143

Spanning Tree Commands Set 145

QOS Commands Set 147

IGMP Commands Set 148

MAC / Filter Table Commands Set 149

SNMP Commands Set 150

Port Mirroring Commands Set 153

802.1x Commands Set 154

TFTP Commands Set 156

SystemLog, SMTP and Event Commands Set 157

SNTP Commands Set 159
X-ring Commands Set 160
PoE Command Set 161

Chapter 7 Switch Operation 163

Address Table 163

Chapter 8 Power Over Ethernet Overview 165

What is PoE? 165

Appendix A RJ-45 Pin Assignment 171

Switch's RJ-45 Pin Assignments 171

10/100Mbps, 10/100Base-TX 172

Appendix B Troubleshooting 175

Chapter 1

Introduction



GE-DSH-82

GE-DSH-82-PoE

GE-DSH-73

The GE Security Managed Industrial Ethernet Switch series - the GE-DSH-82, GE-DSH-82-PoE and GE-DSH-73 are multiple 10/100Mbps ports Ethernet Switches with Gigabit TP/SFP fiber optical combo connective ability and robust layer 2 features. The description of these models is below:

GE-DSH-82

8-Port 10/100Base-TX + 2-Port Gigabit TP/SFP Combo Managed Industrial Ethernet Switch

GE-DSH-82-PoE

8-Port 10/100Base-TX + 2-Port Gigabit TP/SFP Combo Managed Industrial PoE Switch

GE-DSH-73

7-Port 10/100Base-TX + 3-Port Gigabit TP/SFP Combo Managed Industrial Ethernet Switch

Package Contents

What's in the box

Open the Managed Industrial Switch box and carefully unpack it. The box should contain the following items:

The Managed Industrial Switch	x1
User's manual on CD	x1
Installation Sheet	x1
RJ-45 to RS-232 Cable	x1

If any of these are missing or damaged, please contact your dealer immediately, if possible, retain the carton including the original packing material, and use them again to repack the product in case there is a need to return it to us.

Product Description

Enhanced Reliability for Industrial Networks

The GE Security GE-DSH-82 series Managed Industrial Ethernet Switch with multiple redundant ring technology is equipped with 8 10/100Mbps Fast Ethernet ports and 2 Gigabit TP/SFP combo interfaces and the GE-DSH-73 is equipped with 7 10/100Mbps Fast Ethernet ports and 3 Gigabit TP/SFP combo interfaces. All of them are delivered in a rugged high-strength case. It is an industrially (substation) hardened and fully managed Ethernet Switch specifically designed to operate reliably in electrically harsh and climatically demanding environments. The GE-DSH-82 / GE-DSH-73 series is the most reliable choice for highly managed and Fiber Ethernet applications.

- Wide Range Operating Temperature
- Redundant Ethernet Network
- Manageable
- Power Redundant
- Gigabit / Fiber uplink capability

Fast Recovery to a Redundant Ethernet Network

The GE-DSH-82 / GE-DSH-73 series features strong and rapid self-recovery capability to prevent interruptions and outside intrusions. It incorporates advanced redundant data Ring technology; Rapid Spanning Protocol (IEEE 802.1w RSTP) and a redundant power supply system into customers' industrial automation network to enhance system reliability and uptime in the harsh factory environments. It also protects customer's industrial network connectivity with switching recovery capability that is used for implementing fault tolerant ring and mesh network architectures. If the Industrial network was interrupted accidentally, the fault recovery times could be less than 20ms to quickly bring the network back to normal operation.

Tough, Environmentally Hardened Design

With IP-30 aluminum industrial case protection, the GE-DSH-82 / GE-DSH-73 series provides a high level of immunity against electromagnetic interference and heavy electrical surges which are usually found on plant floors or in curb side traffic control cabinets. The GE-DSH-82 / GE-DSH-73 series also provides a wide range of power supply options suitable for multiple industries and for worldwide operation. The feature of operating temperature range from -40 to 75 Degree C allows the Managed Industrial Switch to be placed in almost any difficult environment.

Robust Layer 2 Features and Advanced Security

The GE-DSH-82 / GE-DSH-73 series supports robust advanced features including IEEE 802.1Q VLAN, GVRP, Port link aggregation, QoS, broadcast storm control, MAC address filtering, IGMP snooping enhanced security and bandwidth utilization to fit a variety of applications. Via aggregation of supporting port, the GE-DSH-82 / GE-DSH-73 series allows the operation of high-speed trunk combining multiple ports. Maximum up to 4 ports of the GE-DSH-82 / GE-DSH-73 series can be assigned for 4 trunk groups and support fail-over as well. Additionally, its standard-compliant implementation ensures interoperability with equipments from other vendors.

Product Features

- **Physical Port**
 - o GE-DSH-82
 - 8-Port 10/100Base-TX RJ-45
 - 2-Port 10/100/1000Base-T TP combo interfaces
 - 2 mini-GBIC / SFP slots shared with Gigabit copper ports and support 100/1000 Dual Mode

- 1 RJ-45 Console interface for Switch basic management and setup
- o GE-DSH-82-PoE (Power Over Ethernet)
 - 2-Port 10/100/1000Base-T TP combo interfaces
 - 2 mini-GBIC / SFP slots shared with Gigabit copper ports and support 100/1000 Dual Mode
 - 1 RJ-45 Console interface for Switch basic management and setupGE-DSH-73
 - Supports 48VDC, 15.4 watts PoE power outputs to 9 IEEE 802.3af compliant Powered Devices
 - Power feeding On/Off and priority configuration
 - Powered Device Auto detection
 - LED PoE Status Monitoring

Note: The GE-DSH-82-PoE, PoE requires the use of the recommended external power source.

- o GE-DSH-73
 - 7-Port 10/100Base-TX RJ-45
 - 3-Port 10/100/1000Base-T TP combo interfaces
 - 3 mini-GBIC / SFP slots shared with Gigabit copper ports and support 100/1000 Dual Mode
 - 1 RJ-45 Console interface for Switch basic management and setup
 - Industrial Conformance
 - Wide range redundant power with polarity reverse protect function
 - -40 to 75 Degree C operation temperature
 - IP-30 metal case
 - Relay alarm for port breakdown, power failure
 - Supports 4000 VDC Ethernet ESD protection
 - Free fall, Shock and Vibration Stability
 - Rapid Ring
 - Rapid Ring, Dual Homing, Couple Ring Topology
 - Provides redundant backup feature and the recovery time less than 20ms

- **Layer 2 Features**
 - o Complies with the IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z Gigabit Ethernet standards
 - o Supports Auto-negotiation and half duplex/full duplex modes for all 10Base-T/100Base-TX and 1000Base-T ports
 - o Auto-MDI/MDI-X detection on each RJ-45 port
 - o Prevents packet loss with back pressure (Half-Duplex) and IEEE 802.3x PAUSE frame flow control (Full-Duplex)
 - o Supports VLANs
 - IEEE 802.1Q Tagged based VLAN
 - Port-Based VLAN
 - GVRP
 - Up to 255 VLANs groups, out of 4K VLAN IDs
 - o Supports Spanning Tree Protocol
 - STP, IEEE 802.1D Spanning Tree Protocol
 - RSTP, IEEE 802.1w Rapid Spanning Tree Protocol
 - o Supports Link Aggregation
 - Up to 4 Trunk groups
 - Up to 4 ports per trunk group with 800Mbps bandwidth (Full Duplex mode)
 - IEEE 802.3ad LACP (Link Aggregation Control Protocol)
 - Cisco ether-Channel (Static Trunk)
- Quality of Service
 - o 4 priority queues on all switch ports
 - o Traffic classification by:
 - Port-Based priority
 - IEEE 802.1p Class of Service
 - IP TOS (Type of Service) priority
 - o Supports strict priority and Weighted Round Robin (WRR) policies
 - o Ingress/Egress Bandwidth control on each port
- Multicast
 - o IGMP Snooping v1 and v2
 - o IGMP Query mode for Multicast Media application

- Security
 - o IEEE 802.1x Port-Based Authentication
 - o MAC address Filtering and MAC address Binding
 - o IP address security management to prevent unauthorized intruder
 - o Port Mirroring to monitor the incoming or outgoing traffic on a particular port
 - o Management
 - WEB-based, Telnet, Console Command Line management
 - Access through SNMP v1, v2c and v3 set and get requests
 - SNMP Trap / SMTP email for alarm notification of events
 - System Log Server / Client
 - Configuration backup / restore
 - E-mail event alert
 - TFTP firmware upgrade
 - Support LLDP to allow switch to advise its identification and capability on the LAN

Product Specifications

Product	GE-DSH-82	GE-DSH-82-PoE	GE-DSH-73
Hardware Specification			
10/100Mbps Copper Ports	8 10/ 100Base-TX RJ-45 Auto-MDI/MDI-X ports	8 10/ 100Base-TX RJ-45 Auto-MDI/MDI-X ports	7 10/ 100Base-TX RJ-45 Auto-MDI/MDI-X ports
1000Mbps Copper Ports	2 10/100/1000Base-T RJ-45 ports	2 10/100/1000Base-T RJ-45 ports	3 10/100/1000Base-T RJ-45 ports
SFP/mini-GBIC Slots	2 SFP interfaces, shared with Port-9 and Port-10	2 SFP interfaces, shared with Port-9 and Port-10	3 SFP interfaces, shared with Port-7, Port-9 and Port-10
Switch Architecture	Store-and-Forward		
Switch Fabric	5.6Gbps / non-blocking	5.6Gbps / non-blocking	7.4Gbps / non-blocking
Switch Throughput	4.16Mpps @64Bytes	4.16Mpps @64Bytes	5.5Mpps@64bytes
Address Table	8K entries		

Share Data Buffer	1Mbit		
Maximum Frame Size	1522 Bytes packet		
Flow Control	Back pressure for Half-Duplex IEEE 802.3x Pause Frame for Full-Duplex		
LED	Per unit: Power (Green), Ring Master (Green), Power 1 (Green), Power 2 (Green), Fault (Red) 8 port 10/100: Link/Activity (Green), Full duplex/Collision (Yellow) 2 SFP port: LNK/ACT(Green) 2 1000T: LNK/ACT(Green), 1000M(Green)	Per unit: Power (Green), Ring Master (Green), Power 1 (Green), Power 2 (Green), Fault (Red) 8 port 10/100: Link/Activity (Green), Full duplex/Collision (Yellow) 2 SFP port: LNK/ACT(Green), 2 1000T: LNK/ACT(Green), 1000M(Green) PoE: PoE In-use (Green)	Per unit: Power (Green), Ring Master (Green), Power 1 (Green), Power 2 (Green), Fault (Red) 7 port 10/100: Link/Activity (Green), Full duplex/Collision (Yellow) 3 SFP port: LNK/ACT(Green) 3 1000T: LNK/ACT(Green), 1000M(Green)
DI/DO	---	2 Digital Input (DI): Level 0: -30~2V Level 1: 10~30V Max. input current: 8mA 2 Digital Output(DO): Open collector to 40VDC, 200mA	---
ESD Protection	4KV DC	6KV DC	6KV DC
EFT Protection	3KV DC	3KV DC	3KV DC
Console Interface	One RJ-45-to -RS-232 male connector for switch management		
Power Over Ethernet			
PoE Standard	---	IEEE 802.3af PSE (Power Sourcing Equipment)	---
Units can be Powered	---	8	---
PoE Power Output	---	48V DC, Max. 15.4 watts, 350mA	---
Power Pin Assignment	---	1/2(+), 3/6(-)	---

Layer 2 function	
Management Interface	Console, Telnet, Web Browser, SNMP v1, v2c and v3
Port Configuration	Port disable/enable. Auto-negotiation 10/100Mbps full and half duplex mode selection. Flow Control disable / enable. Bandwidth control on each port.
Port Status	Display each port's speed duplex mode, link status, Flow control status. Auto negotiation status
VLAN	Port-Based VLAN, up to 9 VLAN groups IEEE 802.1q Tagged Based VLAN , 4K VLAN ID, up to 256 VLAN groups
Spanning Tree	IEEE 802.1d Spanning Tree IEEE 802.1w Rapid Spanning Tree
Link Aggregation	Static Port Trunk IEEE 802.3ad LACP (Link Aggregation Control Protocol) Supports 4groups of 4-Port trunk
QoS	Traffic classification based on : Port Number, 802.1Q Tag, 802.1p priority, IP DSCP/TOS field in IP Packet
IGMP Snooping	v1 and v2 256 multicast groups and IGMP query
Bandwidth Control	Per port bandwidth control Ingress: 500Kb~80Mbps Egress: 64Kb~80Mbps
Port Mirror	RX / TX / Both
Security	Support 100 entries of MAC address for static MAC and another 100 for MAC filter Support 10 IP addresses that have permission to access the switch management and to prevent unauthorized intruder

SNMP MIBs	RFC-1213 MIB-II RFC-2863 Interface MIB RFC-1493 Bridge MIB RFC-2819 RMON MIB (Group 1, 2, 3, 9) RFC-2674 Extended Bridge MIB (Q-Bridge) Private MIB
Standards Conformance	
Regulation Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX/100Base-FX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x Flow Control and Back pressure IEEE 802.1d Spanning tree protocol IEEE 802.1w Rapid spanning tree protocol IEEE 802.1p Class of service IEEE 802.1Q VLAN Tagging IEEE 802.1x Port Authentication Network Control IEEE 802.3af Power over Ethernet (GE-DSH-82-PoE) RFC 768 UDP RFC 793 TFTP RFC 791 IP RFC 792 ICMP RFC 2068 HTTP RFC 1112 IGMP version 1 RFC 2236 IGMP version 2

Chapter 2

Installation

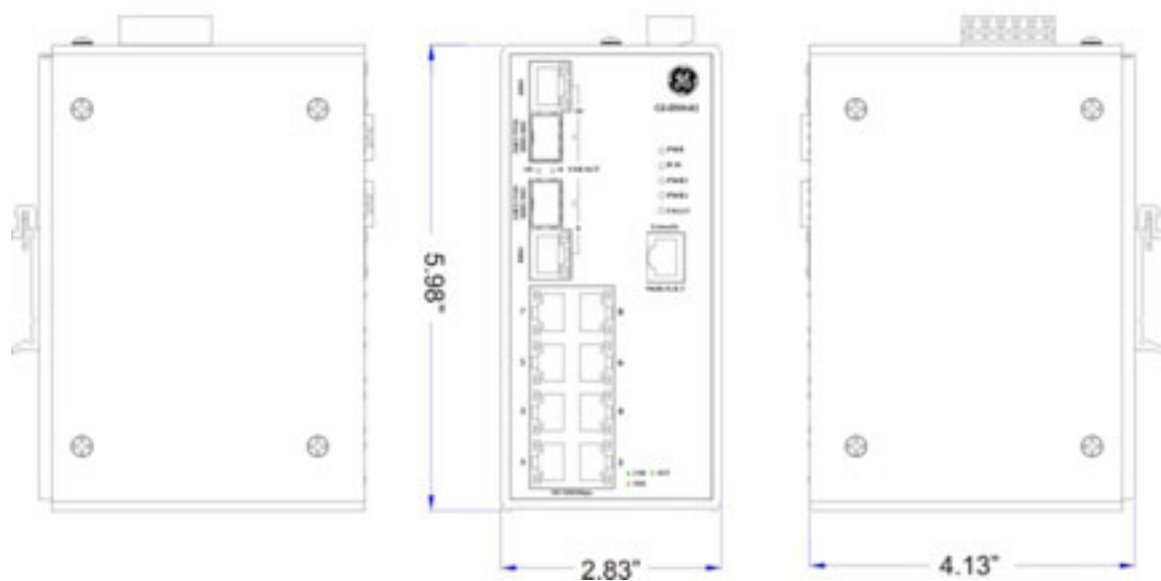
Hardware Description

Physical Dimensions

GE-DSH-82

(W x D x H): 2.83" x 4.13" x 5.98" / 72mm x 105mm x 152mm.

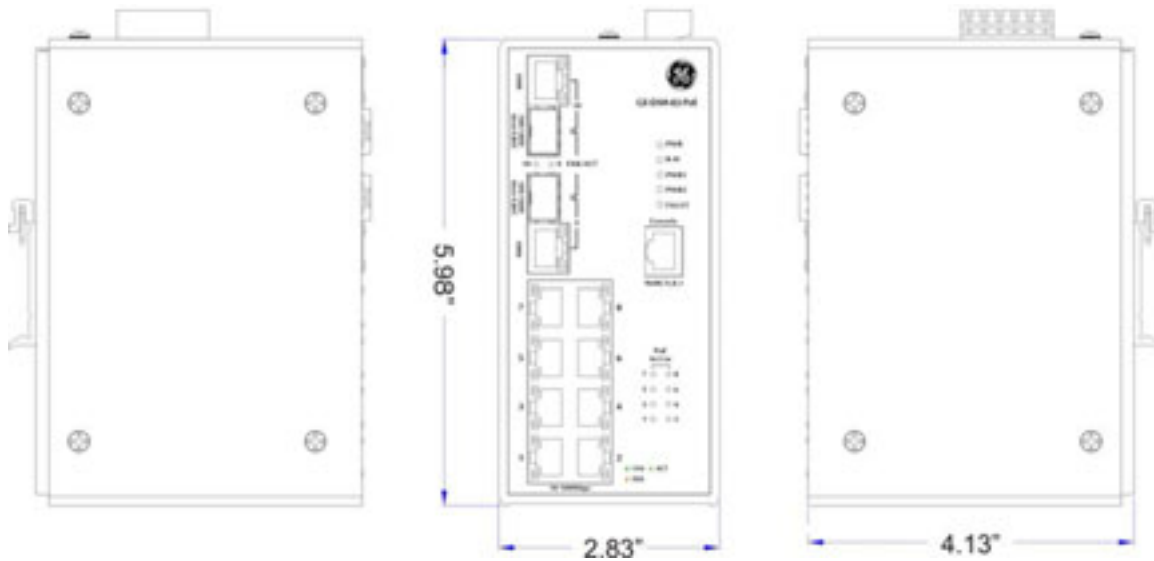
Figure 2-1: GE-DSH-82 panel layout



GE-DSH-82-PoE

(W x D x H): 2.83" x 4.13" x 5.98" / 72mm x 105mm x 152mm

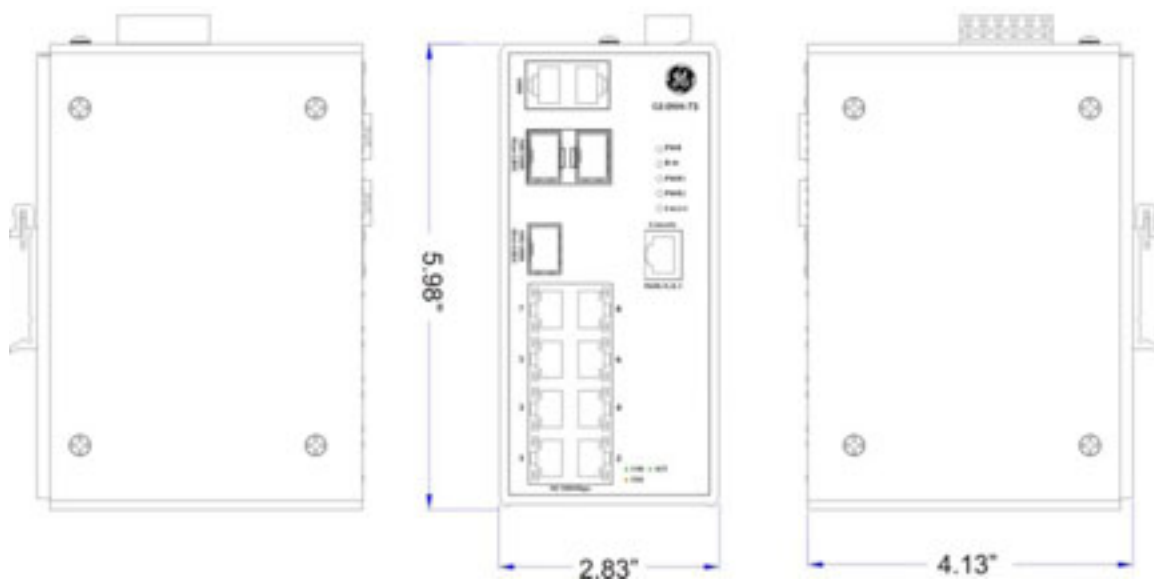
Figure 2-2: GE-DSH-82-PoE panel layout



GE-DSH-73

(W x D x H): 2.83" x 4.13" x 5.98" / 72mm x 105mm x 152mm

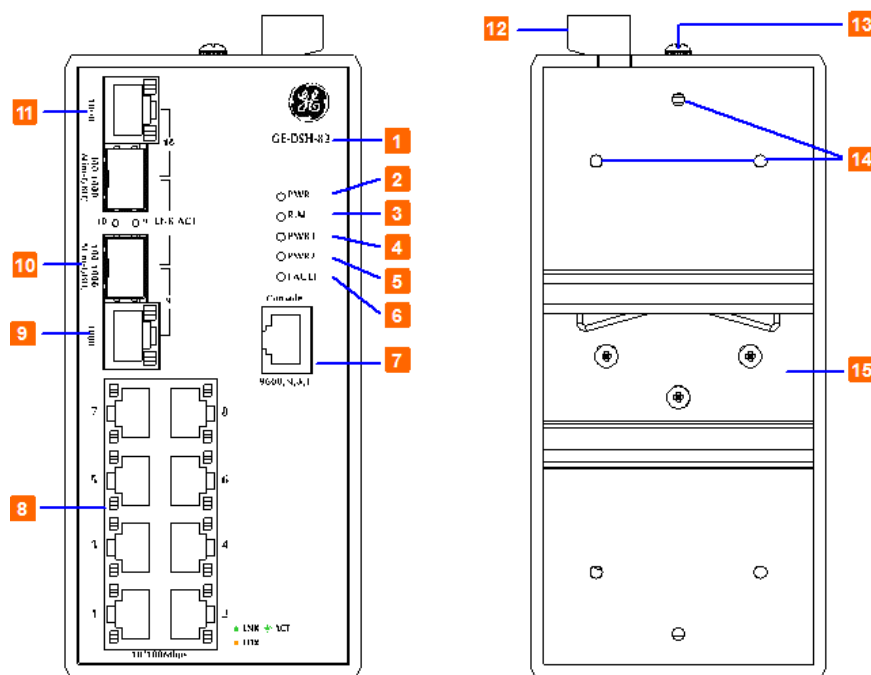
Figure 2-3: GE-DSH-73 panel layout



Front / Rear Panel

The Front Panel and Rear Panel of the GE-DSH-82 Managed Industrial Switch are shown below:

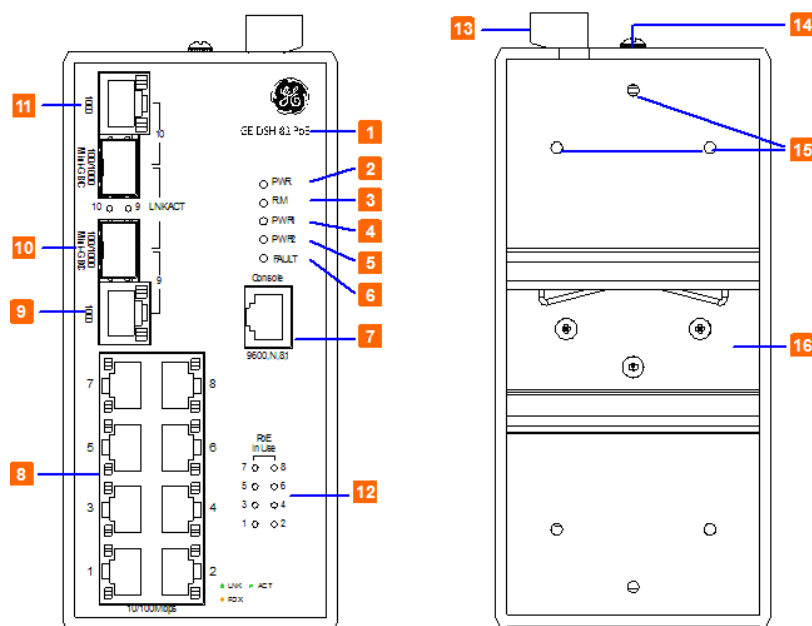
Figure 2-4: Front and Rear Panel of GE-DSH-82



1. Model Name	9. 10/100/1000Base-T port
2. System Power: LED	10. 1000Base-SX/LX SFP slot
3. Ring Master: LED indicator	11. LED indicators for 1000Base-SX/LX port
4. LED for power 1 input	12. 6-Pin Terminal Block
5. LED for power 2 input	13. Ground Screw
6. FAULT: LED indicator	14. Screw holes for Wall Mounting kit
7. RJ-45 type RS-232 Console	15. DIN-Rail Kit
8. 8 x 10/100Base-TX port	

The Front Panel and Rear Panel of the GE-DSH-82-PoE Managed Industrial Switch are shown below:

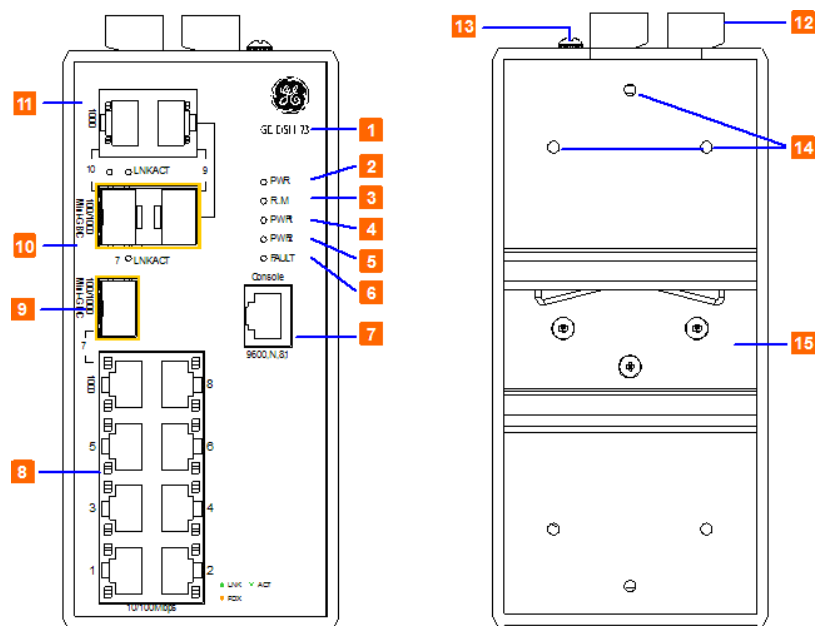
Figure 2-5: Front and Rear Panel of GE-DSH-82-PoE



1. Model Name	9. 10/100/1000Base-T port
2. System Power: LED	10. 1000Base-SX/LX SFP slot
3. Ring Master: LED indicator	11. LED indicators for 1000Base-SX/LX port
4. LED for power 1 input	12. LED indicators for PoE power output
5. LED for power 2 input	13. 6-Pin Terminal Block
6. FAULT: LED indicator	14. Ground Screw
7. RJ-45 type RS-232 Console	15. Screw holes for Wall Mounting kit
8. 8 x 10/100Base-TX port	16. DIN-Rail Kit

The Front Panel and Rear Panel of the GE-DSH-73 Managed Industrial Switch are shown below:

Figure 2-6: Front and Rear Panel of GE-DSH-73



1. Model Name	9. 1000Base-SX/LX SFP slot (Port-7)
2. System Power: LED	10. 1000Base-SX/LX SFP slots (Port-9 / Port-10)
3. Ring Master: LED indicator	11. 10/100/1000Base-T ports (Port-9 / Port-10)
4. LED for power 1 input	12. 6-Pin Terminal Block
5. LED for power 2 input	13. Ground Screw
6. FAULT: LED indicator	14. Screw holes for Wall Mounting kit
7. RJ-45 type RS-232 Console	15. DIN-Rail Kit
8. 8 x 10/100Base-TX port	

Top View

The top panel of the GE-DSH-82 Managed Industrial Switch has one terminal block connector of two DC power inputs and one fault alarm.

Figure 2-7: Top Panel of GE-DSH-82

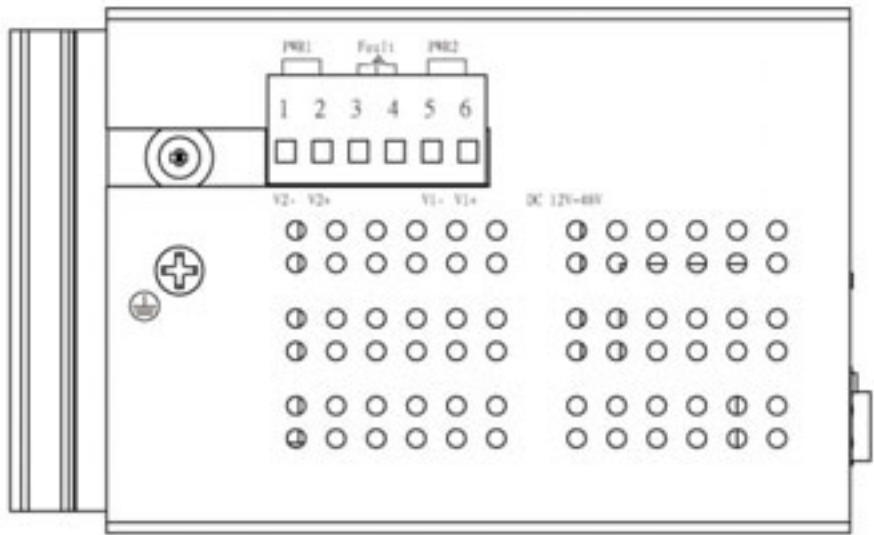
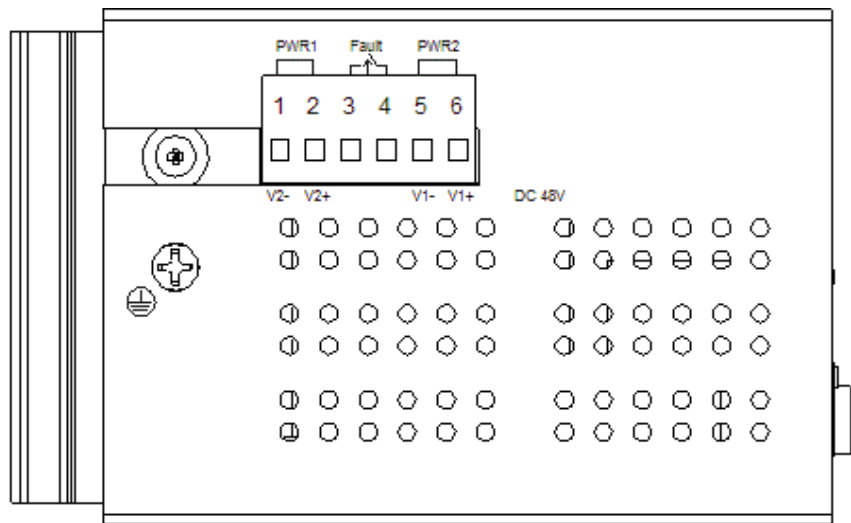


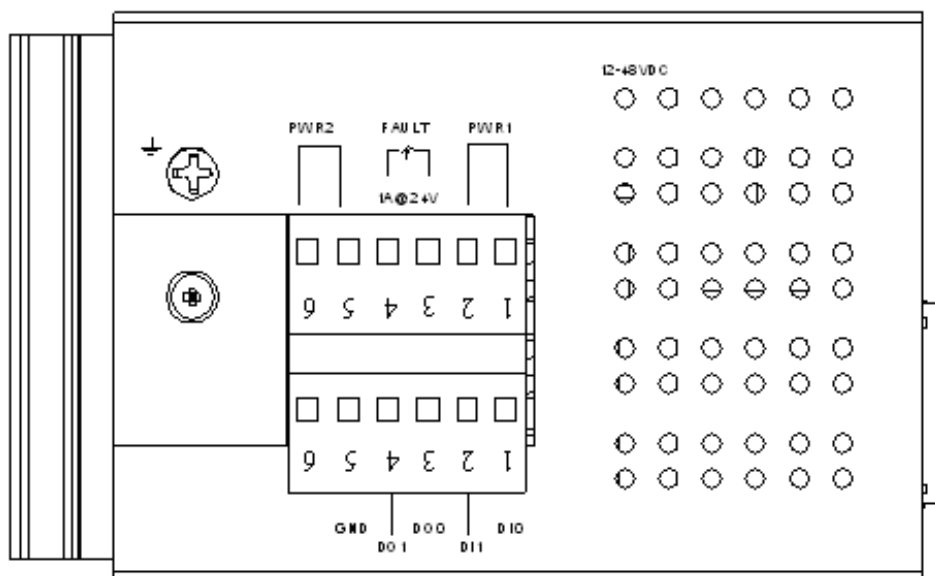
Figure 2-8: Top Panel of GE-DSH-82-PoE



The top panel of the GE-DSH-73 Managed Industrial Switch has two terminal block connectors:

- Power connector - consists of two DC power inputs and one fault alarm.
- DI/DO connector - comprises two digital inputs-DI0 and DI1 and two digital outputs-DO0 and DO1.

