



KGS-0841-W

KGS-0860-WP KGS-0861-WP

KGS-0862-WP KGS-0863-WP

IP65/67 Rated Gigabit Ethernet Switches

Firmware Rev1.04 up

User's Manual



DOC.150331

©2013-2015 KTI Networks Inc.

All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation or transformation) without permission from KTI Networks Inc.

KTI Networks Inc. reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of KTI Networks Inc. to provide notification of such revision or change.

For more information, contact:

United States KTI Networks Inc.
 P.O. BOX 631008
 Houston, Texas 77263-1008

Phone: 713-2663891
Fax: 713-2663893
E-mail: kti@ktinet.com
URL: <http://www.ktinet.com/>

International Fax: 886-2-26983873
 E-mail: kti@ktinet.com.tw
 URL: <http://www.ktinet.com.tw/>

The information contained in this document is subject to change without prior notice.

Copyright © All Rights Reserved.

TRADEMARKS

Ethernet is a registered trademark of Xerox Corp.

FCC NOTICE

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including the interference that may cause undesired operation.

CE NOTICE

Marking by the symbol indicates compliance of this equipment to the EMC directive of the European Community. Such marking is indicative that this equipment meets or exceeds the following technical standards:

VCCI-A Notice

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

Table of Contents

1. Introduction	7
1.1 Features.....	8
1.2 Product Model Options	8
1.3 Product Panels.....	10
1.3.1 KGS-0841-W.....	10
1.3.2 KGS-0860-WP	10
1.3.3 KGS-0861-WP	11
1.3.4 KGS-0862-WP	11
1.3.5 KGS-0863-WP	12
1.3.6 KGS-086x-WP Fiber Interfaces	13
1.4 LED Indicators	14
1.5 Specifications.....	14
2. Installation	20
2.1 Unpacking.....	20
2.1.1 Package Accessory Kit	20
2.2 Safety Cautions.....	20
2.3 Panel Mounting	21
2.4 Flat Mounting	23
2.5 Applying Power	24
2.5.1 Direct DC Power	24
2.5.2 Powered via PoE over Cat.5.....	26
2.6 Making Cat.5 Connections.....	28
2.6.1 Patch Cables for Fast Ethernet Port Types	28
2.6.2 Patch Cables for Gigabit Ethernet Port Types	29
2.6.3 Important Functions of M12 Copper Ports	31
2.7 Making Console Connection.....	32
2.8 Making PoE PSE Connection to PD Device	33
2.9 Making Fiber Connection	35
2.10 LED Indication.....	37
2.11 Configuring IP Address for the Switch	38
2.12 Abbreviation for Console Interface and Web Interface	38
3. Console Command Line Interface.....	40
3.1 Console CLI	40
3.2 System Command	40

3.3 Console Commands	45
3.4 IP Commands	47
4. Web Management	50
4.1 Start Browser Software and Making Connection	50
4.2 Login to the Switch Unit	50
4.3 Main Management Menu	53
4.4 System	55
4.4.1 Management VLAN.....	57
4.5 Ports.....	58
4.5.1 Port Type	60
4.5.2 FX DDM Status	61
4.6 VLANs.....	62
4.6.1 VLAN Function.....	63
4.6.2 Port-based VLAN Mode.....	67
4.6.3 Port-based VLAN ISP Mode	68
4.6.4 Simplified Tag-based VLAN Mode.....	69
4.6.4.1 VLAN Groups.....	70
4.6.4.2 Per Port Settings.....	71
4.6.4.3 Simplified Tag-based VLAN Operation	72
4.6.5 Advanced VLAN Mode.....	74
4.6.5.1 Ingress Default Tag.....	75
4.6.5.2 Ingress Settings	76
4.6.5.3 Egress Settings.....	78
4.6.5.4 VLAN Groups.....	79
4.6.6 Simplified Tag-based VLAN vs. Advanced VLAN.....	80
4.6.7 Important Notes for VLAN Configuration	81
4.7 LACP.....	82
4.8 RSTP	83
4.9 802.1X Authentication.....	85
4.9.1 802.1X Configuration	86
4.9.2 802.1X Re-authentication Parameters.....	88
4.10 IGMP Snooping.....	89
4.11 Mirroring.....	90
4.12 Quality of Service.....	91
4.12.1 QoS Configuration	93

4.12.2 802.1p Mapping	94
4.12.3 DSCP Mapping	95
4.12.4 QoS Service Policy	96
4.13 Storm Control.....	97
4.14 Multi Ring.....	98
4.15 Statistics Overview.....	99
4.16 Detailed Statistics	100
4.17 LACP Status	101
4.18 RSTP Status	103
4.19 IGMP Status.....	105
4.20 PoE Status.....	106
4.21 Multi Ring Status.....	107
4.22 Ping.....	110
4.23 Reboot System	111
4.24 Restore Default.....	111
4.25 Update Firmware	111
4.26 Configuration File Transfer	112
4.27 Logout.....	112
5. SNMP Support.....	113
Appendix A Specifications of Fiber Interface Options	114

1. Introduction

KTI's KGS-0860 IP65/67 switch series offers a diverse range of managed Ethernet switches with the ruggedized hardware design for protection against strong jets of water and temporary immersion in water. The series includes a variety of 8-ports switches featured with different configurations composed of Fast Ethernet ports and Gigabit Ethernet ports. The available port types are copper port, fiber optical port and combo port with dual-media support (copper and fiber optical).

In addition to standard direct power input, the series provides optional solution that the switch can be powered over network cable instead of direct power input. This way called "Power over Ethernet" allows the switch receives electric power along with data from the connected network cable and the switch can be installed in place where power is not present. Not only PoE powered switch solutions the series also offers PoE power sourcing switches which can deliver power to other switches over the connected cables. It provides complete and diversified solutions for PoE deployment with the IP65/67 switches.

Designed to operate reliably in harsh industrial environments the series provides a high level of immunity to electromagnetic interference and heavy electrical surges usually found in industrial environments. An operating temperature range of -40°C to +70°C coupled with IP65/67 rated waterproof design allows the switches to be installed in any locations virtually.

To meet requirements for advanced applications, the switch series provides advanced layer 2 network functions, a variety of management interfaces enhanced with security features, and a full array of useful functions for high network availability and manageability. Featured with the ruggedized hardware design, the KGS-0860 series provides ideal solutions for any harsh environments, such as strong vibrations, extreme temperatures and wet or dusty conditions.



1.1 Features

- Diverse range of 8-port unmanaged and managed switches for selection
- Full wire speed forwarding and filtering
- Provide optional fiber interfaces to support variety of fiber connections
- Provide 802.1Q VLAN, 802.1p QoS, DSCP QoS functions
- Provide LACP port link aggregation function
- Provide port mirroring function
- Support jumbo frame up to 9.6K bytes
- Provide packet storm control function
- Support console, web, SNMP management interfaces
- Support DHCP for IP configuration
- Provide password authentication for management access
- Provide 802.1x authentication for port access
- Support 802.1w RSTP, 8021D STP for preventing loop connection
- Support redundant ring applications with enhanced industrial RSTP
- Support IGMP snooping function
- Waterproof enclosure design, LAN port connectors and power connector
- IP67 rated for protection against temporary immersion in water
- IP65 rated for protection against strong jets of water
- Support either direct DC input or PoE over network cable
- Offer optional high power PoE+ PSE switch models

1.2 Product Model Options

Model Name	Managed ^{*7}	Fast Ethernet	Gigabit Ethernet	Fiber options	PoE feature
KGS-0841-W	-	8 ports	-	-	-
KGS-0860-WP	√	8 ports	-	-	PD ^{*5}
KGS-0860-WP-x	√	8 ports	-	1 100Base-FX ^{*1}	PD
KGS-0860-WP-2x	√	8 ports	-	2 100Base-FX ^{*2}	PD
KGS-0861-WP	√	-	8 ports	-	PD
KGS-0861-WP-x	√	-	8 ports	1 1000Base-X ^{*3}	PD
KGS-0861-WP-2x	√	-	8 ports	2 1000Base-X ^{*4}	PD
KGS-0862-WP	√	-	8 ports	-	8 PSE ^{*6}
KGS-0862-WP-x	√	-	8 ports	1 1000Base-X	8 PSE
KGS-0862-WP-2x	√	-	8 ports	2 1000Base-X	8 PSE
KGS-0863-WP	√	6 ports	2 ports	-	8 PSE
KGS-0863-WP-x	√	6 ports	2 ports	1 1000Base-X	8 PSE
KGS-0863-WP-2x	√	6 ports	2 ports	2 1000Base-X	8 PSE

Remark:

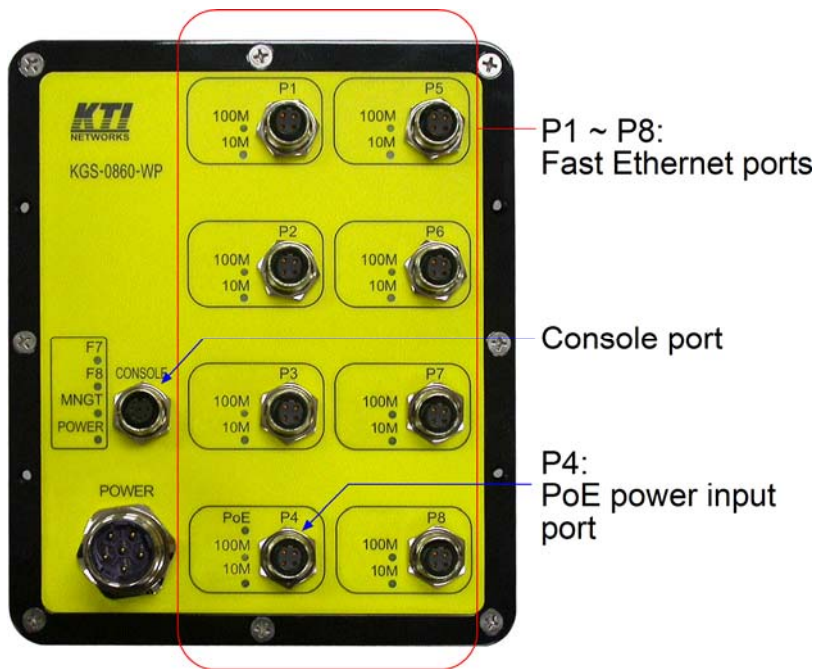
- *1: Additional 100Base-FX fiber interface on Port #8
- *2: Additional two 100Base-FX fiber interfaces on Port #7 and Port #8
- *3: Additional 1000Base-X fiber interface on Port #8
- *4: Additional two 1000Base-X fiber interfaces on Port #7 and Port #8
- *5: PoE PD function on Port #4 (The switch can be powered via PoE on Port #4.)
- *6: All ports are featured with PoE+ PSE function.
- *7: Featured with management interfaces.

1.3 Product Panels

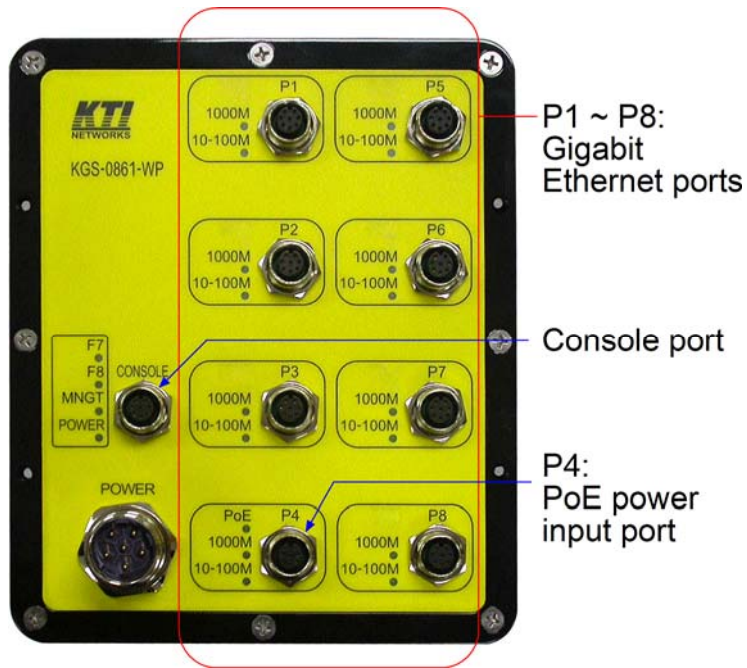
1.3.1 KGS-0841-W



1.3.2 KGS-0860-WP



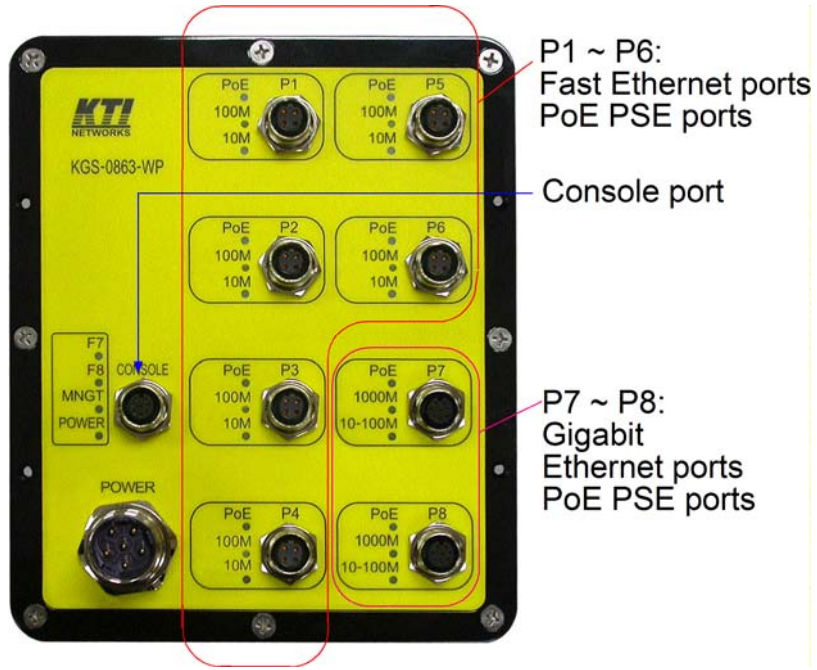
1.3.3 KGS-0861-WP



1.3.4 KGS-0862-WP



1.3.5 KGS-0863-WP



1.3.6 KGS-086x-WP Fiber Interfaces

The following figures illustrate the fiber interfaces of the models with fiber options:

No fiber interface



One fiber interface



P8 fiber interface

Two fiber interfaces



P8 fiber interface

P7 fiber interface

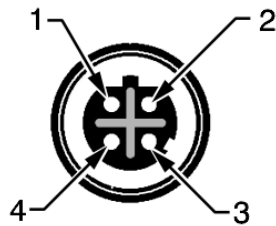
1.4 LED Indicators

<u>LED</u>	<u>Function</u>
POWER	Power status
1000M	1000M link & activities status (Gigabit Ethernet ports)
10-100M	10M or 100M link & activities status (Gigabit Ethernet ports)
100M	100M link & activities status (Fast Ethernet ports)
10M	10M link & activities status (Fast Ethernet ports)
PoE	PoE power status (PoE input ports, PoE output ports)
F7	Port 7 fiber transceiver in use
F8	Port 8 fiber transceiver in use
MNGT	Management operation status

1.5 Specifications

Fast Ethernet (FE) Ports

Compliance	IEEE 802.3 10Base-T, 100Base-TX
Connector	M12 D-code, 4-pole, female, 60V/2A rated per pole per IEC 61076-2-101, IP67 rated



Configuration	Auto-negotiation or software control
Transmission rate	10Mbps, 100Mbps
Duplex support	Full duplex, Half duplex
Network cable	Cat.5 or better
Pin assignments	Auto MDI/MDI-X detection

Pin#	LAN Signal
1	TX+
2	RX+
3	TX-
4	RX-

Fast Ethernet (FE) Port built-in PoE Input

PoE Standard	IEEE 802.3af PoE PD (Powered Device)
PSE Support	IEEE 802.3af & 802.3at PSE
Power Classification	Class 0
Input Voltage (V_{poe})	36 ~ 57VDC via Cat.5
Power Reception	Pin assignments

Pin#	PoE Input	LAN Signal
1	V_{poe+}	TX+
2	V_{poe-}	RX+
3	V_{poe+}	TX-
4	V_{poe-}	RX-

Power polarity protection

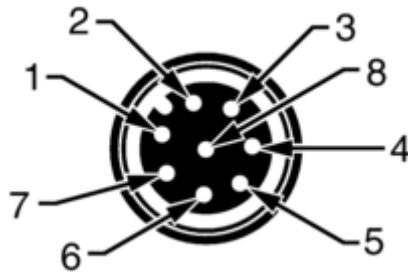
Fast Ethernet (FE) Port built-in PoE Output

PoE Standard IEEE 802.3at PSE (High power PoE+)
 PD Support Type 1 Class 0 ~ 3, Type 2 Class 4
 Power Delivery 30W max. (per port)
 Protection Under voltage, Over voltage, Over current, Over temperature
 PSE Power Pins

