



KGD-600-B

**Industrial Web Smart 6-Port Gigabit
Ethernet Switch with Fiber Connectivity**

Installation Guide



DOC.120606

(C) 2012 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 (C). All Rights Reserved.

TRADEMARKS

Ethernet is a registered trademark of Xerox Corp.

WARNING:

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

NOTICE:


- (1) The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- (2) Shielded interface cables and AC power cord, if any, must be used in order to comply with the emission limits.

CISPR A COMPLIANCE:

This device complies with EMC directive of the European Community and meets or exceeds the following technical standard.

EN 55022 - Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment. This device complies with CISPR Class A.

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:

EN 55022: Limits and Methods of Measurement of Radio Interference characteristics of Information Technology Equipment.

EN 50082/1: Generic Immunity Standard -Part 1: Domestic Commercial and Light Industry.

EN 60555-2: Disturbances in supply systems caused by household appliances and similar electrical equipment - Part 2: Harmonics.

Table of Contents

| | |
|---|-----------|
| 1. Introduction | 6 |
| 1.1 Features | 7 |
| 1.2 Product Panels | 8 |
| 1.3 LED Indicators | 9 |
| 1.4 Specifications | 9 |
| 2. Installation | 11 |
| 2.1 Unpacking | 11 |
| 2.2 Safety Cautions | 11 |
| 2.3 Mounting the Switch on a Wall..... | 11 |
| 2.4 Din-Rail Mounting | 12 |
| 2.5 Panel Mounting | 13 |
| 2.6 Applying Power | 14 |
| 2.7 Reset Button | 15 |
| 2.8 Making UTP Connections | 16 |
| 2.9 Making Fiber Connection | 17 |
| 2.10 LED Indication | 18 |
| 2.11 Configuring IP Address and Password for the Switch | 18 |
| 3. Advanced Functions | 19 |
| 3.1 Abbreviation | 19 |
| 3.2 QoS Function | 20 |
| 3.2.1 Packet Priority Classification | 21 |
| 3.2.2 Priority Class Queues | 21 |
| 3.2.3 Egress Service Policy | 21 |
| 3.3 VLAN Function | 22 |
| 3.3.1 VLAN Operation | 22 |
| 3.3.2 Ingress Rules | 22 |
| 3.3.2.1 802.1Q Tag Aware Per port setting | 22 |
| 3.3.2.2 Keep Tag Per port setting | 22 |
| 3.3.2.3 Drop Untag Per Port Setting | 23 |
| 3.3.2.4 Drop Tag Per Port Setting | 23 |
| 3.3.3 Ingress Default Tag Per Port Setting..... | 23 |
| 3.3.4 Packet Tag Information | 23 |
| 3.3.5 VLANGroup Table Configuration | 24 |
| 3.3.6 VLANClassification | 24 |
| 3.3.7 Packet Forwarding | 24 |
| 3.3.8 Egress Tagging Rules | 25 |
| 3.3.8.1 Egress Settings | 25 |
| 3.3.9 Summary of VLAN Function | 25 |
| 3.4 802.1X Authentication Port Access Control | 26 |

| | |
|--|-----------|
| 4. Web Management | 27 |
| 4.1 Start Browser Software and Making Connection | 27 |
| 4.2 Login to the Switch Unit | 27 |
| 4.3 Main Management Menu | 28 |
| 4.4 System | 30 |
| 4.4.1 Management VLAN | 32 |
| 4.5 Ports | 33 |
| 4.6 VLANs | 35 |
| 4.6.1 Port-based VLAN Mode | 36 |
| 4.6.2 Port-based VLAN ISP Mode | 37 |
| 4.6.3 Advanced VLAN Mode | 38 |
| 4.6.3.1 Ingress Default Tag | 39 |
| 4.6.3.2 Ingress Settings | 40 |
| 4.6.3.3 Egress Settings | 41 |
| 4.6.3.4 VLAN Groups | 43 |
| 4.6.4 Important Notes for VLAN Configuration | 44 |
| 4.7 LACP | 45 |
| 4.8 RSTP | 46 |
| 4.9 802.1X Configuration | 47 |
| 4.9.1 802.1X Statistics | 49 |
| 4.9.2 802.1X Re-authentication Parameters | 50 |
| 4.10 IGMP Snooping | 51 |
| 4.11 Mirroring | 52 |
| 4.12 Quality of Service | 53 |
| 4.12.1 802.1p Mapping | 54 |
| 4.12.2 DSCP Mapping | 55 |
| 4.12.3 QoS Service Policy | 56 |
| 4.13 Storm Control | 57 |
| 4.14 Statistics Overview | 58 |
| 4.15 Detailed Statistics | 59 |
| 4.16 LACP Status | 60 |
| 4.17 RSTP Status | 62 |
| 4.18 IGMP Status | 64 |
| 4.19 Ping | 65 |
| 4.20 Reboot System | 66 |
| 4.21 Restore Default | 66 |
| 4.22 Update Firmware | 66 |
| 4.23 Configuration File Transfer | 67 |
| 4.24 Logout | 67 |
| 5. SNMP Support | 68 |
| Appendix. Factory Default Settings | 69 |