Figure 2-9: Top Panel of GE-DSH-73



LED Indicators

The diagnostic LEDs that provide real-time information of system and optional status are located on the front panel of the GE-DSH series. The following table provides the description of the LED status and their meanings for the Managed Industrial Switch.

GE-DSH-82 LED Indicators

- System**

LED	Color	Status	Meaning
PWR	Green	On	The switch unit is power on.
		Off	No power.
R.M.	Green	On	The industrial switch is the master of X-Ring group.
		Off	The industrial switch is not a ring master in X-Ring group.
PWR1	Green	On	Power 1 is active.
		Off	Power 1 is inactive.
PWR2	Green	On	Power 2 is active.
		Off	Power 2 is inactive.
FAULT	Red	On	Power or port failure.
		Off	No failure.

- 10/100Base-TX Ports – Port-1 to Port-8**

LED	Color	Status	Meaning
Port-1 ~ Port-8	Green	On	A network device is detected.
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached.
	Amber	On	The port is operating in full-duplex mode.
		Blinking	Collision of Packets occurs.
		Off	The port is in half-duplex mode or no device is attached.

- 10/100Base-TX Ports – **Port-9, Port-10**

LED	Color	Status	Meaning
Port 9, Port 10 (RJ-45)	Green (Upper LED)	On	A network device is detected.
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached
	Green (Lower LED)	On	1000M
		Off	10/100M
Link/Active (P9, P10 SFP)	Green	On	The SFP port is linking
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached

GE-DSH-73 LED Indicators

- System**

LED	Color	Status	Meaning
PWR	Green	On	The switch unit is power on.
		Off	No power.
R.M.	Green	On	The industrial switch is the master of X-Ring group.
		Off	The industrial switch is not a ring master in X-Ring group.
PWR1	Green	On	Power 1 is active.
		Off	Power 1 is inactive.
PWR2	Green	On	Power 2 is active.
		Off	Power 2 is inactive.
FAULT	Red	On	Power or port failure.
		Off	No failure.

- 10/100Base-TX Ports – Port-1 to Port-8

LED	Color	Status	Meaning
Port-1 ~ 6 & Port-8	Green	On	A network device is detected.
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached.
	Amber	On	The port is operating in full-duplex mode.
		Blinking	Collision of Packets occurs.
		Off	The port is in half-duplex mode or no device is attached.

- 10/100Base-TX Ports – Port-7, Port-9 and Port-10

LED	Color	Status	Meaning
Port 7, Port 9, Port 10 (RJ-45)	Green (Upper LED)	On	A network device is detected.
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached
	Green (Lower LED)	On	1000M
		Off	10/100M
Link/Active (P7, P9, P10 SFP)	Green	On	The SFP port is linking
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached

GE-DSH-82-PoE LED Indicators

- **System**

LED	Color	Status	Meaning
PWR	Green	On	The switch unit is power on.
		Off	No power.
R.M.	Green	On	The industrial switch is the master of X-Ring group.
		Off	The industrial switch is not a ring master in X-Ring group.
PWR1	Green	On	Power 1 is active.
		Off	Power 1 is inactive.
PWR2	Green	On	Power 2 is active.
		Off	Power 2 is inactive.
FAULT	Red	On	Power or port failure.
		Off	No failure.

- **10/100Base-TX Ports – Port-1 to Port-8**

LED	Color	Status	Meaning
Port-1 ~ Port-8	Green	On	A network device is detected.
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached.
	Amber	On	The port is operating in full-duplex mode.
		Blinking	Collision of Packets occurs.
		Off	The port is in half-duplex mode or no device is attached.

- **PoE port link – Port-1 to Port-8**

LED	Color	Status	Meaning
FWD (P1 to P8)	Green	On	An IEEE 802.3af PoE power device is detected.
		Off	No IEEE 802.3af PoE power device attached

- **10/100/1000Base-T / SFP combo interface - Port-9, Port-10**

LED	Color	Status	Meaning
Port 9, Port 10 (RJ-45)	Green (Upper LED)	On	A network device is detected.
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached
	Green (Lower LED)	On	1000M
		Off	10/100M
Link/Active (P9, P10 SFP)	Green	On	The SFP port is linking
		Blinking	The port is transmitting or receiving packets from the TX device.
		Off	No device attached

Installing the Switch

This section describes how to install your Managed Industrial Switch and make connections to the Managed Industrial Switch. Please read the following topics and perform the procedures in the order being presented. To install your switch on a desktop or shelf, simply complete the following steps.

In this paragraph, we will describe how to install the 8 10/100TX w/ X-Ring Managed Industrial Switch and the installation points attended to it.

Installation Steps

1. Unpack the Industrial switch
2. Check if the DIN-Rail is screwed on the Industrial switch or not. If the DIN-Rail is not screwed on the Industrial switch, please refer to DIN-Rail Mounting section for DIN-Rail installation. If users want to wall mount the Industrial switch, please refer to Wall Mount Plate Mounting section for wall mount plate installation.
3. To hang the Industrial switch on the DIN-Rail track or wall.
4. Power on the Industrial switch. Refer to the Wiring the Power Inputs section for knowing the information about how to wire the power. The power LED on the Industrial switch will light up. Please refer to the LED Indicators section for indication of LED lights.
5. Prepare the twisted-pair, straight through Category 5 cable for Ethernet connection.
6. Insert one side of RJ-45 cable (category 5) into the Industrial switch Ethernet port (RJ-45 port) and another side of RJ-45 cable (category 5) to the network device's Ethernet port (RJ-45 port), ex: Switch PC or Server. The UTP port (RJ-45) LED on the Industrial switch will light up when the cable is connected with the network device. Please refer to the LED Indicators section for LED light indication.

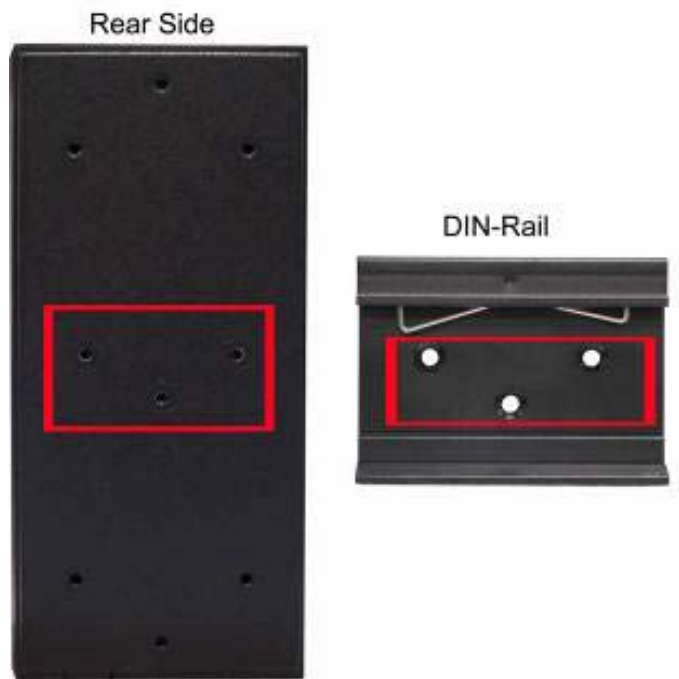
NOTE: Make sure that the connected network devices support MDI/MDI-X. If it does not support, use the crossover category-5 cable.

7. When all connections are set and LED lights all show in normal, the installation is complete.

DIN-Rail Mounting

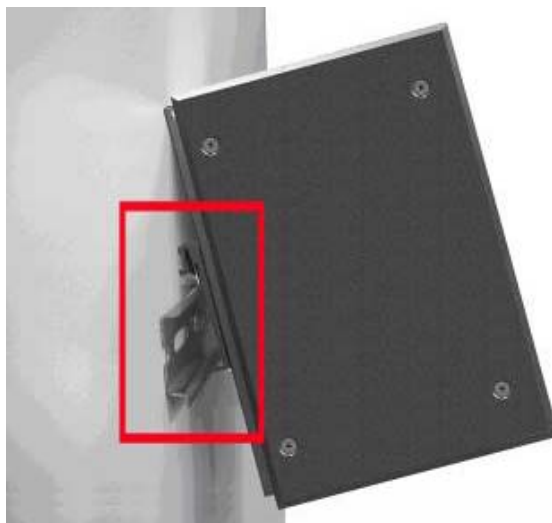
The DIN-Rail is screwed on the Industrial Switch when out of factory. If the DIN-Rail is not screwed on the Industrial Switch, please see the following pictures to screw the DIN-Rail on the Switch. Follow the steps below to hang the Industrial Switch.

Figure 2-10: Rear Panel - DIN-Rail Kit



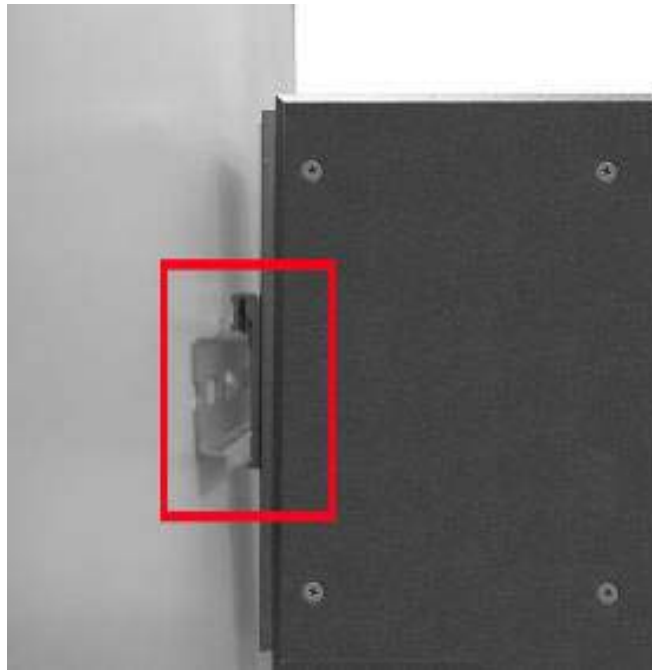
1. Insert the top of DIN-Rail into the track.

Figure 2-11: Rear Panel - DIN-Rail Kit



2. Lightly push the DIN-Rail into the track.

Figure 2-12: DIN-Rail mounting



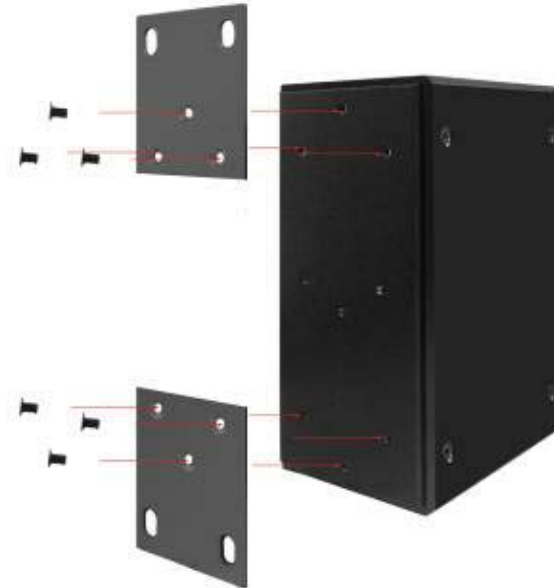
3. Check if the DIN-Rail is tightened on the track or not.
4. To remove the industrial switch from the track, reverse above steps.

Wall Mount Plate Mounting

Follow the steps below to mount the Industrial Switch with wall mount plate.

1. Remove the DIN-Rail from the Industrial Switch; loose the screws to remove the DIN-Rail.
2. Place the wall mount plate on the rear panel of the Industrial Switch.
3. Use the screws to screw the wall mount plate on the Industrial Switch.
4. Use the hook holes at the corners of the wall mount plate to hang the Industrial Switch on the wall.
5. To remove the wall mount plate, reverse the above steps.

Figure 2-13: Wall mounting



Wiring the Power Inputs

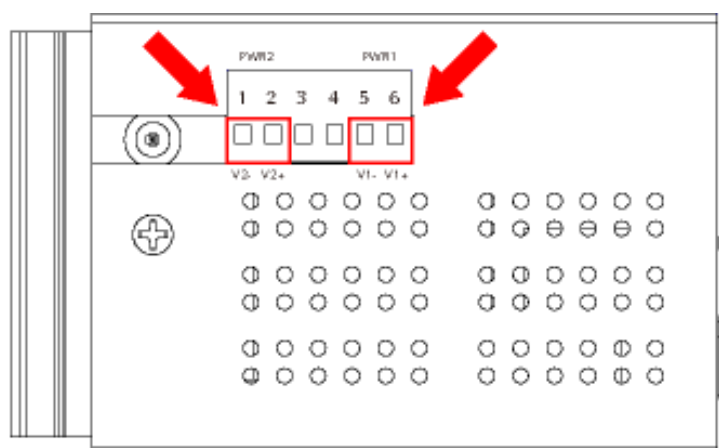
The 6-contact terminal block connector on the top panel of GE-DSH-82-PoE is used for two DC redundant power inputs.

NOTE: This product is intended to be supplied by a UL Listed Direct Plug-In Power Unit marked "Class 2" or "LPS" and output rated 48 VDC, 380 mA minimum.

Please follow the steps below to insert the power wire.

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

Figure 2-14: Wiring the redundant power inputs



3. Tighten the wire-clamp screws to prevent the wires from coming loose.

Figure 2-15: Wiring the redundant power inputs



1	2	3	4	5	6
Power 2			Power 1		
-	+			-	+

NOTE: The wire gauge for the terminal block should be in the range between 12 ~ 24 AWG.

For the GE-DSH-82-PoE, A 48VDC, 3A power input is required for full PoE load on the PoE. Please connect an external power source to the terminal block that can supply steady power at 48VDC.

Wiring the Fault Alarm Contact

The fault alarm contacts are in the middle of the terminal block connector as the picture shows below. Inserting the wires, the Industrial Switch will detect the fault status of the power failure, or port link failure (available for managed model) and then

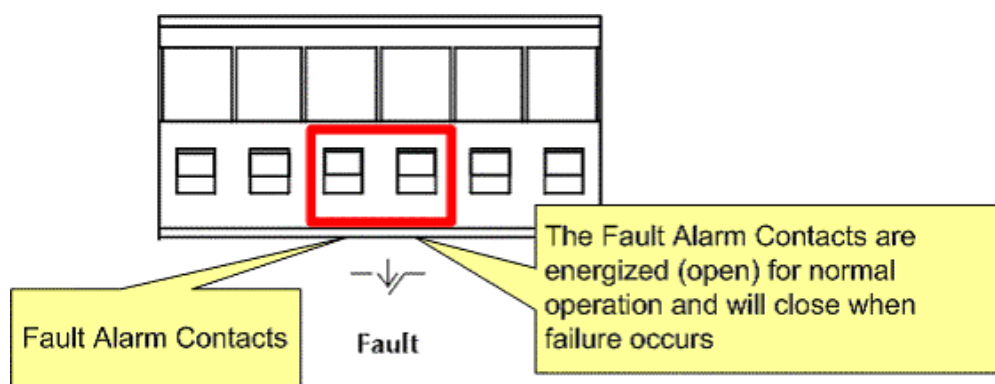
forms an open circuit. The following illustration shows an application example for wiring the fault alarm contacts.

Figure 2-16: 6-Pin Terminal Block Fault Alarm contact



NOTE: The wire gauge for the terminal block should be in the range between 12 ~ 24 AWG.

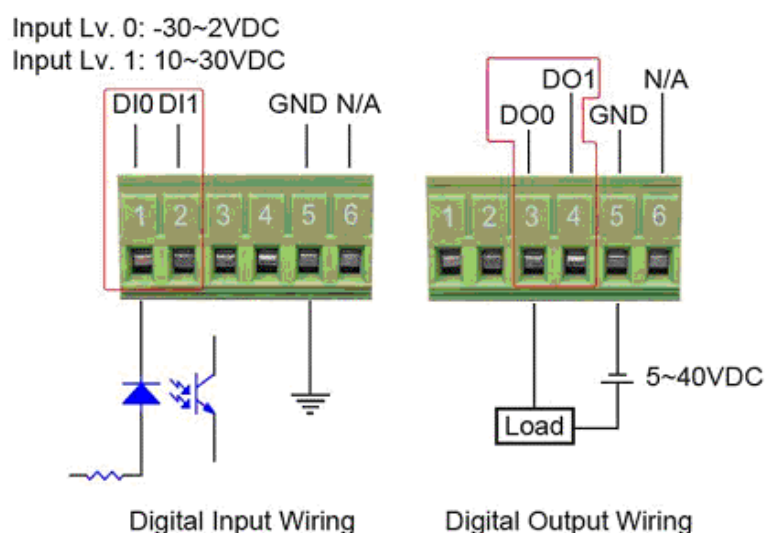
Figure 2-17: Power Fault Alarm trigger description



Wiring the Digital Inputs / Outputs (GE-DSH-73)

There is another terminal block comprising two sets of digital input/output contacts on the topside of GE-DSH-73. Please refer to the Digital Input/Output section for how to configure Digital Input/Output. The following illustration shows the pin assignment of the DIDO connector. Please note do not connect DO0/DO1 to the external device using power higher than 40V/200mA.

Figure 2-18: DI/DO terminal block of GE-DSH-73



Installing the SFP transceiver

The section describes how to insert an SFP transceiver into an SFP slot.

The SFP transceivers are hot pluggable and hot swappable. You can plug-in and out the transceiver to/from any SFP port without having to power down the Industrial Switch. Shown in Figure 2-19.

Figure 2-19: Plug-in the SFP transceiver



Approved GE Security SFP Transceivers

GE Security Industrial Switch supports both Single mode and Multi-mode SFP transceiver. The following list of approved GE Security SFP transceivers is correct at the time of publication:

- o SFP1000SX-220 SFP (1000Base-SX SFP transceiver / Multi-mode / 850nm / 220m~550m)
- o SFP1000LX-10Km SFP (1000Base-LX SFP transceiver / Single mode / 1310nm / 10km)
- o SFP100FX1310-TSC-2Km SFP (100Base-FX SFP transceiver / Multi-mode / 1310nm / 2km)
- o SFP100FX1310-TSC-20Km SFP (100Base-FX SFP transceiver / Single mode / 1310nm / 20km)

NOTE: We recommend using GE Security SFPs on the Managed Industrial Switch. If you insert a SFP transceiver that is not supported, the Managed Industrial Switch will not recognize it.

Before connecting the other switches, workstation or Media Converter:

1. Make sure both side of the SFP transceiver are with the same media type, for example: 1000Base-SX to 1000Base-SX, 1000Bas-LX to 1000Base-LX.
2. Check the fiber-optic cable type match the SFP transceiver model.
 - o To connect to 1000Base-SX SFP transceiver, use the Multi-mode fiber cable- with one side must be male duplex LC connector type.
 - o To connect to 1000Base-LX SFP transceiver, use the Single-mode fiber cable- with one side must be male duplex LC connector type.

• Connect the fiber cable

1. Attach the duplex LC connector on the network cable into the SFP transceiver.
2. Connect the other end of the cable to a device - switches with SFP installed, fiber NIC on a workstation or a Media Converter.
3. Check the LNK/ACT LED of the SFP slot on the front of the Managed Industrial Switch. Ensure that the SFP transceiver is operating correctly.
4. Check the Link mode of the SFP port if the link failed. Co works with some fiber-NICs or Media Converters, set the Link mode to "1000 Force" is needed.

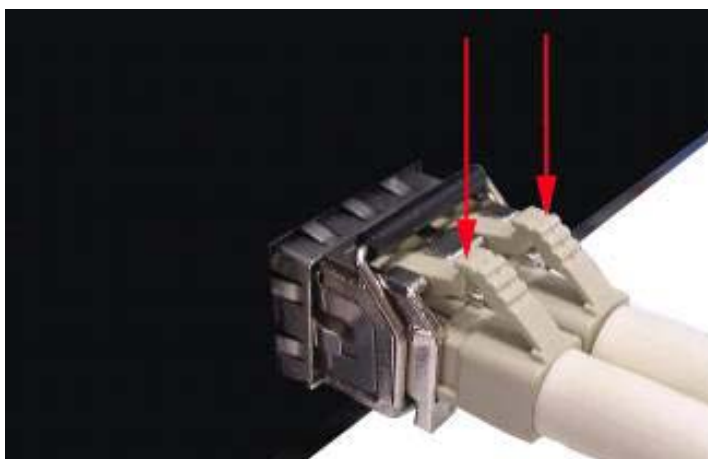
Figure 2-20: LC fiber optical cable connects to the transceiver



- **Remove the transceiver module**

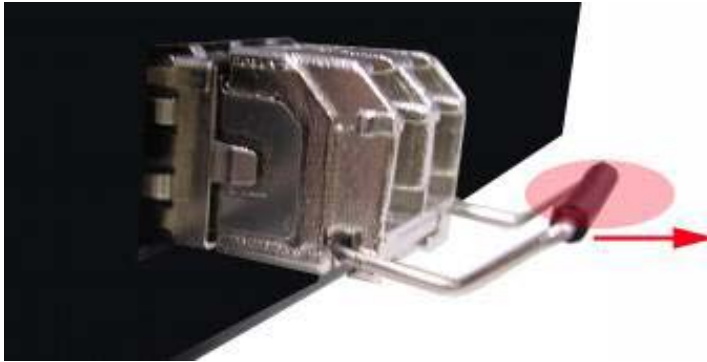
1. Make sure there is no network activity by consulting or checking with the network administrator or through the management interface of the switch/converter (if available) to disable the port in advance.
2. Remove the Fiber Optic Cable gently.

Figure 2-21: Pull out the SFP transceiver



3. Turn the handle of the MGB module horizontally.
4. Pull out the module gently through the handle.

Figure 2-22: Pull out from the transceiver



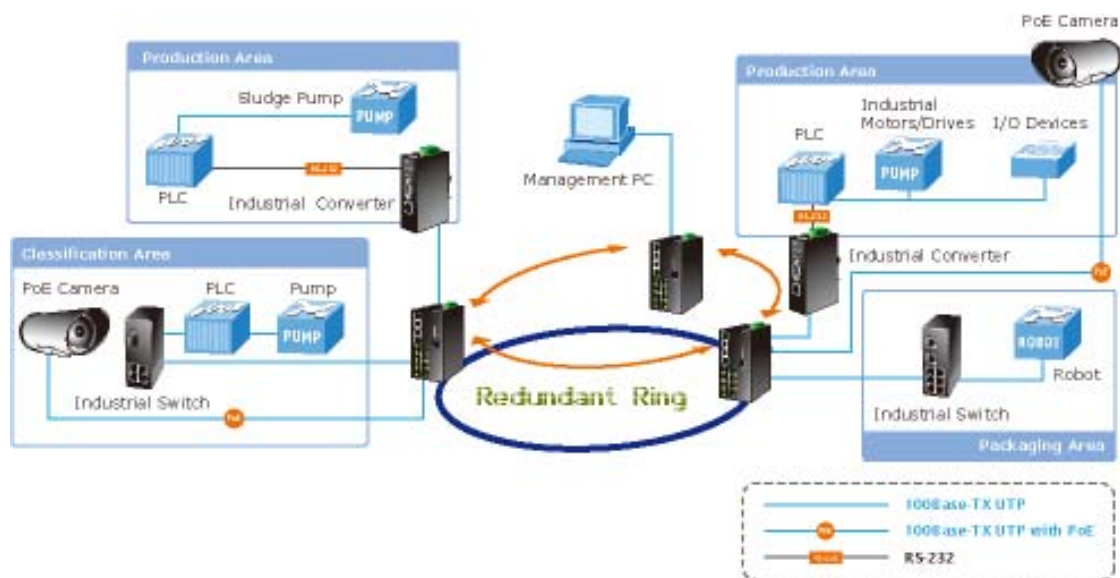
NOTE: Never pull out the module without pull the handle or the push bolts on the module. Pulling out the module with too much force could damage the module and SFP module slot of the Managed Industrial Switch.

Chapter 3

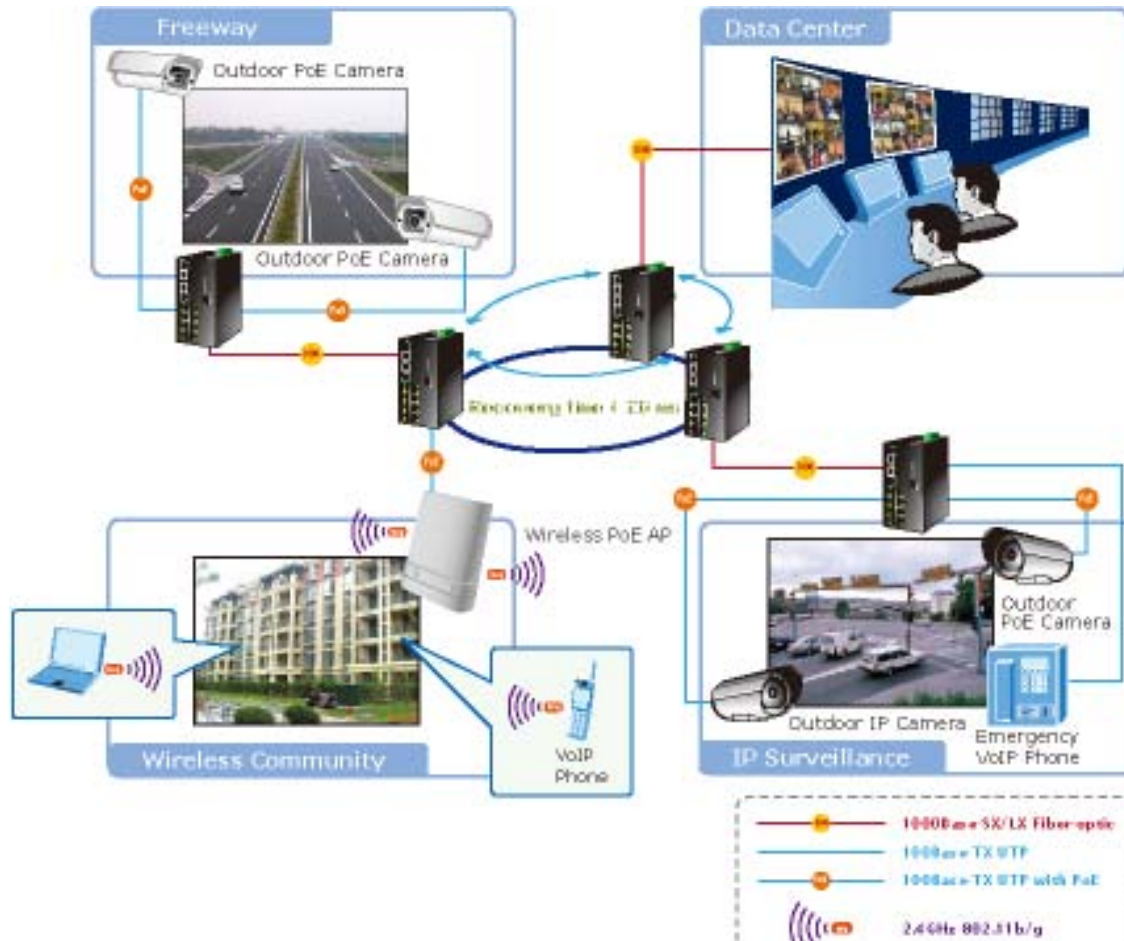
Network Application

This chapter discusses how the Switches function in various Network environments. A couple sample applications of the industrial switch are shown below.