Pin#	PoE Output	LAN Signal
1	V_{poe+}	TX+
2	V_{poe-}	RX+
3	V_{poe+}	TX-
4	V_{poe-}	RX-

Gigabit Ethernet (GbE) Ports

Compliance IEEE 802.3 10Base-T, 100Base-TX, 1000Base-T
 Connector M12 A-code, 8-pole, female,
 IP67 rated, 60V/2A rated per pole



Configuration Auto-negotiation or software control
 Transmission rate 10Mbps, 100Mbps, 1000Mbps
 Duplex support Full duplex, Half duplex
 Network cable Cat.5 or better
 Pin assignments Auto MDI/MDI-X detection

Pin#	Signal
1	D1+
2	D1-
3	D0+
4	D3+
5	D3-

6	D0-
7	D2+
8	D2-

Gigabit Ethernet (GbE) Port built-in PoE Input

Standard	IEEE 802.3af PD (Powered Device)
PSE Support	IEEE 802.3af & 802.3at PSE
Power Classification	Class 0
Input Voltage (V_{poe})	36 ~ 57VDC via Cat.5
Power Reception	Pin assignments

Pin#	PoE	Signal
1	V_{poe-}	D1+
2	V_{poe-}	D1-
3	V_{poe+}	D0+
4	V_{poe-}	D3+
5	V_{poe-}	D3-
6	V_{poe+}	D0-
7	V_{poe+}	D2+
8	V_{poe+}	D2-

Power polarity protection

Gigabit Ethernet (GbE) Port built-in PoE Output

PoE Standard	IEEE 802.3at PSE (High power PoE+)
PD Support	Type 1 Class 0 ~ 3, Type 2 Class 4
Power Delivery	30W max. (per port)
Protection	Under voltage, Over voltage, Over current, Over temperature
PSE Power Pins	Pin assignments

Pin#	PoE	Signal
1	V_{poe-}	D1+
2	V_{poe-}	D1-
3	V_{poe+}	D0+
4	V_{poe-}	D3+
5	V_{poe-}	D3-
6	V_{poe+}	D0-
7	V_{poe+}	D2+
8	V_{poe+}	D2-

100Base-FX Fiber interface

Compliance	100Base-FX
Connector	LC for single fiber, Dual LC for duplex fiber

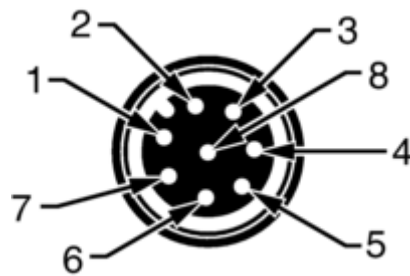
Configuration	100Mbps, Full duplex
Transmission rate	100Mbps
Network cables	MMF 50/125 60/125, SMF 9/125
Eye safety	IEC 825 compliant
Optical Specifications	Refer to Appendix X for variety of fiber options

1000Base-X Fiber interface

Compliance	1000Base-SX/LX/BX
Connector	LC for single fiber, Dual LC for duplex fiber
Configuration	Auto/Forced, 1000Mbps, Full duplex
Transmission rate	1000Mbps
Network cables	MMF 50/125µm 60/125µm, SMF 9/125µm
Eye safety	IEC 825 compliant
Optical Specifications	Refer to Appendix X for variety of fiber options

Console Port

Interface	RS-232, DTE type
Connector	M12 A-code, 8-pole, female, IP67 rated

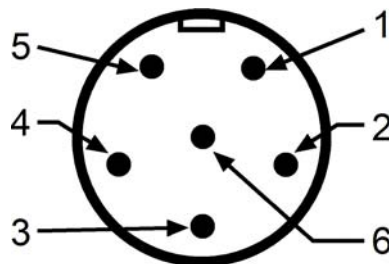


Pin assignments

Pin#	Signal
1, 2, 3, 7, 8	NC
4	SG
5	RXD
6	TXD

Power Interface

Connector	M23 6-pole, male
-----------	------------------



Operating Voltages	+7.5 ~ +60VDC (For no PoE PSE option) +45 ~ +57VDC for support Type 1 PDs
--------------------	--

+51 ~ +57VDC for support Type 1 and Type 2 PDs
 * Warning: The -48VDC power supply is not supported.

Power Consumption 11.5W max. (No PoE support)

Pin Assignments

Pin#	Signal
1	DC+
2	DC-
3	Frame Ground
4, 5, 6	NC

Insulation FG vs. DC power lines (500VDC/10M-Ohm)

Switch Functions

MAC Addresses Table 8K entries
 Forwarding & filtering Non-blocking, full wire speed
 Switching technology Store and forward
 Maximum packet length 1526 bytes (Jumbo frame support disabled)
 Jumbo frame support Up to 9.6K bytes
 IP Multicast groups 8192 supported
 Flow control IEEE 802.3x pause frame base for full duplex operation
 Back pressure for half duplex operation
 VLAN function Port-based VLAN and IEEE 802.1Q Tag-based VLAN
 QoS function Port-based, 802.1p-based, IP DSCP-based
 Port control Port configuration control via software management
 Storm control Broadcast, Multicast storm protection control via software management
 Aggregation Link aggregation (port trunking)
 Port Mirroring Mirror received frames to a sniffer port

Mechanical

Dimension (base) 163 x 195 x 60.5 mm (WxDxH)
 Housing Aluminum housing with no fan
 IP Protection IP65, IP67
 Mounting Panel mounting, flat mounting

Environmental

Operating Temperature Typical -40°C ~ +70°C
 Storage Temperature -40°C ~ +85°C
 Relative Humidity 5% ~ 90% non-condensing

Test

FCC Part 15 rule Class A
 CE EMC

EN 55011, EN 61000-3-2, EN 61000-3-3
EN 61000-6-2 industrial environment
IEC 60068-2-1 cold temperature test
IEC 60068-2-2 dry heat test
IEC 60068-2-30 damp heat test
IEC 60068-2-48 storage temperature test
IEC 60068-2-27 shock test
EN 50155 railway applications for rolling stock
NEMA TS2 Environment
IPX5 water jets test
IPX7 water immersion test
IP6X ingress of dust test
Safety / LVD IEC 60950-1

2. Installation

2.1 Unpacking

The product package contains:

- The switch unit
- One accessory kit
- One product CD-ROM

2.1.1 Package Accessory Kit

Panel mount bracket	1 pc
M4-6mm screw (for panel mounting)	4 pcs
PWR3PE-PMF-2 DC power cable 2 meters	1 pc
C5EFPE-CMR-2 Console cable 2 meters	1 pc
C5EFPE-FMR-2 Patch cable for Fast Ethernet port	1 pc
C5EFPE-GMR-2 Patch cable for Gigabit Ethernet port	1 pc
M5-15mm screw (for flat mounting)	4 pcs

2.2 Safety Cautions

To reduce the risk of bodily injury, electrical shock, fire and damage to the product, observe the following precautions.

- Do not service any product except as explained in your system documentation.
- Opening or removing covers may expose you to electrical shock.
- Only a trained service technician should service components inside these compartments.
- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:
 - The power cable, extension cable, or plug is damaged.
 - The product has been dropped or damaged.
 - The product does not operate correctly when you follow the operating instructions.
- Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.
- Operate the product only from the type of external power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult your service provider or local power company.

2.3 Panel Mounting

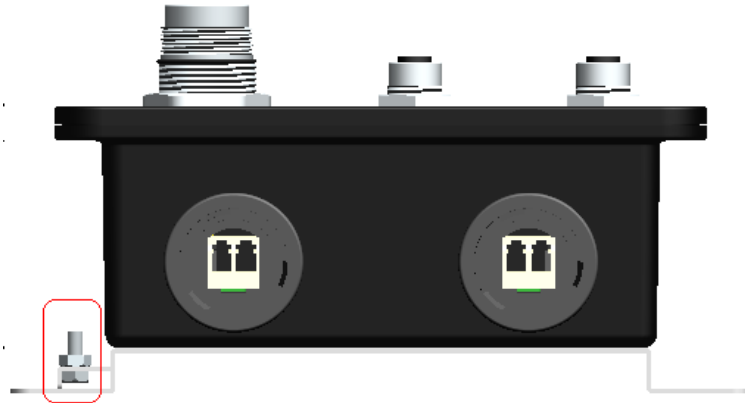
One stainless panel mount bracket is included in product package as shown below:



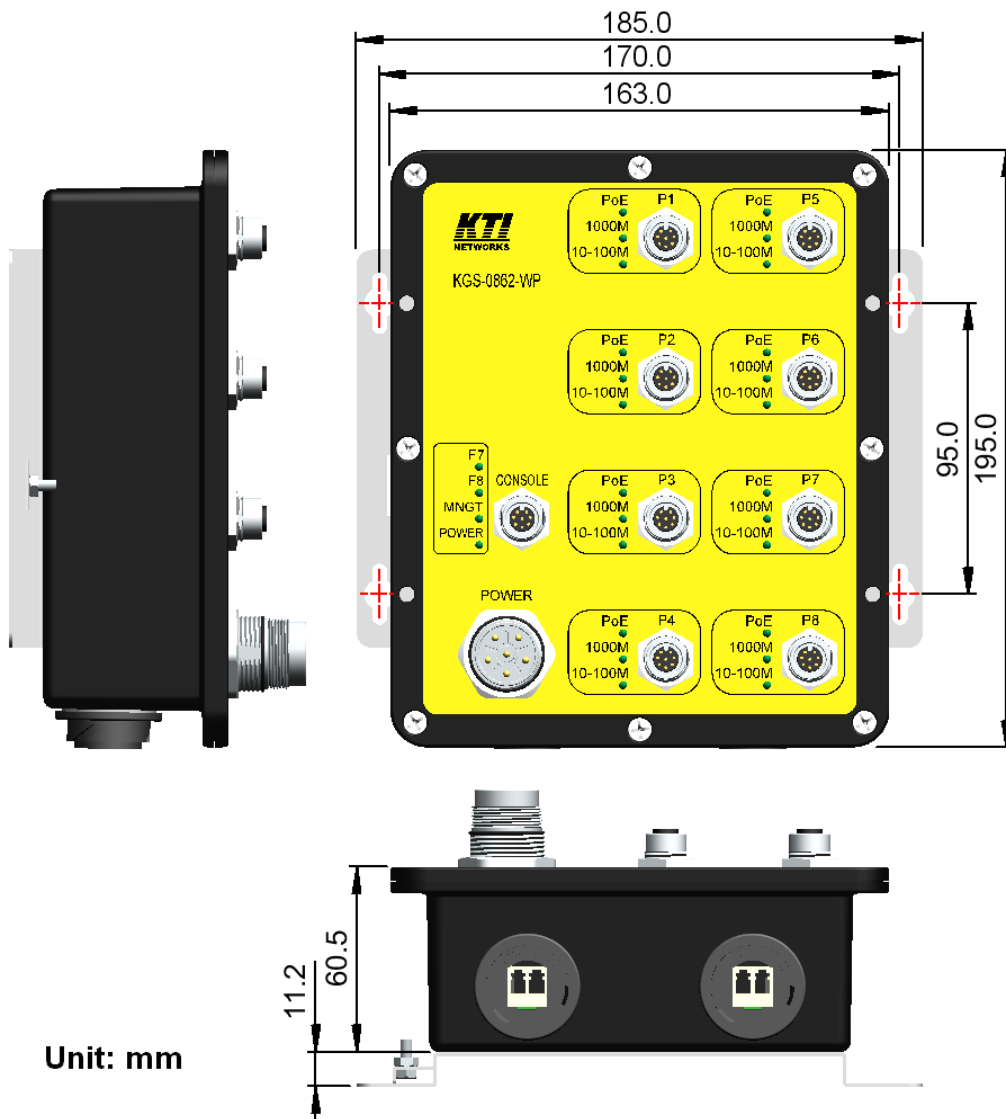
Install the bracket on the bottom with M4 screws.



There is one screw is provided on panel mount bracket. It can be used for PE (Protective Earth) connection if needed.



Dimension of the device with mounting bracket



2.4 Flat Mounting

The device can support flat mount onto a flat panel face as illustrated below:



There are four screw holes located on the front. Use M5-15mm screw for fixing the device on the flat panel.



After installation



2.5 Applying Power

Two methods for applying power to the device are:

1. Direct DC power input via Power connector
2. PoE power input via Port 4

The table below lists the available power method for different models:

Model Name	PoE feature	Direct DC	PoE via Port 4
KGS-0841-W	-	√	-
KGS-0860-WP-xx	PD	√	√
KGS-0861-WP-xx	PD	√	√
KGS-0862-WP-xx	8 PSE	√	-
KGS-0863-WP-xx	8 PSE	√	-

2.5.1 Direct DC Power

The power connector is shown below:



Use appropriate power cable as shown below to supply DC power from external power supply.



The pin assignments are:

Pin#	Contacts
1	DC+
2	DC-
3	Frame Ground
4, 5, 6	NC

Pin #3 connects to device frame ground and it is isolated from power lines DC+/DC-. It can be used for PE (Protective Earth) connection.

Plug the cable



The working voltages and maximal power required for different applications are listed as follows:

Model Name	Application	Operating voltage range	Max. power
KGS-0841-W	General	+6.5 ~ +60VDC	11.5W
KGS-0860-WP-xx	General	+6.5 ~ +60VDC	11.5W
KGS-0861-WP-xx	General	+6.5 ~ +60VDC	11.5W
KGS-0862-WP-xx	Type 1 PoE	+45 ~ +57VDC	135W
KGS-0862-WP-xx	High power PoE	+51 ~ +57VDC	256W
KGS-0863-WP-xx	Type 1 PoE	+45 ~ +57VDC	135W
KGS-0863-WP-xx	High power PoE	+51 ~ +57VDC	256W

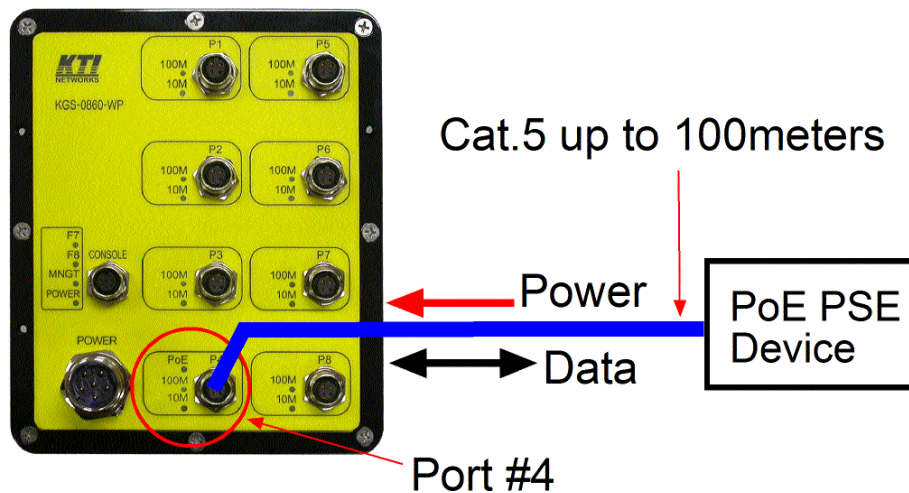
2.5.2 Powered via PoE over Cat.5

The following model series provide optional PoE power method:

Model Name	Direct DC	PoE via Port 4
KGS-0860-WP-xx	√	√
KGS-0861-WP-xx	√	√

Port #4 is equipped with function of receiving power from connected PoE PSE device over Cat.5 cable. The remote PoE PSE devices can be a mid-span PoE injector or end-span PoE switched port.