1. Introduction

The KGD-600 is a managed 6-port Gigabit Ethernet switch which is featured with five copper ports, one mini-GBIC (SFP) port and the following advantages in a small footprint box:



Plug and Play

The switch is shipped with factory default configuration which behaves like an unmanaged Gigabit switch for workgroup. It provides five 10/100/1000Mbps copper ports for connections to Ethernet, Fast Ethernet, and Gigabit Ethernet devices. With the featured auto-negotiation function, the switch can detect and configure the connection speed and duplex automatically. The switch also provides auto MDI/MDI-X function, which can detect the connected cable and switch the transmission wire pair and receiving pair automatically. This auto-crossover function can simplify the type of network cables used.

Fiber Connectivity

The mini-GBIC (SFP) port can be installed with an optional SFP optical fiber transceiver to support one Gigabit fiber connection when needed.

Web Management

The switch is embedded with an Http server which provides management functions for advanced network functions including Port Control, Quality of Service, and Virtual LAN functions. The management can be performed via Web browser based interface over TCP/IP network.

Virtual LAN (VLAN)

For increasing Tagged VLAN applications, the switch is also featured with powerful VLAN function to fulfill the up-to-date VLAN requirements. The switch supports both port-based VLAN and tagged VLAN in per-port basis.

Quality of Service

For advanced application, the switch is featured with powerful Quality of Service (QoS) function which can classify the priority for received network frames based on the ingress port and frame contents. Furthermore, many service priority policies can be configured for egress operation in per-port basis.

Industrial Features

For industrial environment, the devices are designed with the following enhanced features exceeding that of commercial Ethernet switches:

- High and wide operating Temperature
- Power input interface: Industrial screw terminal block and DC power jack for external commercial power adapter as option
- Screw panel and DIN rail mounting support for industrial enclosure
- Industrial-rated Emission and Immunity performance