Factory Redundant Ring Application

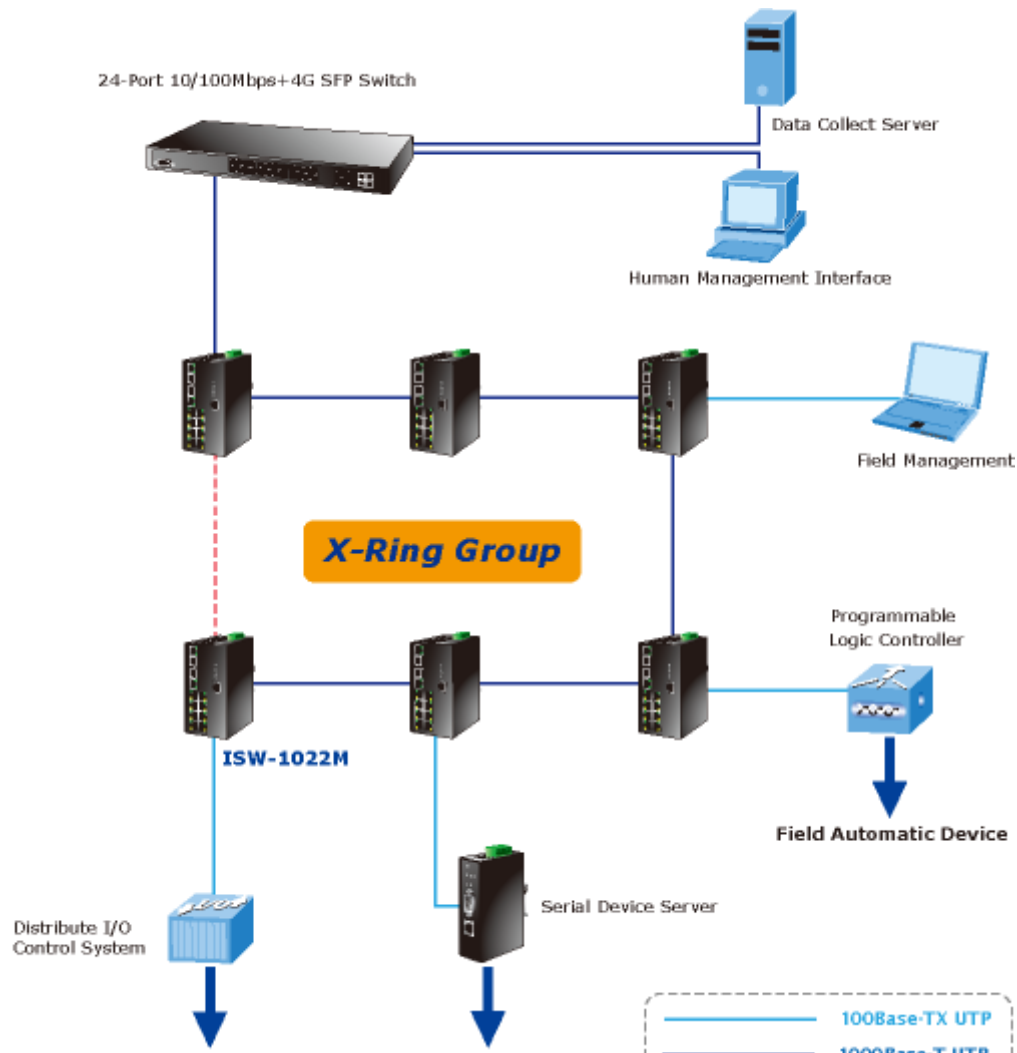


Transportation Networking and Public Wireless Service



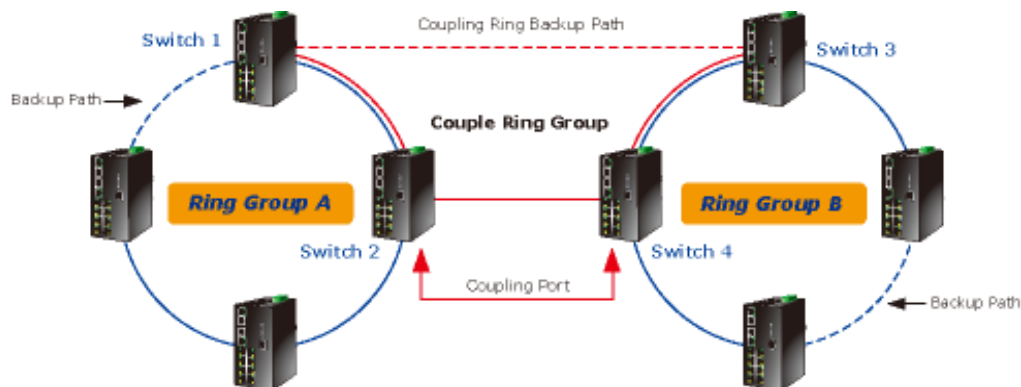
X-Ring Application

The industrial Switch supports the Rapid Ring (X-Ring) protocol that can help the network system to recovery from network connection failure within 20ms or less, and make the network system more reliable. The X-Ring algorithm is similar to spanning tree protocol (STP) algorithm but its recovery time is faster than STP. The following figure is a sample X-Ring application.



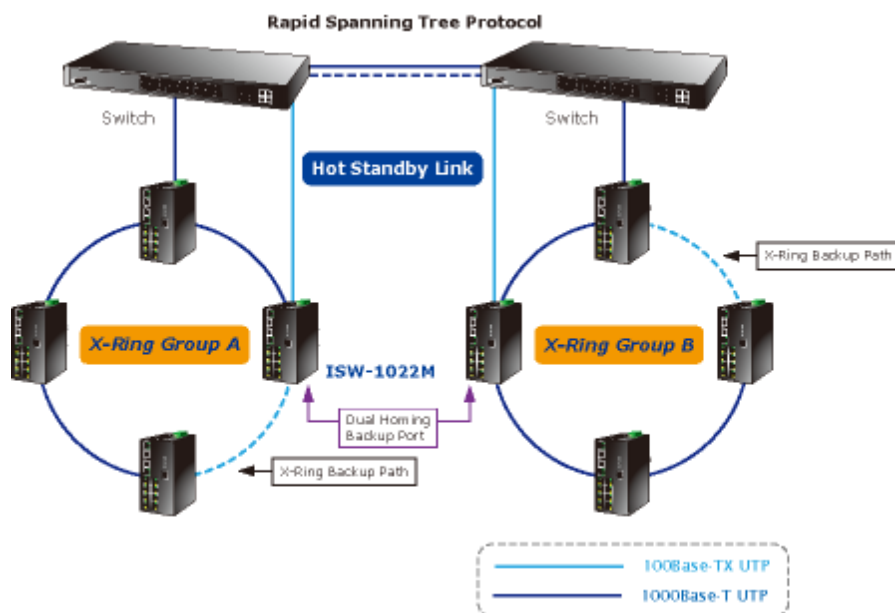
Coupling Ring Application

In the network, it may have more than one X-Ring group. By using the coupling ring function, it can connect each X-Ring for the redundant backup. It can ensure the transmissions between two ring groups not to fail. The following figure is a sample of coupling ring application.



Dual Homing Application

Dual Homing function is to prevent the connection loss from between X-Ring group and upper level/core switch. Assign two ports to be the Dual Homing port that is backup port in the X-Ring group. The Dual Homing function only works when the X-Ring function is active. Each X-Ring group only has one Dual Homing port.



NOTE: In Dual Homing application architecture, the upper level switches need to enable the Rapid Spanning Tree protocol.

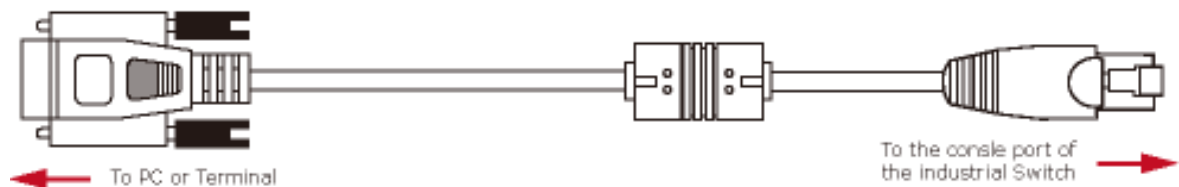
Chapter 4

Console Management

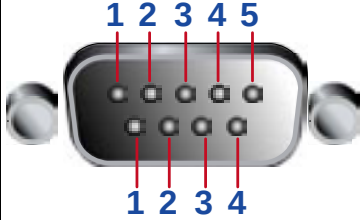
Connecting to the Console Port

The supplied cable which one end is RS-232 connector and the other end is RJ-45 connector. Attach the end of RS-232 connector to PC or terminal and the other end of RJ-45 connector to the console port of the switch. The connected terminal or PC must support the terminal emulation program.

Figure 4-1: RS-232 to RJ-45 cable



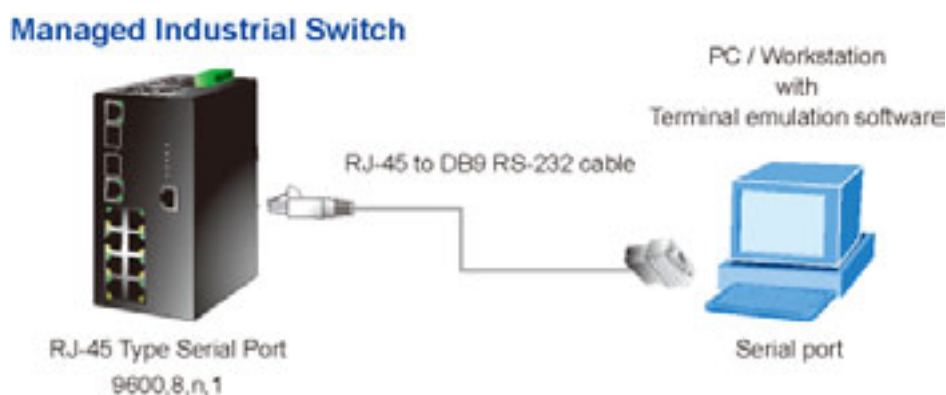
DB9/ RJ-45 Connector Pinouts

	DB9-PIN	RJ-45 Connector
	1	1 Orange/White
	2	2 Orange
	3	3 Green/White
	4	4 Blue
	5	5 Blue/White
	6	6 Green
	7	7 Brown/White
	8	8 Brown
	9	

Login in the Console Interface

To configure the system, connect a serial cable to a COM port on a PC or notebook computer and to RJ-45 type serial (console) port of the Managed Industrial Switch. The console port of the Managed Industrial Switch is DCE already, so that you can connect the console port directly through PC without the need of Null Modem.

Figure 4-2: Connecting the Switch to a PC



A terminal program is required to make the software connection to the GE-DSH series Managed Industrial Switch. Windows' Hyper Terminal program is a good choice. Hyper Terminal can be accessed from the Start menu.

1. Click **START**, then **Programs/Accessories** and then **Hyper Terminal**.

When the following screen appears, make sure that the COM port should be configured as:

Baud Rate: 9600 bps

Data Bits: 8

Parity: none

Stop Bit: 1

Flow control: None

Figure 4-3: The COM1 properties window

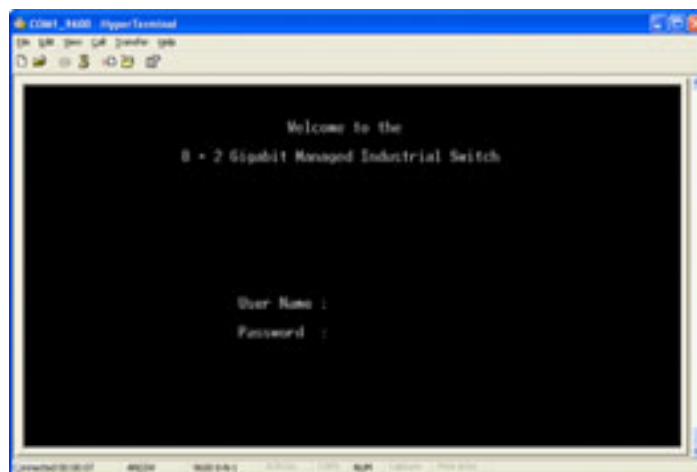


2. Once the terminal has connected to the device, power on the GE-DSH series Managed Industrial Switch, the terminal will display that it is running testing procedures.
3. Then, the following message asks the login password. The factory default password as following and the login screen in below figure appears.

User name: **admin**

Password: **admin**

Figure 4-4: The login screen



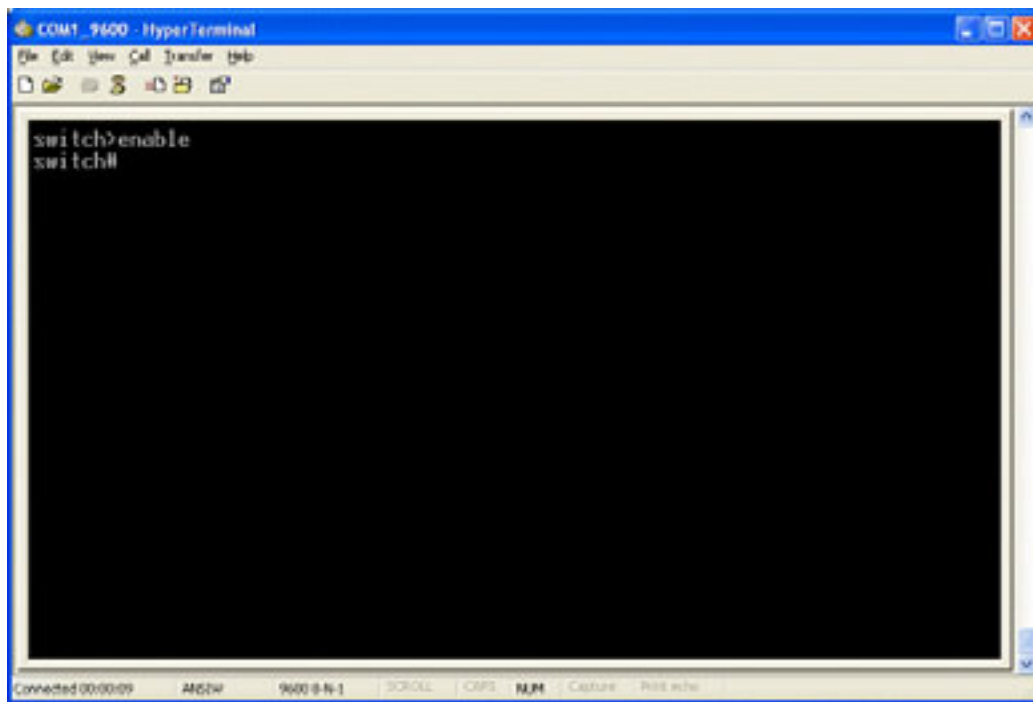
NOTE: For security reasons, please change and memorize the new password after this first setup.

Only enter commands in lowercase letters when in the console interface.

CLI Management

The system supports the console management-CLI command. After you log in on to the system, you will see a command prompt. To enter CLI management interface, type in "enable" command.

Figure 4-5: The CLI command interface



CLI commands and descriptions

Modes	Access Method	Prompt	Exit Method	About This Model
User EXEC	Begin a session with your switch.	switch>	Enter logout or quit.	The user commands available at the user level are a subset of those available at the privileged level. Use this mode to: • Perform basic tests. • Display system information.
Privileged EXEC	Enter the enable command while in User EXEC mode.	switch#	Enter disable to exit.	The privileged command is the advanced mode. Use this mode to • Display advanced function status • Save configuration
Global Configuration	Enter the configure command while in privileged EXEC mode.	switch (config)#	To exit to privileged EXEC mode, enter exit or end	Use this mode to configure those parameters that are going to be applied to your switch.
VLAN database	Enter the vlan database command while in privileged EXEC mode.	switch (vlan)#	To exit to user EXEC mode, enter exit.	Use this mode to configure VLAN-specific parameters.
Interface configuration	Enter the interface of fast Ethernet command (with a specific interface) while in global configuration mode.	switch (config-if)#	To exit to global configuration mode, enter exit. To exit to privileged EXEC mode, enter exit or end.	Use this mode to configure parameters for the switch and Ethernet ports.

Chapter 5

Web-Based Management

About Web-based Management

The Managed Industrial Switch offers management features that allow users to manage the Managed Industrial Switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer.

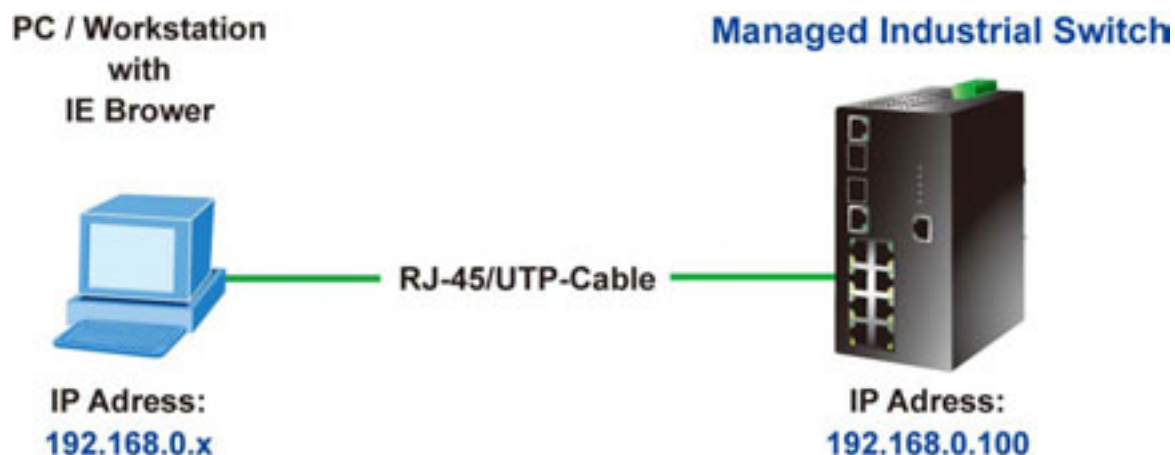
The Web-Based Management supports Internet Explorer 6.0. It is based on Java Applets with an aim to reduce network bandwidth consumption, enhance access speed and present an easy viewing screen.

NOTE: By default, IE 6.0 or later version does not allow Java Applets to open sockets. The user has to explicitly modify the browser setting to enable Java Applets to use network ports.

The Managed Industrial Switch can be configured through an Ethernet connection, make sure the manager PC must be set on same the IP subnet address with the Managed Industrial Switch.

For example, the default IP address of the Managed Industrial Switch is 192.168.0.100, then the manager PC should be set at 192.168.0.x (where x is a number between 1 and 254, except 100), and the default subnet mask is 255.255.255.0.

If you have changed the default IP address of the Managed Industrial Switch to 192.168.1.1 with subnet mask 255.255.255.0 via console, then the manager PC should be set at 192.168.1.x (where x is a number between 2 and 254) to do the relative configuration on manager PC.



Requirements

- Workstations of subscribers running Windows 98/ME, NT4.0, 2000/2003/XP, MAC OS9 or later, Linux, UNIX or other platform compatible with TCP/IP protocols.
- Workstation installed with Ethernet NIC (Network Card)
- Ethernet Port connect
 - o Network cables - Use standard network (UTP) cables with RJ45 connectors.
 - o Above PC installed with WEB Browser and JAVA runtime environment Plug-in

NOTE: We recommend using Internet Explorer 6.0 or above to access GE-DSH series Managed Industrial Switch.

Logging on the Switch

1. Use Internet Explorer 6.0 or above Web browser. Enter the factory-default IP address to access the Web interface. The factory-default IP Address as following:

`http://192.168.0.100`

2. When the following login screen appears, please enter the default username "admin" with password "admin" (or the username/password you have changed via console) to login the main screen of Managed Industrial Switch. The login screen in Figure 5-1 appears.

Default User name: **admin**

Default Password: **admin**

Figure 5-1: Login screen



3. After entering the username and password, the main screen appears as shown in Figure 5-2.

Figure 5-2: Default main page



4. The Switch Menu on the left of the Web page let you access all the commands and statistics the Switch provides.

Now, you can use the Web management interface to continue the switch management or manage the Managed Industrial Switch by Web interface. The Switch Menu on the left of the web page let you access all the commands and statistics the Managed Industrial Switch provides.

NOTE:

1. We recommend using Internet Explorer 6.0 or above to access GE-DSH-82 series Managed Industrial Switch.
2. The changed IP address take effect immediately after clicking on the Save button. You need to use the new IP address to access the Web interface.
3. For security reasons, please change and memorize the new password after this first setup.
4. Only enter commands in lowercase letters when using the web interface.

System

Use the System menu items to display and configure basic administrative details of the Managed Industrial Switch. Under System the following topics are provided to configure and view the system information: This section has the following items:

System Information	Provides basic system description, including contact information
IP Configuration	Sets the IP address for management access
DHCP Server	Configure the Switch as a DHCP server for assigning dynamic IP addresses to devices on a network.
TFTP	Upgrade the firmware via TFTP server Save/view the switch configuration to remote host Upload the switch configuration from remote host
Fault Relay Alarm	Provides relay output for port breakdown, power fail
SNTP Configuration	Simple Network Time Protocol. Configures SNTP client settings, including broadcast mode or a specified list of servers
IP Security	Supports 10 IP addresses that have permission to access the switch management and to prevent unauthorized intruder.
User Authentication	Allows configuring the system user name and password required to access the web pages or log in from CLI.
Factory Default	Reset the configuration of the Managed Industrial Switch
System Reboot	Restarts the switch

System Information

The System Info page provides information for the current device information. The System Information page helps a switch administrator to identify the hardware MAC address, software version and system uptime. The screen in Figure 5-3 appears.

Figure 5-3: Switch settings interface

This page includes the following fields:

Object	Description
System Name:	Assign the system name of the switch (The maximum length is 64 bytes)
System Description:	Describes the switch
System Location:	Assign the switch physical location (The maximum length is 64 bytes).
System Contact:	Enter the name of contact person or organization.
Firmware Version:	Displays the switch's firmware version
Kernel Version:	Displays the kernel software version
MAC Address:	Displays the unique hardware address assigned by manufacturer (default)

IP Configuration

The IP Configuration includes the IP Address, Subnet Mask and Gateway. The Configured column is used to view or change the IP configuration. Fill up the IP Address, Subnet Mask and Gateway for the device. The screen in Figure 5-4 appears.

Figure 5-4: IP configuration interface

	Configured	Current
DHCP Client	☐	<button>Renew</button>
IP Address	10.1.1.241	10.1.1.241
IP Mask	255.255.255.0	255.255.255.0
IP Router	10.1.1.254	10.1.1.254
VLAN ID	1	1

Save Reset

This page includes the following fields:

Object	Description
DHCP Client:	Enable or disable the DHCP client function. When DHCP client function is enabled, the switch will be assigned an IP address from the network DHCP server. The default IP address will be replaced by the assigned IP address on DHCP server. After the user clicks Apply, a popup dialog shows up to inform the user that when the DHCP client is enabled, the current IP will lose and user should find the new IP on the DHCP server.
IP Address:	Assign the IP address that the network is using. If DHCP client function is enabled, this switch is configured as a DHCP client. The network DHCP server will assign the IP address to the switch and display it in this column. The default IP is 192.168.0.100 or the user has to assign an IP address manually when DHCP Client is disabled.
Subnet Mask:	Assign the subnet mask to the IP address. If DHCP client function is disabled, the user has to assign the subnet mask in this column field.
Gateway:	Assign the network gateway for the switch. If DHCP client function is disabled, the user has to assign the gateway in this column field. The default gateway is 192.168.0.1.
DNS1:	Assign the primary DNS IP address.
DNS2:	Assign the secondary DNS IP address.

DHCP Server

DHCP is the abbreviation of Dynamic Host Configuration Protocol that is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

The system provides the DHCP server function. Having enabled the DHCP server function, the switch system will be configured as a DHCP server.

System configuration

The Dynamic Host Configuration Protocol (DHCP) Server gives out IP addresses when a device is booting up and request an IP to logged on to the network. It must be set as a DHCP client to obtain the IP address automatically.

Figure 5-5: DHCP Server Configuration interface

DHCP Server - System Configuration	
System Configuration Client Entries Port and IP Binding	
DHCP Server : Disable	
Low IP Address	192.168.0.101
High IP Address	192.168.0.200
Subnet Mask	255.255.255.0
Gateway	192.168.0.254
DNS	0.0.0.0
Lease Time (sec)	86400
Apply Help	

This page includes the following fields:

Object	Description
DHCP Server:	Enable or Disable the DHCP Server function. Enable—the switch will be the DHCP server on your local network.
Low IP Address:	Type in an IP address. Low IP address is the beginning of the dynamic IP range. For example, dynamic IP is in the range between 192.168.0.101 ~ 192.168.0.200. In contrast, 192.168.0.101 is the Low IP address.
High IP Address:	Type in an IP address. High IP address is the end of the dynamic IP range. For example, dynamic IP is in the range between 192.168.0.101 ~ 192.168.0.200. In contrast, 192.168.0.200 is the High IP address.
Subnet Mask:	Type in the subnet mask of the IP configuration.
Gateway:	Type in the IP address of the gateway in your network.
DNS:	Type in the Domain Name Server IP Address in your network.
Lease Time (sec):	It is the time period that system will reset the dynamic IP assignment to ensure the dynamic IP will not been occupied for a long time or the server doesn't know that the dynamic IP is idle.

Client Entries

When the DHCP server function is enabled, the system will collect the DHCP client information including the assigned IP address, the MAC address of the client device, the IP assigning type, status and lease time.

Figure 5-6: DHCP Client Entries interface



This page includes the following fields:

Object	Description
IP Addr	Specifies the Client's IP Address.
Client ID	Specifies the Client's Hardware Address.
Type	Specifies the Type of Binding: Dynamic / Manual.
Lease	Specifies the Lease time left in seconds.

Port and IP Bindings

Assign the dynamic IP address bound with the port to the connected client. The user is allowed to fill each port column with one particular IP address. When the device is connecting to the port and asks for IP assigning, the system will assign the IP address bound with the port.

Figure 5-7: Port and IP Bindings interface

DHCP Server - Port and IP Binding

System Configuration Client Entries **Port and IP Binding**

Port	IP
Port.01	0.0.0.0
Port.02	0.0.0.0
Port.03	192.168.0.180
Port.04	192.168.0.181
Port.05	0.0.0.0
Port.06	0.0.0.0
Port.07	0.0.0.0
Port.08	0.0.0.0
Port.09	0.0.0.0
Port.10	0.0.0.0

Apply Help

TFTP

It provides the functions allowing the user to update the switch firmware via the Trivial File Transfer Protocol (TFTP) server. Before updating, make sure the TFTP server is ready and the firmware image is located on the TFTP server.

Update Firmware

Use this menu to download a file from specified TFTP server to the Managed Industrial Switch.

Figure 5-8: Update Firmware interface



This page includes the following fields:

Object	Description
TFTP Server IP Address:	Type in your TFTP server IP.
Firmware File Name:	Type in the name of the firmware image file to be updated.

Restore Configuration

You can restore a previous backup configuration from the TFTP server to recover the settings. Before doing that, you must locate the image file on the TFTP server first and the Managed Industrial Switch will download back the flash image.

Figure 5-9: Restore Configuration interface

This page includes the following fields:

Object	Description
TFTP Server IP Address:	Type in the TFTP server IP.
Restore File Name:	Type in the correct file name for restoring.

Backup Configuration

You can back up the current configuration from flash ROM to the TFTP server for the purpose of recovering the configuration later. It helps you to avoid wasting time on configuring the settings by backing up the configuration.

Figure 5-10: Backup Configuration interface

This page includes the following fields:

Object	Description
TFTP Server IP Address:	Type in the TFTP server IP.
Backup File Name:	Type in the file name.

System Event Log

This page allows the user to decide whether to send the system event log, and select the mode which the system event log will be sent to client only, server only, or both client and server. What kind of event log will be issued to the client/server depends on the selection on the Event Configuration tab. There are five types of event available to be issued as the event log.

- Device Cold Start
- Device Warm Start
- Authentication Failure
- X-Ring Topology Change
- Port Event

Syslog Configuration

The System Logs enable viewing device events in real time, and recording the events for later usage. System Logs record and manage events and report errors or informational messages.

Figure 5-11: Syslog Configuration interface

This page includes the following fields:

Object	Description
Syslog Client Mode:	Select the system log mode—Client Only, Server Only, or Both. Client Only: the system event log will only be sent to this interface of the switch Server Only: the system log will only be sent to the remote system log server with its IP assigned. Both: the system event log will be sent to the remote server and this interface.
System Log Server IP Address:	When the 'Syslog Mode' item is set as Server Only/Both, the user has to assign the system log server IP address to which the log will be sent.

System Event Log-SMTP Configuration

Simple Mail Transfer Protocol (SMTP) is the standard for email transmissions across the network. You can configure the SMTP server IP, mail subject, sender, mail account, password, and the recipient email addresses, which the e-mail alert will send to. There are also five types of event-Device Cold Start, Device Warm Start, Authentication Failure, X-Ring Topology Change, and Port Event-available to be issued as the e-mail alert. Besides, this function provides the authentication mechanism including an authentication step through which the client effectively logs in to the SMTP server during the process of sending e-mail alert.

Figure 5-12: SMTP Configuration interface

This page includes the following fields:

Object	Description
Email Alert:	With this function being enabled, the user is allowed to configure the detail settings for sending the e-mail alert to the SMTP server when the events occur.
SMTP Server IP:	Assign the mail server IP address (when Email Alert is enabled, this function will then be available).
Sender:	Type in an alias of the switch in complete email address format, e.g., to identify where the e-mail alert comes from.

Object	Description
Authentication:	Having ticked this checkbox, the mail account, password and confirm password column fields will then show up. Configure the email account and password for authentication when this switch logs in to the SMTP server.
Mail Account:	Set up the email account, e.g. jack, to receive the email alert. It must be an existing email account on the mail server.
Password:	Type in the password for the email account.
Confirm Password:	Reconfirm the password.
Rcpt e-mail Address 1 ~ 6:	You can also fill each of the column fields with up to 6 e-mail accounts to receive the email alert.

System Event Log-Event Configuration

Having ticked the Syslog/SMTP checkboxes, the event log/email alert will be sent to the system log server and the SMTP server respectively. Also, Port event log/alert (link up, link down, and both) can be sent to the system log server/SMTP server respectively by setting the trigger condition.

Figure 5-13: Event Configuration interface

System Event Log - Event Configuration

Syslog Configuration | SMTP Configuration | **Event Configuration**

System event selection

Event Type	Syslog	SMTP
Device cold start	☒	☒
Authentication Failure	☒	☒
X-Ring topology change	☒	☒

Port event selection

Port	Syslog	SMTP
Port.01	Link Up & Link Down ☒	Link Up & Link Down ☒
Port.02	Link Up & Link Down ☒	Link Up & Link Down ☒
Port.03	Link Up & Link Down ☒	Link Up & Link Down ☒
Port.04	Link Up & Link Down ☒	Link Up & Link Down ☒
Port.05	Link Up & Link Down ☒	Link Up & Link Down ☒
Port.06	Link Up & Link Down ☒	Link Up & Link Down ☒
Port.07	Link Up & Link Down ☒	Link Up & Link Down ☒
Port.08	Link Up & Link Down ☒	Link Up & Link Down ☒
Port.09	Link Up & Link Down ☒	Link Up & Link Down ☒
Port.10	Link Up & Link Down ☒	Link Up & Link Down ☒

Apply Help

This page includes the following fields:

Object	Description
System event selection:	There are 4 event types—Device Cold Start, Device Warm Start, Authentication Failure, and X-ring Topology Change. The checkboxes are not available for ticking unless the Syslog Client Mode on the Syslog Configuration tab and the E-mail Alert on the SMTP Configuration tab are enabled first. Device cold start: When the device executes cold start action, the system will issue the event log/email alert to the system log/SMTP server respectively. Device warm start: When the device executes warm start, the system will issue the event log/email alert to the system log/SMTP server respectively. Authentication Failure: When the SNMP authentication fails, the system will issue the event log/email alert to the system log/SMTP server respectively. X-ring topology change: When the X-ring topology has changed, the system will issue the event log/email alert to the system log/SMTP server respectively.
Port event selection:	Also, before the drop-down menu items are available, the Syslog Client Mode selection item on the Syslog Configuration tab and the E-mail Alert selection item on the SMTP Configuration tab must be enabled first. Those drop-down menu items have 3 selections—Link UP, Link Down, and Link UP & Link Down. Disable means no event will be sent to the system log/SMTP server. Link UP: The system will only issue a log message when the link-up event of the port occurs. Link Down: The system will only issue a log message when the link-down event of port occurs. Link UP & Link Down: The system will issue a log message at the time when port connection is link-up and link-down.