The figure below illustrates a connection example:



The switches can support the following PSE:

- 802.3af compliant PSE (Typical, Type 1 PSE)
Possible voltages received: +36 ~ +57VDC
- 802.3at compliant PSE (High power PoE, Type 2 PSE)
Possible voltages received: +42.5 ~ +57VDC

PoE LED Indicator on “FE port built-in PoE input” and “GbE port built-in PoE input”:



2.6 Making Cat.5 Connections

2.6.1 Patch Cables for Fast Ethernet Port Types

Types: Fast Ethernet Ports (Typical)

Fast Ethernet Ports with built-in PoE power input

Fast Ethernet Ports with built-in PoE power output (PSE)

Available patch cable specifications

- IP65/67 protection with M12 connector
- M12 D-code connector compliant with IEC 61076-2-101
- HDPE Cat.5e for outdoor and harsh environment
- Temperature range -40°C to 80°C
- Solutions with RJ-45 (TIA/EIA-568B std.) for general purpose connection

Optional Part List

Part numbers	1st end	Cord	2nd end	Length
C5EFPE-FMR-2	M12DM-4-P	Cat.5e/FTP/PE	RJ-45	2m
C5EFPE-FMR-20	M12DM-4-P	Cat.5e/FTP/PE	RJ-45	20m
C5EFPE-FMR-50	M12DM-4-P	Cat.5e/FTP/PE	RJ-45	50m
C5EFPE-FMR-100	M12DM-4-P	Cat.5e/FTP/PE	RJ-45	100m
C5EFPE-FMM-20	M12DM-4-P	Cat.5e/FTP/PE	M12DM-4-P	20m
C5EFPE-FMM-50	M12DM-4-P	Cat.5e/FTP/PE	M12DM-4-P	50m
C5EFPE-FMM-100	M12DM-4-P	Cat.5e/FTP/PE	M12DM-4-P	100m



C5EFPE-FMM-100



C5EFPE-FMR-2

Cable Pin Assignments

1st end M12DM-4-P	Cat.5e/FTP/PE Cord wire color	2nd end	
		RJ-45	M12DM-4-P
Pin 1	White/orange	1	1
Pin 2	White/green	3	2
Pin 3	Orange solid	2	3
Pin 4	Green solid	6	4
-	Blue solid	4	-
-	White/blue	5	-
-	White/brown	7	-
-	Brown solid	8	-

2.6.2 Patch Cables for Gigabit Ethernet Port Types

Types: Gigabit Ethernet Ports (Typical)

Gigabit Ethernet Ports with built-in PoE power input

Gigabit Ethernet Ports with built-in PoE power output (PSE)

Available patch cable specifications

- IP65/67 protection with M12 connector
- HDPE Cat.5e for outdoor and harsh environment
- Temperature range -40°C to 80°C
- Solutions with RJ-45 (TIA/EIA-568B std.) for general purpose connection

Optional Part List

Part numbers	1st end	Cord	2nd end	Length
C5EFPE-GMR-2	M12AM-8-P	Cat.5e/FTP/PE	RJ-45	2m
C5EFPE-GMR-20	M12AM-8-P	Cat.5e/FTP/PE	RJ-45	20m
C5EFPE-GMR-50	M12AM-8-P	Cat.5e/FTP/PE	RJ-45	50m
C5EFPE-GMR-100	M12AM-8-P	Cat.5e/FTP/PE	RJ-45	100m
C5EFPE-GMM-20	M12AM-8-P	Cat.5e/FTP/PE	M12AM-8-P	20m
C5EFPE-GMM-50	M12AM-8-P	Cat.5e/FTP/PE	M12AM-8-P	50m
C5EFPE-GMM-100	M12AM-8-P	Cat.5e/FTP/PE	M12AM-8-P	100m



C5EFPE-GMM-100



C5EFPE-GMR-2

Cable Pin Assignments

1st end M12AM-8-P	Cat.5e/FTP/PE Cord wire color	2nd end	
		RJ-45	M12AM-8-P
Pin 1	White/orange	1	1
Pin 2	Orange solid	2	2
Pin 3	White/green	3	3
Pin 4	Blue solid	4	4
Pin 5	White/blue	5	5
Pin 6	Green solid	6	6
Pin 7	White/brown	7	7
Pin 8	Brown solid	8	8

Plug cable to the device and screw it securely.



2.6.3 Important Functions of M12 Copper Ports

Auto MDI/MDI-X Function

This function allows the port to auto-detect the twisted-pair signals and adapts itself to form a valid MDI to MDI-X connection with the remote connected device automatically. No matter a straight through cable or crossover cable connected, the ports can sense the receiving pair automatically and configure self to match the rule for MDI to MDI-X connection. It simplifies the cable installation.

Auto-negotiation Function

The ports are featured with auto-negotiation function and full capability to support connection to any Ethernet devices. The port performs a negotiation process for the speed and duplex configuration with the connected device automatically when each time a link is being established. If the connected device is also auto-negotiation capable, both devices will come out the best configuration after negotiation process. If the connected device is incapable in auto-negotiation, the switch will sense the speed and use half duplex for the connection.

Port Configuration Management

For making proper connection to an auto-negotiation incapable device, it is suggested to use port control function via software management to set forced mode and specify speed and duplex mode which match the configuration used by the connected device.

2.7 Making Console Connection

Use the listed cable below for console connection.

Part numbers	Type	1st end	Cord	2nd end	Length
C5EFPE-CMR-2	Console	M12AM-8-M	Cat.5e/FTP/PE	DB9	2m

C5EFPE-CMR-2



Cable Pin Assignments

1st end M12AM-8-P	Cat.5e/FTP/PE Cord wire color	2nd end RJ-45	DB9F-2-RJ45P Adapter -DB9	RS-232 signals
Pin 1	White/orange	1	9	-
Pin 2	Orange solid	2	1	-
Pin 3	White/green	3	4	-
Pin 4	Blue solid	4	5	SG
Pin 5	White/blue	5	2	RXD
Pin 6	Green solid	6	3	TXD
Pin 7	White/brown	7	8	-
Pin 8	Brown solid	8	7	-

Baud Rate information:

Baud rate – 115200 Data bits - 8
 Parity – None Stop bit – 1 Flow control – None

Plug the cable to the console port and screw it securely.



2.8 Making PoE PSE Connection to PD Device

Cables

No special cable is required for this connection. Depending on the port types, use the suggested cables listed in Section 2.6.1 and 2.6.2.

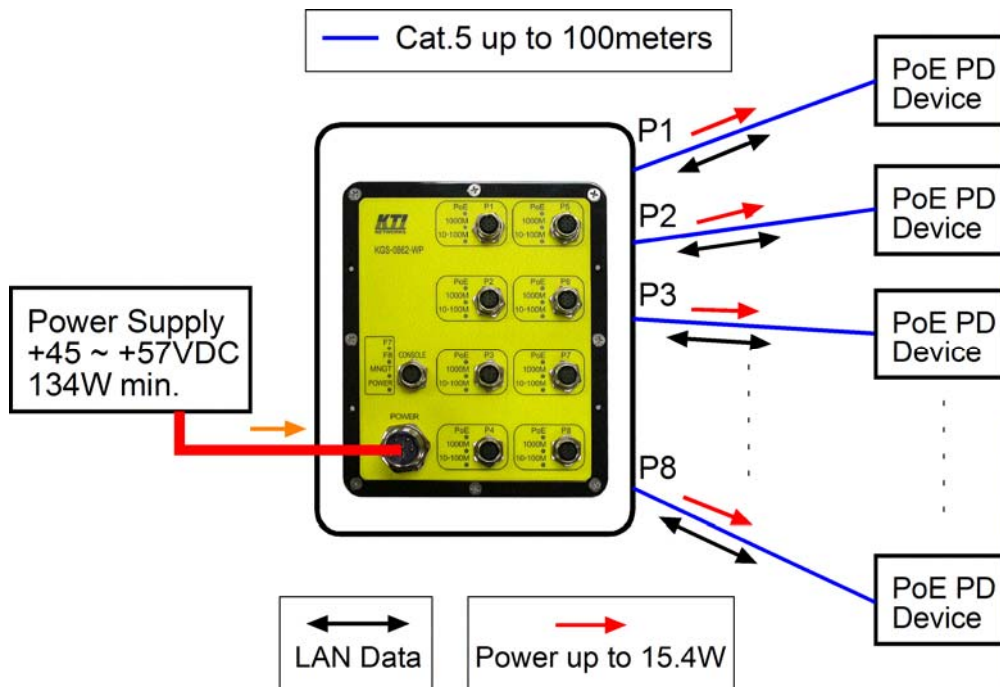
Typical PoE Applications

Supported Powered Devices (PD): 802.3af compliant devices

PoE Power output: 15.4W max. per PSE port

DC power input working voltage range: +45 ~ +57VDC

Total required power input: 135W (PoE output plus switch basic consumption)



High Power PoE Applications

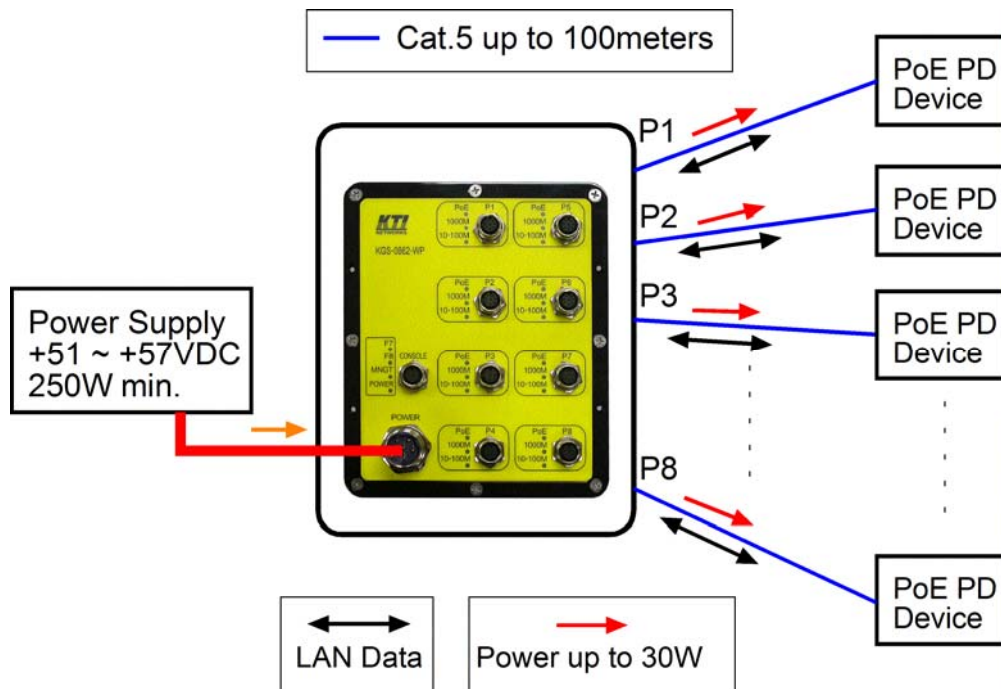
The switches can support PoE high power applications. It means the power delivered can be up to 30watts by single PSE port connection to a PD device which consumes larges power than typical PoE 15.4W.

Supported Powered Devices (PD): 802.3af or 802.3at compliant devices

PoE Power output: 30W max. per PSE port

DC power input working voltage range: **+51 ~ +57VDC**

Total required power input: 252W (PoE output plus switch basic consumption)



2.9 Making Fiber Connection

Some models provide optional fiber interfaces for Port #8 or Port #7 and Port #8 both as shown below:



P8 fiber interface



P8 fiber interface

P7 fiber interface

The fiber interface may come with one LC connector for single fiber cable or come with two LC connectors for duplex fiber cables depending on the model optical specification. Refer to Appendix A for details.

LED Display for fiber interface



F7 & F8 LEDs turned ON to indicate fiber interfaces are selected for Port #7 and Port #8.

Network Cables

Multimode (MMF) - 50/125 μ m, 62.5/125 μ m

Single mode (SMF) - 9/125 μ m

Cable Installation for IP67

For IP65 and IP67 protection, one optional fiber accessory part, FO-PLUG-P-L is required for fiber cable installation. The part is for protection purpose only.

FO-PLUG-P-L Fiber port plug kit, IP67 rated

The installation of the part with fiber cable is shown as follows:



There are four seals packed in the kit. The seals support installation for the following cables:

- Single fiber, diameter 2.8mm
- Duplex fiber, diameter 2.8mm
- Single fiber, diameter 1.8mm
- Duplex fiber, diameter 1.8mm

2.10 LED Indication

LED	Function
POWER	Power status ON: power on OFF: power off
1000M	1000M link & activities status (Gigabit Ethernet ports) ON: port link on, speed 1000M BLINK: data in transmission OFF: port link off
10-100M	10M or 100M link & activities status (Gigabit Ethernet ports) ON: port link on, speed 100M or 10M BLINK: data in transmission OFF: port link off
100M	100M link & activities status (Fast Ethernet ports) ON: port link on, speed 100M BLINK: data in transmission OFF: port link off
10M	10M link & activities status (Fast Ethernet ports) ON: port link on, speed 10M BLINK: data in transmission OFF: port link off
PoE	PoE power status (PoE input ports, PoE output ports) ON: PoE power On OFF: PoE power Off
F7/F8	Port 7 Port 8 fiber interface in use ON: fiber interface in use OFF: not use
MNGT	Management operation status ON: System diagnostics & initialization finished BLINK: Failure detected on Main chip, Phy chip, and PoE chip OFF: System diagnostics & initialization in process

2.11 Configuring IP Address for the Switch

The switch is shipped with the following factory default settings for software management:

Default IP address of the switch: **192.168.0.2 / 255.255.255.0**

The IP Address is an identification of the switch in a TCP/IP network. Each switch should be designated a new and unique IP address in the network. Two methods to configure the IP address are:

1. Use console port

The console command sequence to set a fixed IP for the switch is:

```
>IP↵  
IP>Setup [<ipaddress>[<ipmask>[<ipgateway>]]]↵
```

The console command sequence to use DHCP mode for IP is:

```
>IP↵  
IP>Dhcp enable  
IP>
```

2. Use Web management

Refer to Web management interface for System Configuration. The switch is shipped with factory default password **123** for software management. The password is used for authentication in accessing to the switch via Http web-based interface. For security reason, it is recommended to change the default settings for the switch before deploying it to your network. Refer to Web management interface for System Configuration.

2.12 Abbreviation for Console Interface and Web Interface

Ingress Port: Ingress port is the input port on which a packet is received.

Egress Port: Egress port is the output port from which a packet is sent out.

IEEE 802.1Q Packets: A packet which is embedded with a VLAN Tag field

VLAN Tag: In IEEE 802.1Q packet format, 4-byte tag field is inserted in the original Ethernet frame between the Source Address and Type/Length fields. The tag is composed of:

#of bits	16	3	1	12
Frame field	TPID	User priority	CFI	VID

TPID: 16-bit field is set to 0x8100 to identify a frame as an IEEE 802.1Q tagged packet

User Priority: 3-bit field refer to the 802.1p priority

CFI: The Canonical Format Indicator for the MAC address is a 1 bit field.

VID: VLAN identifier, 12-bit field identifies the VLAN to which the frame belongs to.

Untagged packet: A standard Ethernet frame with no VLAN Tag field

Priority-tagged packet: An IEEE 802.1Q packet which VID filed value is zero (VID=0)

VLAN-Tagged packet: An IEEE 802.1Q packet which VID filed value is not zero (VID<>0)

PVID (Port VID): PVID is the default VID of an ingress port. It is often used in VLAN classification for untagged packets. It is also often used for egress tagging operation.

DSCP: Differentiated Service Code Point, 6-bit value field in an IP packet

VLAN Table lookup: The process of searching VLAN table to find a VLAN which matches the given VID index

MAC address table lookup: The process of searching MAC address table to find a MAC entry which matches the given destination MAC address and the port where the MAC address is located

Packet forwarding: also known as packet switching in a network switch based on MAC address table and VLAN table information

VLAN forwarding: the operation that a packet is forwarded to an egress destination port based on VLAN table information

VLAN group: configuration information about a VLAN which can be recognized in the switch. The information includes a VID associated to the VLAN, member ports, and some special settings.

3. Console Command Line Interface

3.1 Console CLI

System Boot Up Message

```
Booting ...image 1
EEPROM 25LC640 USED : 727 / 8192 Byte

IP address : 192.168.0.2

KGS-0862-WP IP65/67 Gigabit Ethernet Switch
*** CPU Check           : OK !!
*** VSC7398 PHY Check   : OK !!
*** VSC8211 PHY Check   : OK !!
*** PoE Chip(1) Check   : OK !! (Ver:06)
*** PoE Chip(2) Check   : OK !! (Ver:06)
*** Bord Type           ID0-2(0) : 2xGiga Fiber
                        ID3-4(3) : PSE
                        ID5-6(0) : 8xGiga
MAC address: 00-40-F6-EA-12-34
S/W Version: 1.02
H/W Version: 1.0

Password: _
```

Enter default Password: 123 to enter CLI mode.

Top level commands

Press ? or help to get help. The help depends on the context:

- At top level, a list of command groups will be shown.
- At group level, a list of the command syntaxes will be shown.
- If given after a command, the syntax and a description of the command will be shown.

>help

Commands at top level:

System - System commands
Console - Console commands
IP - IP commands

>

3.2 System Command

>sys

System>?

System *Configuration* [all]

System *Restore Default* [keepIP]

System *Name* [<name>]

System *Reboot*

System *SNMP* [enable/disable]

System Trap [*<IP Address>*]
System Readcommunity [*<community string>*]
System Writecommunity [*<community string>*]
System Trapcommunity [*<community string>*]
System Power Saving [*full|up/down/disable*]

Configuration

System>Config help

Syntax:

System Configuration [*all*]

Description:

Show system name, software version, hardware version and management MAC address.

[all]: Show the total switch configuration (default: System configuration only)

System>Config

System Configuration:

Name:

S/W Version: 1.02

CVS Tag: sw_8051_2_34d

Compile Date: Mar 28 2013 15:40:27

H/W Version: 1.0

MAC address: 00-40-F6-EA-12-34

SNMP: enabled

Trap IP: 0.0.0.0

Readcommunity: public

Writecommunity: private

Trapcommunity: public

Restore Default

System>Restore Default help

Syntax:

System Restore Default [*keepIP*]

Description:

Restore factory default configuration.

[keepIP]: Preserve IP configuration (default: Not preserved).

Name

System>Name help

Syntax:

System Name [<name>]

Description:

Set or show the system name.

[<name>]: String of up to 16 characters (default: Show system name).