1.1 Features

Basic functions

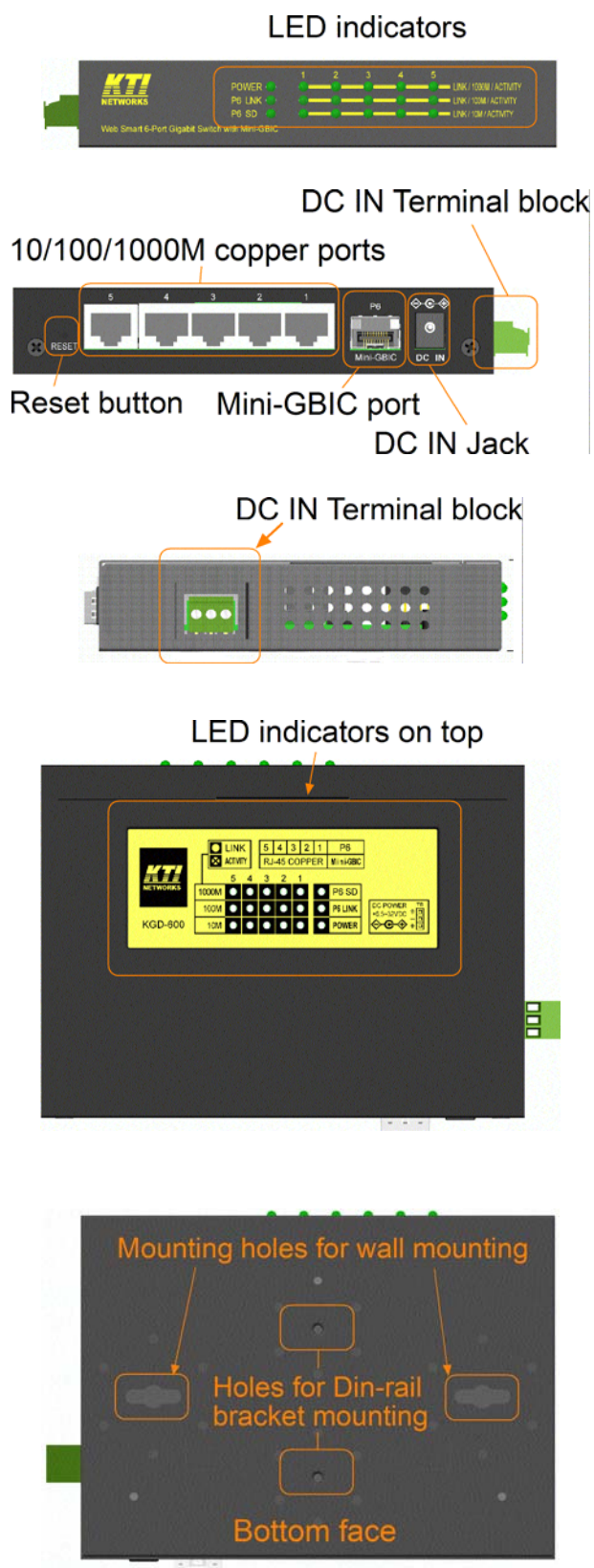
- Provides 5 10/100/1000Mbps Gigabit Ethernet ports and 1 SFP port
- Provides in-band web-based management interface
- All copper ports support auto-negotiation and auto-MDI/MDI-X detection
- Provides full wire speed forwarding
- Supports 802.3x flow control for full-duplex and backpressure for half-duplex
- Provides port status, statistic monitoring and control function
- Supports port-based and 802.1Q Tag-based VLAN
- Provides QoS function
- Provides port mirroring function

Management functions

- Web-based browsing interface
- Port configuration control and status monitoring
- Quality of Service (QoS) control for packet traffic
- Port-based and Tagged Virtual LAN (VLAN) function
- 802.1x authentication for port access control
- Port mirroring function
- Configuration file backup and upload
- In-band embedded firmware upgrade function

1.2 Product Panels

The following figure illustrates the faces of the switch:



1.3 LED Indicators

| <u>LED</u> | <u>Function</u> |
|-------------------|--|
| POWER | Power status |
| LNK/1000M/ACT | Network port 1000M link status (Port 1 - Port 5) |
| LNK/100M/ACT | Network port 100M link status (Port 1 - Port 5) |
| LNK/10M/ACT | Network port 10M link status (Port 1 - Port 5) |
| P6 LNK | Port 6 1000M link status |
| P6 OL | Port 6 optical link status |

1.4 Specifications

10/100/1000 Copper Ports

| | |
|-------------------|--|
| Compliance | IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3u 1000Base-T |
| Connectors | Shielded RJ-45 jacks |
| Pin assignments | Auto MDI/MDI-X detection |
| Configuration | Auto-negotiation or software control |
| Transmission rate | 10Mbps, 100Mbps, 1000Mbps |
| Duplex support | Full/Half duplex |
| Network cable | Cat.5 UTP |

1000Mbps Mini-GBIC Fiber Port

| | |
|-------------------|--|
| Compliance | IEEE 802.3z 1000Base-SX/LX (mini-GBIC) |
| Connectors | SFP for optional SFP type fiber transceivers |
| Configuration | Auto/Forced, 1000Mbps, Full duplex |
| Transmission rate | 1000Mbps |
| Network cables | MMF 50/125 60/125, SMF 9/125 |
| Eye safety | IEC 825 compliant |

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) 9.6K bytes (Jumbo frame) |
| 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 |
| Port Mirroring | Mirror received frames to a sniffer port |

Software Management Functions

| | |
|--------------------|--|
| Interfaces | Web browser |
| Management objects | System configuration - IP settings, Name, Password Port configuration control and status VLAN function settings QoS function settings Port mirroring settings 802.1x authentication port-access control Port Statistic Reboot, restore factory default, update firmware |

DC Power Input

| | |
|--------------------------|---|
| Interfaces | DC IN Jack (-D 6.3mm / + D 2.0mm) DC IN Terminal Block - screw type |
| Operating Input Voltages | +6.5 ~ 32VDC |
| Power Consumption | 5W max. @7.5V |