Fault Relay Alarm

The Fault Relay Alarm function provides the Power Failure and Port Link Down/Broken detection. With both power input 1 and power input 2 installed and the check boxes of power 1/power 2 ticked, the FAULT LED indicator will then be possible to light up when any one of the power failures occurs. As for the Port Link Down/Broken detection, the FAULT LED indicator will light up when the port failure occurs; certainly the check box beside the port must be ticked first. Please refer to the segment of 'Wiring the Fault Alarm Contact' for the failure detection.

Figure 5-14: Fault Relay Alarm interface

This page includes the following fields:

Object	Description
Power Failure:	Tick the check box to enable the function of lighting up the FAULT LED on the panel when power fails.
Port Link Down/Broken:	Tick the check box to enable the function of lighting up FAULT LED on the panel when Ports' states are link down or broken.

SNTP Configuration

SNTP (Simple Network Time Protocol) is a simplified version of NTP, which is an Internet protocol used to synchronize the clocks of computers to some time reference. Because time usually just advances, the time on different node stations will be different. With the communicating programs running on those devices, it would cause time to jump forward and back, a non-desirable effect. Therefore, the switch provides comprehensive mechanisms to access national time and frequency dissemination services, organize the time-synchronization subnet and the local clock in each participating subnet peer.

Daylight saving time (DST) is the convention of advancing clocks so that afternoons have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn.

Figure 5-15: SNTP Configuration interface

This page includes the following fields:

Object	Description
SNTP Client:	Enable/disable SNTP function to get the time from the SNTP server.
Daylight Saving Time:	This is used as a control switch to enable/disable daylight saving period and daylight saving offset. Users can configure Daylight Saving Period and Daylight Saving Offset in a certain period time and offset time while there is no need to enable daylight saving function. Afterwards, users can just set this item as enable without assign Daylight Saving Period and Daylight Saving Offset again.

UTC Timezone:	Universal Time, Coordinated. Set the switch location time zone. The following table lists the different location time zone for your reference.
SNTP Sever URL:	Set the SNTP server IP address. You can assign a local network time server IP address or an internet time server IP address.
Switch Timer:	When the switch has successfully connected to the SNTP server whose IP address was assigned in the column field of SNTP Server URL, the current coordinated time is displayed here.
Daylight Saving Period:	Set up the Daylight Saving beginning date/time and Daylight Saving ending date/time. Please key in the value in the format of 'YYYYMMDD' and 'HH:MM' (leave a space between 'YYYYMMDD' and 'HH:MM'). YYYYMMDD: an eight-digit year/month/day specification. HH:MM: a five-digit (including a colon mark) hour/minute specification. For example, key in '20070701 02:00' and '20071104 02:04' in the two column fields respectively to represent that DST begins at 2:00 a.m. on March 11, 2007 and ends at 2:00 a.m. on November 4, 2007.
Daylight Saving Offset (mins):	For non-US and European countries, specify the amount of time for day light savings. Please key in the valid figure in the range of minute between 0 and 720, which means you can set the offset up to 12 hours.

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
CCT - China Coast, USSR Zone 7	+8 hours	8 pm
JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

IP Security

IP security function allows the user to assign 10 specific IP addresses that have permission to manage the switch through the http and telnet services for the securing switch management. The purpose of giving the limited IP addresses permission is to allow only the authorized personnel/device can do the management task on the switch.

Figure 5-16: SNTP Configuration interface

IP Security

IP Security Mode: Enable

☒ Enable HTTP Server

☒ Enable Telnet Server

Security IP1	192.168.0.1
Security IP2	0.0.0.0
Security IP3	0.0.0.0
Security IP4	0.0.0.0
Security IP5	0.0.0.0
Security IP6	0.0.0.0
Security IP7	0.0.0.0
Security IP8	0.0.0.0
Security IP9	0.0.0.0
Security IP10	0.0.0.0

Apply Help

This page includes the following fields:

Object	Description
IP Security Mode:	Having set this selection item in the Enable mode, the Enable HTTP Server, Enable Telnet Server checkboxes and the ten security IP column fields will then be available. If not, those items will appear in grey.
Enable HTTP Server:	Having ticked this checkbox, the devices whose IP addresses match any one of the ten IP addresses in the Security IP1 ~ IP10 table will be given the permission to access this switch via HTTP service.
Enable Telnet Server:	Having ticked this checkbox, the devices whose IP addresses match any one of the ten IP addresses in the Security IP1 ~ IP10 table will be given the permission to access this switch via telnet service.
Security IP 1 ~ 10:	The system allows the user to assign up to 10 specific IP addresses for access security. Only these 10 IP addresses can access and manage the switch through the HTTP/Telnet service once IP Security Mode is enabled.

NOTE: Remember to execute the "Save Configuration" action, otherwise the new configuration will be lost when the switch powers off.

User Authentication

Change web management login user name and password for the management security issue.

Figure 5-17: User Authentication interface



The screenshot shows a web-based user authentication interface. At the top, the title "User Authentication" is displayed in a bold, dark blue font. Below the title, there are three input fields arranged vertically. The first field is labeled "User Name :" and contains the text "admin". The second field is labeled "New Password :" and contains six asterisks "*****". The third field is labeled "Confirm Password :" and also contains six asterisks "*****". To the right of each input field is a small, empty square box. At the bottom of the form, there are two buttons: "Apply" and "Help", both with a yellow background and a green border.

This page includes the following fields:

Object	Description
User name:	Type in the new user name The default user name is 'admin'
Password:	Type in the new password The default is 'admin'
Confirm password:	Re-type the new password

Port Management

Port Statistics

The following chart provides the current statistic information, which displays the real-time packet transfer status for each port. The user might use the information to plan and implement the network, or check and find the problem when the collision or heavy traffic occurs.

Figure 5-18: Port Statistics interface

Port Statistics												
Port	Type	Link	State	Tx Good Packet	Tx Bad Packet	Rx Good Packet	Rx Bad Packet	Tx Abort Packet	Collision	Packet Dropped	RX Broadcast Packet	RX Multicast Packet
Port.01	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.07	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.08	100TX	Down	Enable	0	0	0	0	0	0	0	0	0
Port.09	1GTX/mGBIC	Down	Enable	0	0	0	0	0	0	0	0	0
Port.10	1GTX/mGBIC	Up	Enable	4610	0	33375612	0	0	0	0	180950	50959

Clear Help

This page includes the following fields:

Object	Description
Port:	The port number.
Type:	Displays the current speed of connection to the port.
Link:	The status of linking—'Up' or 'Down'.
State:	It's set by Port Control. When the state is disabled, the port will not transmit or receive any packet.
Tx Good Packet:	The counts of transmitting good packets via this port.
Tx Bad Packet:	The counts of transmitting bad packets (including undersize [less than 64 octets], oversize, CRC Align errors, fragments and jabbers packets) via this port.
Rx Good Packet:	The counts of receiving good packets via this port.
Rx Bad Packet:	The counts of receiving good packets (including undersize [less than 64 octets], oversize, CRC error, fragments and jabbers) via this port.
Tx Abort Packet:	The aborted packet while transmitting.
Packet Collision:	The counts of collision packet.
Packet Dropped:	The counts of dropped packet.
Rx Bcast Packet:	The counts of broadcast packet.
Rx Mcast Packet:	The counts of multicast packet.

Port Control

In Port control you can configure the settings of each port to control the connection parameters, and the status of each port is listed beneath.

Figure 5-19: Port Control interface

Port Control

Port	State	Negotiation	Speed	Duplex	Flow Control	Security
Port.01	Enable	Auto	100	Full	Enable	Off
Port.02						
Port.03						
Port.04						

Apply Help

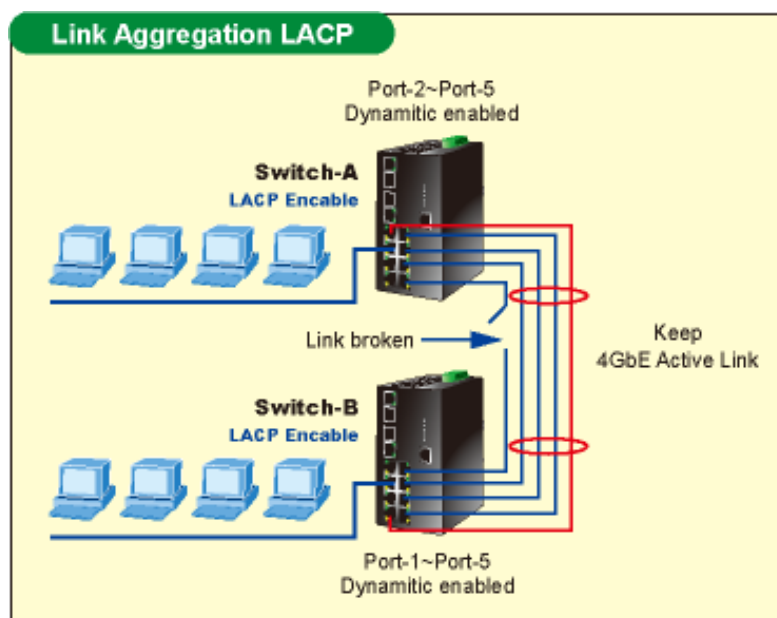
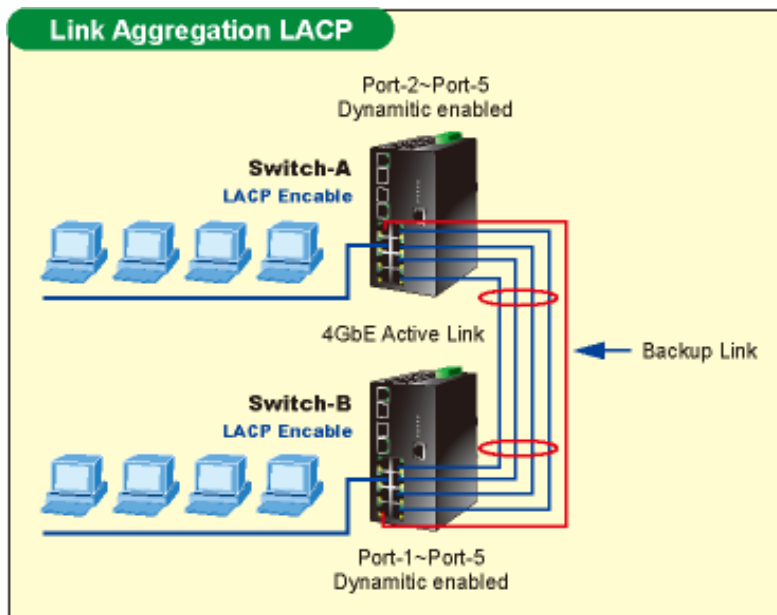
Port	Group ID	Type	Link	State	Negotiation	Speed Config	Duplex Actual	Flow Control Config	Security Actual
Port.01	N/A	100TX	Down	Enable	Auto	100	Full	N/A	Enable
Port.02	N/A	100TX	Down	Enable	Auto	100	Full	N/A	Enable
Port.03	N/A	100TX	Down	Enable	Auto	100	Full	N/A	Enable
Port.04	N/A	100TX	Down	Enable	Auto	100	Full	N/A	Enable
Port.05	N/A	100TX	Down	Enable	Auto	100	Full	N/A	Enable
Port.06	N/A	100TX	Down	Enable	Auto	100	Full	N/A	Enable
Port.07	N/A	100TX	Down	Enable	Auto	100	Full	N/A	Enable
Port.08	N/A	100TX	Down	Enable	Auto	100	Full	N/A	Enable
Port.09	N/A	1GTX/mGBIC	Down	Enable	Auto	1G	Full	N/A	Enable
Port.10	N/A	1GTX/mGBIC	Up	Enable	Auto	1G	Full	1G	Full

This page includes the following fields:

Object	Description
Port:	Use the scroll bar and click on the port number to choose the port to be configured.
State:	Current port state. The port can be set to disable or enable mode. If the port state is set as 'Disable', it will not receive or transmit any packet.
Negotiation:	Auto and Force. Being set as Auto, the speed and duplex mode are negotiated automatically. When you set it as Force, you have to set the speed and duplex mode manually.
Speed:	It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read-only.
Duplex:	It is available for selecting when the Negotiation column is set as Force. When the Negotiation column is set as Auto, this column is read-only.
Flow Control:	Whether or not the receiving node sends feedback to the sending node is determined by this item. When enabled, once the device exceeds the input data rate of another device, the receiving device will send a PAUSE frame which halts the transmission of the sender for a specified period of time. When disabled, the receiving device will drop the packet if too much to process.
Security:	When the Security selection is set as 'On', any access from the device which connects to this port will be blocked unless the MAC address of the device is included in the static MAC address table. See the segment of MAC Address Table—Static MAC Addresses.

Port Trunk

Port trunking is the combination of several ports or network cables to expand the connection speed beyond the limits of any one single port or network cable. Link Aggregation Control Protocol (LACP), which is a protocol running on layer 2, provides a standardized means in accordance with IEEE 802.3ad to bundle several physical ports together to form a single logical channel. All the ports within the logical channel or so-called logical aggregator work at the same connection speed and LACP operation requires full-duplex mode.



Aggregator setting

This section provides Port Trunk-Aggregator Setting of each port from the Switch, the screen in Figure 5-20 appears.

Figure 5-20: Port Trunk-Aggregator Setting interface (two ports are added to the left field with LACP enabled)

This page includes the following fields:

Object	Description
System Priority:	A value which is used to identify the active LACP. The Managed Industrial Switch with the lowest value has the highest priority and is selected as the active LACP peer of the trunk group.
Group ID:	There are 13 trunk groups to be selected. Assign the "Group ID" to the trunk group.
LACP:	When enabled, the trunk group is using LACP. A port which joins an LACP trunk group has to make an agreement with its member ports first. Please notice that a trunk group, including member ports split between two switches, has to enable the LACP function of the two switches. When disabled, the trunk group is a static trunk group. The advantage of having the LACP disabled is that a port joins the trunk group without any handshaking with its member ports; but member ports won't know that they should be aggregated together to form a logic trunk group.

Object	Description
Work ports:	This column field allows the user to type in the total number of active port up to four. With LACP static trunk group, e.g. you assign four ports to be the members of a trunk group whose work ports column field is set as two; the exceed ports are standby/redundant ports and can be aggregated if working ports fail. If it is a static trunk group (non-LACP), the number of work ports must equal the total number of group member ports.

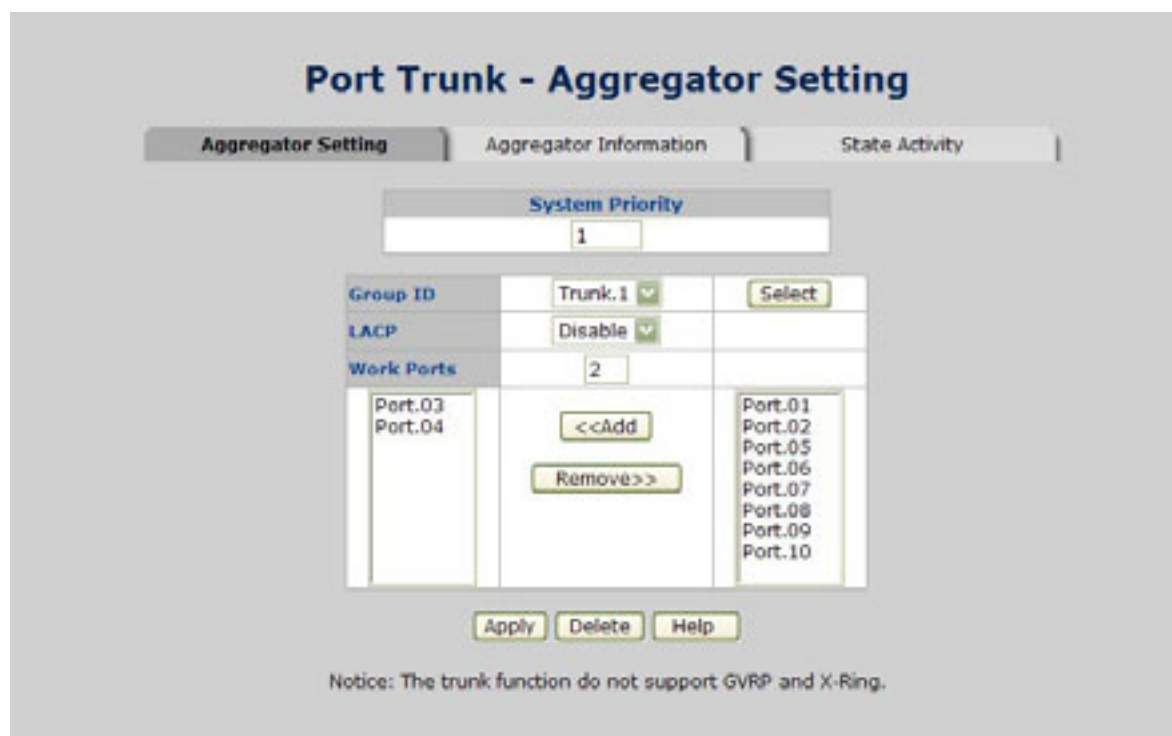
Aggregator Information

When you have setup the LACP aggregator, you will see relevant information in here.

- LACP disabled

Having set up the aggregator setting with LACP disabled, you will see the local static trunk group information on the tab of Aggregator Information.

Figure 5-21: Assigning 2 ports to a trunk group with LACP disabled



Port Trunk - Aggregator Setting

Aggregator Setting | Aggregator Information | State Activity

System Priority: 1

Group ID: Trunk.1 [Select]

LACP: Disable [v]

Work Ports: 2

Port.03
Port.04

<<Add
Remove>>

Port.01
Port.02
Port.05
Port.06
Port.07
Port.08
Port.09
Port.10

Apply Delete Help

Notice: The trunk function do not support GVRP and X-Ring.

Figure 5-22: Static Trunking Group information



This page includes the following fields:

Object	Description
Group Key:	This is a read-only column field that displays the trunk group ID.
Port Member:	This is a read-only column field that displays the members of this static trunk group.

- LACP enabled

Having set up the aggregator setting with LACP enabled, you will see the trunking group information between two switches on the tab of Aggregator Information.

- o Switch 1 configuration

1. Set System Priority of the trunk group. The default is 1.
2. Select a trunk group ID by pull down the drop-down menu bar.
3. Enable LACP.
4. Include the member ports by clicking the Add button after selecting the port number and the column field of Work Ports changes automatically.

Figure 5-23: Aggregation Information of Switch 1

Port Trunk - Aggregator Setting

Aggregator Setting | Aggregator Information | State Activity

System Priority: 1

Group ID: Trunk.1 [Select]

LACP: Enable

Work Ports: 2

Port.03
Port.04

<<Add
Remove>>

Port.01
Port.02
Port.03
Port.04
Port.05
Port.06
Port.07
Port.08
Port.09
Port.10

Apply Delete Help

Notice: The trunk function do not support GVRP and X-Ring.

5. Click on the tab of Aggregator Information to check the trunked group information as the illustration shown above after the two switches configured.

- o Switch 2 configuration

6. Set System Priority of the trunk group. For example: 32768.

7. Select a trunk group ID by pull down the drop-down menu bar.

8. Enable LACP.

9. Include the member ports by clicking the Add button after selecting the port number and the column field of Work Ports changes automatically.

Figure 5-24: Switch 2 configuration interface

Port Trunk - Aggregator Setting

Aggregator Setting | Aggregator Information | State Activity

System Priority: 32768

Group ID: Trunk.1 [Select]

LACP: Disable

Work Ports: 2

Port.01
Port.02

<<Add
Remove>>

Port.01
Port.02
Port.03
Port.04
Port.05
Port.06
Port.07
Port.08
Port.09
Port.10

Apply Delete Help

Notice: The trunk function do not support GVRP and X-Ring.

10. Click on the tab of Aggregator Information to check the trunked group information as the illustration shown above after the two switches configured.

Figure 5-25: Switch 1 Aggregator Information

Port Trunk - Aggregator Information

Aggregator Setting | **Aggregator Information** | State Activity

Static Trunking Group

Group Key	1
Port Member	1 2

State Activity

Having set up the LACP aggregator on the tab of Aggregator Setting, you can configure the state activity for the members of the LACP trunk group. You can tick or cancel the checkbox beside the state label. When you remove the tick mark of the port and click APPLY, the port state activity will change to Passive.

Figure 5-26: State Activity of Switch 1

Port Trunk - State Activity

Aggregator Setting | Aggregator Information | **State Activity**

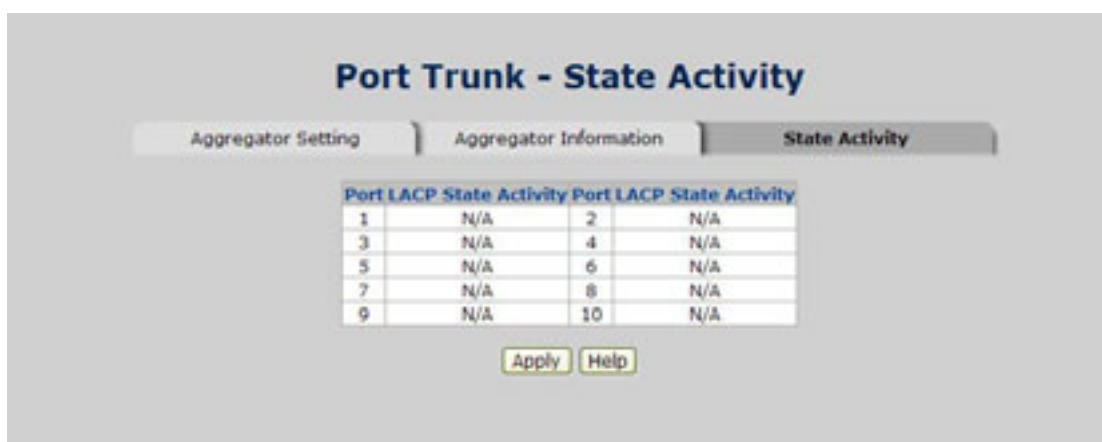
Port LACP State Activity	Port LACP State Activity
1	N/A
2	N/A
3	N/A
4	N/A
5	N/A
6	N/A
7	N/A
8	N/A
9	N/A
10	N/A

Apply Help

This page includes the following fields:

Object	Description
Active:	The port automatically sends LACP protocol packets.
Passive:	The port does not automatically send LACP protocol packets, and responds only if it receives LACP protocol packets from the opposite device.

Figure 5-27: State Activity of Switch 2



NOTE: A link having two passive LACP nodes will not perform dynamic LACP trunk because both ports are waiting for an LACP protocol packet from the opposite device.

Port Mirroring

The Port mirroring is a method for monitor traffic in switched networks. Traffic through ports can be monitored by one specific port, which means traffic goes in or out monitored (source) ports will be duplicated into mirror (destination) port.

Figure 5-28: Port Trunk - Port Mirroring interface



This page includes the following fields:

Object	Description
Destination Port:	There is only one port can be selected to be destination (mirror) port for monitoring both RX and TX traffic which come from source port. Or, use one of two ports for monitoring RX traffic only and the other one for TX traffic only. User can connect mirror port to LAN analyzer or Netxray.
Source Port:	The ports that user wants to monitor. All monitored port traffic will be copied to mirror (destination) port. User can select multiple source ports by checking the RX or TX check boxes to be monitored.

Rate Limiting

You can set up every port's bandwidth rate and frame limitation type.

- Ingress Limit Frame type: select the frame type that wants to filter. There are four frame types for selecting:
 - o All
 - o Broadcast/Multicast/Flooded Unicast
 - o Broadcast/Multicast
 - o Broadcast only

Broadcast/Multicast/Flooded Unicast, Broadcast/Multicast and Broadcast only types are only for ingress frames. The egress rate only supports All type.

Figure 5-29: Rate Limiting interface

	Ingress Limit Frame Type	Ingress	Egress
Port.01	Broadcast/Multicast/Flooded Unicast	256 kbps	0 kbps
Port.02	All	0 kbps	0 kbps
Port.03	All	0 kbps	0 kbps
Port.04	All	0 kbps	0 kbps
Port.05	All	0 kbps	0 kbps
Port.06	All	0 kbps	0 kbps
Port.07	All	0 kbps	0 kbps
Port.08	All	0 kbps	0 kbps
Port.09	All	0 kbps	0 kbps
Port.10	All	0 kbps	0 kbps

Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.

Apply Help

- All the ports support port ingress and egress rate control. For example, assume port 1 is 10Mbps, users can set its effective egress rate is 1Mbps, ingress rate is 500Kbps. The switch performs the ingress rate by packet counter to meet the specified rate
 - Ingress: Enter the port effective ingress rate (The default value is "0").
 - Egress: Enter the port effective egress rate (The default value is "0").
- And then, click APPLY to apply the settings

Protocol

This section has the following items:

- VLAN
- Rapid Spanning Tree protocol
- SNMP
- QoS
- IGMP Snooping

VLAN Configuration

VLAN Overview

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plug into the same switch physically.

The Managed Industrial Switch supports IEEE 802.1Q (tagged-based) and Port-Base VLAN setting in web management page. In the default configuration, VLAN support is "Disable".

- Port-based VLAN

Port-based VLAN limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On port-based VLAN, NIC do not need to be able to identify 802.1Q tags in packet headers. NIC send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet is dropped by the Switch or delivered.

- IEEE 802.1Q VLANs

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

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

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

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

Some relevant terms:

Tagging - The act of putting 802.1Q VLAN information into the header of a packet.

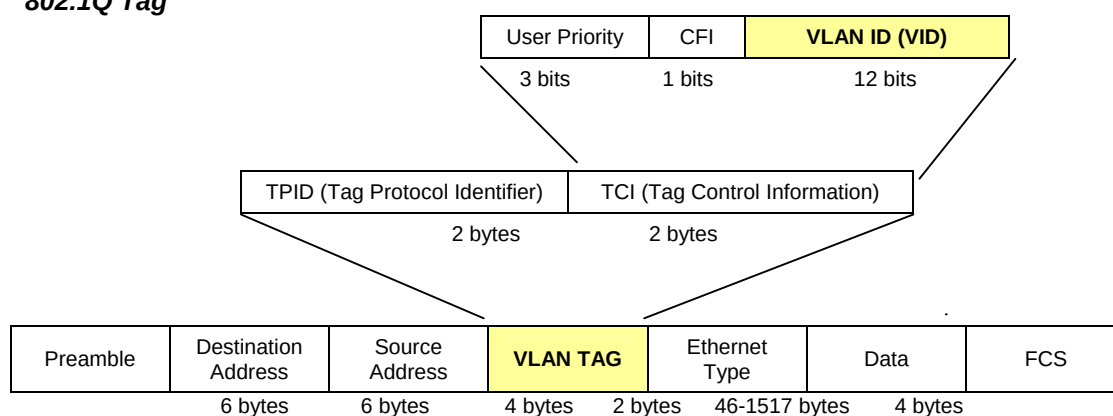
Untagging - The act of stripping 802.1Q VLAN information out of the packet header.

- 802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the Ether Type field. When a packet's Ether Type field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLAN can be identified.

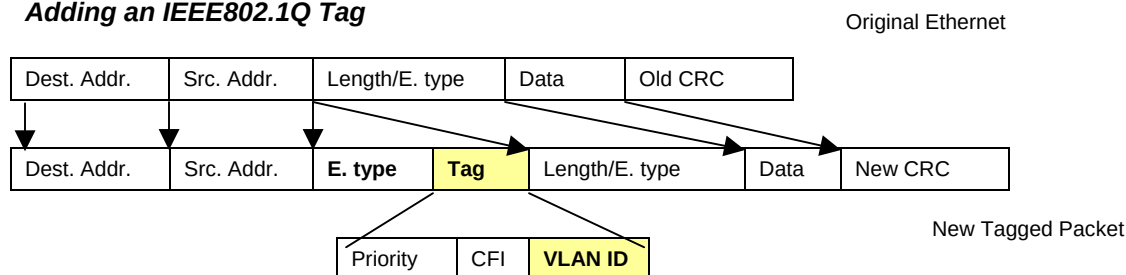
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

802.1Q Tag



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

Adding an IEEE802.1Q Tag



- Port VLAN ID

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

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

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

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

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

- Default VLANs

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

NOTE: No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLAN.

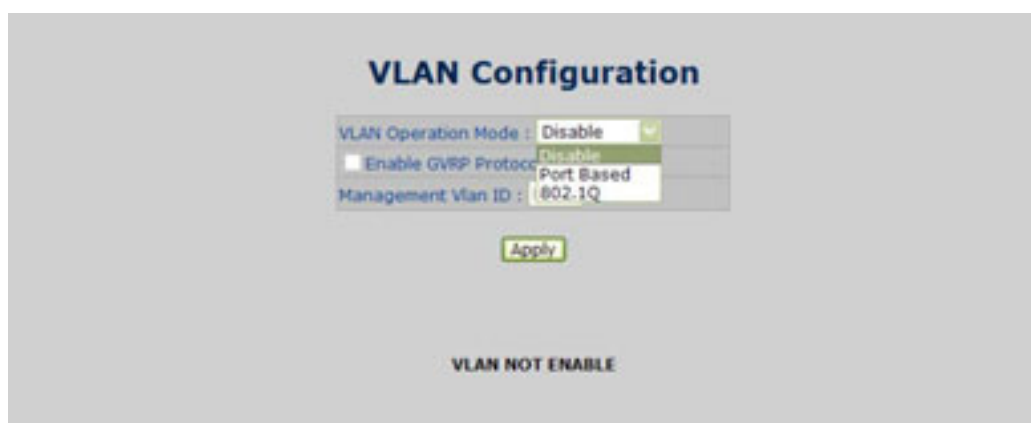
The Switch supports Port-based VLAN and IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.

VLAN Configuration

A Virtual LAN (VLAN) is a logical network grouping that limits the broadcast domain. It allows you to isolate network traffic so only members of the VLAN receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is logically equivalent of reconnecting a group of network devices to another Layer 2 switch. However, all the network devices are still plug into the same switch physically.

The Industrial Switch supports Port-based, 802.1Q (Tagged-based) and GVRP VLAN in web management page. In the default configuration, VLAN support is "Disable".

Figure 5-30: VLAN Configuration interface



Port-based VLAN

A port-based VLAN basically consists of its members-ports, which means that the VLAN is created by grouping the selected ports. This method provides the convenience for users to configure a simple VLAN easily without complicated steps. Packets can go among only members of the same VLAN group. Note all unselected ports are treated as belonging to another single VLAN. If the port-based VLAN enabled, the VLAN-tagging is ignored. The port-based VLAN function allows the user to create separate VLANs to limit the unnecessary packet flooding; however, for the purpose of sharing resource, a single port called a common port can belongs to different VLANs, which all the member devices (ports) in different VLANs have the permission to access the common port while they still cannot communicate with each other in different VLANs.