Reboot

System>Reboot help

Syntax:

System Reboot

Description:

Reboot the switch.

SNMP

System>SNMP help

Syntax:

SNMP [enable/disable]

Description:

Activate or deactivate the SNMP.

[enable/disable]: Enable/disable SNMP (default: Show SNMP mode).

Trap

System>Trap help

Syntax:

Trap [<IP Address>]

Description:

Set or show SNMP traps destination.

<IP Address>: IP address to send traps to. (default: Show trap configuration)

Readcommunity

System>Readcommunity help

Syntax:

Readcommunity [<community string>]

Description:

Set or show SNMP read community string.

[<community string>]: New community string. (default: Show current value).

Writecommunity

System>Writecommunity help

Syntax:

Writecommunity [<community string>]

Description:

Set or show SNMP write community string.

[<community string>]: New community string. (default: Show current value).

Trapcommunity

System>Trapcommunity help

Syntax:

Trapcommunity [<community string>]

Description:

Set or show SNMP trap community string.

[<community string>]: New community string. (default: Show current value).

Power Saving

System>Power Saving help

Syntax:

Sytem Power Saving [full/up/down/disable]

Description:

Configure mode of power saving.

[full|up|down|disable]:

full: Power saving at both link-up and link-down.

up: Power saving at link-up only.

down: Power saving at link-down only.

disable: No power saving.

3.3 Console Commands

Console>?

Commands at Console level:

Console [Configuration](#)

Console [Password](#) [*<password>*]

Console [Timeout](#) [*<timeout>*]

Console [Prompt](#) [*<prompt string>*]

Configuration

Console> Configuration help

Syntax:

Console Configuration

Description:

Show configured console password and timeout.

Password

Console>Password help

Syntax:

Console Password [*<password>*]

Description:

Set or show the console password. The empty string ("") disables the password check.

[*<password>*]: Password string of up to 16 characters.

Timeout

Console>Timeout help

Syntax:

Console Timeout [*<timeout>*]

Description:

Set or show the console inactivity timeout in seconds. The value zero disables timeout.

[*<timeout>*]: Timeout value in seconds, 0,60-10000.

Prompt

Console>Prompt help

Syntax:

Console Prompt [*<prompt_string>*]

Description:

Set or show the console prompt string.

[*<prompt_string>*]: Command prompt string of up to 10 characters.

3.4 IP Commands

IP>help

Commands at IP level:

IP Configuration

IP Status

IP Setup [*<ipaddress>* [*<ipmask>* [*<ipgateway>*]]] [*<vid>*]

IP Mode [*enable/disable*]

IP Ping [*-n <count>*] [*-w <timeout>*] *<ipaddress>*

IP Arp

IP Dhcp [*enable/disable*]

Configuration

IP>Configuration help

Syntax:

IP Configuration

Description:

Show IP configured IP address, mask, gateway, VLAN ID and mode.

IP>config

IP Configuration:

Address: 192.168.0.2

Subnet Mask: 255.255.255.0

Gateway: 192.168.0.1

VID: 0

Mode: enabled

dhcp: disabled

Status

IP>Status help

Syntax:

IP Status

Description:

Show current IP status.

Setup

IP>Setup help

Syntax:

IP Setup [<ipaddress> [<ipmask> [<ipgateway>]]] [<vid>]

Description:

Setup or show IP configuration.

[<ipaddress>]: IP address. (default: Show IP configuration)

[<ipmask>]: IP subnet mask (default: Subnet mask for address class).

[<ipgateway>]: Default IP gateway, (default: 0.0.0.0).

[<vid>]: VLAN ID, 1-4094 (default: 1).

Mode

IP>Mode help

Syntax:

IP Mode [enable/disable]

Description:

Activate or deactivate the IP configuration.

[enable|disable]: Enable/disable IP (default: Show IP mode).

Ping

IP>Ping help

Syntax:

IP Ping [-n <count>][-w <timeout>] <ipaddress>

Description:

Ping the specified IP address.

[-n <count>]: Number of echo requests to send (default: 1).

[-w <timeout>]: Timeout in seconds to wait for each reply (default: 2).

Arp

IP>Arp help

Syntax:

IP Arp

Description:

Show the content of the ARP table.

Dhcp

IP>Dhcp help

Syntax:

IP DHCP [enable/disable]

Description:

Activate or deactivate the DHCP protocol.

[enable|disable]: Enable/disable DHCP (default: Show DHCP mode).

4. Web Management

The switch features an http server which can serve the management requests coming from any web browser software over TCP/IP network.

Compatible Web Browser

Compatible web browser software with JAVA script support

Microsoft Internet Explorer 6.0 or later

Google Chrome

Mozilla Firefox

Set IP Address for the System Unit

Before the switch can be managed from web browser software, make sure a unique IP address is configured for the switch.

4.1 Start Browser Software and Making Connection

Start your browser software and enter the IP address of the switch unit to which you want to connect. The IP address is used as URL for the browser software to search the device.

URL: `http://xxx.xxx.xxx.xxx/`

Factory default IP address: 192.168.0.2

4.2 Login to the Switch Unit

When browser software connects to the switch unit successfully, a Login screen is provided for you to login to the device as the left is played below:



Duplicated Administrator
This device is managed by 192.168.0.102
currently!!

Factory default password: 123

The switch will accept only one successful IP connection at the same time. The other connection attempts will be prompted with a warning message as the right is played above.

A new connection will be accepted when the current user logout successfully or auto logout by the switch due to no access for time out of 300 seconds.

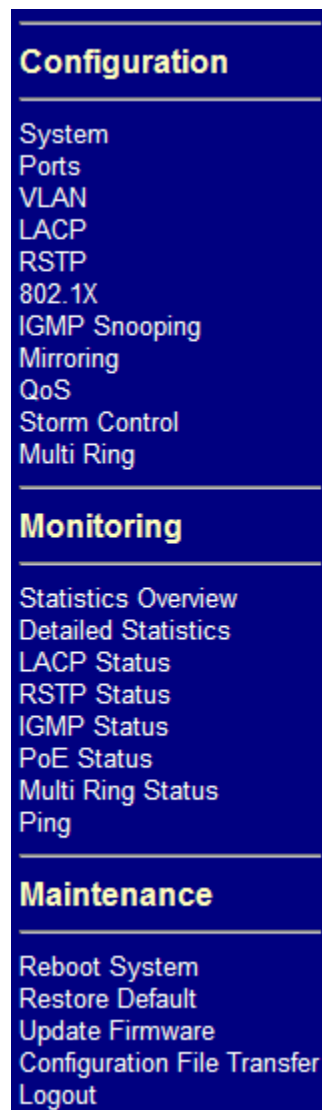
System Configuration is displayed as follows after a successful login:

System Configuration

MAC Address	00-40-F6-E0-00-12
S/W Version	1.04 Beta 20130903PM1544
H/W Version	1.0
Active IP Address	192.168.0.174
Active Subnet Mask	255.255.255.0
Active Gateway	0.0.0.0
DHCP Server	0.0.0.0
Lease Time Left	0 secs

DHCP Enabled	<input type="checkbox"/>
Fallback IP Address	<input type="text" value="192.168.0.174"/>
Fallback Subnet Mask	<input type="text" value="255.255.255.0"/>
Fallback Gateway	<input type="text" value="0.0.0.0"/>
WDT	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Management VLAN	<input type="text" value="0"/>
Name	<input type="text"/>
Password	<input type="password" value="•••"/>
Inactivity Timeout (seconds)	<input type="text" value="300"/> (0 or 60~10000)
SNMP enabled	<input checked="" type="checkbox"/>
SNMP Trap destination	<input type="text" value="0.0.0.0"/>
SNMP Read Community	<input type="text" value="public"/>
SNMP Write Community	<input type="text" value="private"/>
SNMP Trap Community	<input type="text" value="public"/>

4.3 Main Management Menu



Configuration

System	Switch information, system and IP related settings
Ports	Port link status, port operation mode configuration
VLAN	VLAN related configuration
LACP	LACP configuration for port link aggregation
RSTP	RSTP (Rapid spanning tree protocol) related configuration
802.1X	802.1X authentication related configuration
IGMP Snooping	IGMP snooping related configuration
Mirroring	Port mirroring related configuration
QoS	Quality of Service related configuration
Storm Control	Packet Storm protection control configuration
Multi Ring	Multiple Redundant Rings configuration

Monitoring

Statistics Overview	List simple statistics for all ports
Detailed Statistics	List detailed statistics for all ports
LACP Status	LACP port status
RSTP Status	RSTP protocol status
IGMP Status	IGMP snooping status
PoE Status	Power over Ethernet function status
Multi Ring Status	Multi redundant ring status
Ping	Ping command from the switch to other IP devices

Maintenance

Reboot System	Command to reboot the switch
Restore Default	Command to restore the switch with factory default settings
Update Firmware	Command to update the switch firmware
Configuration File Transfer	Command to transfer (upload/download) configuration file
Logout	Command to logout from the switch management

4.4 System

System Configuration

MAC Address	00-40-F6-E0-00-12
S/W Version	1.04 Beta 20130903PM1544
H/W Version	1.0
Active IP Address	192.168.0.174
Active Subnet Mask	255.255.255.0
Active Gateway	0.0.0.0
DHCP Server	0.0.0.0
Lease Time Left	0 secs

DHCP Enabled	<input type="checkbox"/>
Fallback IP Address	<input type="text" value="192.168.0.174"/>
Fallback Subnet Mask	<input type="text" value="255.255.255.0"/>
Fallback Gateway	<input type="text" value="0.0.0.0"/>
WDT	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Management VLAN	<input type="text" value="0"/>
Name	<input type="text"/>
Password	<input type="password" value="..."/>
Inactivity Timeout (seconds)	<input type="text" value="300"/> (0 or 60~10000)
SNMP enabled	<input checked="" type="checkbox"/>
SNMP Trap destination	<input type="text" value="0.0.0.0"/>
SNMP Read Community	<input type="text" value="public"/>
SNMP Write Community	<input type="text" value="private"/>
SNMP Trap Community	<input type="text" value="public"/>

Configuration	Description
MAC Address	The MAC address factory configured for the switch. It can not be changed in any cases.
S/W Version	Firmware version currently running
H/W Version	Hardware version currently operating
Active IP Address	Current IP address for the switch management

Active Subnet Mask	Current subnet mask for IP address for the switch management
Active Gateway	Current gateway IP address for the switch management
DHCP Server	Current IP address of the DHCP server
Lease Time Left	The time left for the lease IP address currently used
DHCP Enabled	Use DHCP to get dynamic IP address configuration for the switch
Fallback IP Address	IP address used when DHCP mode is disabled
Fallback Subnet Mask	Subnet mask for IP address used when DHCP mode is not enabled
Fallback Gateway	Default gateway IP address used when DHCP mode is not enabled
WDT	Watch Dog Timer configuration
Management VLAN	Set management VLAN ID
Name * ¹	Set the system name for this switch unit
Password	Set new password
Inactivity Timeout	No user interaction timeout for web disconnection. Options: 0 - no timeout 60 ~ 10000 seconds
SNMP enabled	Enable SNMP agent
SNMP Trap destination	The IP address of the SNMP trap manager
SNMP Read community	SNMP community allowed for the SNMP [get] message
SNMP Write community	SNMP community allowed for the SNMP [set] message
SNMP Trap community	SNMP community used for the SNMP trap messages sent by the switch
<hr/>	
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration
<hr/>	

Note:

1. *It is suggested to give each switch unit a system name as an alternative unique identification beside IP address.*
2. *Setting change of DHCP mode takes effective in next boot-up.*

4.4.1 Management VLAN

Management VLAN settings allow administrator to access the switch and perform the switch management over a dedicated VLAN.

The following rules are applied with the Management VLAN:

1. If [Management VLAN] setting is zero, no VLAN limitation is applied in accessing the switch web management interface.
2. If [Management VLAN] setting is not zero, the switch web (http) server only replies to the management hosts located in the matched VLAN group. That means the egress port will be limited in the member ports of the matched VLAN group.
3. The switch web (http) server can accept untagged or tagged management accessing packets. Reply to the web access host based on the following rule:

Incoming web access packets	Reply packets (Outgoing to the management host)
Untagged packets	Untagged packets
Tagged packets	Packets tagged with configured management VLAN ID

4. The system will cross-check VLAN group table and reject un-existing VLAN setting during configuring Management VLAN value.
5. If VLAN group configuration causes a result that no VLAN group matches the management VLAN setting, the management VLAN setting will be reset to zero by the system automatically.

Notes:

1. *To apply management VLAN function, be sure to configure a VLAN group that matches the management VLAN first.*
2. *No matter how management VLAN is configured, login password authentication is still required.*

4.5 Ports

Port Configuration

Enable Jumbo Frames	<input type="checkbox"/>			
Power Saving Mode:	Disable ▾			
Port	Link	Mode	Flow Control	PoE Enable
1	Down	Auto Speed ▾	<input type="checkbox"/>	<input type="checkbox"/>
2	100FDX	Auto Speed ▾	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3	Down	Auto Speed ▾	<input type="checkbox"/>	<input type="checkbox"/>
4	Down	Auto Speed ▾	<input type="checkbox"/>	<input type="checkbox"/>
5	Down	Auto Speed ▾	<input type="checkbox"/>	<input type="checkbox"/>
6	Down	Auto Speed ▾	<input type="checkbox"/>	<input type="checkbox"/>
7(GE FX)	Down	Auto 1000 Full ▾	<input type="checkbox"/>	<input type="checkbox"/>
8(GE FX)	1000FDX	Auto 1000 Full ▾	<input type="checkbox"/>	<input type="checkbox"/>
Drop frames after excessive collisions	<input type="checkbox"/>			
FX DDM		Port Type		
Apply		Refresh		

Configuration	Function
Enable Jumbo Frames	Set to enable jumbo frame support
Power Saving Mode	<i>Full</i> - all the time <i>Link-up</i> - power saving only when link up <i>Link-down</i> - power saving only when link down <i>Disable</i> - disable port power saving
Port	The port number Ex. 8 Indicates Port 8 media type – M12 (Copper interface) 8(GE FX) Indicates Port 8 current media type – Gigabit fiber interface 8(FE FX) Indicates Port 8 current media type – Fast Ethernet fiber interface In some model options, Port 7 and Port 8 support dual media. Use [Port Type] button to change media type to be used. (GE FX) and (FE FX) are model-dependent.
Link	Speed and duplex status with green background - port is link on

Down with red background - port is link down

Mode

Select port operating mode

Disabled - disable the port operation

Mode	Auto-negotiation	Speed capability	Duplex capability
Auto	Enable	10, 100, 1000M	Full, Half
10 Half	Disable	10M	Half
10 Full	Disable	10M	Full
100 Half	Disable	100M	Half
100 Full	Disable	100M	Full
1000 Full	Enable	1000M	Full
Auto 1000 Full	Enable	1000M	Full
Force 1000 Full	Disable	1000M	Full

Flow Control

Set port flow control function

v - set to enable 802.3x pause flow control for ingress and egress

PoE Enable

Set port PoE PSE function

v - set to enable port PoE PSE function (Optional model-dependent function)

Drop frame after excessive collision

v - set to enable the function

[FX DDM]

Click to display DDM information and status of the fiber transceivers

[Port Type]

Click to set port media type, <M12> or <Fiber> for Port 7 and Port 8 options

[Apply]

Click to apply the configuration change

Above port configuration example illustrates that both Port #7 and Port #8 are equipped with two media interfaces, M12 copper interface and FX fiber interface. Click [Port Type] button to select preferred media type.

4.5.1 Port Type

Port 7 and Port 8 supports two media types, M12 copper and FX fiber interface. Use this button to select the port type.

Port Type Configuration

The screenshot shows a configuration window titled "Port Type Configuration". It contains two rows of controls. The first row is for "Port 7" and has a dropdown menu currently showing "Fiber". The second row is for "Port 8" and has two radio buttons: "M12" and "Fiber", with "Fiber" selected. At the bottom of the window are two buttons: "Apply" and "Back".