Mechanical

| | |
|------------------|--|
| Dimension (base) | 144 x 104.5 x 26 mm |
| Housing | Enclosed metal with no fan |
| Mounting Support | Din-rail mounting, Panel mounting, Wall mounting, Desktop mounting |

Environmental

| | |
|-----------------------|---|
| Operating Temperature | Typical -40°C ~ 70°C |
| Storage Temperature | -40°C ~ 85°C |
| Relative Humidity | 10% ~ 90% |
| Special Test | NEMA TS2-2003 Environment: Endurance Vibration, Mechanical shock test, Temperature/Humidity test (Condition combination : -34°C ~ +74°C, 0 ~90%RH, +6.5 ~ +30VDC) |

Electrical Approvals

| | |
|--------|----------------------|
| FCC | Part 15 rule Class A |
| CE | EMC, CISPR22 Class A |
| Safety | IEC60950-1 / EN60950 |

2. Installation

2.1 Unpacking

The product package contains:

- The switch unit
- One product CD-ROM

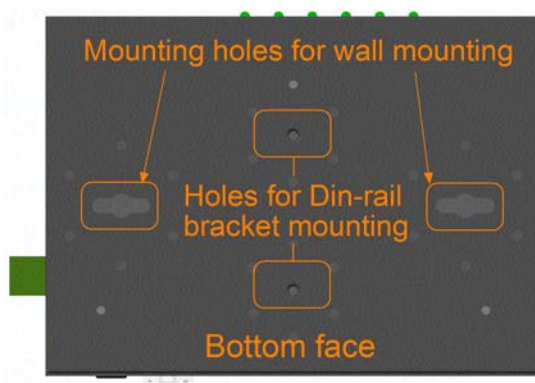
2.2 Safety Cautions

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.
 - An object has fallen into the product.
 - The product has been exposed to water.
 - 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 Mounting the Switch on a Wall

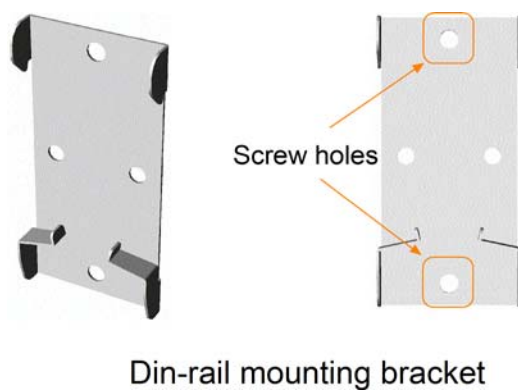
The switch can be mounted on a desktop or shelf or a wall. Make sure that there is proper heat dissipation from and adequate ventilation around the device. Do not place heavy objects on the device.



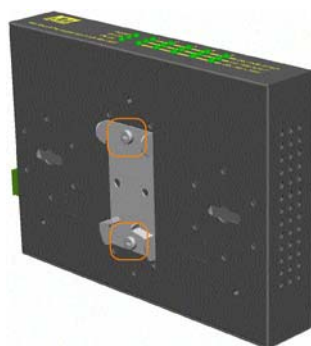
2.4 Din-Rail Mounting

The steps to mount the switch on a Din-rail are:

One Din-rail mounting bracket is provided in the product package as shown below:



Install the bracket on the bottom of the switch unit.

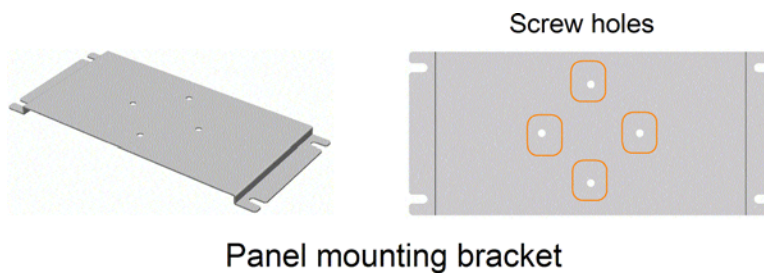


Mount the device on a Din-rail.