Figure 5-31: VLAN - Port Based interface

VLAN Configuration

VLAN Operation Mode : Port Based

☐ Enable GVRP Protocol

Management Vlan ID : 0

Apply

VLAN NOT ENABLE

- Pull down the selection item and focus on Port Based then press to set the VLAN Operation Mode in Port Based mode.

Click **ADD** to add a new VLAN group (The maximum VLAN groups are up to 64).

Figure 5-32: VLAN - Port Based Add interface

VLAN Configuration

VLAN Operation Mode : Port Based

☐ Enable GVRP Protocol

Management Vlan ID : 0

Apply

Group Name : VLAN2

VLAN ID : 2

Port.01		Port.03
Port.02		Port.04
Port.07		Port.05
Port.08		Port.06
Port.09		
Port.10		

Add

Remove

Apply Help

- Enter the group name and VLAN ID. Add the selected port number into the right field to group these members to be a VLAN group, or remove any of them listed in the right field from the VLAN.
- And then, click **APPLY** to have the configuration take effect.
- You will see the VLAN list displays.

Figure 5-33: VLAN-Port Based Edit/Delete interface

- Use **DELETE** to delete the VLAN.
- Use **EDIT** to modify group name, VLAN ID, or add/remove the members of the existing VLAN group.

NOTE: Remember to execute the "Save Configuration" action, otherwise the new configuration will be lost when switch power off.

802.1Q VLAN

Virtual Local Area Network (VLAN) can be implemented on the Industrial Switch to logically create different broadcast domain.

When the 802.1Q VLAN function is enabled, all ports on the switch belong to default VLAN of VID 1, which means they logically are regarded as members of the same broadcast domain. The valid VLAN ID is in the range of number between 1 and 4094. The amount of VLAN groups is up to 256 including default VLAN that cannot be deleted.

Each member port of 802.1Q is on either an Access Link (no VLAN-tagged) or a Trunk Link (VLAN-tagged)[KK1]. All frames on an Access Link carry no VLAN identification. Conversely, all frames on a Trunk Link are VLAN-tagged. Besides, there is the third mode-Hybrid. A Hybrid Link can carry both VLAN-tagged frames and untagged frames. A single port is supposed to belong to one VLAN group, except it is on a Trunk/Hybrid Link.

The technique of 802.1Q tagging inserts a 4-byte tag, including VLAN ID of the destination port-PVID, in the frame. With the combination of Access/Trunk/Hybrid Links, the communication across switches also can make the packet sent through tagged and untagged ports.

- 802.1Q VLAN Port Configuration

This page is used for configuring the Industrial Switch port VLAN. The VLAN per Port Configuration page contains fields for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the VLAN Port Configuration page. All untagged packets arriving to the device are tagged by the ports PVID.

Understanding the nomenclature of the Switch

- IEEE 802.1Q Tagged and Untagged

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

Tagged (Trunk Link)	Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.
Untagged (Access Link)	Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

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

Here pay attention to the explaining of "Access", "Trunk" and "Hybrid".

- Access: Ports will strip the 802.1Q tag from all packets that out of those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Ports with "Access" mode belong to a single untagged VLAN.

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

- Hybrid: The port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode). Ports will strip the 802.1Q tag from all packets that out of those ports.

Port Mode	VLAN Membership	Frame Leave
Access Link	Belongs to a single untagged VLAN	Untagged (Tag=PVID be removed)
Trunk Link	Allowed to belongs to multiple Tagged VLANs at the same time	Tagged (Tag=PVID or Original VID be remained)
Hybrid Link	Allowed to belongs to multiple untagged VLANs at the same time	Untagged by specify VID

The 802.1Q VLAN Port Configuration screen is shown below:

Figure 5-34: 802.1Q VLAN mode

The screenshot displays the 'VLAN Configuration' web interface. At the top, 'VLAN Operation Mode' is set to '802.1Q'. Below it, there is an unchecked checkbox for 'Enable GVRP Protocol' and a text field for 'Management Vlan ID' set to '0'. An 'Apply' button is located below these settings.

Below the main settings, there are two tabs: '802.1Q Configuration' (which is active) and 'Group Configuration'. Under the '802.1Q Configuration' tab, there is a configuration area for a specific port. It shows 'Port.01' selected from a dropdown, 'Access Link' as the 'Link Type', and '1' as the 'Untagged Vid'. There is an empty field for 'Tagged Vid'. 'Apply' and 'Help' buttons are present below this configuration area.

At the bottom of the screen, there is a table listing the configuration for multiple ports:

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	
Port.02	Access Link	1	
Port.03	Access Link	1	
Port.04	Access Link	1	
Port.05	Access Link	1	
Port.06	Access Link	1	

This page includes the following fields:

Object	Description
Enable GVRP Protocol:	GVRP (GARP VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices. For example, having enabled GVRP on two switches, they are able to automatically exchange the information of their VLAN database. Therefore, the user doesn't need to manually configure whether the link is trunk or hybrid, the packets belonging to the same VLAN can communicate across switches. Tick this checkbox to enable GVRP protocol. This checkbox is available while the VLAN Operation Mode is in 802.1Q mode.
Management VLAN ID:	Only when the VLAN members, whose Untagged VID (PVID) equals to the value in this column, will have the permission to access the switch. The default value is '0' that means this limit is not enabled (all members in different VLANs can access this switch).
Link Type:	There are 3 types of link type. Access Link: A segment which provides the link path for one or more stations to the VLAN-aware device. An Access Port (untagged port), connected to the access link, has an untagged VID (also called PVID). After an untagged frame gets into the access port, the switch will insert a four-byte tag in the frame. The contents of the last 12-bit of the tag is untagged VID. When this frame is sent out through any of the access port of the same PVID, the switch will remove the tag from the frame to recover it to what it was. Those ports of the same untagged VID are regarded as the same VLAN group members. Trunk Link: A segment which provides the link path for one or more VLAN-aware devices (switches). A Trunk Port, connected to the trunk link, has an understanding of tagged frame, which is used for the communication among VLANs across switches. Which frames of the specified VIDs will be forwarded depends on the values filled in the Tagged VID column field. Please insert a comma between two VIDs. Hybrid Link: A segment which consists of Access and Trunk links. The hybrid port has both the features of access and trunk ports. A hybrid port has a PVID belonging to a particular VLAN, and it also forwards the specified tagged-frames for the purpose of VLAN communication across switches.
Untagged VID:	This column field is available when Link Type is set as Access Link and Hybrid Link. Assign a number in the range between 1 and 4094.

Object	Description
Tagged VID:	This column field is available when Link Type is set as Trunk Link and Hybrid Link. Assign a number in the range between 1 and 4094.

NOTE: Access Link:

Because the access port doesn't have an understanding of tagged frame, the column field of Tagged VID is not available.

NOTE: Trunk Link

1. A trunk port doesn't insert tag into an untagged frame, and therefore the untagged VID column field is not available.
2. It's not necessary to type '1' in the tagged VID. The trunk port will forward the frames of VLAN 1.
3. The trunk port has to be connected to a trunk/hybrid port of the other switch. Both the tagged VID of the two ports have to be the same.

NOTE: Hybrid Link

1. It's not necessary to type '1' in the tagged VID. The hybrid port will forward the frames of VLAN 1.
2. The trunk port has to be connected to a trunk/hybrid port of the other switch. Both the tagged VID of the two ports have to be the same.

- Pull down the selection item and focus on 802.1Q then press to set the VLAN Operation Mode in 802.1Q mode
- You can see the link type, untagged VID, and tagged VID information of each port in the table below on the screen.

Figure 5-35: 802.1Q VLAN interface

The interface shows the '802.1Q Configuration' tab. At the top, there is a 'Group Configuration' tab. Below it, a table shows the configuration for Port.01, which is an Access Link with an Untagged Vid of 1. Below the table are 'Apply' and 'Help' buttons. At the bottom, a larger table lists ports Port.01 through Port.10, all configured as Access Links with an Untagged Vid of 1.

Port	Link Type	Untagged Vid	Tagged Vid
Port.01	Access Link	1	
Port.02	Access Link	1	
Port.03	Access Link	1	
Port.04	Access Link	1	
Port.05	Access Link	1	
Port.06	Access Link	1	
Port.07	Access Link	1	
Port.08	Access Link	1	
Port.09	Access Link	1	
Port.10	Access Link	1	

- **Group Configuration**

Edit the existing VLAN Group.

- Select the VLAN group in the table list.
- Click **EDIT**.

Figure 5-36: Group Configuration interface

The interface shows the 'VLAN Configuration' title. Below it, there are settings for 'VLAN Operation Mode' (set to 802.1Q), 'Enable GVRP Protocol' (unchecked), and 'Management Vlan ID' (set to 0). Below these settings is an 'Apply' button. At the bottom, there are two tabs: '802.1Q Configuration' and 'Group Configuration'. The 'Group Configuration' tab is active, showing a table with one entry: 'Default' with a value of '1'. Below the table are 'Edit' and 'Delete' buttons.

Group	Value
Default	1

- You can modify the VLAN group name and VLAN ID.

Figure 5-37: Group Configuration interface

- Click **APPLY**.

Rapid Spanning Tree Protocol

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol and provides for faster spanning tree convergence after a topology change. The system also supports STP and the system will auto-detect the connected device that is running STP or RSTP protocol.

Theory

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

- STP - Spanning Tree Protocol (IEEE 802.1D)
- RSTP - Rapid Spanning Tree Protocol (IEEE 802.1w)

The IEEE 802.1D Spanning Tree Protocol and IEEE 802.1W Rapid Spanning Tree Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The

protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

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

The Switch STP performs the following functions:

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

Bridge Protocol Data Units

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

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

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

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

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

The communication between switches via BPDUs results in the following:

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

Creating a Stable STP Topology

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

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

STP Port States

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

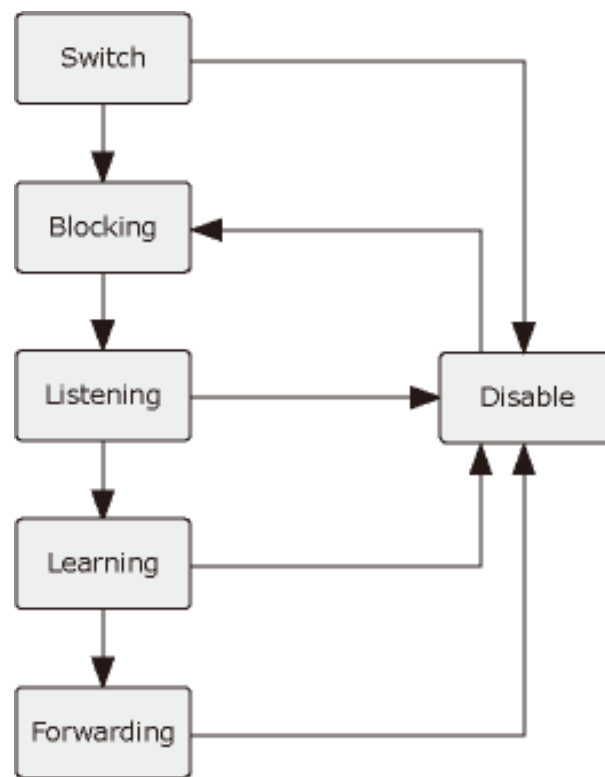
Each port on a switch using STP exists in one of the following five states:

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

A port transitions from one state to another as follows:

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

Figure 5-38: STP Port State Transitions



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

RSTP Parameters

RSTP Operation Levels

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

NOTE: On the switch level, RSTP calculates the Bridge Identifier for each switch and then sets the Root Bridge and the Designated Bridges.

On the port level, RSTP sets the Root Port and the Designated Ports.

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

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

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

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

Default Spanning-Tree Configuration

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

User-Changeable STA Parameters

The Switch's factory default setting should cover the majority of installations. However, it is advisable to keep the default settings as set at the factory; unless, it is absolutely necessary. The user changeable parameters in the Switch are as follows:

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

Hello Time – The Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

NOTE: The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur.

Max. Age – The Max Age can be from 6 to 40 seconds. At the end of the Max Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

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

NOTE: Observe the following formulas when setting the above parameters:

Max. Age $\geq 2 \times (\text{Forward Delay} - 1 \text{ second})$

Max. Age $\geq 2 \times (\text{Hello Time} + 1 \text{ second})$

Port Priority – A Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port.

Port Cost – A Port Cost can be set from 0 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.

Illustration of STP

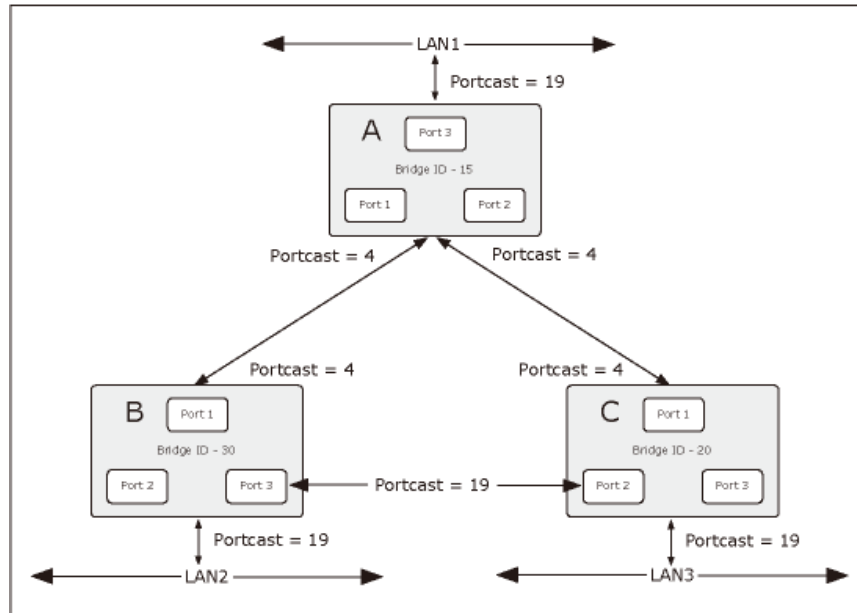
A simple illustration of three switches connected in a loop is depicted in the below diagram. In this example, you can anticipate some major network problems if the STP assistance is not applied.

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

Now, if switch A broadcasts a packet to switch C, then switch C will drop the packet at port 2 and the broadcast will end there. Setting-up STP using values other than the defaults, can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using

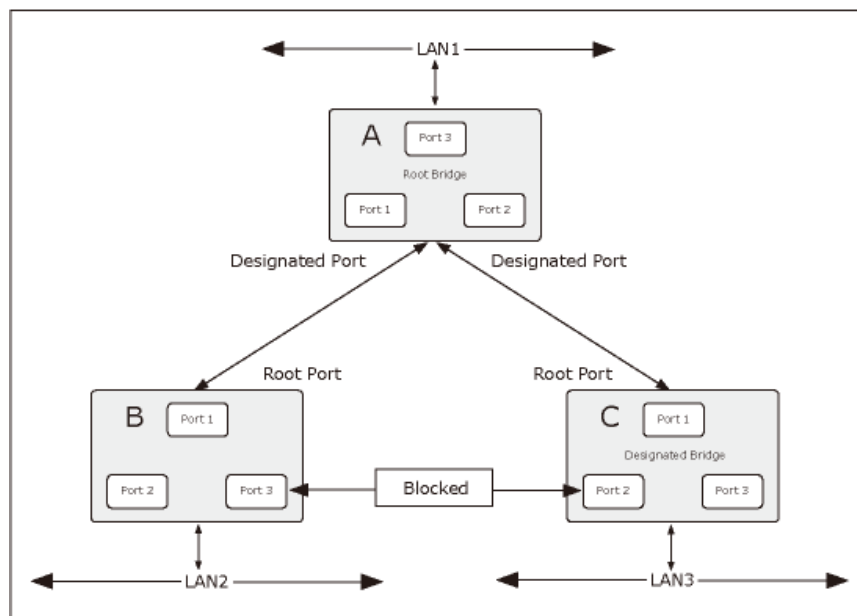
the Priority setting, or influencing STP to choose a particular port to block using the Port Priority and Port Cost settings is, however, relatively straight forward.

Figure 5-39: Before Applying the STA Rules



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

Figure 5-40: After Applying the STA Rules



The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 4) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 19). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between switch B and switch C is the blocked link.

RSTP System Configuration

This section provides RSTP-System Configuration from the Switch, the screen in Figure 5-41 appears.

- The user can view spanning tree information of Root Bridge.
- The user can modify RSTP state. After modification, click **APPLY**.

Figure 5-41: RSTP System Configuration interface

RSTP - System Configuration

System Configuration | Port Configuration

RSTP Mode	Enable
Priority (0-61440)	32768
Max Age (6-40)	20
Hello Time (1-10)	2
Forward Delay Time (4-30)	15

Priority must be a multiple of 4096
 $2 * (\text{Forward Delay Time} - 1)$ should be greater than or equal to the Max Age.
 The Max Age should be greater than or equal to $2 * (\text{Hello Time} + 1)$.

Apply Help

Root Bridge Information

Bridge ID	0080000F3801C976
Root Priority	32768
Root Port	Root
Root Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15

This page includes the following fields:

Object	Description
RSTP mode:	The user must enable the RSTP function first before configuring the related parameters.
Priority (0-61440):	The switch with the lowest value has the highest priority and is selected as the root. If the value is changed, the user must reboot the switch. The value must be a multiple of 4096 according to the protocol standard rule.
Max Age (6-40):	The number of seconds a switch waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration. Enter a value between 6 through 40.
Hello Time (1-10):	The time that controls the switch to send out the BPDU packet to check RSTP current status. Enter a value between 1 through 10.
Forward Delay Time (4-30):	The number of seconds a port waits before changing from its Rapid Spanning-Tree Protocol learning and listening states to the forwarding state. Enter a value between 4 through 30.

NOTE: Follow the rule as below to configure the MAX Age, Hello Time, and Forward Delay Time.

$2 \times (\text{Forward Delay Time value} - 1) \geq \text{Max Age value} \geq 2 \times (\text{Hello Time value} + 1)$.

Port Configuration

This web page provides the port configuration interface for RSTP. You can assign higher or lower priority to each port. Rapid spanning tree will have the port with the higher priority in forwarding state and block other ports to make certain that there is no loop in the LAN.

Figure 5-42: RSTP Port Configuration interface

RSTP - Port Configuration

System Configuration | Port Configuration

Port	Path Cost (1-20000000)	Priority (0-240)	Admin P2P	Admin Edge	Admin Non STP
Port.01	200000	128	Auto	true	false
Port.02					
Port.03					
Port.04					
Port.05					

priority must be a multiple of 16

Apply Help

RSTP Port Status

Port	Path Cost	Port Priority	Oper P2P	Oper Edge	STP Neighbor	State	Role
Port.01	200000	128	True	True	False	Disabled	Disabled
Port.02	200000	128	True	True	False	Disabled	Disabled
Port.03	200000	128	True	True	False	Disabled	Disabled
Port.04	200000	128	True	True	False	Disabled	Disabled
Port.05	200000	128	True	True	False	Disabled	Disabled
Port.06	200000	128	True	True	False	Disabled	Disabled
Port.07	200000	128	True	True	False	Disabled	Disabled
Port.08	200000	128	True	True	False	Disabled	Disabled
Port.09	200000	128	True	True	False	Disabled	Disabled
Port.10	200000	128	True	True	False	Forwarding	Designated

This page includes the following fields:

Object	Description
Path Cost:	The cost of the path to the other bridge from this transmitting bridge at the specified port. Enter a number 1 through 200,000,000.
Priority:	Decide which port should be blocked by setting its priority as the lowest. Enter a number between 0 and 240. The value of priority must be the multiple of 16.
Admin P2P:	The rapid state transitions possible within RSTP are dependent upon whether the port concerned can only be connected to exactly another bridge (i.e. it is served by a point-to-point LAN segment), or can be connected to two or more bridges (i.e. it is served by a shared medium LAN segment). This function allows the P2P status of the link to be manipulated administratively. True means the port is regarded as a point-to-point link. False means the port is regarded as a shared link. Auto means the link type is determined by the auto-negotiation between the two peers.
Admin Edge:	The port directly connected to end stations won't create bridging loop in the network. To configure the port as an edge port, set the port to "True" status.
Admin Non STP:	The port includes the STP mathematic calculation. True is not including STP mathematic calculation. False is including the STP mathematic calculation.

NOTE: Path cost "0" is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021w standard exceeds 65,535, the default is set to 65,535.

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below.

Table 5-1: Recommended STP Path Cost Range

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

Table 5-2: Recommended STP Path Costs

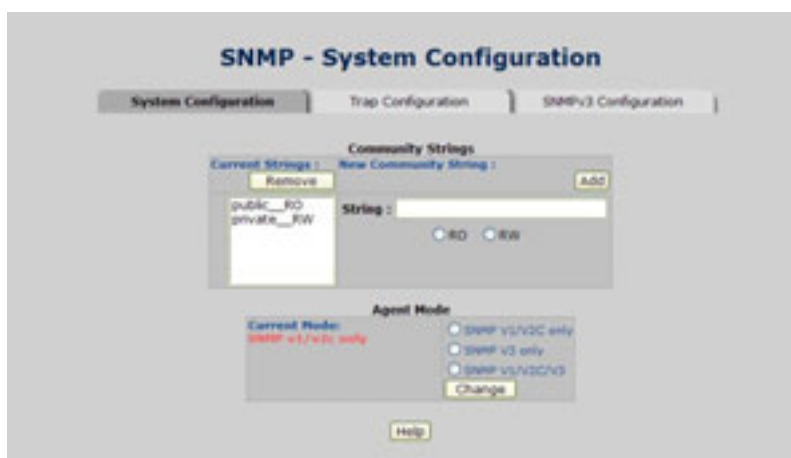
Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

SNMP Configuration

Simple Network Management Protocol (SNMP) is the protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. Network management systems learn of problems by receiving traps or change notices from network devices implementing SNMP.

System Configuration

Figure 5-43: SNMP System Configuration interface



This page includes the following fields:

Object	Description
Community Strings:	Here you can define the new community string set and remove the unwanted community string. String: Fill the name string. RO: Read only. Enables requests accompanied by this community string to display MIB-object information. RW: Read/write. Enables requests accompanied by this community string to display MIB-object information and to set MIB objects. Click APPLY. To remove the community string, select the community string that you defined before and click REMOVE. The strings of Public_RO and Private_RW are default strings. You can remove them but after resetting the switch to default, the two strings show up again.
Agent Mode:	Select the SNMP version that you want to use it. And then click CHANGE to switch to the selected SNMP version mode.

Trap Configuration

A trap manager is a management station that receives the trap messages generated by the switch. If no trap manager is defined, no traps will be issued. To define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version.

Figure 5-44: Trap Managers interface

The interface is titled "SNMP - Trap Configuration" and has three tabs: "System Configuration", "Trap Configuration" (selected), and "SNMPv3 Configuration".

Trap Managers

Current Managers : A list box containing "192.168.0.52: public, v2" with a "Remove" button next to it.

New Manager : Fields for "IP Address :", "Community :", and "Trap version:" (with radio buttons for "v1" and "v2c"). An "Add" button is next to the "New Manager" label.

A "Help" button is located at the bottom center.

This page includes the following fields:

Object	Description
IP Address:	Enter the IP address of the trap manager.
Community:	Enter the community string for the trap station.
Trap Version:	Select the SNMP trap version type—v1 or v2c.

SNMPV3 Configuration

Configure the SNMP V3 function.

Figure 5-45: SNMP V3 configuration interface - User Table

The interface is titled "SNMP - SNMPv3 Configuration" and has three tabs: "System Configuration", "Trap Configuration", and "SNMPv3 Configuration" (selected).

Context Table

Context Name : A text input field with an "Apply" button.

User Table

Current User Profiles : A list box with a "Remove" button.

New User Profile : Fields for "User ID:", "Authentication Password:", and "Privacy Password:". An "Add" button is next to the "New User Profile" label.

Group Table

Current Group context : A list box with a "Remove" button.

New Group Table: Fields for "Security Name (User ID):" and "Group Name:". An "Add" button is next to the "New Group Table" label.

- **Context Table**

Configure SNMP v3 context table. Assign the context name of context table. Click ADD to add context name. Click REMOVE to remove unwanted context name.

- **User Table**

Configure SNMP v3 user table.

This page includes the following fields:

Object	Description
User ID:	Set up the user name.
Authentication Password:	Set up the authentication password.
Privacy Password:	Set up the private password.

- **Group Table**

Configure SNMP v3 group table.

Figure 5-46: SNMP V3 configuration interface - Group Table

The screenshot displays the SNMP V3 configuration interface, specifically the Group Table section. It is divided into three main parts: Group Table, Access Table, and MIBView Table.

Group Table: This section includes a 'Current Group content' list with a 'Remove' button. To the right, the 'New Group Table' section has an 'Add' button and two input fields: 'Security Name (User ID):' and 'Group Name:'.

Access Table: This section includes a 'Current Access Tables' list with a 'Remove' button. To the right, the 'New Access Table' section has an 'Add' button and several input fields: 'Context Prefix:', 'Group Name:', 'Security Level:' (with radio buttons for 'NoAuthNoPriv.', 'AuthNoPriv.', and 'AuthPriv.'), 'Context Match Rule' (with radio buttons for 'Exact' and 'Prefix'), 'Read View Name:', 'Write View Name:', and 'Notify View Name:'.

MIBView Table: This section includes a 'Current MIBTables' list with a 'Remove' button. To the right, the 'New MIBView Table' section has an 'Add' button.

This page includes the following fields:

Object	Description
Security Name (User ID):	Assign the user name that you have set up in user table.
Group Name:	Set up the group name.

- **Access Table**

Configure SNMP v3 access table.

Figure 5-47: SNMP V3 configuration interface - Access Table

This page includes the following fields:

Object	Description
Context Prefix:	Set up the context name.
Group Name:	Set up the group.
Security Level:	Select the access level.
Context Match Rule:	Select the context match rule.
Read View Name:	Set up the read view.
Write View Name:	Set up the write view.
Notify View Name:	Set up the notify view.

- **MIBview Table**

Configure MIB view table.

Figure 5-48: SNMP V3 configuration interface - MIBView Table

MIBView Table

Current MIBTables : Remove

New MIBView Table : Add

View Name:

SubOld-Tree:

Type: ☐ Excluded ☐ Included

Help

Note:
Any modification of SNMPv3 tables might cause MIB accessing rejection. Please take notice of the causality between the tables before you modify these tables.

This page includes the following fields:

Object	Description
ViewName:	Set up the name.
Sub-Oid Tree:	Fill the Sub OID.
Type:	Select the type – exclude or included.

QoS Configuration

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

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want the switch to treat selected applications and types of traffic.

You can use QoS on your system to:

- Control a wide variety of network traffic by:
- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Provide predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage network congestion.

The QoS page of the Switch contains three types of QoS mode - the CoS mode, TOS mode or Port-based mode can be selected. Both the three mode rely on predefined fields within the packet to determine the output queue.

- CoS / 802.1p Tag Priority Mode -The output queue assignment is determined by the IEEE 802.1p VLAN priority tag.
- TOS / DSCP Mode - The output queue assignment is determined by the TOS or DSCP field in the IP packets.
- Port-Based Priority Mode - Any packet received from the specify high priority port will treated as a high priority packet.

QoS Policy and Priority Type

Here you can choose to use an 8-4-2-1 queuing scheme or a strict priority scheme, or select the priority type to configure QoS policy.

Figure 5-49: QoS Configuration interface

This page includes the following fields:

Object	Description
Qos Policy:	Select the QoS policy rule.
	Using the 8,4,2,1 weight fair queue scheme: The switch will follow 8:4:2:1 rate to process priority queue from High to lowest queue.
	For example, while the system processing, 1 frame of the lowest queue, 2 frames of the low queue, 4 frames of the middle queue, and 8 frames of the high queue will be processed at the same time in accordance with the 8,4,2,1 policy rule.
Priority Type:	Use a strict priority scheme: Always the higher queue will be processed first, except the higher queue is empty.
	There are 5 priority type selections available—
	Port-based
	TOS only
	COS only
	TOS first
	COS first
	Disable means no priority type is selected.

Port-based Priority

Configure the priority level for each port. With the drop-down selection item of Priority Type above being selected as Port-based, this control item will then be available to set the queuing policy for each port.

Figure 5-50: QoS Configuration - Port-Based Priority

Port-based Priority:

Port.01	Port.02	Port.03	Port.04	Port.05	Port.06	Port.07	Port.08	Port.09	Port.10
Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼

Apply Help

CoS:

Priority 0	1	2	3	4	5	6	7
Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼

Apply Help

ToS:

Priority 0	1	2	3	4	5	6	7
Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼
Priority 8	9	10	11	12	13	14	15
Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼
Priority 16	17	18	19	20	21	22	23
Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼
Priority 24	25	26	27	28	29	30	31
Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼
Priority 32	33	34	35	36	37	38	39
Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼
Priority 40	41	42	43	44	45	46	47
Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼	Lowest ▼

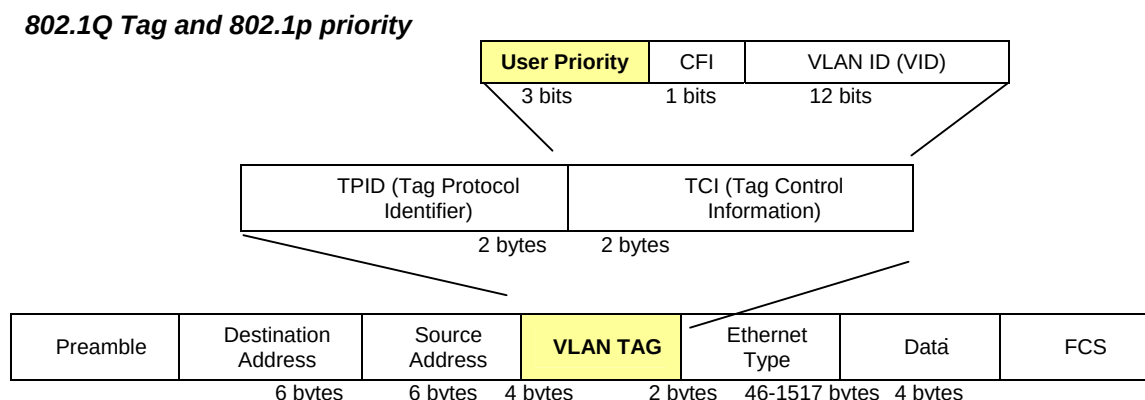
This page includes the following fields:

Object	Description
Port x:	Each port has 4 priority levels—High, Middle, Low, and Lowest—to be chosen.

COS Configuration

QoS settings allow customization of packet priority in order to facilitate delivery of data traffic that might be affected by latency problems. When CoS / 802.1p Tag Priority is applied, the Switch recognizes 802.1Q VLAN tag packets and extracts the VLAN tagged packets with User Priority value.

Figure 5-51: 802.1p Tag Priority



Set up the COS priority level. With the drop-down selection item of Priority Type above being selected as COS only/COS first, this control item will then be available to set the queuing policy for each port.