Information	Function
Port #	Port number (Port 7 & Port 8)
Type	<p>Only Port 7 and Port 8 support dual media types, M12 copper and FX fiber and the available options are model-dependent. For fiber support, the port is built-in with an internal fiber transceiver.</p> <p><i>M12</i> Use Copper interface <i>Fiber</i> Use fiber interface.</p> <p>If <M12> is the only available option, the associated port does not support fiber media.</p>

Notes:

The available mode options are:

<u>Mode (M12)</u>	<u>Auto-negotiation</u>	<u>Speed capability</u>	<u>Duplex capability</u>
<i>Auto</i>	<i>Enable</i>	<i>10, 100, 1000M</i>	<i>Full, Half</i>
<i>10 Half</i>	<i>Disable</i>	<i>10M</i>	<i>Half</i>
<i>10 Full</i>	<i>Disable</i>	<i>10M</i>	<i>Full</i>
<i>100 Half</i>	<i>Disable</i>	<i>100M</i>	<i>Half</i>
<i>100 Full</i>	<i>Disable</i>	<i>100M</i>	<i>Full</i>
<i>1000 Full</i>	<i>Enable</i>	<i>1000M</i>	<i>Full</i>

<u>Mode (GE FX)</u>	<u>Auto-negotiation</u>	<u>Speed capability</u>	<u>Duplex capability</u>
<i>Auto 1000 Full</i>	<i>Enable</i>	<i>1000M</i>	<i>Full</i>
<i>Force 1000 Full</i>	<i>Disable</i>	<i>1000M</i>	<i>Full</i>

<u>Mode (FE FX)</u>	<u>Auto-negotiation</u>	<u>Speed capability</u>	<u>Duplex capability</u>
<i>Force 100 Full</i>	<i>Disable</i>	<i>100M</i>	<i>Full</i>

4.5.2 FX DDM Status

DDM (Digital Diagnostic Monitoring) information and status are provided in some transceivers. Part of the information are retrieved and listed as follows:

FX DDM

Port	7	8
Identifier	SFP transceiver	SFP transceiver
Connector	LC	LC
SONET Compliance	N/A	N/A
Ethernet Compliance	1000BASE-SX	1000BASE-LX
Vendor Name	APAC Opto	APAC Opto
Vendor OUI	000F99	000F99
Temperature	N/A	42.41 (°C)
Voltage	N/A	3.37 (V)
TX Power	N/A	-5.68 (dBm)

Refresh Back

Information	Function
Port	Port number which has fiber interface
Identifier	The identifier information of the fiber transceiver
Connector	The connector type used on the fiber transceiver
SONET Compliance	SONET compliance information of the transceiver
GbE Compliance	Gigabit Ethernet compliance information of the transceiver
Vendor Name	The vendor name of the transceiver
Vendor OUI	The vendor OUI of the transceiver
Temperature	The current temperature sensed inside the transceiver
Voltage	The working voltage sensed inside the transceiver
TX Power	The transmission optical power sensed
[Refresh]	Click to refresh current configuration
[Back]	Click to back to previous page

Note:

1. TX power data is displayed with unit of dBm.
2. N/A: the information is not available in the transceiver

4.6 VLANs

VLAN Configuration

- VLAN Disable
- Port-based VLAN Mode > [Setting](#)
- Port-based VLAN ISP Mode > [Setting](#)
- Simplified Tag-based VLAN Mode > [Setting](#)
- Advanced VLAN Mode > [Setting](#)

Apply

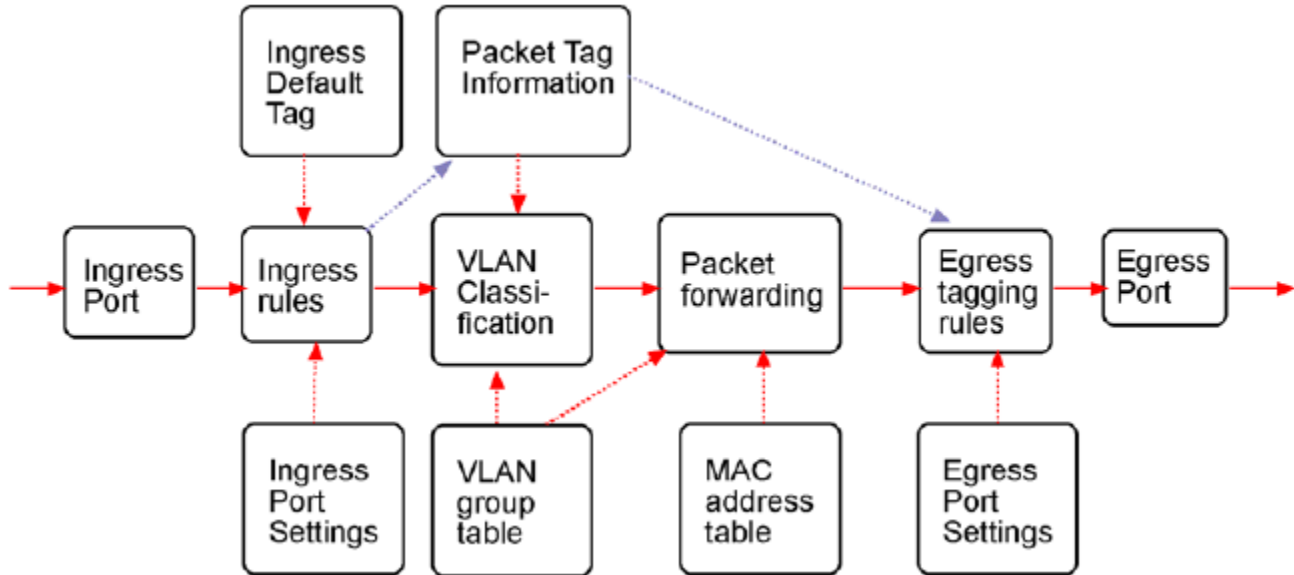
Refresh

VLAN Configuration	Description
VLAN Disable	Select to disable VLAN function All ports are allowed to communicate with each others freely with no VLAN limitation.
Port-based VLAN Mode	Simple configuration for 2 port-based VLAN groups
Port-based VLAN ISP Mode	Simple configuration for 7 port-based VLAN groups (also called metro-mode sometimes)
Simplified Tag-based VLAN Mode	Simple configuration for Tag-based VLAN (Less optional settings)
Advanced VLAN Mode	Full VLAN configuration for port-based and Tag-based VLAN

[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration

4.6.1 VLAN Function

The switch can support port-based VLAN, 802.1Q Tag VLAN and eight VLAN groups. The following figure illustrates the basic VLAN operation flow beginning from a packet received on an ingress port until it is transmitted from an egress port.



The following sections describe the VLAN processes and Advanced VLAN mode settings provided by the switch. A global setting means the setting is applied to all ports of the switch. A per port setting means each port can be configured for the setting respectively.

Ingress Rules

When a packet is received on an ingress port, the ingress rules are applied for packet filtering and packet tag removal. The related Ingress port settings are:

802.1Q Tag Aware Per port setting

Tag-aware - 802.1Q Tag Aware mode is used. The switch examines the tag content of every received packet. For a VLAN tagged packet, the packet VLAN tag data is retrieved as packet tag information for VLAN classification and egress tagging operation. For untagged packet and priority-tagged packet, port-based mode is used.

Tag-ignore - Port-based mode is used. The switch ignores the tag content of every received packets. Ingress Port Default Tag is always used as packet tag information for VLAN classification.

Keep Tag Per port setting

Enable - The VLAN tag in the received VLAN tagged packet will be kept as it is and is not stripped in whole forwarding operation.

Disable - The VLAN tag data in the received VLAN tagged packet is stripped (removed).

Drop Untag Per Port Setting

Enable - All untagged packets and priority-tagged packets are dropped. A priority-tagged packet is treated as an untagged packet in this switch. Only VLAN-tagged packets are admitted.

Disable - Disable untagged packet filtering

Drop Tag Per Port Setting

Enable - All VLAN-tagged packets are dropped. A priority-tagged packet is treated as an untagged packet in this switch. Only untagged packets are admitted.

Disable - Disable VLAN-tagged packet filtering

Ingress Default Tag Per Port Setting

Each port can be configured with one Ingress Default Tag. This ingress port default tag is used when ingress port is in Tag-ignore mode or for the received untagged packets in Tag-aware mode. The Ingress Default Tag includes PVID, CFI and User Priority configuration.

When Ingress port default tag is used, it is copied as packet associated Packet Tag Information for VLAN classification. The PVID is used as index to one VLAN group in VLAN group table.

Packet Tag Information

Under VLAN process, every packet is associated with one Packet Tag information in packet forwarding operation. The tag information includes VID, CFI and User Priority data and is used for two purposes:

- The VID in tag is used as index for VLAN classification.
- The tag is used for egress tag insertion if egress tagging is enabled.

The following table lists how the Packet Tag information is generated:

<u>Tag Aware setting</u>	<u>Received Packet Type</u>	<u>Packet Tag information source</u>
<i>Tag-ignore</i>	Untagged packet	Ingress Port Default Tag
<i>Tag-ignore</i>	Priority-tagged packet	Ingress Port Default Tag
<i>Tag-ignore</i>	VLAN-tagged packet	Ingress Port Default Tag
<i>Tag-aware</i>	Untagged packet	Ingress Port Default Tag
<i>Tag-aware</i>	Priority-tagged packet	Ingress Port Default Tag
<i>Tag-aware</i>	VLAN-tagged packet	Received packet VLAN Tag

VLAN Group Table Configuration

The switch provides a table of eight VLAN groups to support up to eight VLANs at the same time. Each VLAN group is associated to one unique VLAN. The table is referred for VLAN classification.

A VLAN group contains the following configuration settings:

- VID:* 12-bit VLAN Identifier index to the VLAN to which the group is associated
- Member Ports:* The admitted egress ports for packets belonging to this VLAN
- Source Port Check:* The ingress port of the packet must also be the member port of this VLAN. Otherwise, the packet is discarded.

VLAN Classification

VLAN classification is a process to classify a VLAN group to which a received packet belongs. The VID of the generated Packet Tag information associated to the received packet is used as an index for VLAN group table lookup. The VID matched VLAN group will be used for packet forwarding. If no matched VLAN group is found in table lookup, the packet is dropped.

Refer to section 4.6.1.7 for details of how Packet Tag information is generated.

The member ports specified in the matched VLAN group are the admitted egress port range for the packet. The packet will never be forwarded to other ports which are not in the member ports.

The Source Port Check setting of the matched VLAN group is also referred. If it is enabled, the ingress port will be checked whether it is a member port of this group.

Packet Forwarding

The forwarding is a process to forward the received packet to one or more egress ports. The process uses the following information as forwarding decision:

Member ports of the matched VLAN group: the egress port range for forwarding

Source Port Check setting of the matched VLAN group: check ingress port membership

The packet destination MAC address: for MAC address table loop up

The switch MAC address table: to find the associated port where a MAC address is learned

If the MAC address table lookup is matched and the learned port is the VLAN member port, the packet is forwarded to the port (egress port). If the lookup failed, the switch will broadcast the packet to all member ports.

Egress Tagging Rules

Egress Tagging rules are used to make change to the packet before it is stored into egress queue of an egress port. The egress settings are provided for each port and are described as follows:

Egress Settings

Insert Tag (per port setting)

Enable - Insert the Tag data of the associated Packet Tag information into the packet

Disable - No tagging is performed.

Untagging Specific VID (per port setting)

Enable - No tag insertion if the VID data of the associated Packet Tag information matches the Untagged VID configured in next setting even [Insert Tag] is enabled.

Disable - This rule is not applied.

Summary of VLAN Function

VLAN Modes (Configuration methods)

Port-based VLAN Mode: Simple UI to configure Port-based 2-VLAN-groups

Port-based VLAN ISP Mode: Simple UI to configure Port-based 7-VLAN-groups

Simplified VLAN Mode: Simple UI to configure Tag-based VLAN

Advanced VLAN Mode: Full VLAN configuration for port-based and Tag-based VLAN

VLAN range supported: 1 ~ 4095 (eight VLANs at the same time)

[PVID] [VID] [Untagged VID] value range: 1 ~ 4095

4.6.2 Port-based VLAN Mode

VLAN Configuration

- VLAN Disable
- Port-based VLAN Mode > [Setting](#)
- Port-based VLAN ISP Mode > [Setting](#)
- Simplified Tag-based VLAN Mode > [Setting](#)
- Advanced VLAN Mode > [Setting](#)

Port-based VLAN Mode

Group	Member ports							
	1	2	3	4	5	6	7	8
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

=>

Configuration	Description
Group 1, 2	Port-based VLAN group number
Member ports	Select member ports for the group
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration
[Back]	Click to go back to upper menu

Operation in this mode:

1. The member ports of two groups are allowed to overlap.
2. The member ports in same group can communicate with other members only.
3. No packet tag is examined.
4. A received packet will not be modified (i.e. tagging or untagging) through VLAN operation till it is transmitted.

Note:

VLAN group 1 is configured with VID (VLAN ID) 1 and group 2 is configured with VID 2 by the system automatically.

4.6.3 Port-based VLAN ISP Mode

VLAN Configuration

- VLAN Disable
- Port-based VLAN Mode > [Setting](#)
- Port-based VLAN ISP Mode > [Setting](#)
- Simplified Tag-based VLAN Mode > [Setting](#)
- Advanced VLAN Mode > [Setting](#)

Port-based VLAN ISP Mode

Joint port

=>

Configuration	Description
Joint port	Select a port as the joint port for all 7 port-based VLAN groups
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration
[Back]	Click to go back to upper menu

Example:

If Port 8 is selected as the joint port, the 7 port-based VLAN groups are configured as follows automatically:

*Group 1 - member [Port 1, Port 8], Group 2 - member [Port 2, Port 8]
Group 3 - member [Port 3, Port 8], Group 4 - member [Port 4, Port 8]
Group 5 - member [Port 5, Port 8], Group 6 - member [Port 6, Port 8]
Group 7 - member [Port 7, Port 8]*

Mode Operation:

1. The joint port is the shared member port for all groups.
2. Two member ports are configured in each group.
3. The member ports in same group can communicate with other only.
4. No packet tag is examined.
5. A received packet will not be modified (i.e. tagging or untagging) through VLAN operation till it is transmitted.

Note:

The seven groups are configured with associated VID 1 ~ 7 respectively by the system.

4.6.4 Simplified Tag-based VLAN Mode

VLAN Configuration

- VLAN Disable
- Port-based VLAN Mode > [Setting](#)
- Port-based VLAN ISP Mode > [Setting](#)
- Simplified Tag-based VLAN Mode > [Setting](#)
- Advanced VLAN Mode > [Setting](#)

Apply

Refresh

=>

Simplified Tag-based VLAN Mode

VLAN Groups

VLAN Per Port

VLAN Groups

Group	VID	Member Ports								Source Port Check
		1	2	3	4	5	6	7	8	
1	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Disable ▾
2	2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disable ▾
3	3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disable ▾
4	4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disable ▾
5	5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disable ▾
6	6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disable ▾
7	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disable ▾
8	8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disable ▾

Apply

Refresh

Back

Configuration

Description

[VLAN Groups]

Click to configure VLAN groups first

[VLAN Per Port]

Click to configure per port simplified VLAN settings

4.6.4.1 VLAN Groups

Configuration	Description
Group	Group number
VID	VID of the VLAN to which this group is associated <i>1 ~ 4095</i> - decimal 12-bit VID value
Member Ports	Select the admitted egress ports for the packets belong to the VLAN Port 1 ~ 8 - click to select
Source Port Check	Check whether the ingress port is the member port of the VLAN <i>Enable</i> - set to enable this check, the packet is dropped if ingress port is not member port of the VLAN. <i>Disable</i> - set to disable this check
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration
[Back]	Click to go back to upper menu

Note: This VLAN group configuration is also applied to Advanced VLAN configuration

4.6.4.2 Per Port Settings

VLAN Per Port

Port	Ingress		Egress	
	PVID	Drop Untag	Egress Tagging	Untagged VID
1	1	Disable	UnTag	1
2	1	Disable	UnTag	1
3	1	Disable	UnTag	1
4	1	Disable	UnTag	1
5	1	Disable	UnTag	1
6	1	Disable	UnTag	1
7	1	Disable	UnTag	1
8	1	Disable	UnTag	1

Configuration	Description
Port	Port number
PVID	Port VID, VID of Ingress Default Tag (See section 4.6.4.1) 1 ~ 4095 - decimal 12-bit VID value
Drop Untag	Drop all untagged packets and priority-tagged packets (ingress) <i>Enable</i> - drop untagged packets and priority-tagged packets <i>Disable</i> - admit untagged packets and priority-tagged packets
Egress Tagging	Tagging rule for egress operation <i>Tag</i> - Tagging all egress packets <i>Untag</i> - No tagging for all egress packets <i>Specific Tag</i> - Tagging egress packets except those matched [Untagged VID]
Untagged VID	VID for Specific Tag in [Egress Tagging] setting 1 ~ 4095 - decimal 12-bit VID value
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration
[Back]	Click to go back to upper menu

4.6.4.3 Simplified Tag-based VLAN Operation

Ingress filtering setting [Drop Untag] = Enable

<u>Ingress Packets</u>	<u>Rule</u>
Untagged packets	Dropped
Priority packets	Dropped
Tagged packets	Admitted to get into forwarding operation

Ingress filtering setting [Drop Untag] = Disable

<u>Ingress Packets</u>	<u>Rule</u>
Untagged packets	Admitted to get into forwarding operation
Priority packets	Admitted to get into forwarding operation
Tagged packets	Admitted to get into forwarding operation

Ingress filtering setting [Drop Untag] = Disable

Egress rule setting [Egress Tagging] = Tag

<u>Ingress Packets</u>	<u>Egress rule</u>
Untagged packets	Tagging with Ingress Default Tag* (Tagging)
Priority packets	Tagging with Ingress Default Tag* (Tagging)
Tagged packets	Egress with no packet modification

* *Ingress Default Tag = Ingress port PVID + CFI (0) + User priority (0)*

Ingress filtering setting [Drop Untag] = Disable

Egress rule setting [Egress Tagging] = Untag

<u>Ingress Packets</u>	<u>Egress rule</u>
Untagged packets	Egress with no packet modification (untagged)
Priority packets	Egress with no packet modification (untagged)
Tagged packets	Tag is removed (Untagging)

* *Ingress Default Tag = Ingress port PVID + CFI (0) + User priority (0)*

Ingress filtering setting [Drop Untag] = Disable

Egress rule setting [Egress Tagging] = Specific Tag

<u>Ingress Packets</u>	<u>Egress rule</u>
Untagged packets	Tagging with Ingress Default Tag* (Tagging)
Priority packets	Tagging with Ingress Default Tag* (Tagging)
Tagged packets	Egress with no packet modification except the packets with VID equal to [Untagged VID] setting*

* Ingress Default Tag = Ingress port PVID + CFI (0) + User priority (0)
& not equal to [Untagged VID] setting

* The packets with VID equal to [Untagged VID] setting are removed the tag.