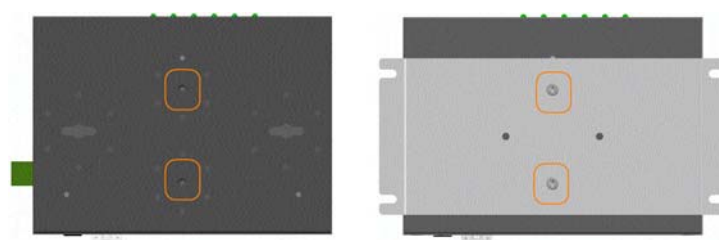


2.5 Panel Mounting

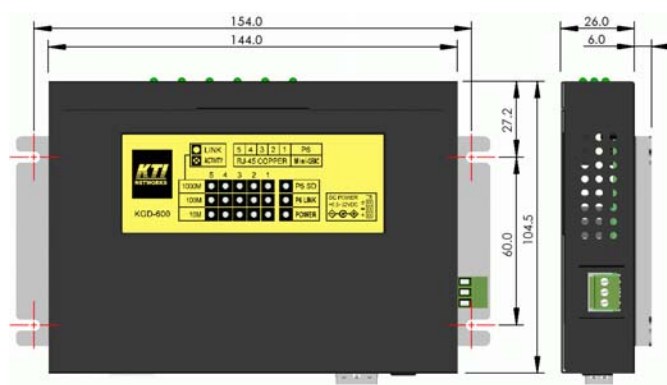
One optional panel mounting bracket is available for purchase as shown below:



Install the bracket on the bottom of the switch unit.

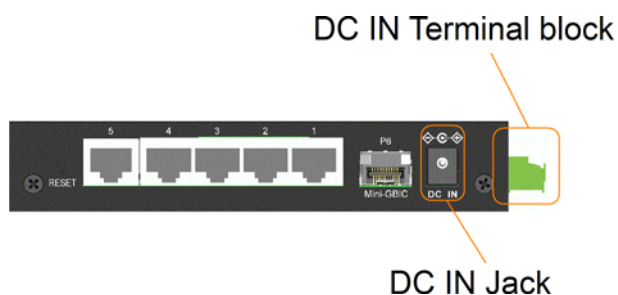


The final dimension after panel bracket is installed is shown below:

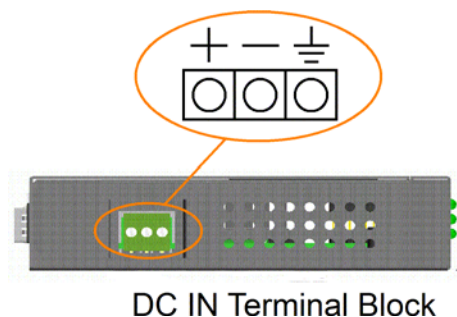


2.6 Applying Power

The switch provides two types of power interfaces, terminal block and DC power jack for receiving DC power input from external power supply system.



Using Terminal Blocks



Three terminal contacts are provided:

Vdc Positive (+) terminal

Vdc Negative (-) terminal

Chassis ground

(Vdc : +6.5V ~ +32VDC)

One 3P terminal plugs are provided together with the switch. The plug is shown below:



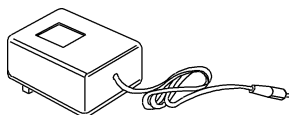
Power wires : 24 ~ 12AWG (IEC 0.5~2.5mm²)

Install the power source wires with the plug properly. Then, plug in the terminal block socket.

Using DC Power Jack

When an external power system is not available, the switch provides a DC jack to receive power from typical AC-DC power adapter alternatively.

AC Power Adapters: Optional commercial rated adapters are available for purchase.



AC input power: AC power voltage of your area, options -
Rated AC120V/60Hz DC7.5V 1A
Rated AC230V/50Hz DC7.5V 1A
Rated AC100V/50-60Hz DC7.5V 1A
Rated AC240V/50Hz DC7.5V 1A

Note: Before you begin the installation, check the AC voltage of your area. The AC power adapter which is used to supply the DC power for the unit should have the AC voltage matching the commercial power voltage in your area.

2.7 Reset Button

The reset button is used to perform a reset to the switch. It is not used in normal cases and can be used for diagnostic purpose. If any network hanging problem is suspected, it is useful to push the button to reset the switch without turning off the power. Check whether the network is recovered.

The button can also be used to restore the software configuration settings to factory default values.