Figure 5-52: QoS Configuration - COS Priority

The screenshot shows the QoS Configuration - COS Priority web interface. It features two main sections: **CoS:** and **ToS:**. The **CoS:** section has a table with 8 columns (Priority 0 to 7) and 8 rows (Priority 0 to 7). Each cell contains a dropdown menu set to 'Lowest'. Below the table are 'Apply' and 'Help' buttons. The **ToS:** section has a similar table with 8 columns (Priority 0 to 7) and 8 rows (Priority 0 to 7). Each cell contains a dropdown menu set to 'Lowest'. Below the table are 'Apply' and 'Help' buttons.

This page includes the following fields:

Object	Description
COS priority:	Set up the COS priority level 0~7—High, Middle, Low, Lowest.

NOTE: 802.1p Priority: Priority classifiers of the Switch forward packet. COS range is from 0 to 7. Seven is the high class. Zero is the less class. The user may configure the mapping between COS and Traffic classifiers.

TOS Configuration

DiffServ Code Point (DSCP) - is the traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network.

The Quality of Service page provides fields for defining output queue to specific DSCP fields. When TCP/IP's TOS/DSCP mode is applied, the Switch recognizes TCP/IP Differentiated Service Codepoint (DSCP) priority information from the DS-field defined in RFC2474. Select the QoS mode to TOS, the TOS to priority mapping page appears, as the Figure 5-53 shows.

Set up the TOS priority. With the drop-down selection item of Priority Type above being selected as TOS only/TOS first, this control item will then be available to set the queuing policy for each port.

Figure 5-53: QoS Configuration - TOS Priority

This page includes the following fields:

Object	Description
TOS priority:	The system provides 0~63 TOS priority level. Each level has 4 types of priority—High, Middle, Low, and Lowest. The default value is 'Lowest' priority for each level. When the IP packet is received, the system will check the TOS level value in the IP packet that has received. For example, the user sets the TOS level 25 as high, the system will check the TOS value of the received IP packet. If the TOS value of received IP packet is 25 (priority = high), and then the packet priority will have highest priority.

IGMP Snooping

Theory

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

About the Internet Group Management Protocol (IGMP) Snooping

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

Figure 5-54: Multicast Service

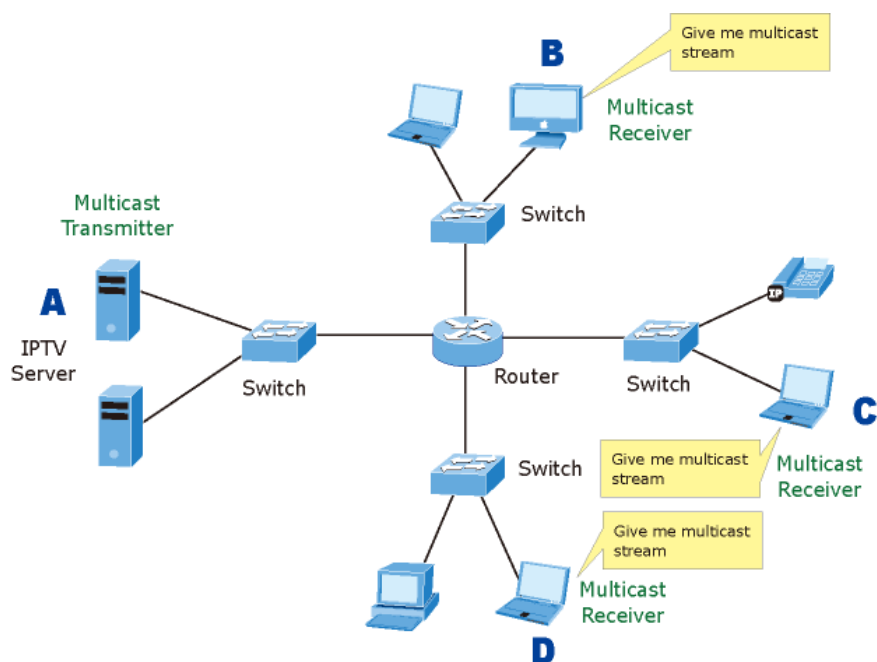


Figure 5-55: Multicast flooding

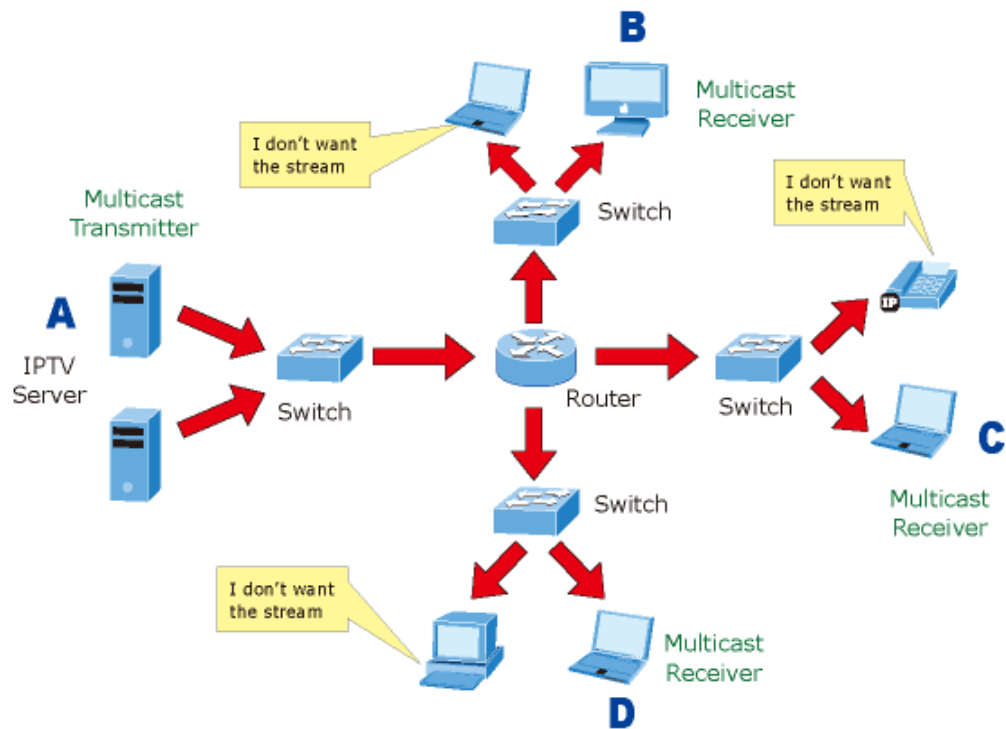
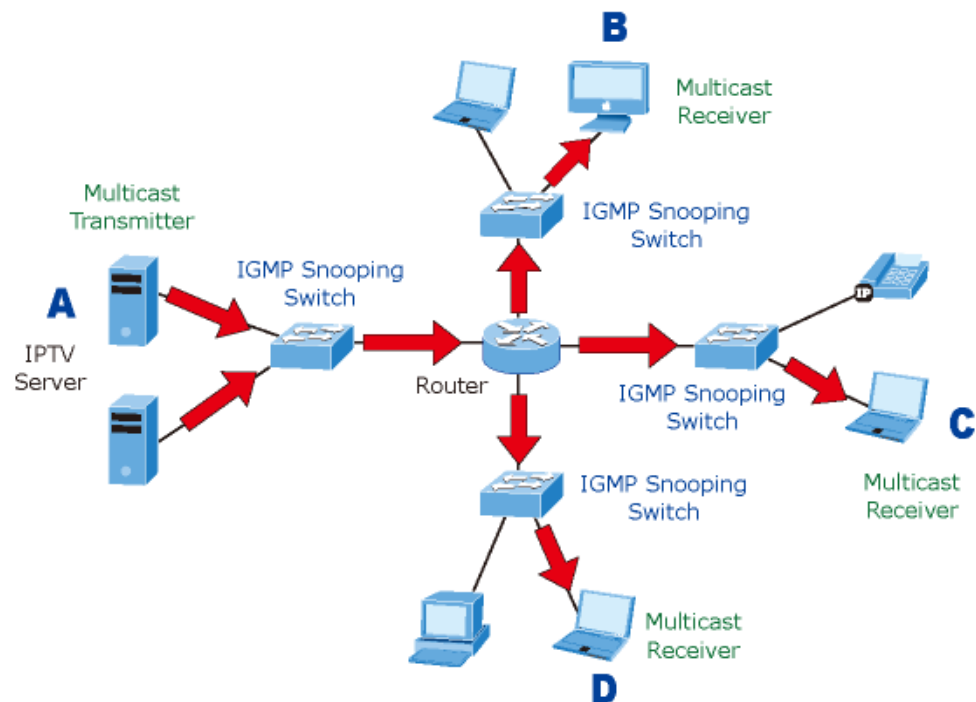


Figure 5-56: IGMP Snooping multicast stream control



IGMP Versions 1 and 2

Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group.

IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data.

The format of an IGMP packet is shown below:

IGMP Message Format

Octets

0	8	16	31
Type	Response Time	Checksum	
Group Address (all zeros if this is a query).			

The IGMP Type codes are shown below:

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

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

A host sends an IGMP "report" to join a group.

A host will never send a report when it wants to leave a group (for version 1).

A host will send a "leave" report when it wants to leave a group (for version 2).

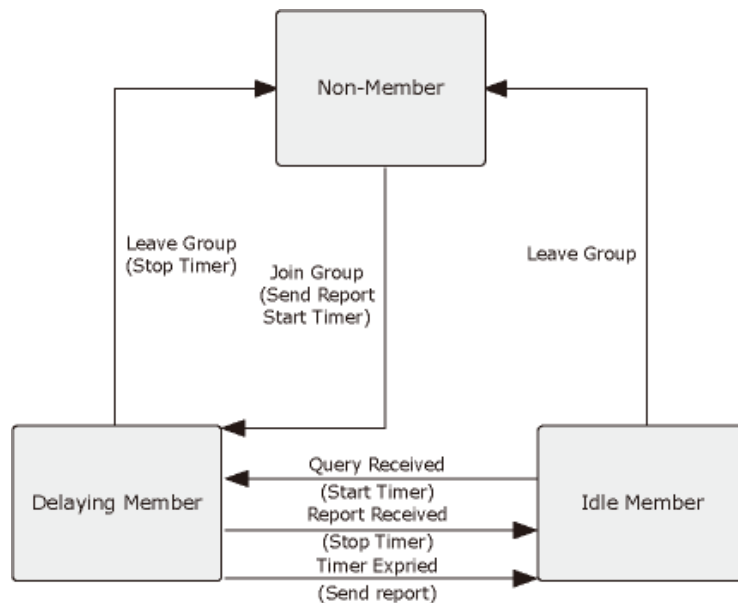
Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their sub networks. If there is no response from a particular group, the router assumes that there are no group members on the network.

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

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

The states a computer will go through to join or to leave a multicast group are shown below:

Figure 5-57: IGMP State Transitions



- IGMP Querier

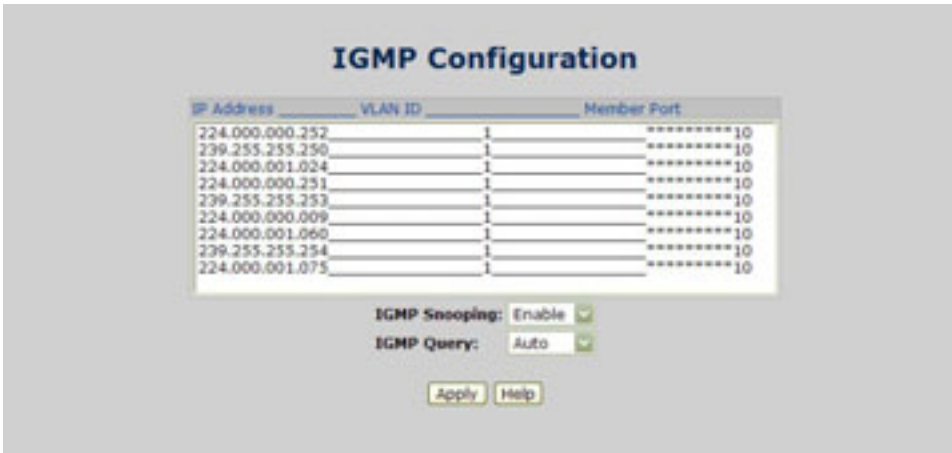
A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the role of querying the LAN for group members. It then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

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

IGMP Configuration

The Industrial Switch support IP multicast, you can enable IGMP protocol on web management's switch setting advanced page, then the IGMP snooping information displays. IP multicast addresses range are from 224.0.0.0 through 239.255.255.255.

Figure 5-58: IGMP Configuration interface



This page includes the following fields:

Object	Description
IGMP Protocol:	Enable or disable the IGMP protocol.
IGMP Query:	Enable or disable the IGMP query function. The IGMP query information will be displayed in IGMP status section.

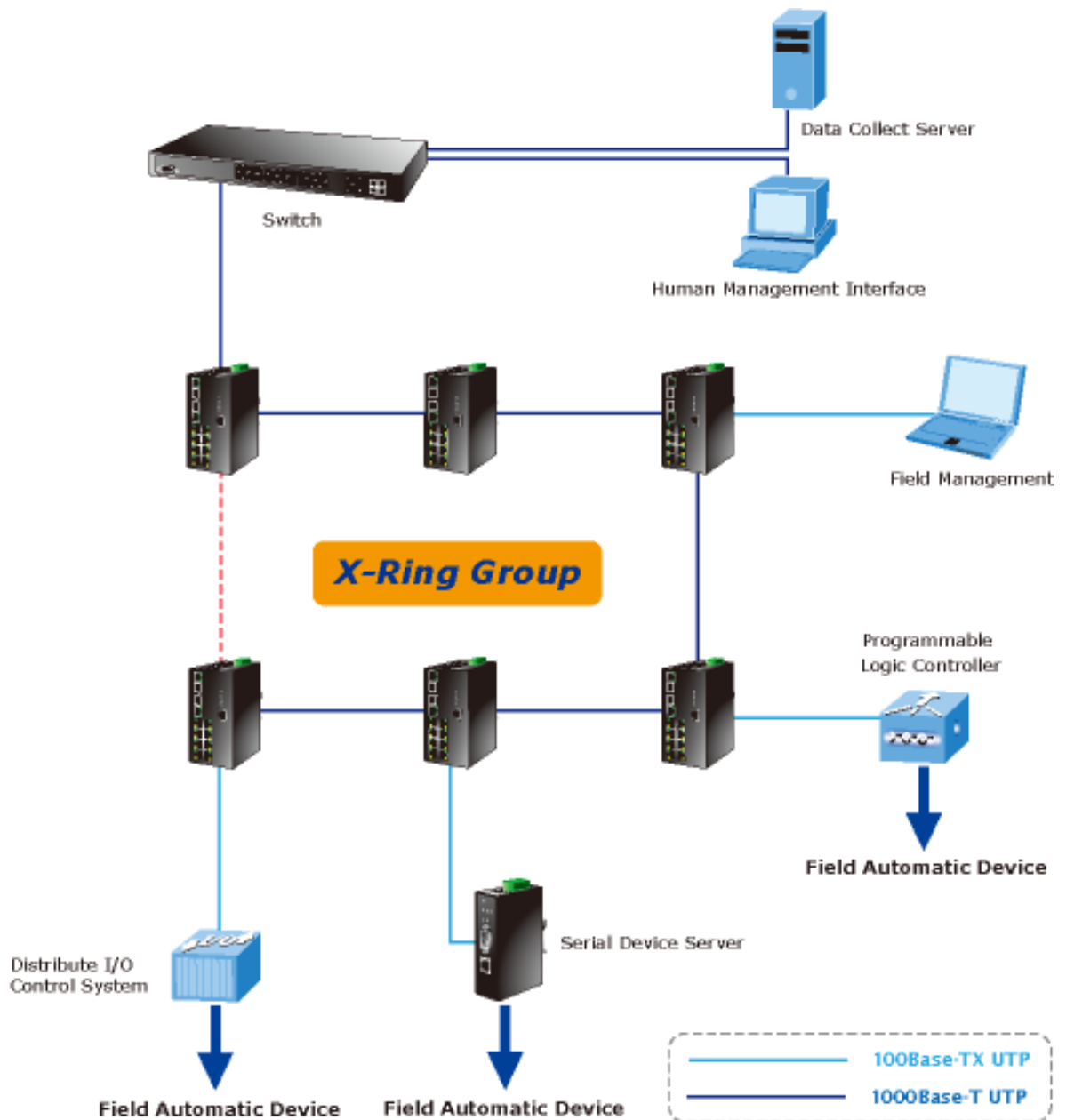
X-Ring

X-Ring provides a faster redundant recovery than Spanning Tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same. In the X-Ring topology, every switch should be enabled with X-Ring function and two ports should be assigned as the member ports in the ring. Only one switch in the X-Ring group would be set as the master switch that one of its two member ports would be blocked, called backup port, and another port is called working port. Other switches in the X-Ring group are called working switches and their two member ports are called working ports. When the failure of network connection occurs, the backup port of the master switch (Ring Master) will automatically become a working port to recover from the failure.

X-Ring Application

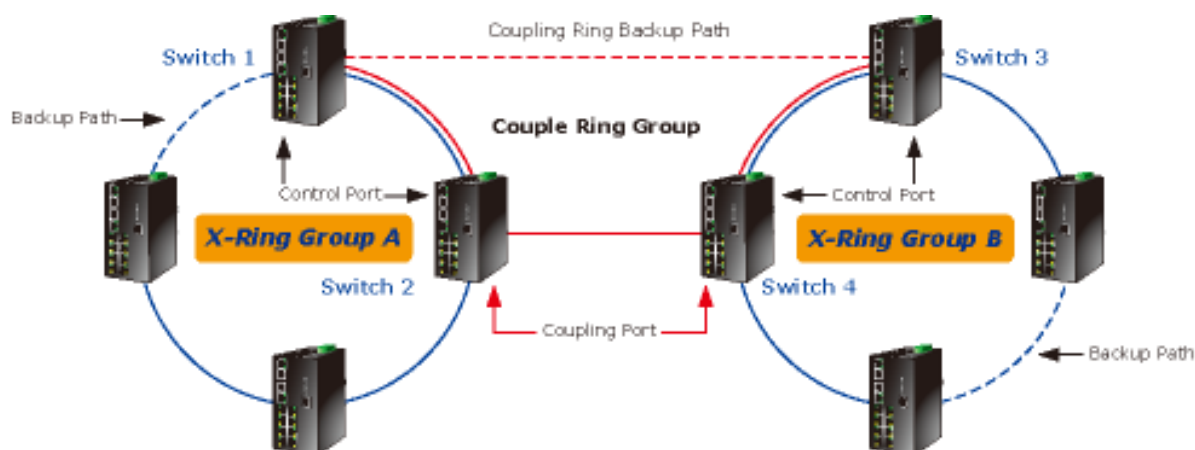
The Industrial Switch supports the X-Ring protocol that can help the network system to recovery from network connection failure within 20ms or less, and make the network system more reliable. The X-Ring algorithm is similar to spanning tree protocol (STP) algorithm but its recovery time is faster than STP. The following figure is a sample X-Ring application.

Figure 5-59: X-Ring Application



In the network, it may have more than one X-Ring group. By using the coupling ring function, it can connect each X-Ring for the redundant backup. It can ensure the transmissions between two ring groups not to fail. The following figure is a sample of coupling ring application.

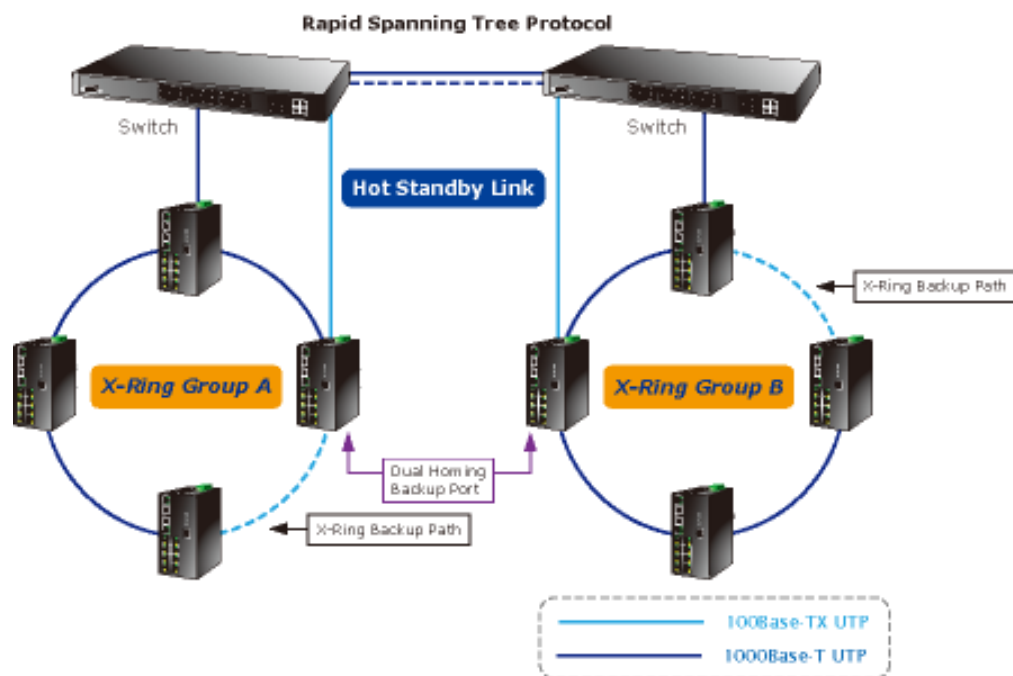
Figure 5-60: Coupling Ring Application



Dual Homing Application

Dual Homing function is to prevent the connection lose from between X-Ring group and upper level/core switch. Assign two ports to be the Dual Homing port that is backup port in the X-Ring group. The Dual Homing function only works when the X-Ring function is active. Each X-Ring group only has one Dual Homing port.

Figure 5-61: Dual Homing Ring Application



NOTE: In Dual Homing application architecture, the upper level switches need to enable the Rapid Spanning Tree protocol.

X-Ring Configuration

The Managed Industrial Switch supports the function and interface for setting the switch as the ring master or not. The ring master can negotiate and place command to other switches in the X-Ring group. If there are 2 or more switches in master mode, the software will select the switch with lowest MAC address number as the ring master. The X-Ring master ring mode can be enabled by setting the X-Ring configuration interface. Also, the user can identify whether the switch is the ring master by checking the R.M. LED indicator on the panel of the Switch.

The system also supports the Couple Ring that can connect 2 or more X-Ring group for the redundant backup function; Dual Homing function that can prevent connection lose between X-Ring group and upper level/core switch.

Figure 5-62: X-Ring Interface

X-Ring Configuration

☒ Enable Ring

☒ Enable Ring Master

1st Ring Port Port.01

2nd Ring Port Port.02

☐ Enable Couple Ring

Coupling Port Port.03

Control Port Port.04

☐ Enable Dual Homing

1st Ring Port 2nd Ring Port Coupling Port Control Port Homing Port

LINK DOWN LINK DOWN LINK DOWN LINK DOWN LINK DOWN

This switch is Ring Master.

Apply Help

This page includes the following fields:

Object	Description
Enable Ring:	To enable the X-Ring function, tick the checkbox beside the Enable Ring string label. If this checkbox is not ticked, all the ring functions are unavailable.
	Enable Ring Master: Tick the checkbox to enable this switch to be the ring master.
	1 st & 2 nd Ring Ports: Pull down the selection menu to assign the

	ports as the member ports. 1 st Ring Port is the working port and 2 nd Ring Port is the backup port. When 1 st Ring Port fails, the system will automatically upgrade the 2 nd Ring Port to be the working port.
Enable Couple Ring:	To enable the couple ring function, tick the checkbox beside the Enable Couple Ring string label. Couple Port: Assign the member port which is connected to the other ring group. Control Port: When the Enable Couple Ring checkbox is ticked, you have to assign the control port to form a couple-ring group between the two X-rings.
Enable Dual Homing:	Set up one of the ports on the switch to be the Dual Homing port. For a switch, there is only one Dual Homing port. Dual Homing function works only when the X-Ring function enabled.

NOTE: When the X-Ring function enabled, the user must disable the RSTP. The X-Ring function and RSTP function cannot exist on a switch at the same time.

Remember to execute the "Save Configuration" action, otherwise the new configuration will lose when switch powers off.

Security

The Security page has the following settings:

- 802.1x/Radius,
- Static MAC address,
- MAC filter

Security-802.1X/Radius Configuration

802.1x is an IEEE authentication specification which prevents the client from accessing a wireless access point or wired switch until it provides authority, like the user name and password that are verified by an authentication server (such as RADIUS server).

Understanding IEEE 802.1X Port-Based Authentication

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client

connected to a switch port before making available any services offered by the switch or the LAN.

Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

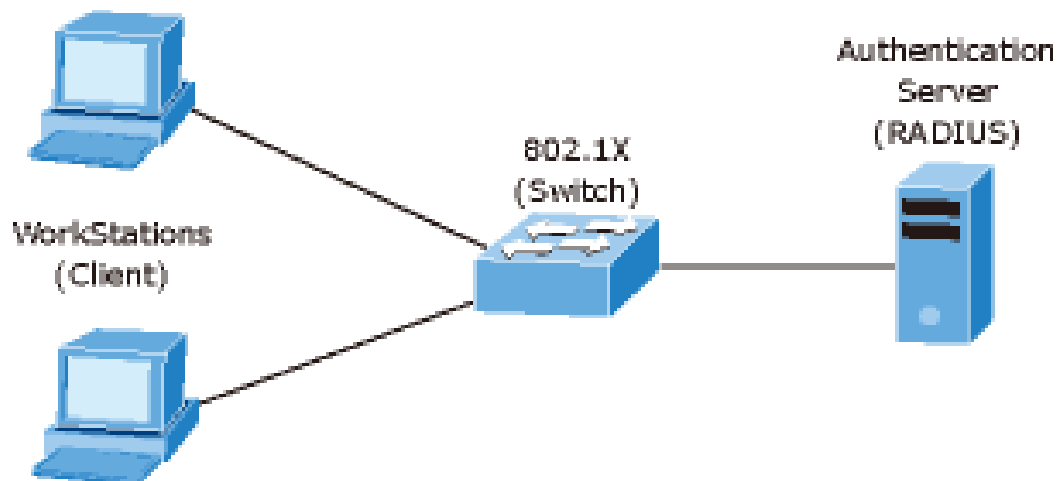
This section includes this conceptual information:

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

• Device Roles

With 802.1X port-based authentication, the devices in the network have specific roles as shown below.

Figure 5-63: 802.1x device role



- Client-the device (workstation) that requests access to the LAN and switch services and responds to requests from the switch. The workstation must be running 802.1X-compliant client software such as that offered in the Microsoft Windows XP operating system. (The client is the supplicant in the IEEE 802.1X specification.)
- Authentication server-performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to

the client. In this release, the Remote Authentication Dial-In User Service (RADIUS) security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

- Switch (802.1X device)-controls the physical access to the network based on the authentication status of the client. The switch acts as an intermediary (proxy) between the client and the authentication server, requesting identity information from the client, verifying that information with the authentication server, and relaying a response to the client. The switch includes the RADIUS client, which is responsible for encapsulating and decapsulating the Extensible Authentication Protocol (EAP) frames and interacting with the authentication server. When the switch receives EAPOL frames and relays them to the authentication server, the Ethernet header is stripped and the remaining EAP frame is re-encapsulated in the RADIUS format. The EAP frames are not modified or examined during encapsulation, and the authentication server must support EAP within the native frame format. When the switch receives frames from the authentication server, the server's frame header is removed, leaving the EAP frame, which is then encapsulated for Ethernet and sent to the client.

- Authentication Initiation and Message Exchange

The switch or the client can initiate authentication. If you enable authentication on a port by using the `dot1x port-control auto` interface configuration command, the switch must initiate authentication when it determines that the port link state transitions from down to up. It then sends an EAP-request/identity frame to the client to request its identity (typically, the switch sends an initial identity/request frame followed by one or more requests for authentication information). Upon receipt of the frame, the client responds with an EAP-response/identity frame.

However, if during bootup, the client does not receive an EAP-request/identity frame from the switch, the client can initiate authentication by sending an EAPOL-start frame, which prompts the switch to request the client's identity

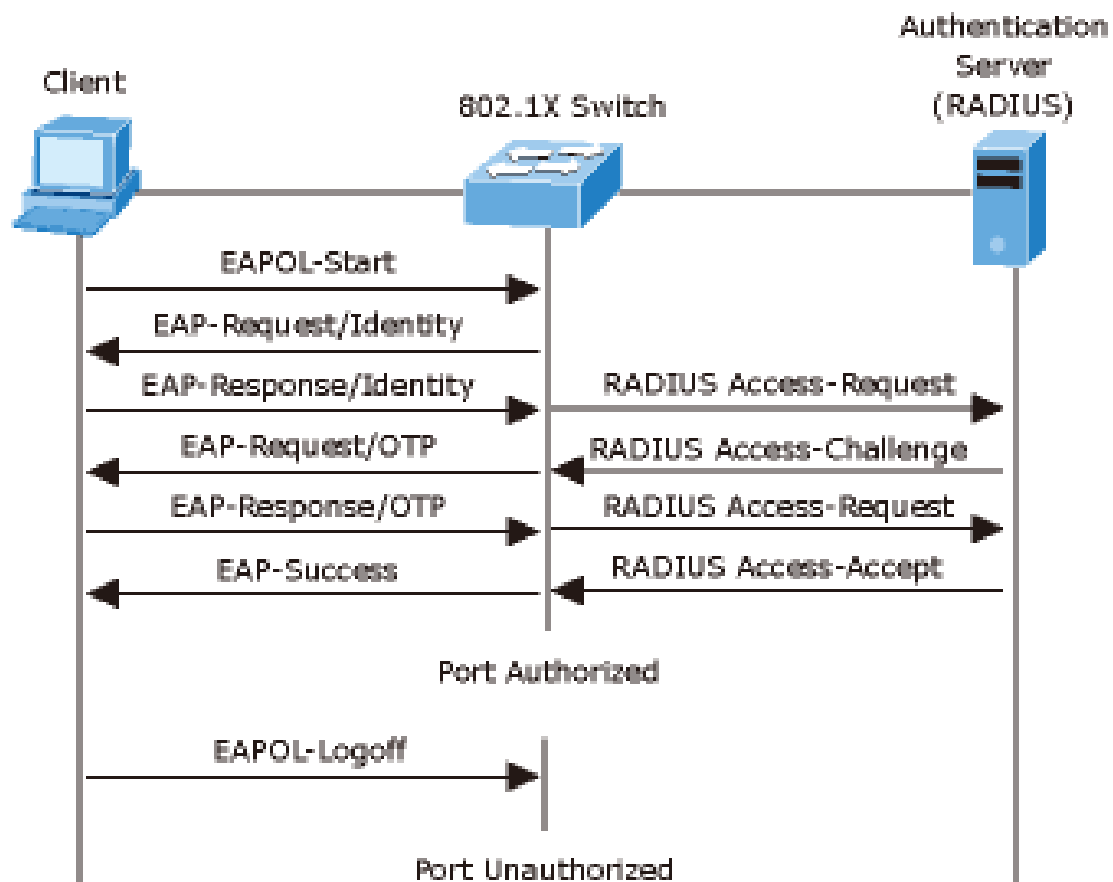
NOTE: If 802.1X is not enabled or supported on the network access device, any EAPOL frames from the client are dropped. If the client does not receive an EAP-request/identity frame after three attempts to start authentication, the client transmits frames as if the port is in the authorized state. A port in the authorized state effectively means that the client has been successfully authenticated.