For more information about Ingress Default Tag, refer to section 4.6.1.

4.6.5 Advanced VLAN Mode

VLAN Configuration

- VLAN Disable
- Port-based VLAN Mode > [Setting](#)
- Port-based VLAN ISP Mode > [Setting](#)
- Simplified Tag-based VLAN Mode > [Setting](#)
- Advanced VLAN Mode > [Setting](#)

Apply

Refresh

Advanced VLAN Mode

Ingress Default Tag

Ingress Settings

Egress Settings

VLAN Groups

Configuration	Description
Ingress Default Tag	Click to configure per port Ingress Default Tag settings
Ingress Settings	Click to configure per port ingress settings
Egress Settings	Click to configure per port egress settings
VLAN Groups	Click to configure VLAN group table

4.6.5.1 Ingress Default Tag

Ingress Default Tag

Port	PVID	CFI	User Priority
1	1	0	0
2	1	0	0
3	1	0	0
4	1	0	0
5	1	0	0
6	1	0	0
7	1	0	0
8	1	0	0

Apply Refresh Back

Configuration	Description
Port	Port number
PVID	Port VID, VID for Ingress Default Tag <i>1 ~ 4095</i> - decimal 12-bit VID value
CFI	CFI for Ingress Default Tag <i>0, 1</i> - 1-bit CFI value
User Priority	User priority for Ingress Default Tag <i>0 ~ 7</i> - decimal 3-bit value
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration
[Back]	Click to go back to upper menu

PVID is used as index for VLAN classification (VLAN group table lookup) in one of the following conditions:

1. Ingress port [Tag Aware] setting = Tag-ignore
2. Ingress port [Tag Aware] setting = Tag-aware
and the received packet is untagged or priority-tagged

[PVID+CFI+User Priority] = Ingress Default Tag for the ingress port

It is used as the tag for insertion in egress tagging operation in one of the following conditions:

1. Ingress port [Tag Aware] setting = Tag-ignore, Egress port [Insert Tag] = Enable
2. Ingress port [Tag Aware] setting = Tag-aware, Egress port [Insert Tag] = Enable
and the received packet is untagged or priority-tagged

4.6.5.2 Ingress Settings

Ingress Settings

Port	Tag Aware	Keep Tag	Drop Untag	Drop Tag
1	Tag-aware ▾	Disable ▾	Disable ▾	Disable ▾
2	Tag-aware ▾	Disable ▾	Disable ▾	Disable ▾
3	Tag-aware ▾	Disable ▾	Disable ▾	Disable ▾
4	Tag-aware ▾	Disable ▾	Disable ▾	Disable ▾
5	Tag-aware ▾	Disable ▾	Disable ▾	Disable ▾
6	Tag-aware ▾	Disable ▾	Disable ▾	Disable ▾
7	Tag-aware ▾	Disable ▾	Disable ▾	Disable ▾
8	Tag-aware ▾	Disable ▾	Disable ▾	Disable ▾

Configuration	Description
Port	Port number
Tag Aware	Check tag data for every received packet <i>Tag-aware</i> - set to activate Tag-based mode <i>Tag-ignore</i> - set to use port-based mode and ignore any tag in packet
Keep Tag	Tag is removed from the received packet if exists <i>Enable</i> - set to activate tag removal for VLAN-tagged packets <i>Disable</i> - set to disable tag removal function
Drop Untag	Drop all untagged packets and priority-tagged packets <i>Enable</i> - drop untagged packets and priority-tagged packets <i>Disable</i> - admit untagged packets and priority-tagged packets
Drop Tag	Drop all VLAN-tagged packets <i>Enable</i> - drop VLAN-tagged packets <i>Disable</i> - admit VLAN-tagged packets
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration

Note:

1. Priority-tagged packet (VID=0) is treated as untagged packet in the switch.
2. [Tag Aware] setting affects the index used for VLAN classification (VLAN table lookup). The following

table lists the index used:

Ingress [Tag Aware] setting

<u>Received packet type</u>	<u>Tag-ignore</u>	<u>Tag-aware</u>
<i>Untagged</i>	<i>PVID</i>	<i>PVID</i>
<i>Priority-tagged (VID=0)</i>	<i>PVID</i>	<i>PVID</i>
<i>VLAN-tagged (VID>0)</i>	<i>PVID</i>	<i>Packet tag VID</i>

3. Both [Drop Untag] and [Drop Tag] are set to Disable to admit all packets.

4.6.5.3 Egress Settings

Egress Settings

Port	Insert Tag	Untagging Specific VID	Untagged VID
1	Disable ▾	Disable ▾	1
2	Disable ▾	Disable ▾	1
3	Disable ▾	Disable ▾	1
4	Disable ▾	Disable ▾	1
5	Disable ▾	Disable ▾	1
6	Disable ▾	Disable ▾	1
7	Disable ▾	Disable ▾	1
8	Disable ▾	Disable ▾	1

Configuration

Description

Port	Port number
Insert Tag	Activate tagging (Insert a tag to the packet) <i>Enable</i> - set to activate tagging <i>Disable</i> - set to disable tagging function
Untagging Specific VID	No tag insertion if packet tag information matches [Untagged VID] <i>Enable</i> - set to enable this function <i>Disable</i> - set to disable this function
Untagged VID	VID for [Untagging Specific VID] setting <i>1 ~ 4095</i> - decimal 12-bit VID value

[Apply] Click to apply the configuration change

[Refresh] Click to refresh current configuration

[Back] Click to go back to upper menu

The inserted tag sources when [Insert Tag] = Enable are listed as follows:

Received packet type [Tag Aware]=Tag-ignore [Tag Aware]=Tag-aware

Untagged	Ingress Default Tag	Ingress Default Tag
Priority-tagged (VID=0)	Ingress Default Tag	Ingress Default Tag
VLAN-tagged (VID>0)	Ingress Default Tag	Packet own tag

4.6.5.4 VLAN Groups

VLAN Groups

Group	VID	Member Ports								Source Port Check
		1	2	3	4	5	6	7	8	
1	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Disable ▾
2	2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disable ▾
3	3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disable ▾
4	4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disable ▾
5	5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disable ▾
6	6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disable ▾
7	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disable ▾
8	8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Disable ▾

[Apply]

[Refresh]

[Back]

Configuration	Description
Group	Group number
VID	VID of the VLAN to which this group is associated <i>1 ~ 4095</i> - decimal 12-bit VID value
Member Ports	Select the admitted egress ports for the packets belong to the VLAN Port 1 ~ 8 - click to select
Source Port Check	Check whether the ingress port is the member port of the VLAN <i>Enable</i> - set to enable this check, the packet is dropped if ingress port is not member port of the VLAN. <i>Disable</i> - set to disable this check
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration
[Back]	Click to go back to upper menu

Note: This VLAN groups configuration is also applied to Advanced VLAN configuration.

4.6.6 Simplified Tag-based VLAN vs. Advanced VLAN

Simplified Tag-based mode comes from “Advanced” mode actually. Some optional settings in “Advanced” mode are pre-configured and hidden for no change under Simplified mode. The following table lists the setting relations between Simplified mode and Advanced:

Hidden Advanced settings & pre-configured value in Simplified Mode

<u>Setting</u>	<u>Value</u>
[CFI]	0
[User Priority]	0
[Tag Aware]	enable
[Keep Tag]	disable
[Drop Tag]	disable

Simplified Mode [Egress Tagging] is equal to combination of Advanced Mode [Insert Tag] & [Untagging Specific VID]. The setting options are:

Simplified Mode	Advanced Mode	
<u>[Egress Tagging]</u>	<u>[Insert Tag]</u>	<u>[Untagging Specific VID]</u>
Tag	Enable	Disable
Untag	Disable	Disable
Specific Tag	Enable	Enable

4.6.7 Important Notes for VLAN Configuration

Some considerations should be checked in configuring VLAN settings:

1. Switch VLAN Mode selection

It is suggested to evaluate your VLAN application first and plan your VLAN configuration carefully before applying it. Any incorrect setting might cause network problem.

2. Aggregation/Trunking configuration

Make sure the members of a link aggregation (trunk) group are configured with same VLAN configuration and are in same VLAN group.

3. Double Tagged in Advanced VLAN Mode

For a received packet, Ingress port [Keep Tag] setting and Egress port [Insert Tag] setting are enabled at the same time. It will cause the packet double-tagged when egress. Although, it is often applied in Q-in-Q provider bridging application. However, such condition should be avoided in normal VLAN configuration. See table below:

Settings		Ingress port	Egress port
<u>[Keep Tag]</u>	<u>[Insert Tag]</u>	<u>> Received Packet</u>	<u>> Packet Transmitted</u>
Enable	Enable	Priority-tagged	Double-tagged
Enable	Enable	VLAN-tagged	Double-tagged

4.7 LACP

LACP Port Configuration

Port	Protocol Enabled	Key Value
1	<input type="checkbox"/>	auto
2	<input type="checkbox"/>	auto
3	<input type="checkbox"/>	auto
4	<input type="checkbox"/>	auto
5	<input type="checkbox"/>	auto
6	<input type="checkbox"/>	auto
7	<input type="checkbox"/>	auto
8	<input type="checkbox"/>	auto

Apply

Refresh

Configuration	Description
Port	Port number
Protocol Enabled	Enable LACP support for the port
Key Value	An integer value assigned to the port that determines which ports are aggregated into an LACP link aggregate. Set same value to the ports in same LACP link aggregate. Value: 1 ~ 255. Auto - key value is assigned by the system
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration

Notes:

1. This configuration is used to configure LACP aggregate groups.
2. The ports which have same key value are in same LACP aggregate group.
3. The ports with Auto key are in same LACP aggregate group.
4. The ports configured in non-LACP aggregation are not available in this configuration.

4.8 RSTP

RSTP System Configuration

System Priority	32768 ▾
Hello Time	2
Max Age	20
Forward Delay	15
Force version	Normal ▾

RSTP Port Configuration

Port	Protocol Enabled	Edge	Path Cost
Aggregations	<input type="checkbox"/>		
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
7	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto
8	<input type="checkbox"/>	<input checked="" type="checkbox"/>	auto

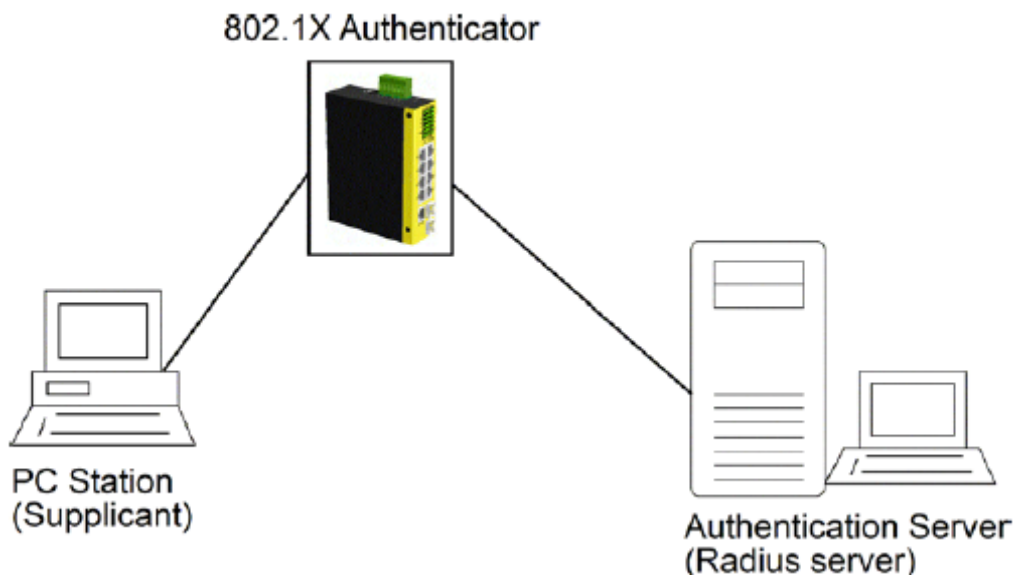
Apply Refresh

Configuration	Description
System Priority	The lower the bridge priority is the higher priority it has. Usually, the bridge with the highest bridge priority is the root. Value: 0 ~ 61440
Hello Time	Hello Time is used to determine the periodic time to send normal BPDU from designated ports among bridges. It decides how long a bridge should send this message to other bridge to tell I am alive. Value: 1 ~ 10
Max Age	When the switch is the root bridge, the whole LAN will apply this setting as their maximum age time. Value: 6 ~ 40
Forward Delay	This figure is set by Root Bridge only. The forward delay time is defined as the time spent from Listening state moved to Learning state and also from Learning state moved to Forwarding state of a port in bridge. Value: 4 ~ 30

Force Version	Two options are offered for choosing STP algorithm. <i>Compatible</i> - STP (IEEE 802.1D) <i>Normal</i> - RSTP (IEEE 802.1w)								
Aggregations	Enabled to support port trunking in STP. It means a link aggregate is treated as a physical port in RSTP/STP operation.								
Port Protocol Enabled	Port is enabled to support RSTP/STP.								
Port Edge	An Edge Port is a port connected to a device that knows nothing about STP or RSTP. Usually, the connected device is an end station. Edge Ports will immediately transit to forwarding state and skip the listening and learning state because the edge ports cannot create bridging loops in the network.								
Port Path Cost	Specifies the path cost of the port that switch uses to determine which port are the forwarding ports the lowest number is forwarding ports, the range is 1 ~ 200,000,000 and Auto. Auto means a default cost is automatically calculated in RSTP operation based on the port link speed. The default costs are: <table border="1"> <thead> <tr> <th><u>Link Speed</u></th> <th><u>Auto Default Cost</u></th> </tr> </thead> <tbody> <tr> <td>10Mbps</td> <td>2000000</td> </tr> <tr> <td>100Mbps</td> <td>200000</td> </tr> <tr> <td>1000Mbps</td> <td>20000</td> </tr> </tbody> </table>	<u>Link Speed</u>	<u>Auto Default Cost</u>	10Mbps	2000000	100Mbps	200000	1000Mbps	20000
<u>Link Speed</u>	<u>Auto Default Cost</u>								
10Mbps	2000000								
100Mbps	200000								
1000Mbps	20000								
[Apply]	Click to apply the configuration change								
[Refresh]	Click to refresh current configuration								

4.9 802.1X Authentication

For some IEEE 802 LAN environments, it is desirable to restrict access to the services offered by the LAN to those users and devices that are permitted to make use of those services. IEEE 802.1X Port-based network access control function provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails. The 802.1X standard relies on the client to provide credentials in order to gain access to the network. The credentials are not based on a hardware address. Instead, they can be either a username/password combination or a certificate. The credentials are not verified by the switch but are sent to a Remote Authentication Dial-In User Service (RADIUS) server, which maintains a database of authentication information. 802.1X consists of three components for authentication exchange, which are as follows:



- 802.1X authenticator: This is the port on the switch that has services to offer to an end device, provided the device supplies the proper credentials.
- 802.1X supplicant: This is the end device; for example, a PC that connects to a switch that is requesting to use the services (port) of the device. The 802.1X supplicant must be able to respond to communicate.
- 802.1X authentication server: This is a RADIUS server that examines the credentials provided to the authenticator from the supplicant and provides the authentication service. The authentication server is responsible for letting the authenticator know if services should be granted.

802.1X authenticator operates as a go-between with the supplicant and the authentication server to provide services to the network. When a switch is configured as an authenticator, the ports of the switch must then be configured for authorization. In an authenticator-initiated port authorization, a client is powered up or plugs into the port, and the authenticator port sends an Extensible Authentication Protocol (EAP) PDU to the supplicant requesting the identification of the supplicant. At this point in the process, the port on the switch is

connected from a physical standpoint; however, the 802.1X process has not authorized the port and no frames are passed from the port on the supplicant into the switching engine. If the PC attached to the switch did not understand the EAP PDU that it was receiving from the switch, it would not be able to send an ID and the port would remain unauthorized. In this state, the port would never pass any user traffic and would be as good as disabled. If the client PC is running the 802.1X EAP, it would respond to the request with its configured ID. (This could be a username/password combination or a certificate.)