The operations are:

| Operation | Function |
|--|--------------------------------------|
| Press the button more than 5 seconds when power up | Restore all factory default settings |
| Press the button and release during switch operation | Reboot the switch |

2.8 Making UTP Connections

The 10/100/1000 copper ports support the following connection types and distances:

Network Cables

10BASE-T: 2-pair UTP Cat. 3,4,5 , EIA/TIA-568B 100-ohm

100BASE-TX: 2-pair UTP Cat. 5, EIA/TIA-568B 100-ohm

1000BASE-T: 4-pair UTP Cat. 5 or higher (Cat.5e is recommended), EIA/TIA-568B 100-ohm

Link distance: Up to 100 meters

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 is connected, the ports can sense the receiving pair automatically and configure itself 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.

2.9 Making Fiber Connection

The mini-GBIC (SFP) port must be installed with an SFP fiber transceiver for making fiber connection. Your switch may come with an SFP transceiver pre-installed when it is shipped.

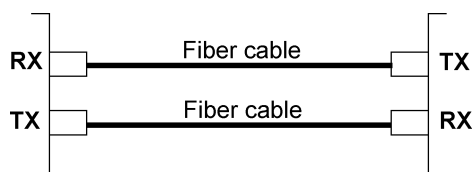
Installing SFP Fiber Transceiver

To install an SFP fiber transceiver into mini-GBIC port, the steps are:

1. Turn off the power to the switch.
2. Insert the SFP fiber transceiver into the mini-GBIC port. Normally, a bail is provided for every SFP transceiver. Hold the bail and make insertion.
3. Until the SFP transceiver is seated securely in the slot, place the bail in lock position.

Connecting Fiber Cables

LC connectors are commonly equipped on most SFP transceiver modules. Identify TX and RX connector before making cable connection. The following figure illustrates a connection example between two fiber ports:



Make sure the Rx-to-Tx connection rule is followed on the both ends of the fiber cable.

Network Cables

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

Single mode (SMF) - 9/125

2.10 LED Indication

| LED | Function | State | Interpretation |
|---------------|--------------------|-------|---|
| POWER | Power status | ON | The power is supplied to the switch. |
| | | OFF | The power is not supplied to the switch. |
| LNK/1000M/ACT | Port link status | ON | A 1000M link is established. (No traffic) |
| | | BLINK | Port link is up and there is traffic. |
| | | OFF | Port link is down. |
| LNK/100M/ACT | Port link status | ON | A 100M link is established. (No traffic) |
| | | BLINK | Port link is up and there is traffic. |
| | | OFF | Port link is down. |
| LNK/1000M/ACT | Port link status | ON | A 10M link is established. (No traffic) |
| | | BLINK | Port link is up and there is traffic. |
| | | OFF | Port link is down. |
| P6 LNK | Port6 link status | ON | A 1000M link is established on Port 6. |
| | | BLINK | Port 6 link is up and there is traffic. |
| | | OFF | Port 6 link is down. |
| P6 OL | Port6 optical link | ON | Optical signal is detected on Port 6. |
| | | OFF | No optical signal is detected on Port 6. |

2.11 Configuring IP Address and Password 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. 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.

3. Advanced Functions

To help a better understanding about the software management interfaces, this chapter describes some advanced functions provided by the switch.

3.1 Abbreviation

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 :

| | | | | |
|-----------------|-----------|---------------|----------|-----------|
| <u>#of bits</u> | <u>16</u> | <u>3</u> | <u>1</u> | <u>12</u> |
| 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