When the client supplies its identity, the switch begins its role as the intermediary, passing EAP frames between the client and the authentication server until

authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized.

The specific exchange of EAP frames depends on the authentication method being used. "Figure 5-64" shows a message exchange initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server.

Figure 5-64: EAP message exchange



- **Ports in Authorized and Unauthorized States**

The switch port state determines whether or not the client is granted access to the network. The port starts in the unauthorized state. While in this state, the port disallows all ingress and egress traffic except for 802.1X protocol packets. When a client is successfully authenticated, the port transitions to the authorized state, allowing all traffic for the client to flow normally.

If a client that does not support 802.1X is connected to an unauthorized 802.1X port, the switch requests the client's identity. In this situation, the client does not respond to the request, the port remains in the unauthorized state, and the client is not granted access to the network.

In contrast, when an 802.1X-enabled client connects to a port that is not running the 802.1X protocol, the client initiates the authentication process by sending the EAPOL-start frame. When no response is received, the client sends the request for a fixed number of times. Because no response is received, the client begins sending frames as if the port is in the authorized state.

If the client is successfully authenticated (receives an Accept frame from the authentication server), the port state changes to authorized, and all frames from the authenticated client are allowed through the port. If the authentication fails, the port remains in the unauthorized state, but authentication can be retried. If the authentication server cannot be reached, the switch can retransmit the request. If no response is received from the server after the specified number of attempts, authentication fails, and network access is not granted.

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

If the link state of a port transitions from up to down, or if an EAPOL-logoff frame is received, the port returns to the unauthorized state.

System Configuration

After enabling the IEEE 802.1X function, you can configure the parameters of this function.

Figure 5-65: 802.1x System Configuration interface

802.1x/RADIUS - System Configuration	
System Configuration Port Configuration Misc Configuration	
802.1x Protocol	Enable
Radius Server IP	192.168.0.52
Server Port	1812
Accounting Port	1813
Shared Key	12345678
NAS Identifier	NAS_L2_SWITCH
Apply Help	

This page includes the following fields:

Object	Description
IEEE 802.1x Protocol:	Enable or disable 802.1x protocol.
Radius Server IP:	Assign the RADIUS Server IP address.
Server Port:	Set the UDP destination port for authentication requests to the specified RADIUS Server.
Accounting Port:	Set the UDP destination port for accounting requests to the specified RADIUS Server.
Shared Key:	Set an encryption key for using during authentication sessions with the specified RADIUS server. This key must match the encryption key used on the RADIUS Server.
NAS, Identifier:	Set the identifier for the RADIUS client.

Port Configuration

You can configure the 802.1x authentication state for each port. The state provides Disable, Accept, Reject, and Authorize.

Figure 5-66: 802.1x Per Port Setting interface

802.1x/RADIUS - Port Configuration

System Configuration | **Port Configuration** | Misc Configuration

Port: Port.01, Port.02, Port.03, Port.04, Port.05 (all with green checkmarks)

State: Authorize (with green checkmark)

Apply Help

Port Authorization

Port	State
Port.01	Disable
Port.02	Disable
Port.03	Disable
Port.04	Disable
Port.05	Disable
Port.06	Disable
Port.07	Disable
Port.08	Disable
Port.09	Disable
Port.10	Disable

This page includes the following fields:

Object	Description
Reject:	The specified port is required to be held in the unauthorized state.
Accept:	The specified port is required to be held in the authorized state.
Authorize:	The specified port is set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the authentication server.
Disable:	When disabled, the specified port works without complying with 802.1x protocol.

Port Configuration

You can configure the 802.1x authentication state for each port. The state provides Disable, Accept, Reject, and Authorize.

Figure 5-67: 802.1x Misc Configuration interface

802.1x/RADIUS - Misc Configuration

System Configuration | Port Configuration | **Misc Configuration**

Quiet Period	60
Tx Period	30
Supplicant Timeout	30
Server Timeout	30
Max Requests	2
Reauth Period	3600

Apply Help

This page includes the following fields:

Object	Description
Quiet Period:	Set the period, which the port doesn't try to acquire a supplicant.
TX Period:	Set the period the port waits for retransmit next EAPOL PDU during an authentication session.
Supplicant Timeout:	Set the period of time the switch waits for a supplicant response to an EAP request.
Server Timeout:	Set the period of time the switch waits for a server response to an authentication request.
Max Requests:	Set the number of authentication that must time-out before authentication fails and the authentication session ends.
Reauth period:	Set the period of time which clients connected must be re-authenticated.

MAC Address Table

Use the MAC address table to ensure the port security.

Static MAC Address

You can add a static MAC address that remains in the switch's address table regardless of whether the device is physically connected to the switch. This saves the switch from having to re-learn a device's MAC address when the disconnected or powered-off device is active on the network again. Via this interface, you can add / modify / delete a static MAC address.

- Add the Static MAC Address

You can add static MAC address in the switch MAC table here.

Figure 5-68: Static MAC Addresses interface



This page includes the following fields:

Object	Description
MAC Address:	Enter the MAC address of the port that should permanently forward traffic, regardless of the device network activity.
Port No.:	Pull down the selection menu to select the port number.

MAC Filtering

By filtering MAC address, the switch can easily filter the pre-configured MAC address and reduce the un-safety. You can add and delete filtering MAC address.

Figure 5-69: MAC Filtering interface



This page includes the following fields:

Object	Description
MAC Address:	Enter the MAC address that you want to filter.

All MAC Addresses

You can view all of the MAC addresses learned by the selected port.

- Select the port number.
- The selected port of static & dynamic MAC address information will be displayed in here.
- Click **CLEAR MAC TABLE** to clear the dynamic MAC addresses information of the current port shown on the screen.

Figure 5-70: All MAC Address interface



Multicast Filtering

Multicasts are similar to broadcasts, they are sent to all end stations on a LAN or VLAN. Multicast filtering is the function, which end stations can receive the multicast traffic if the connected ports had been included in the specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to the registered end stations.

Figure 5-71: Multicast Filtering interface



This page includes the following fields:

Object	Description
IP Address:	Assign a multicast group IP address in the range of 224.0.0.0 ~ 239.255.255.255.
Member Ports:	Tick the check box beside the port number to include them as the member ports in the specific multicast group IP address.

Digital Input/Output (GE-DSH-73)

The 7 10/100TX + 3 10/100/1000T/100/1000 SFP Combo w/ X-Ring L2 Managed Industrial Switch contains two digital inputs and two digital outputs. The digital inputs may be used to receive the voltage-changing signal of the remote equipment to sense the state of the remote equipment like heater, pump, and other electrical equipment. Therefore the switch can be configured to send system log, SMTP and SNMP traps to syslog server, SMTP server and SNMP trap station respectively (please refer to System Event Log and SNMP configuration section). Outputs are open-collector transistor switches used to connect to the external device like alarm buzzer or LED to inform the user of the port/power status.

Digital Input

- When First/Second Digital Input function is enabled, First Digital Input/Second Digital Input will then be available respectively.
- Digital Input: Choose the transition type to trigger DI0/DI1.
 - Low-->High: Having focused this radio button, DI0/DI1 will only report the status when the external device's voltage changes from low to high.
 - High-->Low: Having focused this radio button, DI0/DI1 will only report the status when the external device's voltage changes from high to low.
- Event description: Please fill in the description for the event.
- Action: Tick the check boxes to decide whether or not to send the events via Syslog, SMTP, or SNMP Trap.

Figure 5-72: Digital Input interface



Digital Output

- When First/Second Digital Output function is enabled, First Digital Output/Second Digital Output will then be available respectively.

- Condition: The system will send an electrical Low-to-High or High-to-Low signal to First Digital Output (DO0)/Second Digital Output (DO1) when the condition of ticked checkbox is met.
 - Port Fail: Having ticked this checkbox, DO0/DO1 will output an electrical Low-to-High or High-to-Low signal when port failure occurs.
 - Power Fail: Having ticked this checkbox, DO0/DO1 will output an electrical Low-to-High or High-to-Low signal when power failure occurs.
- Action: Choose the output type of electrical signal.
 - Low-->High: Having focused this radio button, DO0/DO1 will output an electrical signal of Low-to-High when the condition of the ticked checkbox is met (port/power failure occurs).
 - High-->Low: Having focused this radio button, DO0/DO1 will output an electrical signal of Low-to-High when the condition of the ticked checkbox is met (port/power failure occurs).

Figure 5-73: Digital Output interface



NOTE: Besides ticking the checkboxes in the Condition column field, the power/port failure checkboxes of Fault Relay Alarm have to be ticked as the precondition.

NOTE: Please refer to Fault Relay Alarm section. Also, please notice that the digital output can't connect to the external device using power higher than 40V/200mA.

Power Over Ethernet (GE-DSH-82-PoE)

Providing up to 8 PoE, in-line power interface, the GE-DSH-82-PoE Industrial PoE Switch can easily build a power central-controlled IP phone system, IP Camera system, AP group for the enterprise. For instance, 8 camera / AP can be easily installed around the corner in the company for surveillance demands or build a wireless roaming environment in the office. Without the power-socket limitation, the PoE Switch makes the installation of cameras or WLAN AP more easily and efficiently.

NOTE: PoE functionality requires the use of the recommended a power source.

This product is intended to be supplied by a UL Listed Direct Plug-In Power Unit marked "Class 2" or "LPS" and output rated 48 VDC, 380 mA minimum.

Power over Ethernet Powered Device

 3~5 watts	Voice over IP phones Enterprise can install POE VoIP Phone, ATA and other Ethernet/non-Ethernet end-devices to the central where UPS is installed for un-interrupt power system and power control system.
 6~12 watts	Wireless LAN Access Points Museum, Sightseeing, Airport, Hotel, Campus, Factory, Warehouse can install the Access Point any where with no hesitation
 10~12 watts	IP Surveillance Enterprise, Museum, Campus, Hospital, Bank, can install IP Camera without limits of install location – no need electrician to install AC sockets.
 3~12 watts	PoE Splitter PoE Splitter split the PoE 48V DC over the Ethernet cable into 5/9/12V DC power output. It frees the device deployment from restrictions due to power outlet locations, which eliminate the costs for additional AC wiring and reduces the installation time.

Power Management

In a power over Ethernet system, operating power is applied from a power source (PSU-power supply unit) over the LAN infrastructure to powered devices (PDs), which are connected to ports. Under some conditions, the total output power required by PDs can exceed the maximum available power provided by the PSU. The system may a prior be planed with a PSU capable of supplying less power than the total potential power consumption of all the PoE ports in the system. In order to maintain the majority of ports active, power management is implemented.

The PSU input power consumption is monitored by measuring voltage and current. The input power consumption is equal to the system's aggregated power consumption. The power management concept allows all ports to be active and activates additional ports, as long as the aggregated power of the system is lower than the power level at which additional PDs cannot be connected. When this value is exceeded, ports will be deactivated, according to user-defined priorities. The power budget is managed according to the following user-definable parameters: maximum available power, ports priority, maximum allowable power per port.

This section provides PoE (Power over Ethernet) Configuration and PoE output status of PoE Switch as shown in Figure 5-74.

Figure 5-74: PoE power configuration interface and status

Power over Ethernet

Maximum Power Available: 200 W Actual Power Consumption: 30 W
 System Power Limit: 0 W Main Supply Voltage: 0 dV

Firmware Version: 2.03
 Port Knockoff Disabled: ☐
 AC Disconnect: ☐
 Capacitive Detection: ☐
 Start: ☐

Apply

Port	Enable state	Power Limit from Classification	Legacy	Priority	Power Limit (< 15400) (mW)	Mode	Current (mA)	Voltage (V)	Power (mW)	Determined Class
1	☒	☐	☐	Low	15400	Pwr(IEEE)	248	46.8	11583	0: 15.4W
2	☒	☐	☐	Low	15400	Pwr(IEEE)	192	46.9	9018	0: 15.4W
3	☒	☐	☐	Low	15400	Pwr(IEEE)	196	47.0	9191	0: 15.4W
4	☒	☐	☐	Low	15400	Detecting	0	0.0	0	0: 15.4W
5	☒	☐	☐	Low	15400	Detecting	0	0.0	0	0: 15.4W
6	☒	☐	☐	Low	15400	Detecting	0	0.0	0	0: 15.4W
7	☒	☐	☐	Low	15400	Detecting	0	0.0	0	0: 15.4W
8	☒	☐	☐	Low	15400	Null	0	0.0	0	0: 15.4W

Apply

This page includes the following fields:

Object	Description
Maximum Power Available	Displays the maximum power supply in Watt.
Actual Power Consumption	This column shows the real-time total power consumption.
System Power Limit	User can modify the value to this column field to limit the total output power for the system.
Main Supply Voltage	This column shows the output voltage of the system for PoE ports.
Firmware Version	This column shows the PoE chip's firmware version.
Port Knockoff Disabled	Power Management state where one or more PDs have been powered down so that a higher priority PD may be powered up and yet not exceed the maximum total power available for PDs.
AC Disconnect	Tick this checkbox to monitor the AC impedance on the port terminals and removes power when the impedance rises above a certain value, for a certain period (for details, see the IEEE 802.3af specification).
Capacitive Detection	If the port and capacitive detection are enabled, the capacitances state reads in the voltage result from the constant current. This is then subtracted from the pre-capacitance voltage to get a charge rate. If this charge rate is within the window of the PD signatures, the device is considered to be discovered.
Start	Showing with a tick symbol, the system initializes and resets successfully.
Port	The index of PoE ports.
Enable State	Check it to enable the PoE function to the port.
Power Limit From Classification	Check it to decide the power limit method. When this check box is ticked, the system will limit the power supply to the powered device in accordance with the related class.
Legacy	Check it to support the legacy power devices.
Priority	Pull down the selection menu item to choose the priority of power supplying. Critical High Low High priority is "Critical".
Port Limit (<15400) mW	User can key in the power limit value which is under 15.4 Watts.
Mode	Displays the operating mode of the port.
Current (mA)	Displays the operating current of the port.
Voltage (V)	Displays the operating voltage of the port.
Power (mW)	Displays the power consumption of the port.

Object	Description
Determined Class	Displays the PD's class. Class 0 is the default for PDs. However, to improve power management at the PSE, the PD may opt to provide a signature for Class 1 to 3. The PD is classified based on power. The classification of the PD is the maximum power that the PD will draw across all input voltages and operational modes. A PD shall return Class 0 to 3 in accordance with the maximum power draw as specified by Table 5-12-1.

And then, click **APPLY** to carry into effect.

• PD Classifications

A PD may be classified by the PSE based on the classification information provided by the PD. The intent of PD classification is to provide information about the maximum power required by the PD during operation. Class 0 is the default for PDs. However, to improve power management at the PSE, the PD may opt to provide a signature for Class 1 to 3.

The PD is classified based on power. The classification of the PD is the maximum power that the PD will draw across all input voltages and operational modes.

A PD shall return Class 0 to 3 in accordance with the maximum power draw as specified by Table 5-3.

Table 5-3: Device class

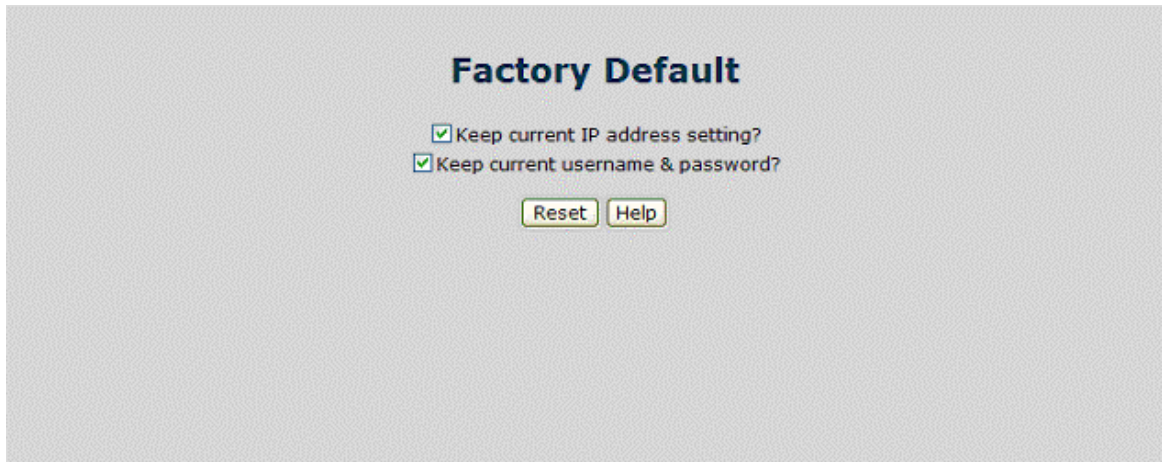
Class	Usage	Range of maximum power used by the PD
0	Default	0.44 to 12.95 Watts
1	Optional	0.44 to 3.84 Watts
2	Optional	3.84 to 6.49 Watts
3	Optional	6.49 to 12.95 Watts
4	Not Allowed	Reserved for Future Use

Class 4 is defined but is reserved for future use. A Class 4 signature cannot be provided by a compliant PD.

Factory Default

Reset switch to default configuration. Click to reset all configurations to the default value.

Figure 5-75: Factory Default interface



Save Configuration

Save all configurations that you have made in the system. To ensure the all configuration will be saved. Click **SAVE** to save the all configuration information to flash memory.

Figure 5-76: Save Configuration interface



System Reboot

Reboots the switch with a software reset. Click **REBOOT** to reboot the system.

Figure 5-77: System Reboot interface



Chapter 6

Command Sets

System Commands Set

Commands	Level	Description	Example
show config	E	Show switch configuration	switch>show config
show terminal	P	Show console information	switch#show terminal
write memory	P	Save user configuration into permanent memory (flash rom)	switch#write memory
system name [System Name]	G	Configure system name	switch(config)#system name xxx
system location [System Location]	G	Set switch system location string	switch(config)#system location xxx
system description [System Description]	G	Set switch system description string	switch(config)#system description xxx
system contact [System Contact]	G	Set switch system contact window string	switch(config)#system contact xxx
show system-info	E	Show system information	switch>show system-info
ip address [Ip-address] [Subnet-mask] [Gateway]	G	Configure the IP address of switch	switch(config)#ip address 192.168.1.1 255.255.255.0 192.168.1.254
ip dhcp	G	Enable DHCP client function of switch	switch(config)#ip dhcp
show ip	P	Show IP information of switch	switch#show ip
no ip dhcp	G	Disable DHCP client function of switch	switch(config)#no ip dhcp

Commands	Level	Description	Example
reload	G	Halt and perform a cold restart	switch(config)#reload
default	G	Restore to default	switch(config)#default
admin username [Username]	G	Changes a login username. (maximum 10 words)	switch(config)#admin username xxxxxx
admin password [Password]	G	Specifies a password (maximum 10 words)	switch(config)#admin password xxxxxx
show admin	P	Show administrator information	switch#show admin
dhcpserver enable	G	Enable DHCP Server	switch(config)#dhcpserver enable
Dhcpserver disable	G	Disable DHCP Server	switch(config)#no dhcpserver
dhcpserver lowip [Low IP]	G	Configure low IP address for IP pool	switch(config)#dhcpserver lowip 192.168.1.100
dhcpserver highip [High IP]	G	Configure high IP address for IP pool	switch(config)#dhcpserver highip 192.168.1.200
dhcpserver subnetmask [Subnet mask]	G	Configure subnet mask for DHCP clients	switch(config)#dhcpserver subnetmask 255.255.255.0
dhcpserver gateway [Gateway]	G	Configure gateway for DHCP clients	switch(config)#dhcpserver gateway 192.168.1.254
dhcpserver dnsip [DNS IP]	G	Configure DNS IP for DHCP clients	switch(config)#dhcpserver dnsip 192.168.1.1
dhcpserver leasetime [Hours]	G	Configure lease time (in hour)	switch(config)#dhcpserver leasetime 1
dhcpserver ipbinding [IP address]	I	Set static IP for DHCP clients by port	switch(config)#interface fastEthernet 2 switch(config)#dhcpserver ipbinding 192.168.1.1
show dhcpserver configuration	P	Show configuration of DHCP server	switch#show dhcpserver configuration
show dhcpserver clients	P	Show client entries of DHCP server	switch#show dhcpserver clients
show dhcpserver ip- binding	P	Show IP-Binding information of DHCP server	switch#show dhcpserver ip-binding
no dhcpserver	G	Disable DHCP server function	switch(config)#no dhcpserver
security enable	G	Enable IP security function	switch(config)#security enable
security http	G	Enable IP security of HTTP server	switch(config)#security http
security telnet	G	Enable IP security of telnet	switch(config)#security telnet

Commands	Level	Description	Example
		server	
<code>security ip</code> [Index(1..10)] [IP Address]	G	Set the IP security list	switch(config)#security ip 1 192.168.1.55
<code>show security</code>	P	Show the information of IP security	switch#show security
<code>no security</code>	G	Disable IP security function	switch(config)#no security
<code>no security http</code>	G	Disable IP security of HTTP server	switch(config)#no security http
<code>no security telnet</code>	G	Disable IP security of telnet server	switch(config)#no security telnet

Port Commands Set

Commands	Level	Description	Example
<code>interface fastEthernet [Portid]</code>	G	Choose the port for modification.	<code>switch(config)#interface fastEthernet 2</code>
<code>duplex [full half]</code>	I	Use the duplex configuration command to specify the duplex mode of operation for Fast Ethernet.	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#duplex full</code>
<code>speed [10 100 1000 auto]</code>	I	Use the speed configuration command to specify the speed mode of operation for Fast Ethernet., the speed can't be set to 1000 if the port isn't a giga port..	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#speed 100</code>
<code>no flowcontrol</code>	I	Disable flow control of interface	<code>switch(config-if)#no flowcontrol</code>
<code>security enable</code>	I	Enable security of interface	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#security enable</code>
<code>no security</code>	I	Disable security of interface	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#no security</code>
<code>bandwidth type all</code>	I	Set interface ingress limit frame type to "accept all frame"	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#bandwidth type all</code>
<code>bandwidth type broadcast-multicast-flooded-unicast</code>	I	Set interface ingress limit frame type to "accept broadcast, multicast, and flooded unicast frame"	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast</code>
<code>bandwidth type broadcast-multicast</code>	I	Set interface ingress limit frame type to "accept broadcast and multicast frame"	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#bandwidth type broadcast-multicast</code>
<code>bandwidth type broadcast-only</code>	I	Set interface ingress limit frame type to "only accept broadcast frame"	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#bandwidth type broadcast-only</code>
<code>bandwidth in [Value]</code>	I	Set interface input bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for	<code>switch(config)#interface fastEthernet 2</code> <code>switch(config-if)#bandwidth in 100</code>

Commands	Level	Description	Example
		giga ports, and zero means no limit.	
<code>bandwidth out [Value]</code>		Set interface output bandwidth. Rate Range is from 100 kbps to 102400 kbps or to 256000 kbps for giga ports, and zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth out 100
<code>Show bandwidth</code>	I	Show interfaces bandwidth control	switch(config)#interface fastEthernet 2 switch(config-if)#show bandwidth
<code>State [Enable Disable]</code>	I	Use the state interface configuration command to specify the state mode of operation for Ethernet ports. Use the disable form of this command to disable the port.	switch(config)#interface fastEthernet 2 switch(config-if)#state Disable
<code>show interface configuration</code>	I	show interface configuration status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface configuration
<code>show interface status</code>	I	show interface actual status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface status
<code>show interface accounting</code>	I	show interface statistic counter	switch(config)#interface fastEthernet 2 switch(config-if)#show interface accounting
<code>no accounting</code>	I	Clear interface accounting information	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting

Trunk Commands Set

Commands	Level	Description	Example
<code>aggregator priority</code> [1~65535]	G	Set port group system priority	switch(config)#aggregator priority 22
<code>aggregator activityport</code> [Group ID] [Port Numbers]	G	Set activity port	switch(config)#aggregator activityport 2
<code>aggregator group</code> [GroupID] [Port-list] <code>lacp</code> <code>workp</code> [Workport]	G	Assign a trunk group with LACP active. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	switch(config)#aggregator group 1 1-4 lacp workp 2 or switch(config)#aggregator group 2 1,4,3 lacp workp 3
<code>aggregator group</code> [GroupID] [Port-list] <code>nolacp</code>	G	Assign a static trunk group. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#aggregator group 1 2-4 nolacp or switch(config)#aggregator group 1 3,1,2 nolacp
<code>show aggregator</code>	P	Show the information of trunk group	switch#show aggregator 1 or switch#show aggregator 2 or switch#show aggregator 3
<code>no aggregator lacp</code> [GroupID]	G	Disable the LACP function of trunk group	switch(config)#no aggreator lacp 1
<code>no aggregator group</code> [GroupID]	G	Remove a trunk group	switch(config)#no aggreator group 2

VLAN Commands Set

Commands	Level	Description	Example
<code>vlan database</code>	P	Enter VLAN configure mode	<code>switch#vlan database</code>
<code>Vlanmode</code> <code>[portbase 802.1q gvrp]</code>	V	To set switch VLAN mode.	<code>switch(vlan)#vlanmode portbase</code> or <code>switch(vlan)#vlanmode 802.1q</code> or <code>switch(vlan)#vlanmode gvrp</code>
<code>no vlan</code>	V	No VLAN	<code>Switch(vlan)#no vlan</code>
Ported based VLAN configuration			
<code>vlan port-based grpname</code> <code>[Group Name]</code> <code>grp-id</code> <code>[GroupID]</code> <code>port</code> <code>[PortNumbers]</code>	V	Add new port based VALN	<code>switch(vlan)#vlan port-based grpname test grp-id 2 port 2-4</code> or <code>switch(vlan)#vlan port-based grpname test grp-id 2 port 2,3,4</code>
<code>show vlan [GroupID]</code> or <code>show vlan</code>	V	Show VLAN information	<code>switch(vlan)#show vlan 23</code>
<code>no vlan group</code> <code>[GroupID]</code>	V	Delete port base group ID	<code>switch(vlan)#no vlan group 2</code>
IEEE 802.1Q VLAN			
<code>vlan 8021q name</code> <code>[GroupName]</code> <code>vid</code> <code>[VID]</code>	V	Change the name of VLAN group, if the group didn't exist, this command can't be applied.	<code>switch(vlan)#vlan 8021q name test vid 22</code>
<code>vlan 8021q port</code> <code>[PortNumber]</code> <code>access-link untag</code> <code>[UntaggedVID]</code>	V	Assign a access link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	<code>switch(vlan)#vlan 8021q port 3 access-link untag 33</code>

Commands	Level	Description	Example
vlan 8021q port [PortNumber] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 8021q port 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q port 3 trunk-link tag 3-20
vlan 8021q port [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for VLAN by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)#vlan 8021q port 3 hybrid-link untag 5 tag 6-8
vlan 8021q trunk [PortNumber] access-link untag [UntaggedVID]	V	Assign a access link for VLAN by trunk group	switch(vlan)#vlan 8021q trunk 3 access-link untag 33
vlan 8021q trunk [PortNumber] trunk-link tag [TaggedVID List]	V	Assign a trunk link for VLAN by trunk group	switch(vlan)#vlan 8021q trunk 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q trunk 3 trunk-link tag 3-20
vlan 8021q trunk [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for VLAN by trunk group	switch(vlan)#vlan 8021q trunk 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)#vlan 8021q trunk 3 hybrid-link untag 5 tag 6-8
show vlan [GroupID] or show vlan	V	Show VLAN information	switch(vlan)#show vlan 23
no vlan group [GroupID]	V	Delete port base group ID	switch(vlan)#no vlan group 2

Spanning Tree Commands Set

Commands	Level	Description	Example
<code>spanning-tree enable</code>	G	Enable spanning tree	<code>switch(config)#spanning-tree enable</code>
<code>spanning-tree priority</code> [0~61440]	G	Configure spanning tree priority parameter	<code>switch(config)#spanning-tree priority 32768</code>
<code>spanning-tree max-age</code> [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	<code>switch(config)#spanning-tree max-age 15</code>
<code>spanning-tree hello-time</code> [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	<code>switch(config)#spanning-tree hello-time 3</code>
<code>spanning-tree forward-time</code> [seconds]	G	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	<code>switch(config)#spanning-tree forward-time 20</code>

Commands	Level	Description	Example
stp-path-cost [1~200000000]	I	Use the spanning-tree cost interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-cost 20
stp-path-priority [Port Priority]	I	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-path-priority 128
stp-admin-p2p [Auto True False]	I	Admin P2P of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-admin-p2p Auto
stp-admin-edge [True False]	I	Admin Edge of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-admin-edge True
stp-admin-non-stp [True False]	I	Admin NonSTP of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)#stp-admin-non-stp False
show spanning-tree	E	Displays a summary of the spanning-tree states.	switch>show spanning-tree
no spanning-tree	G	Disable spanning-tree.	switch(config)#no spanning-tree

QOS Commands Set

Commands	Level	Description	Example
qos policy [weighted-fair strict]	G	Select QOS policy scheduling	switch(config)#qos policy weighted-fair
qos prioritytype [port-based cos-only tos-only cos-first tos-first]	G	Setting of QOS priority type	switch(config)#qos prioritytype
qos priority portbased [Port] [lowest low middle high]	G	Configure Port-based Priority	switch(config)#qos priority portbased 1 low
qos priority cos [Priority][lowest low middle high]	G	Configure COS Priority	switch(config)#qos priority cos 0 middle
qos priority tos [Priority][lowest low middle high]	G	Configure TOS Priority	switch(config)#qos priority tos 3 high
show qos	P	Displays the information of QoS configuration	Switch#show qos
no qos	G	Disable QoS function	switch(config)#no qos

IGMP Commands Set

Commands	Level	Description	Example
<code>igmp enable</code>	G	Enable IGMP snooping function	<code>switch(config)#igmp enable</code>
<code>igmp-query auto</code>	G	Set IGMP query to auto mode	<code>switch(config)#igmp-query auto</code>
<code>igmp-query force</code>	G	Set IGMP query to force mode	<code>switch(config)#igmp-query force</code>
<code>show igmp configuration</code>	P	Displays the details of an IGMP configuration.	<code>switch#show igmp configuration</code>
<code>no igmp</code>	G	Disable IGMP snooping function	<code>switch(config)#no igmp</code>
<code>no igmp-query</code>	G	Disable IGMP query	<code>switch#no igmp-query</code>