After the switch, the authenticator receives the ID from the PC (the supplicant). The switch then passes the ID information to an authentication server (RADIUS server) that can verify the identification information. The RADIUS server responds to the switch with either a success or failure message. If the response is a success, the port will be authorized and user traffic will be allowed to pass through the port like any switch port connected to an access device. If the response is a failure, the port will remain unauthorized and, therefore, unused. If there is no response from the server, the port will also remain unauthorized and will not pass any traffic.

4.9.1 802.1X Configuration

802.1X Configuration

Mode:

RADIUS IP:

RADIUS UDP Port:

RADIUS Secret:

Port	Admin State	Port State			
1	<input type="text" value="Force Authorized"/>	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
2	<input type="text" value="Force Authorized"/>	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
3	<input type="text" value="Force Authorized"/>	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
4	<input type="text" value="Force Authorized"/>	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
5	<input type="text" value="Force Authorized"/>	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
6	<input type="text" value="Force Authorized"/>	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
7	<input type="text" value="Force Authorized"/>	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
8	<input type="text" value="Force Authorized"/>	802.1X Disabled	Re-authenticate	Force Reinitialize	Statistics
			Re-authenticate All	Force Reinitialize All	

Parameters

Apply

Refresh

Configuration	Description
Mode	<i>Disabled</i> - disable 802.1X function <i>Enabled</i> - enable 802.1X function
RADIUS IP	IP address of the Radius server
RADIUS UDP Port	The UDP port for authentication requests to the specified Radius server
RADIUS Secret	The Encryption key for use during authentication sessions with the Radius server. It must match the key used on the Radius server.
Port	Port number
Admin State	Port 802.1X control <i>Auto</i> - set to the Authorized or Unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the Authentication Server. <i>Force Authorized</i> - the port is forced to be in authorized state. <i>Force Unauthorized</i> - the port is forced to be in unauthorized state.
Port State	Port 802.1X state <i>802.1X Disabled</i> - the port is in 802.1X disabled state <i>Link Down</i> - the port is in link down state Authorized (green color) - the port is in 802.1X authorized state Unauthorized (red color) - the port is in 802.1X unauthorized state
[Re-authenticate]	Click to perform a manual authentication for the port
[Force Reinitialize]	Click to perform an 802.1X initialization for the port
[Re-authenticate All]	Click to perform manual authentication for all ports
[Force Reinitialize All]	Click to perform 802.1X initialization for all ports
[Parameters]	Click to configure Re-authentication parameters
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration

4.9.2 802.1X Re-authentication Parameters

802.1X Parameters

Reauthentication Enabled	<input type="checkbox"/> Enabled
Reauthentication Period [1-3600 seconds]	<input type="text" value="3600"/>
EAP timeout [1 - 255 seconds]	<input type="text" value="30"/>

Apply

Refresh

Configuration	Description
Reauthentication Enabled	Check to enable periodical re-authentication for all ports
Reauthentication Period	The period of time after which the connected radius clients must be re-authenticated (unit: second), Value: 1- 3600
EAP timeout	The period of time the switch waits for a supplicant response to an EAP request (unit: second), Value: 1 - 255
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration

4.10 IGMP Snooping

IGMP Configuration

IGMP Enabled	<input type="checkbox"/>
Router Ports	<input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8
Unregistered IPMC Flooding enabled	<input checked="" type="checkbox"/>

VLAN ID	IGMP Snooping Enabled	IGMP Querying Enabled
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Configuration	Description
IGMP Enabled	Check to enable global IGMP snooping.
Router Ports	Specify which ports have multicast router connected and require being forwarding IPMC packets unconditionally.
VLAN ID	List of current existing VLANs
IGMP Snooping Enabled	Check to enable IGMP snooping on the associated VLAN.
IGMP Querying Enabled	Check to enable IGMP querying on the associated VLAN.
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration

4.11 Mirroring

Mirroring Configuration

Port	Mirror Source
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

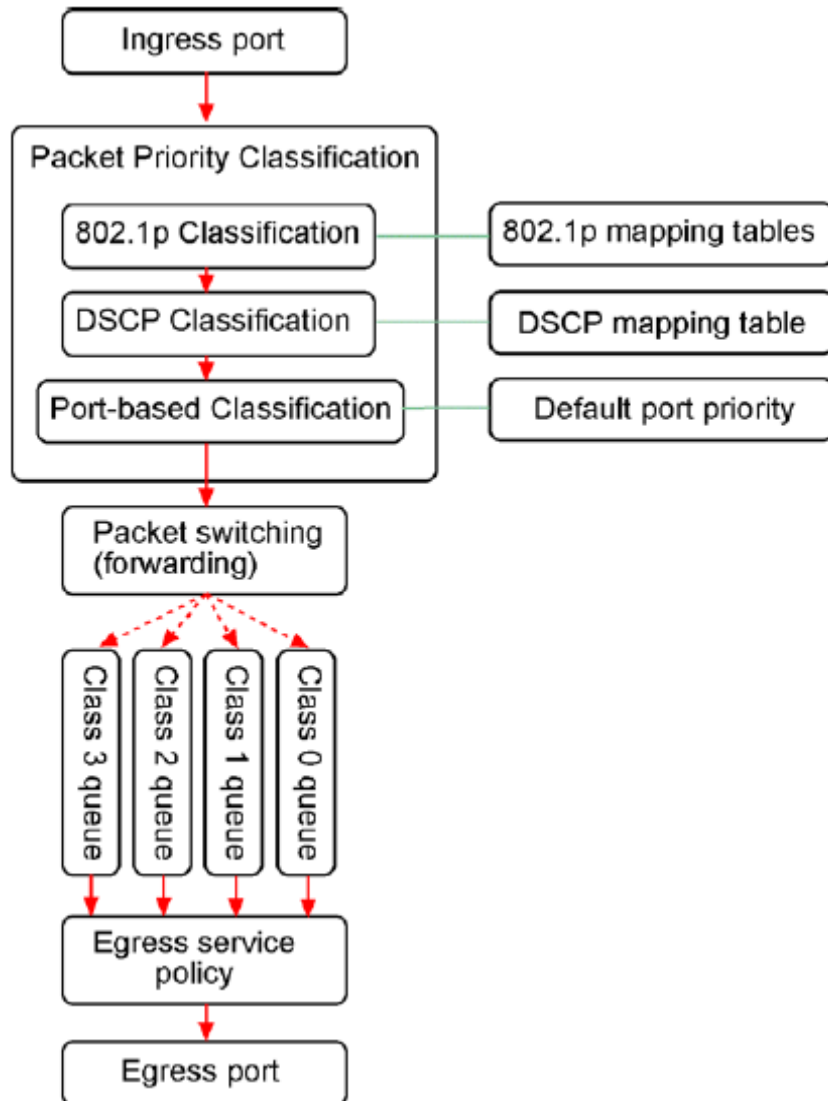
Mirror Port	1 ▾
-------------	-----

Apply	Refresh
-------	---------

Configuration	Description
Mirror Port	The port for being forwarded all packets received on the mirrored ports
Mirror Source	Select the ports which will be mirrored all received packets to the mirror port.
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration

4.12 Quality of Service

The switch provides a powerful Quality of Service (QoS) function to guide the packet forwarding in four priority classes. The versatile classification methods can meet most of the application needs. The following figure illustrates the QoS operation flow when a packet received on the ingress port until it is transmitted out from the egress port:



Packet Priority Classification

Each received packet is examined and classified into one of four priority classes, Class 3, Class 2, Class 1 and Class 0 upon reception. The switch provides the following classification methods:

802.1p classification: use User Priority tag value in the received IEEE 802.1Q packet to map to one priority class

DSCP classification: use DSCP value in the received IP packet to map to one priority class

Port-based classification: used when 802.1p and DSCP are disabled or fail to be applied

They all can be configured to be activated or not. More than one classification methods can be enabled at the same time. However, 802.1p classification is superior over DSCP classification.

802.1p mapping tables: Each ingress port has its own mapping table for 802.1p classification.

DSCP mapping table: All ingress ports share one DSCP mapping table for DSCP classification.

Default port priority: A port default priority class is used when port-based classification is applied

All configuration settings are in per port basis except that DSCP mapping table is global to all ports. A received packet is classified into one of four priority class before it is forwarded to an egress port.

Priority Class Queues

Each egress port in the switch is equipped with four priority class egress queues to store the packets for transmission. A packet is stored into the class queue which is associated to the classified priority class. For example, a packet is stored into Class 3 egress queue if it is classified as priority Class 3.

Egress Service Policy

Each port can be configured with an egress service policy to determine the transmission priority among four class queues. By default, higher class number has higher priority than the lower class numbers.

Four policies are provided for selection as follows:

- Strict priority : Packets in high priority class queue are sent first until the queue is empty
- Weighted ratio priority Class 3:2:1:0 = 4:3:2:1 : four queues are served in 4:3:2:1 ratio
- Weighted ratio priority Class 3:2:1:0 = 5:3:1:1 : four queues are served in 5:3:1:1 ratio
- Weighted ratio priority Class 3:2:1:0 = 1:1:1:1 : four queues are served equally

Strict priority policy lets high priority class queue is served first until it is empty. Lower priority queue may not get any service (or egress bandwidth) when higher priority traffic is heavy for long time. Three weighted ratio policies are provided to resolve such problem. Four class queues are served in weighted round robin basis. Every priority class can get a guaranteed ratio for the egress bandwidth.

4.12.1 QoS Configuration

QoS Configuration

Port	802.1p	DSCP	Port Priority
1	Disable ▾	Disable ▾	Class 3 ▾
2	Disable ▾	Disable ▾	Class 3 ▾
3	Disable ▾	Disable ▾	Class 3 ▾
4	Disable ▾	Disable ▾	Class 3 ▾
5	Disable ▾	Disable ▾	Class 3 ▾
6	Disable ▾	Disable ▾	Class 3 ▾
7	Disable ▾	Disable ▾	Class 3 ▾
8	Disable ▾	Disable ▾	Class 3 ▾

[802.1p Mapping](#) [DSCP Mapping](#) [Service Policy](#)

[Apply](#) [Refresh](#)

QoS Configuration	Description
Port	Port number
802.1p	802.1p priority classification <i>Enable</i> - set to enable this classification to the port for priority-tagged and VLAN-tagged packets <i>Disable</i> - 802.1p classification is not applied to the port
DSCP	DSCP classification <i>Enable</i> - set to enable DSCP classification to the port for IP packets <i>Disable</i> - DSCP classification is not applied to the port
Port Priority	Port default priority class, it is used as a port-based QoS mode when 802.1p and DSCP classifications are disabled. It is also used as default priority class for the received packet when both 802.1p and DSCP classification failed in classification. <i>Class 3 ~ Class 0</i> - priority class
[802.1p Mapping]	Click to configure 802.1p mapping tables.
[DSCP Mapping]	Click to configure DSCP mapping table.
[Service Policy]	Click to configure per port egress service policy mode.
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration

Note:

802.1p classification is superior over DSCP classification if both are enabled. That means if a received packet is classified successfully in 802.1p classification, the classified priority class is used directly for the packet and the result of DSCP classification is ignored.

4.12.2 802.1p Mapping

QoS 802.1p Mapping

Port	tag 0	tag 1	tag 2	tag 3	tag 4	tag 5	tag 6	tag 7
1	Class 0	Class 0	Class 1	Class 1	Class 2	Class 2	Class 3	Class 3
2	Class 0	Class 0	Class 1	Class 1	Class 2	Class 2	Class 3	Class 3
3	Class 0	Class 0	Class 1	Class 1	Class 2	Class 2	Class 3	Class 3
4	Class 0	Class 0	Class 1	Class 1	Class 2	Class 2	Class 3	Class 3
5	Class 0	Class 0	Class 1	Class 1	Class 2	Class 2	Class 3	Class 3
6	Class 0	Class 0	Class 1	Class 1	Class 2	Class 2	Class 3	Class 3
7	Class 0	Class 0	Class 1	Class 1	Class 2	Class 2	Class 3	Class 3
8	Class 0	Class 0	Class 1	Class 1	Class 2	Class 2	Class 3	Class 3

Configuration	Description
Port n	Port number n
tag m	3-bit User priority tag value m (range : 0 ~ 7)
Priority class	Mapped priority class for tag m on Port n Class 3 ~ Class 0
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration
[Back]	Click to go back to upper menu

Every ingress port has its own 802.1p mapping table. The table is referred in 802.1p priority classification for the received packet.

4.12.3 DSCP Mapping

QoS DSCP Mapping

DSCP [0-63]	Priority
<input type="text"/>	Class 3 ▾
<input type="text"/>	Class 3 ▾
<input type="text"/>	Class 3 ▾
<input type="text"/>	Class 3 ▾
<input type="text"/>	Class 3 ▾
<input type="text"/>	Class 3 ▾
<input type="text"/>	Class 3 ▾
All others	Class 0 ▾

Configuration	Description
DSCP [0-63]	Seven user-defined DSCP values which are configured with a priority class <i>0 ~ 63</i> - 6-bit DSCP value in decimal
Priority	The priority class configured for the user-defined DSCP value <i>Class 3 ~ Class 0</i>
All others	The other DSCP values not in the seven user-defined values are assigned a default priority class <i>Class 3 ~ Class 0</i>
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration
[Back]	Click to go back to upper menu

Only one DSCP mapping table is configured and applied to all ports. The table is referred in DSCP priority classification.

4.12.4 QoS Service Policy

QoS Service Policy

Port	Policy
1	Strict priority
2	Strict priority
3	Strict priority
4	Strict priority
5	Strict priority
6	Strict priority
7	Strict priority
8	Strict priority

Configuration	Description
Port	Port number
Policy	Service policy for egress priority among four egress class queues <i>Strict priority</i> - high class queue is served first always till it is empty <i>Weighted ratio priority Class 3:2:1:0 = 4:3:2:1</i> - weighted ratio 4:3:2:1 <i>Weighted ratio priority Class 3:2:1:0 = 5:3:1:1</i> - weighted ratio 5:3:1:1 <i>Weighted ratio priority Class 3:2:1:0 = 1:1:1:1</i> - weighted ratio 1:1:1:1
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration
[Back]	Click to go back to upper menu

Notes:

1. *Queue with higher class number has higher priority than queue with lower class number. That means Class 3 > Class 2 > Class 1 > Class 0 by default.*
2. *In weighted ratio policies, a weighted fairness round robin service is guaranteed normally. However, when excess bandwidth exists higher class queue will take advantage on bandwidth allocation.*

4.13 Storm Control

Storm Control Configuration

Storm Control Number of frames per second	
Broadcast Rate	No Limit ▾
Multicast Rate	No Limit ▾
Flooded unicast Rate	No Limit ▾

Configuration	Description
Broadcast Rate	The rate limit of the broadcast packets transmitted on a port.
Broadcast Rate	The rate limit of the Multicast packets transmitted on a port.
Flooded Unicast Rate	The rate limit of the flooded unicast packets transmitted on a port. The Flooded unicast packets are those unicast packets whose destination address is not learned in the MAC address table.
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration

Notes:

- 1. The unit of the rates is pps (packets per second).*
- 2. No Limit - no protection control*

4.14 Multi Ring

Multi Ring Configuration (v0.1.0)

Group	Ring Port 1	Backup Port	Ring Port 2	Backup Port	ID
Ring Group 1	Port 1 ▾	<input checked="" type="checkbox"/>	Port 2 ▾	<input type="checkbox"/>	2
Ring Group 2	Port 3 ▾	<input type="checkbox"/>	Port 4 ▾	<input checked="" type="checkbox"/>	3
Ring Group 3	Port 5 ▾	<input checked="" type="checkbox"/>	Port 6 ▾	<input type="checkbox"/>	4
Ring Group 4	-- ▾	<input type="checkbox"/>	-- ▾	<input type="checkbox"/>	0

Apply

Refresh

Note

One port can only be configured as either Ring port or RSTP port.

Configuration	Description
Ring Group 1 -4	Up to four redundant rings supported in one switch
Ring Port 1, 2	Two ring ports are needed to support one redundant ring.
Backup Port	Check to specify the ring port as a backup port.
Ring Group ID	One unique ID is assigned for the associated ring group. The ring group ID should be same for all switch members in the associated ring.
[Apply]	Click to apply the configuration change
[Refresh]	Click to refresh current configuration

Notes:

1. One switch provides two ports to support one redundant ring. As a slave switch, both ports are configured <**Ring Port**>. To be a master of a ring, one port must be set to <**Backup Port**>.
2. Only one backup port is configured among the member switches in a redundant ring.
3. One switched port can only be configured either Multi Ring enabled or RSTP enabled.

4.15 Statistics Overview

Statistics Overview for all ports

Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	44092	96	952208	6772	0	1
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0

Statistics

Description

Port	Port number
Tx Bytes	Total of bytes transmitted on the port
Tx Frames	Total of packet frames transmitted on the port
Rx Bytes	Total of bytes received on the port
Rx Frames	Total of packet frames received on the port
Tx Errors	Total of error packet frames transmitted on the port
Rx Errors	Total of error packet frames received on the port

[Clear] Click to reset all statistic counters

[Refresh] Click to refresh all statistic counters

4.16 Detailed Statistics

Statistics for Port 1

Receive Total		Transmit Total	
Rx Packets	7179	Tx Packets	102
Rx Octets	1011357	Tx Octets	45837
Rx High Priority Packets	-	Tx High Priority Packets	-
Rx Low Priority Packets	-	Tx Low Priority Packets	-
Rx Broadcast	-	Tx Broadcast	-
Rx Multicast	-	Tx Multicast	-
Rx Broad- and Multicast	7032	Tx Broad- and Multicast	0
Rx Error Packets	1	Tx Error Packets	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	-	Tx 64 Bytes	-
Rx 65-127 Bytes	-	Tx 65-127 Bytes	-
Rx 128-255 Bytes	-	Tx 128-255 Bytes	-
Rx 256-511 Bytes	-	Tx 256-511 Bytes	-
Rx 512-1023 Bytes	-	Tx 512-1023 Bytes	-
Rx 1024- Bytes	-	Tx 1024- Bytes	-
Receive Error Counters		Transmit Error Counters	
Rx CRC/Alignment	-	Tx Collisions	-
Rx Undersize	-	Tx Drops	-
Rx Oversize	-	Tx Overflow	-
Rx Fragments	-		
Rx Jabber	-		
Rx Drops	-		

Button

Description

[Port #] Click to display the detailed statistics of Port #.

[Clear] Click to reset all statistic counters

[Refresh] Click to refresh the displayed statistic counters

4.17 LACP Status

LACP Aggregation Overview

Group/Port	1	2	3	4	5	6	7	8
Normal								

Legend

Down	Port link down
0	Blocked Port Blocked by RSTP. Number is Partner port number if other switch has LACP enabled
0	Learning Port Learning by RSTP
Forwarding	Port link up and forwarding frames
0	Forwarding Port link up and forwarding by RSTP. Number is Partner port number if other switch has LACP enabled

Refresh

LACP Port Status

Port	Protocol Active	Partner Port Number	Operational Port Key
1	no		
2	no		
3	no		
4	no		
5	no		
6	no		
7	no		
8	no		

Status

Description

Port	The port number
Normal	Display the ports not LACP enabled.
Group #	The LACP group
Status	The LACP port status presented with color and a number <Down> - the port is link down <Blocked & #> - the port is blocked by RSTP and the # is the port number of LACP link partner <Learning> - the port is learning by RSTP <Forwarding> - the port is link up and forwarding frames <Forwarding & #> - the port is link up and forwarding frames and the # is the port number of LACP link partner
Partner MAC address	The MAC address of the link partner at the other end of the LACP aggregate

Local Port Aggregated The ports at local end which are aggregated in same LACP group

[Refresh] Click to refresh the status

Note: the figure shows an example that two LACP link aggregates are configured.

LACP Port Status	Description
-------------------------	--------------------

Port	The port number
------	-----------------

Protocol Active	<i>yes</i> - the port is link up and in LACP operation <i>no</i> - the port is link down or not in LACP operation
-----------------	--

Partner Port Number	The port number of the remote link partner
---------------------	--

Operation Port Key	The operation key generated by the system
--------------------	---

4.18 RSTP Status

The following example shows three RSTP topologies operate in three VLANs configured in a switch.

RSTP VLAN Bridge Overview

VLAN Id	Bridge Id	Hello Time	Max Age	Fwd Delay	Topology	Root Id
1	32769:00-40-F6-E0-00-13	2	20	15	Steady	This switch is Root!

Refresh

RSTP Port Status

Port/Group	Vlan Id	Path Cost	Edge Port	P2p Port	Protocol	Port State
Port 1						Non-STP
Port 2						Non-STP
Port 3						Non-STP
Port 4						Non-STP
Port 5						Non-STP
Port 6						Non-STP
Port 7						Non-STP
Port 8						Non-STP

RSTP Status	Description
VLAN Id	The VLAN which has STP enabled ports
Bridge Id	STP bridge ID [Priority:MAC address] detected in the associated VLAN
Hello Time	Hello Time is used to determine the periodic time to send normal BPDU from designated ports among bridges. It decides how long a bridge should send this message to other bridge to tell I am alive. <i>1 ~ 10 seconds</i>
Max. Age	When the switch is root bridge, the whole LAN uses this setting as the maximum age time. <i>6 ~ 40 seconds</i>
Fwd Delay	This figure is set at Root Bridge only.
Topology	<i>Steady</i> - The STP topology is steady. <i>Changing</i> - The STP topology is changing.
Root Id	The MAC address of current STP root If the switch is STP root, a message of [The switch is Root.] is displayed.
[Refresh]	Click to refresh the status

RSTP Port Status	Description
Port/Group	Port number
VLAN Id	The associated VLAN to which the RSTP port belongs (PVID)
Path Cost	The path cost of the RSTP port
Edge Port	Is the port an edge port?
P2p Port	<i>Yes</i> - The port operates in full duplex.
Protocol	The protocol version configured for the port - RSTP or STP
Port State	<p>Forwarding - A port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.</p> <p><i>Blocking</i> - A port that would cause a switching loop, no user data is sent or received but it may go into forwarding mode if the other links in use were to fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state.</p> <p><i>Listening</i> - The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state.</p> <p><i>Learning</i> - While the port does not yet forward frames (packets) it does learn source addresses from frames received and adds them to the filtering database (switching database)</p> <p><i>Non-STP</i> - RSTP is disabled.</p>

The above status example shows three STP operate in three different VLANs as follows:

VLAN 1 members: P1, P2, P3, P4, P5, P6, P7, P8

VLAN 2 members: P3, P4

VLAN 3 members: P7, P8

P3 PVID = VLAN 2

P4 PVID = VLAN 2

P7 PVID = VLAN 3

P8 PVID = VLAN 3

P3 and P4 connect to same switch as an STP redundant link associated to VLAN 2.

P7 and P8 connect to another switch as an STP redundant link associated to VLAN 3.

The switch supports STP over multiple VLANs. Each VLAN has individual STP mechanism operating independently.

4.19 IGMP Status

IGMP Status

VLAN ID	Querier	Queries transmitted	Queries received	v1 Reports	v2 Reports	v3 Reports	v2 Leaves
1	Idle	0	89	0	474	4	0

Refresh

Member Groups

VLAN ID	Groups	Port Members
1	224.0.1.60	1
1	239.255.255.250	1
1	224.0.0.251	1
1	224.0.0.252	1
1	224.0.1.22	1

Status	Description
VLAN ID	The VLAN ID of the entry.
Querier Status	Show the Querier status is “Active” or “Idle”.
Queries transmitted	The number of Transmitted Queries.
Queries Received	The number of Received Queries.
V1 Reports	The number of Received V1 Reports.
V2 Reports	The number of Received V2 Reports.
V3 Reports	The number of Received V3 Reports.
V2 Leave	The number of Received V2 Leave.
[Refresh]	Click to refresh the page.

Group Member Status	Description
VLAN ID	The VLAN where the groups found
Groups	IPMC group (IP) found on the VLAN
Port Members	Port members found of the group

4.20 PoE Status

Power Over Ethernet Status

Refresh

Port	PD class	Power Used	Current Used	Port Status
1	0	0[W]	0[mA]	PoE Disabled
2	1	2.3[W]	47[mA]	PoE Turned ON
3	0	0[W]	0[mA]	PoE Disabled
4	0	0[W]	0[mA]	PoE Disabled
5	0	0[W]	0[mA]	PoE Disabled
6	0	0[W]	0[mA]	PoE Disabled
7	0	0[W]	0[mA]	PoE Disabled
8	0	0[W]	0[mA]	PoE Disabled
Total	-	2.3[W]	47[mA]	-

Status**Description**

Port

This is the logical port number for this row.

PD class

The power class detected from the remote PD (Powered Device)

Power Used

How much power the port currently is being delivered

Current Used

How much current the port currently is being delivered.

Port Status

The port's PoE status.

PoE Disabled - the PoE PSE function is configured as disabled.*PoE Turned ON* - the port PoE power is ON.*No PD Detected* - PoE function is enabled, but no PD connected*No PoE Chip Found* - PoE controller is not found.

4.21 Multi Ring Status

Multi Ring Group Status

Group	Ring Status	Members	ID
Ring Group 1	STANDBY	3	2
Ring Group 2	STANDBY	3	3
Ring Group 3	STANDBY	5	4
Ring Group 4	--	--	--

Refresh

Local Port Status

Port	Link Status	Protocol	Ring ID
1	1000FDX	Ring (Backup Port)	2
2	1000FDX	Ring	2
3	1000FDX	Ring	3
4	1000FDX	Ring (Backup Port)	3
5	1000FDX	Ring (Backup Port)	4
6	1000FDX	Ring	4
7	1000FDX	RSTP	--
8	1000FDX	RSTP	--

This figure shows an example that three redundant rings are configured and local Port 1/2, Port 3/4 and Port 5/6 connect Ring 2, Ring 3, and Ring 4 respectively. Port 7 and Port 8 connect RSTP network independently.

Status	Description
Group #	Ring entities
Ring Status	Status: [STANDBY] – The ring is normal and with no failure. The backup link is under standby and not activated. [BACKUP] – Failure occurred somewhere on the ring and the master has activated the backup link to support continuous operation of the ring. The ring failure should be repaired immediately by the persons who are in charge. [Master Failed] – Possible failure occurred on the master unit itself. No backup support is available. This is a critical situation and should be repaired immediately. [Backup Port Failed] – Possible failure occurred on the backup link. No backup

support is available. This is a critical situation and should be repaired immediately.

Members

The number of the switch members in the ring.

Click to browse the ring member information and status.

This is a helpful tool for diagnosing where the ring failure is located.

Ring ID

The group ID assigned to the ring

[Refresh]

Click to refresh the page.

Local Port Status

Description

Port #

Port number of this switch

Link Status

Port link status (Refer to the section of Port Configuration.)

Protocol

The protocol and role served by the port -

Ring – normal ring port of the associated redundant ring (Ring ID)

Ring (Backup Port) - Backup port of the associated redundant ring (Ring ID)

RSTP – the port is serving RSTP instead of Multi-Ring protocol.

Ring ID

Ring Group ID the port connected

Ring Member Information and Status

Multi Ring List - Ring Group 3

Mac Address	IP Address	Device Name	Port Number	Port Type	Port Status	Ring ID
00-40-F6-EB-4B-B9	192.168.2.204	Control Room	5	Backup	Link	4
			6		Link	
00-40-F6-EB-4C-25	192.168.2.208	Office 3F-4	1		Link	4
			2		Link	
00-40-F6-EB-4E-F5	192.168.2.207	Office 3F-3	1		Link	4
			2		Link	
00-40-F6-EB-4B-CB	192.168.2.205	Office 3F-1	5		Link	4
			6		Link	
00-40-F6-EB-4E-89	192.168.2.206	Office 3F-2	7		Link	4
			8		Link	

This example shows switch member information and status of Ring group 3.

Status

Description

Mac Address

MAC address of each member switch

IP Address	IP address configured of each member switch (See System Configuration.)
Device Name	The name configured for each member switch (See System Configuration.)
Port Number	The ring port pair of each member switch connected on this ring group
Port Type	Whether the ring port is backup port or not
Port Status	Current link status of the ring ports connected on this ring group
Ring ID	Ring ID of this ring group

4.22 Ping

Ping Parameters

Target IP address	<input type="text"/>
Count	1 ▾
Time Out (in secs)	1 ▾

Apply


Ping Results	
Target IP address	0.0.0.0
Status	Test complete
Received replies	0
Request timeouts	0
Average Response Time (in ms)	0

Refresh

Ping	Description
Target IP Address	The target IP address to which the ping command issues
Count	The number of ping commands generated
Time Out (in secs)	The time out for a reply (in seconds)
[Apply]	Start the ping command
Ping Result	Description
Target IP Address	The target IP address to which the ping command issues
Status	The command status
Received replies	The number of replies received by the system
Request time-outs	The number of requests time out
Average Response Time	The average response time of a ping request (in mini-seconds)

4.23 Reboot System

Reboot System



Are you sure you want to reboot system? Yes No

This menu is used to reboot the switch unit remotely with current configuration. Starting this menu will make your current http connection lost. You must rebuild the connection to perform any management operation to the unit.

4.24 Restore Default

Factory Default



Are you sure you want to perform a Factory Default? Yes No

This menu is used to restore all settings of the switch unit with factory default values. Note that this menu might change the current IP address of the switch and make your current http connection lost.

4.25 Update Firmware

Software Upload



This menu is used to perform in-band firmware (switch software) upgrade. Enter the path and file name of new firmware image file for uploading.

Configuration	Description
Filename	Path and filename (warp format)
[Browse]	Click to browse your computer file system for the firmware image file
[Upload]	Click to start upload

4.26 Configuration File Transfer

Configuration Upload

Upload

Configuration Download

Download

This [download] command can be used to backup current switch configuration and download it to the connected management PC using default filename, switch.cfg.

Configuration	Description
Filename	Path and filename of a backup configuration file to be uploaded
[Browse]	Click to browse your computer file system for the configuration file
[Upload]	Click to start upload operation from the connected PC to the switch
[Download]	Click to start download operation from the switch to the connected PC

4.27 Logout

Please enter password to login

Password:

Apply

This command is used to perform a logout from the switch management and prompt a login interface immediately. If current user does not perform any management operation over 3 minutes, the switch will execute an auto logout and abort the current connection.

5. SNMP Support

SNMP version support	Snmp v1, v2c management
Managed Objects	MIB-II
	system OBJECT IDENTIFIER ::= { mib-2 1 }
	interfaces OBJECT IDENTIFIER ::= { mib-2 2 }
	ip OBJECT IDENTIFIER ::= { mib-2 4 }
	snmp OBJECT IDENTIFIER ::= { mib-2 11 }
	dot1dBridge OBJECT IDENTIFIER ::= { mib-2 17 }
	ifMIB OBJECT IDENTIFIER ::= { mib-2 31 }
Private Objects	enterprise.device.sys_obj
	DDM_Table OBJECT IDENTIFIER ::= { sys_obj 1 } *1
	Reboot OBJECT IDENTIFIER ::= { sys_obj 2 }
RFC	RFC 3418 - Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
	RFC 1907 - Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
	RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets:MIB-II
	RFC 1158 - Management Information Base for network management of TCP/IP-based internets: MIB-II
	RFC 1493 - Definitions of Managed Objects for Bridges
	RFC 2863 - The Interfaces Group MIB
	RFC 1573 - Evolution of the Interfaces Group of MIB-II
SNMP Trap Support	TRAP_COLDSTART - the device boot up trap
	TRAP_LINKUP - the port link recovery trap
	TRAP_LINKDOWN - port link down trap

**1: DDM_Table provides the information and status detected on the ports featured with DDM function. The information table is displayed and indexed by port number.*

Appendix A Specifications of Fiber Interface Options

Model Name	Fast Ethernet	Gigabit Ethernet	Fiber interface	Fiber Compliance
KGS-0860-WP	8 ports	-	-	-
KGS-0860-WP-x	8 ports	-	1 (Port #8)	100Base-FX
KGS-0860-WP-2x	8 ports	-	2 (Port #7, #8)	100Base-FX
KGS-0861-WP	-	8 ports	-	-
KGS-0861-WP-x	-	8 ports	1 (Port #8)	1000Base-X
KGS-0861-WP-2x	-	8 ports	2 (Port #7, #8)	1000Base-X
KGS-0862-WP	-	8 ports	-	-
KGS-0862-WP-x	-	8 ports	1 (Port #8)	1000Base-X
KGS-0862-WP-2x	-	8 ports	2 (Port #7, #8)	1000Base-X
KGS-0863-WP	6 ports	2 ports	-	-
KGS-0863-WP-x	6 ports	2 ports	1 (Port #8)	1000Base-X
KGS-0863-WP-2x	6 ports	2 ports	2 (Port #7, #8)	1000Base-X

Model series: KGS-086X-WP-xxxx (* xxxx = fiber code, 1xxx = one interface, 2xxx = 2 interfaces)

Fiber Options

Fiber code	Interface	Data Rate	Fiber	LC	Ref. distance
-FM	1	100Mbps	MMF	1310nm Duplex	2km
-2FM	2	100Mbps	MMF	1310nm Duplex	2km
-FS30	1	100Mbps	SMF	1310nm Duplex	30km
-2FS30	2	100Mbps	SMF	1310nm Duplex	30km
-FW3520	1	100Mbps	SMF	BiDi Tx 1310nm Rx 1550nm	20km
-2FW3520	2	100Mbps	SMF	BiDi Tx 1310nm Rx 1550nm	20km
-SX	1	1000Mbps	MMF	850nm Duplex	200m (62.5µm/125) 500m (50µm/125)
-2SX	2	1000Mbps	MMF	850nm Duplex	200m (62.5µm/125) 500m (50µm/125)
-LX	1	1000Mbps	SMF	1310nm Duplex	10km
-2LX	2	1000Mbps	SMF	1310nm Duplex	10km
-W3510	1	1000Mbps	SMF	BiDi Tx 1310nm Rx 1550nm	10km
-2W3510	2	1000Mbps	SMF	BiDi Tx 1310nm Rx 1550nm	10km