MAC / Filter Table Commands Set

Commands	Level	Description	Example
<code>mac-address-table static hwaddr [MAC]</code>	I	Configure MAC address table of interface (static).	switch(config)#interface fastEthernet 2 switch(config-if)#mac-address-table static hwaddr 000012345678
<code>mac-address-table filter hwaddr [MAC]</code>	G	Configure MAC address table(filter)	switch(config)#mac-address-table filter hwaddr 000012348678
<code>show mac-address-table</code>	P	Show all MAC address table	switch#show mac-address-table
<code>show mac-address-table static</code>	P	Show static MAC address table	switch#show mac-address-table static
<code>show mac-address-table filter</code>	P	Show filter MAC address table.	switch#show mac-address-table filter
<code>no mac-address-table static hwaddr [MAC]</code>	I	Remove an entry of MAC address table of interface (static)	switch(config)#interface fastEthernet 2 switch(config-if)#no mac-address-table static hwaddr 000012345678
<code>no mac-address-table filter hwaddr [MAC]</code>	G	Remove an entry of MAC address table (filter)	switch(config)#no mac-address-table filter hwaddr 000012348678
<code>no mac-address-table</code>	G	Remove dynamic entry of MAC address table	switch(config)#no mac-address-table

SNMP Commands Set

Commands	Level	Description	Example
snmp system-name [System Name]	G	Set SNMP agent system name	switch(config)#snmp system-name l2switch
snmp system-location [System Location]	G	Set SNMP agent system location	switch(config)#snmp system-location lab
snmp system-contact [System Contact]	G	Set SNMP agent system contact	switch(config)#snmp system-contact where
snmp agent-mode [v1v2c v3 v1v2cv3]	G	Select the agent mode of SNMP	switch(config)#snmp agent-mode v1v2cv3
snmp community-strings [Community] right [RO/RW]	G	Add SNMP community string.	switch(config)#snmp community-strings public right rw
snmp-server host [IP address] community [Community-string] trap-version [v1 v2c]	G	Configure SNMP server host information and community string	switch(config)#snmp-server host 192.168.1.50 community public trap-version v1 (remove) Switch(config)# no snmp-server host 192.168.1.50
snmpv3 context-name [Context Name]	G	Configure the context name	switch(config)#snmpv3 context-name Test
snmpv3 user [User Name] group [Group Name] password [Authentication Password] [Privacy Password]	G	Configure the userprofile for SNMPV3 agent. Privacy password could be empty.	switch(config)#snmpv3 user test01 group G1 password AuthPW PrivPW

Commands	Level	Description	Example
snmpv3 access context-name [Context Name] group [Group Name] security-level [NoAuthNoPriv AuthNoPriv AuthPriv] match-rule [Exact Prefix] views [Read View Name] [Write View Name] [Notify View Name]	G	Configure the access table of SNMPV3 agent	switch(config)#snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1
snmpv3 mibview view [View Name] type [Excluded Included] sub-oid [OID]	G	Configure the mibview table of SNMPV3 agent	switch(config)#snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1
show snmp	P	Show SNMP configuration	switch#show snmp
no snmp community-strings [Community]	G	Remove the specified community.	switch(config)#no snmp community-strings public
no snmp-server host [Host-address]	G	Remove the SNMP server host.	switch(config)#no snmp-server host 192.168.1.50
no snmpv3 user [User Name]	G	Remove specified user of SNMPv3 agent.	switch(config)#no snmpv3 user Test
no snmpv3 access context-name [Context Name] group [Group Name] security-level [NoAuthNoPriv AuthNoPriv AuthPriv] match-rule [Exact Prefix] views	G	Remove specified access table of SNMPv3 agent.	switch(config)#no snmpv3 access context-name Test group G1 security-level AuthPriv iv match-rule Exact views V1 V1 V1

Commands	Level	Description	Example
[Read View Name] [Write View Name] [Notify View Name]			
no snmpv3 mibview view [View Name] type [Excluded Included] sub-oid [OID]	G	Remove specified mibview table of SNMPV3 agent.	switch(config)#no snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1

Port Mirroring Commands Set

Commands	Level	Description	Example
<code>monitor</code> [RX TX Both]	I	Configure source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#monitor RX
<code>monitor rx</code> [Port ID]	G	Set RX destination port of monitor function	switch(config)#monitor rx 2
<code>monitor tx</code> [Port ID]	G	Set TX destination port of monitor function	switch(config)#monitor tx 3
<code>show monitor</code>	P	Show port monitor information	switch#show monitor
<code>show monitor</code>	I	Show port monitor information	switch(config)#interface fastEthernet 2 switch(config-if)#show monitor
<code>no monitor</code>	I	Disable source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#no monitor

802.1x Commands Set

Commands	Level	Description	Example
8021x enable	G	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiusip [IP address]	G	Use the 802.1x system radius IP global configuration command to change the radius server IP.	switch(config)# 8021x system radiusip 192.168.1.1
8021x system serverport [port ID]	G	Use the 802.1x system server port global configuration command to change the radius server port	switch(config)# 8021x system serverport 1812
8021x system accountport [port ID]	G	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# 8021x system accountport 1813
8021x system sharedkey [ID]	G	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# 8021x system sharedkey 123456
8021x system nasid [words]	G	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# 8021x system nasid test1
8021x misc quietperiod [sec.]	G	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# 8021x misc quietperiod 10
8021x misc txperiod [sec.]	G	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# 8021x misc txperiod 5
8021x misc supptimeout [sec.]	G	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# 8021x misc supptimeout 20

Commands	Level	Description	Example
<code>8021x misc servertimeout [sec.]</code>	G	Use the 802.1x misc server timeout global configuration command to set the server timeout.	<code>switch(config)#8021x misc servertimeout 20</code>
<code>8021x misc maxrequest [number]</code>	G	Use the 802.1x misc max request global configuration command to set the MAX requests.	<code>switch(config)# 8021x misc maxrequest 3</code>
<code>8021x misc reauthperiod [sec.]</code>	G	Use the 802.1x misc reauth period global configuration command to set the reauth period.	<code>switch(config)# 8021x misc reauthperiod 3000</code>
<code>8021x portstate [disable reject accept authorize]</code>	I	Use the 802.1x port state interface configuration command to set the state of the selected port.	<code>switch(config)#interface fastethernet 3 switch(config-if)#8021x portstate accept</code>
<code>show 8021x</code>	E	Displays a summary of the 802.1x properties and also the port sates.	<code>switch>show 8021x</code>
<code>no 8021x</code>	G	Disable 802.1x function	<code>switch(config)#no 8021x</code>

TFTP Commands Set

Commands	Level	Description	Defaults Example
<code>backup flash:backup_cfg</code>	G	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	<code>switch(config)#backup flash:backup_cfg</code>
<code>restore flash:restore_cfg</code>	G	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	<code>switch(config)#restore flash:restore_cfg</code>
<code>upgrade flash:upgrade_fw</code>	G	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	<code>switch(config)#upgrade flash:upgrade_fw</code>

SystemLog, SMTP and Event Commands Set

Commands	Level	Description	Example
<code>systemlog ip</code> [IP address]	G	Set System log server IP address.	switch(config)# systemlog ip 192.168.1.100
<code>systemlog mode</code> [client server both]	G	Specified the log mode	switch(config)# systemlog mode both
<code>show systemlog</code>	E	Displays system log.	Switch>show systemlog
<code>show systemlog</code>	P	Show system log client & server information	switch#show systemlog
<code>no systemlog</code>	G	Disable systemlog function	switch(config)#no systemlog
<code>smtp enable</code>	G	Enable SMTP function	switch(config)#smtp enable
<code>smtp serverip</code> [IP address]	G	Configure SMTP server IP	switch(config)#smtp serverip 192.168.1.5
<code>smtp authentication</code>	G	Enable SMTP authentication	switch(config)#smtp authentication
<code>smtp account</code> [account]	G	Configure authentication account	switch(config)#smtp account John
<code>smtp password</code> [password]	G	Configure authentication password	switch(config)#smtp password 1234
<code>smtp rcptemail</code> [Index] [Email address]	G	Configure Rcpt e-mail Address	switch(config)#smtp rcptemail 1 Alert@test.com
<code>show smtp</code>	P	Show the information of SMTP	switch#show smtp
<code>no smtp</code>	G	Disable SMTP function	switch(config)#no smtp
<code>event device-cold-start</code> [Systemlog SMTP Both]	G	Set cold start event type	switch(config)#event device-cold-start both
<code>event authentication-failure</code> [Systemlog SMTP Both]	G	Set Authentication failure event type	switch(config)#event authentication-failure both
<code>event ring-topology-change</code> [Systemlog SMTP Both]	G	Set X-ring topology changed event type	switch(config)#event ring-topology-change both
<code>event systemlog</code> [Link-UP Link-Down Both]	I	Set port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#event systemlog both

Commands	Level	Description	Example
<code>event smtp</code> [Link-UP Link-Down Both]	I	Set port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#event smtp both
<code>show event</code>	P	Show event selection	switch#show event
<code>no event device-cold-start</code>	G	Disable cold start event type	switch(config)#no event device-cold-start
<code>no event authentication-failure</code>	G	Disable Authentication failure event typ	switch(config)#no event authentication-failure
<code>no event ring-topology-change</code>	G	Disable X-ring topology changed event type	switch(config)#no event ring-topology-change
<code>no event systemlog</code>	I	Disable port event for system log	switch(config)#interface fastethernet 3 switch(config-if)#no event systemlog
<code>no event smtp</code>	I	Disable port event for SMTP	switch(config)#interface fastethernet 3 switch(config-if)#no event smtp
<code>show systemlog</code>	P	Show system log client & server information	switch#show systemlog

SNTP Commands Set

Commands	Level	Description	Example
<code>sntp enable</code>	G	Enable SNTP function	<code>switch(config)#sntp enable</code>
<code>sntp daylight</code>	G	Enable daylight saving time, if SNTP function is inactive, this command can't be applied.	<code>switch(config)#sntp daylight</code>
<code>sntp daylight-period</code> [Start time] [End time]	G	Set period of daylight saving time, if SNTP function is inactive, this command can't be applied. Parameter format: [yyyymmdd-hh:mm]	<code>switch(config)# sntp daylight-period 20060101-01:01 20060202-01:01</code>
<code>sntp daylight-offset</code> [Minute]	G	Set offset of daylight saving time, if SNTP function is inactive, this command can't be applied.	<code>switch(config)#sntp daylight-offset 3</code>
<code>sntp ip</code> [IP]	G	Set SNTP server IP, if SNTP function is inactive, this command can't be applied.	<code>switch(config)#sntp ip 192.169.1.1</code>
<code>sntp timezone</code> [Timezone]	G	Set timezone index, use "show sntp timzezone" command to get more information of index number	<code>switch(config)#sntp timezone 22</code>
<code>show sntp</code>	P	Show SNTP information	<code>switch#show sntp</code>
<code>show sntp timezone</code>	P	Show index number of time zone list	<code>switch#show sntp timezone</code>
<code>no sntp</code>	G	Disable SNTP function	<code>switch(config)#no sntp</code>
<code>no sntp daylight</code>	G	Disable daylight saving time	<code>switch(config)#no sntp daylight</code>

X-ring Commands Set

Commands	Level	Description	Example
ring enable	G	Enable X-ring	switch(config)#ring enable
ring master	G	Enable ring master	switch(config)#ring master
ring couplering	G	Enable couple ring	switch(config)#ring couplering
ring dualhoming	G	Enable dual homing	switch(config)#ring dualhoming
ring ringport [1st Ring Port] [2nd Ring Port]	G	Configure 1st/2nd Ring Port	switch(config)#ring ringport 7 8
ring couplingport [Coupling Port]	G	Configure Coupling Port	switch(config)#ring couplingport 1
ring controlport [Control Port]	G	Configure Control Port	switch(config)#ring controlport 2
ring homingport [Dual Homing Port]	G	Configure Dual Homing Port	switch(config)#ring homingport 3
show ring	P	Show the information of X - Ring	switch#show ring
no ring	G	Disable X-ring	switch(config)#no ring
no ring master	G	Disable ring master	switch(config)# no ring master
no ring couplering	G	Disable couple ring	switch(config)# no ring couplering
no ring dualhoming	G	Disable dual homing	switch(config)# no ring dualhoming

PoE Command Set

Commands	Level	Description	Example
<code>poe</code>	P	Configure PoE function	<code>switch# poe</code>
<code>exit</code>	PoE	Exit the PoE command mode	<code>switch(poe)# exit</code>
<code>port [PortNumber] state</code> [Enable Disable]		Set PoE port State	<code>switch(poe)# port 1 state enable</code>
<code>port [PortNumber] plfc</code> [Enable Disable]	PoE	Set PoE port Power Limit from Classification	<code>switch(poe)# port 1 plfc enable</code>
<code>port [PortNumber] legacy</code> [Enable Disable]	PoE	Set PoE port Legacy	<code>switch(poe)# port 1 legacy enable</code>
<code>port [PortNumber] priority</code> [Low High Critical]	PoE	Set PoE port Priority	<code>switch(poe)# port 1 priority critical</code>
<code>port [PortNumber] powerlimit [Value]</code>	PoE	Set PoE port Power Limit Value	<code>switch(poe)# port 1 powerlimit 10</code>
<code>system</code>	PoE	Configure PoE System	<code>switch(poe)# system</code>
<code>system knockoff-disabled</code> [Enable Disable]	PoE	Set PoE system Port Knockoff Disabled	<code>switch(poe)# system knockoff-disabled enable</code>
<code>system ac-disconnect</code> [Enable Disable]	PoE	Set PoE system AC Disconnect	<code>switch(poe)# system ac-disconnect enable</code>
<code>system capacitive-detect</code> [Enable Disable]	PoE	Set PoE system Capacitive Detection	<code>switch(poe)# system capacitive-detect enable</code>
<code>system power-limit [Value]</code>	PoE	Set PoE system System Power Limit	<code>switch(poe)# system power-limit 100</code>

Chapter 7

Switch Operation

Address Table

The Switch is implemented with an address table. This address table composed of many entries. Each entry is used to store the address information of some node in network, including MAC address, port no, etc. This information comes from the learning process of Ethernet Switch.

Learning

When one packet comes in from any port, the Switch will record the source address, port no. And the other related information in address table. This information will be used to decide either forwarding or filtering for future packets.

Forwarding & Filtering

When one packet comes from some port of the Ethernet Switching, it will also check the destination address besides the source address learning. The Ethernet Switching will lookup the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, which this packet comes in. And these ports will transmit this packet to the network it connected. If found, and the destination address is located at different port from this packet comes in, the Ethernet Switching will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port with this packet comes in, then this packet will be filtered. Thereby increasing the network throughput and availability

Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques. A Store-and-Forward Ethernet Switching stores the incoming frame in an internal buffer, do the complete error checking before transmission. Therefore, no error packets occurrence, it is the best choice when a network needs efficiency and stability.

The Ethernet Switch scans the destination address from the packet-header, searches the routing table pro-vided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. However, the switch is most commonly used to segment existence hubs, which nearly always improves overall performance. An Ethernet Switching can be easily configured in any Ethernet network environment to significantly boost bandwidth using conventional cabling and adapters.

Due to the learning function of the Ethernet switching, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain and reduce the overall load on the network.

The Switch performs "Store and forward" therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

Auto-Negotiation

The STP ports on the Switch have built-in "Auto-negotiation". This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detect the modes and speeds at the second of both device is connected and capable of, both 10Base-T and 100Base-TX devices can connect with the port in either Half- or Full-Duplex mode.

If attached device is:	100Base-TX port will set to:
10Mbps, no auto-negotiation	10Mbps.
10Mbps, with auto-negotiation	10/20Mbps (10Base-T/Full-Duplex)
100Mbps, no auto-negotiation	100Mbps
100Mbps, with auto-negotiation	100/200Mbps (100Base-TX/Full-Duplex)

Chapter 8

Power Over Ethernet

Overview

What is PoE?

Based on the global standard IEEE 802.3af, PoE is a technology for wired Ethernet, the most widely installed local area network technology adopted today. PoE allows the electrical power necessary for the operation of each end-device to be carried by data cables rather than by separate power cords. New network applications, such as IP Cameras, VoIP Phones, and Wireless Networking, can help enterprises improve productivity. It minimizes wires that must be used to install the network for offering lower cost, and less power failures.

IEEE802.3af also called Data Terminal equipment (DTE) power via Media dependent interface (MDI) is an international standard to define the transmission for power over Ethernet. The 802.3af is delivering 48V power over RJ-45 wiring. Besides 802.3af also define two types of source equipment: Mid-Span and End-Span.

- Mid-Span

Mid-Span device is placed between legacy switch and the powered device. Mid-Span is tap the unused wire pairs 4/5 and 7/8 to carry power, the other four is for data transmit.

- End-Span

End-Span device is direct connecting with power device. End-Span could also tap the wire 1/2 and 3/6.

PoE System Architecture

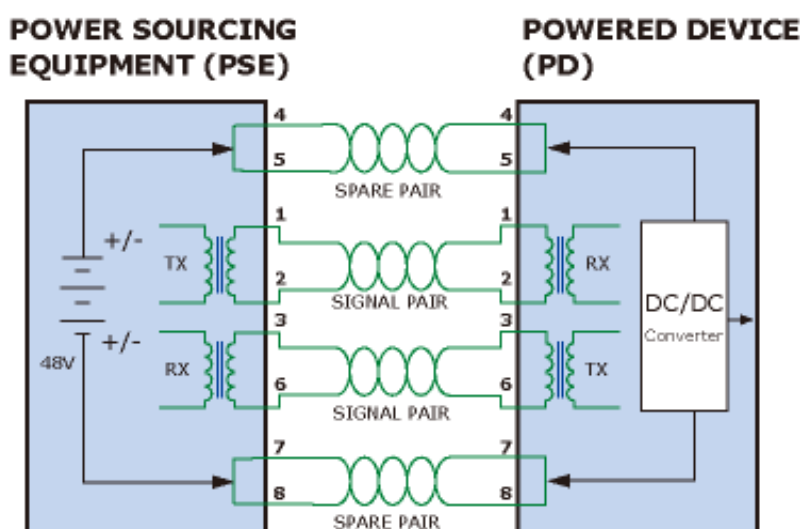
The specification of PoE typically requires two devices: the Powered Source Equipment (PSE) and the Powered Device (PD). The PSE is either an End-Span or a Mid-Span, while the PD is a PoE-enabled terminal, such as IP Phones, Wireless LAN, etc. Power can be delivered over data pairs or spare pairs of standard CAT-5 cabling.

How Power is Transferred Through the Cable

A standard CAT5 Ethernet cable has four twisted pairs, but only two of these are used for 10BASE-T and 100BASE-T. The specification allows two options for using these cables for power, shown in Figure 8-1 and Figure 8-2:

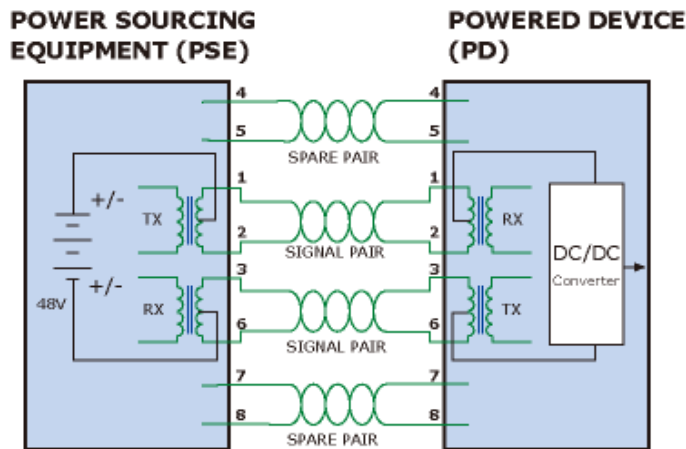
The spare pairs are used. Figure 8-1 shows the pair on pins 4 and 5 connected together and forming the positive supply, and the pair on pins 7 and 8 connected and forming the negative supply. (In fact, a late change to the spec allows either polarity to be used).

Figure 8-1 - Power Supplied over the Spare Pins



The data pairs are used. Since Ethernet pairs are transformer coupled at each end, it is possible to apply DC power to the center tap of the isolation transformer without upsetting the data transfer. In this mode of operation the pair on pins 3 and 6 and the pair on pins 1 and 2 can be of either polarity.

Figure 8-2 - Power Supplied over the Data Pins



When to install PoE?

Consider the following scenarios:

- You're planning to install the latest VoIP Phone system to minimize cabling building costs when your company moves into new offices next month.
- The company staff has been clamoring for a wireless access point in the picnic area behind the building so they can work on their laptops through lunch, but the cost of electrical power to the outside is not affordable.
- Management asks for IP Surveillance Cameras and business access systems throughout the facility, but they would rather avoid another electrician's payment.

References:

IEEE Std 802.3af-2003 (Amendment to IEEE Std 802.3-2002, including IEEE Std 802.3ae-2002), 2003 Page(s):0_1-121

White Paper on Power over Ethernet (IEEE802.3af)

http://www.poweroverethernet.com/articles.php?article_id=52

Microsemi /PowerDsine

<http://www.microsemi.com/PowerDsine/>

Linear Tech

<http://www.linear.com/>

The PoE Provision Process

While adding PoE support to networked devices is relatively painless, it should be realized that power cannot simply be transferred over existing CAT-5 cables. Without proper preparation, doing so may result in damage to devices that are not designed to support provision of power over their network interfaces.

The PSE is the manager of the PoE process. In the beginning, only small voltage level is induced on the port's output, till a valid PD is detected during the Detection period. The PSE may choose to perform classification, to estimate the amount of power to be consumed by this PD. After a time-controlled start-up, the PSE begins supplying the 48 VDC level to the PD, till it is physically or electrically disconnected. Upon disconnection, voltage and power shut down.

Since the PSE is responsible for the PoE process timing, it is the one generating the probing signals prior to operating the PD and monitoring the various scenarios that may occur during operation.

All probing is done using voltage induction and current measurement in return.

Stages of powering up a PoE link

Stage	Action	Volts specified per 802.3af	Volts managed by chipset
Detection	Measure whether powered device has the correct signature resistance of 15–33 kΩ	2.7–10.0	1.8–10.0
Classification	Measure which power level class the resistor indicates	14.5–20.5	12.5–25.0
Startup	Where the powered device will startup	>42	>38
Normal operation	Supply power to device	36–57	25.0–60.0

Line Detection

Before power is applied, safety dictates that it must first be ensured that a valid PD is connected to the PSE's output. This process is referred to as "line detection", and involves the PSE seeking a specific, 25 kΩ signature resistor. Detection of this signature indicates that a valid PD is connected, and that provision of power to the device may commence.

The signature resistor lies in the PD's PoE front-end, isolated from the rest of the PD's circuitries till detection is certified.

Classification

Once a PD is detected, the PSE may optionally perform classification, to determine the maximal power a PD is to consume. The PSE induces 15.5-20.5 VDC, limited to 100 mA, for a period of 10 to 75 ms responded by a certain current consumption by the PD, indicating its power class.

The PD is assigned to one of 5 classes: 0 (default class) indicates that full 15.4 watts should be provided. Classes 1-3 indicate various required power levels and 4 is reserved for future use. PDs that do not support classification are assigned to class 0. Special care must be employed in the definition of class thresholds, as classification may be affected by cable losses.

Classifying a PD according to its power consumption may assist a PoE system in optimizing its power distribution. Such a system typically suffers from lack of power resources, so that efficient power management based on classification results may reduce total system costs.

Start-up

Once line detection and optional classification stages are completed, the PSE must switch from low voltage to its full voltage capacity (44-57 Volts) over a minimal amount of time (above 15 microseconds).

A gradual startup is required, as a sudden rise in voltage (reaching high frequencies) would introduce noise on the data lines.

Once provision of power is initiated, it is common for inrush current to be experienced at the PSE port, due to the PD's input capacitance. A PD must be designed to cease inrush current consumption (of over 350 mA) within 50 ms of power provision startup.

Operation

During normal operation, the PSE provides 44-57 VDC, able to support a minimum of 15.4 watts power.

Power Overloads

The IEEE 802.3af standard defines handling of overload conditions. In the event of an overload (a PD drawing a higher power level than the allowed 12.95 Watts), or an outright short circuit caused by a failure in cabling or in the PD, the PSE must shut

down power within 50 to 75 milliseconds, while limiting current drain during this period to protect the cabling infrastructure. Immediate voltage drop is avoided to prevent shutdown due to random fluctuations.

Power Disconnection Scenarios

The IEEE 802.3af standard requires that devices powered over Ethernet be disconnected safely (i.e. power needs be shut down within a short period of time following disconnection of a PD from an active port).

When a PD is disconnected, there is a danger that it will be replaced by a non-PoE-ready device while power is still on. Imagine disconnecting a powered IP phone utilizing 48 VDC, then inadvertently plugging the powered Ethernet cable into a non-PoE notebook computer. What's sure to follow is not a pretty picture.

The standard defines two means of disconnection, DC Disconnect and AC Disconnect, both of which provide the same functionality - the PSE shuts down power to a disconnected port within 300 to 400ms. The upper boundary is a physical human limit for disconnecting one PD and reconnecting another.

DC Disconnect

DC Disconnect detection involves measurement of current. Naturally, a disconnected PD stops consuming current, which can be inspected by the PSE. The PSE must therefore disconnect power within 300 to 400 ms from the current flow stop. The lower time boundary is important to prevent shutdown due to random fluctuations.

AC Disconnect

This method is based on the fact that when a valid PD is connected to a port, the AC impedance measured on its terminals is significantly lower than in the case of an open port (disconnected PD).

AC Disconnect detection involves the induction of low AC signal in addition to the 48 VDC operating voltage. The returned AC signal amplitude is monitored by the PSE at the port terminals. During normal operation, the PD's relatively low impedance lowers the returned AC signal while a sudden disconnection of this PD will cause a surge to the full AC signal level and will indicate PD disconnection.

Appendix A

RJ-45 Pin Assignment

Switch's RJ-45 Pin Assignments

1000Mbps, 1000Base T

Contact	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

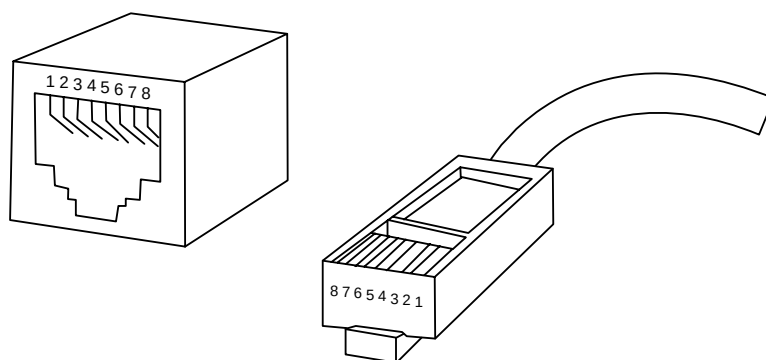
Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

10/100Mbps, 10/100Base-TX

When connecting your 10/100Mbps Ethernet Switch to another switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ-45 receptacle/ connector and their pin assignments:

RJ-45 Connector pin assignment		
Contact	MDI	MDI-X
	Media Dependant Interface	Media Dependant Interface-Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

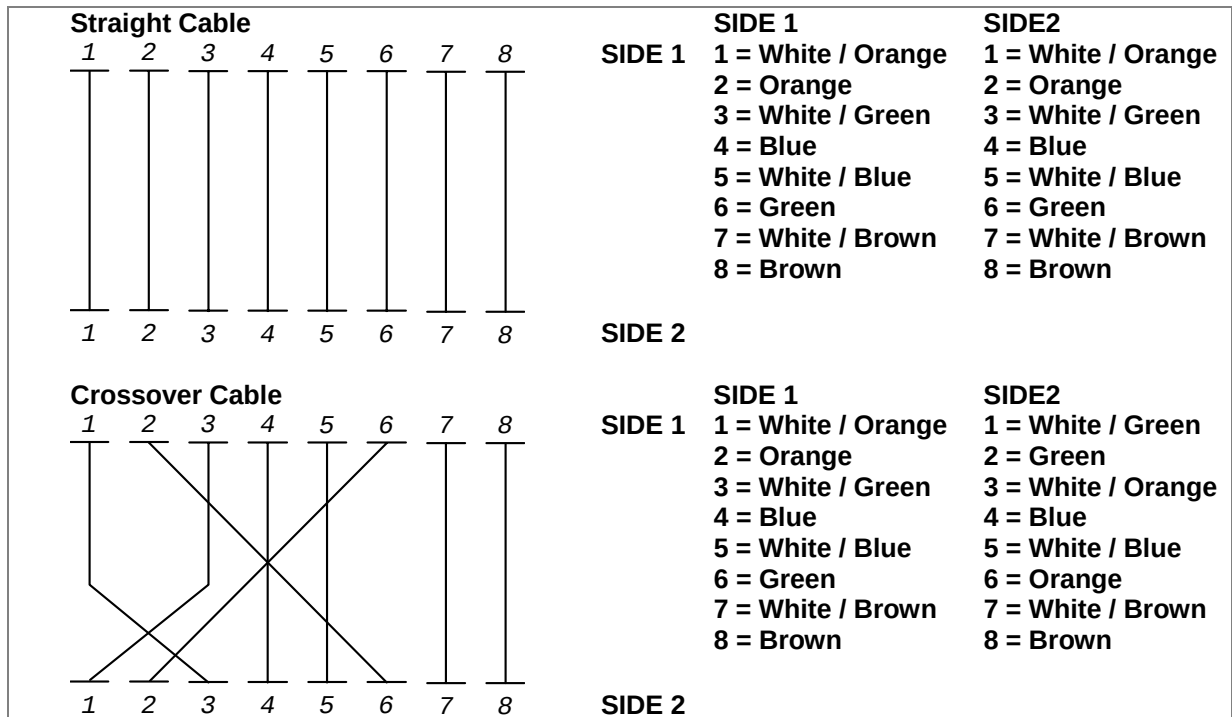
The standard cable, RJ-45 pin assignment



The standard RJ-45 receptacle/connector

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:

Figure A-1: Straight-Through and Crossover Cable



Please make sure your connected cables are with same pin assignment and color as above picture before deploying the cables into your network.

: RJ-45 Pin Assignment

Appendix B

Troubleshooting

- Verify that is using the right power cord/adaptor (DC 24-48V), please don't use the power adapter with DC output higher than 48V, or it may damage this device.
- Select the proper UTP/STP cable to construct the user network. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections that depend on the connector type the switch equipped: 1000 Category 3, 4 or 5 cable for 10Mbps connections, 1000 Category 5 cable for 100Mbps connections, or 1000 Category 5e/above cable for 1000Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).
- Diagnosing LED Indicators: To assist in identifying problems, the switch can be easily monitored through panel indicators, which describe common problems the user may encounter and where the user can find possible solutions.
- If the power indicator does not light on when the power cord is plugged in, you may have a problem with power cord. Then check for loose power connections, power losses or surges at power outlet. If you still cannot resolve the problem, contact the local dealer for assistance.
- If the LED indicators are normal and the connected cables are correct but the packets still cannot be transmitted. Please check the user system's Ethernet devices' configuration or status