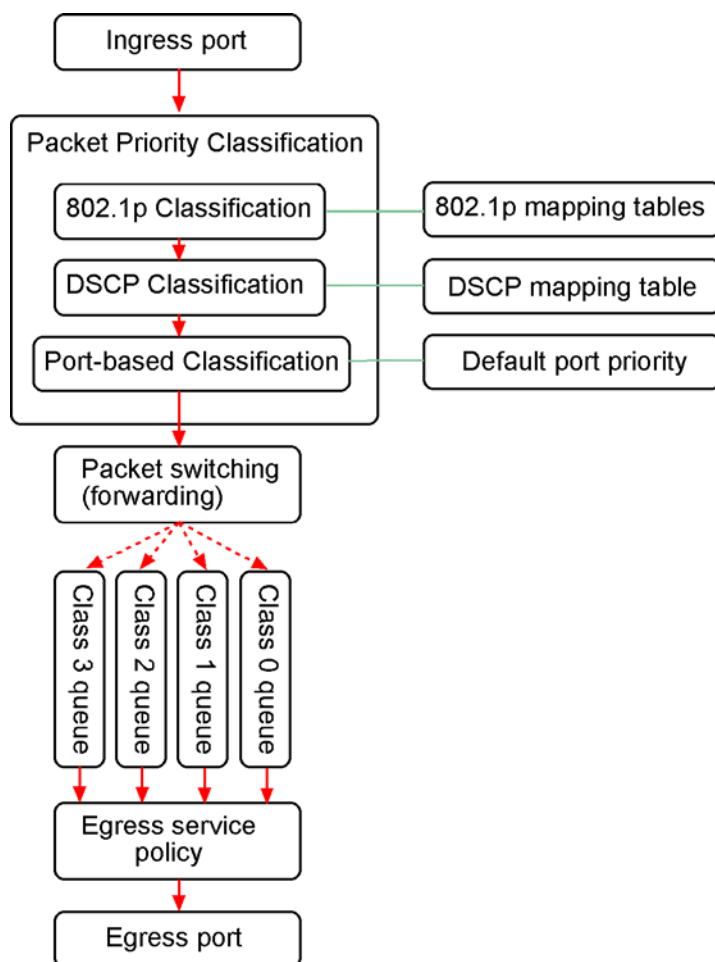
Packet forwarding : also known as packet switching in a network switch based on MAC address table and VLAN table information

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.

3.2 QoS Function

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:



3.2.1 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 than 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.

3.2.2 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.

3.2.3 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

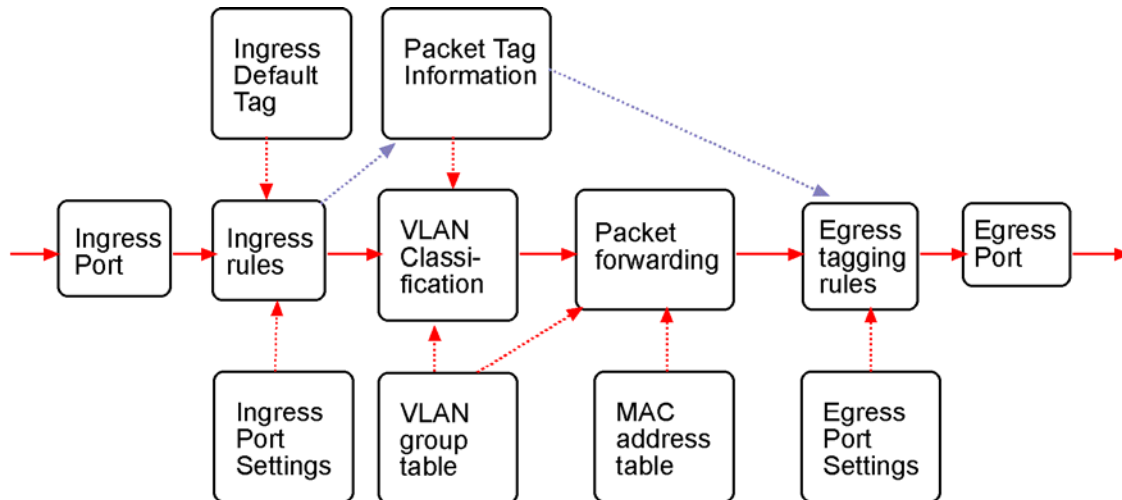
Strict priority policy lets high priority class queue is served first until it is empty. Lower priority queue may not get any service (or egress bandwidth) when higher priority traffic is heavy for long time. Three weighted ratio policies are provided to resolve such problem. Four class queues are served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

3.3 VLAN Function

The switch supports port-based VLAN, 802.1Q Tag VLAN and eight VLAN groups.

3.3.1 VLAN Operation

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.

3.3.2 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:

3.3.2.1 802.1Q Tag Aware Per port setting

Tag-aware - 802.1Q Tag Aware mode is used. The switch examines the tag content of every received packets. 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.

3.3.2.2 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).

3.3.2.3 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

3.3.2.4 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

3.3.3 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.

3.3.4 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 |

3.3.5 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.

3.3.6 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 3.2.4 for details about how the 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.

3.3.7 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.

3.3.8 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. Three egress settings are provided for each port and are described as follows:

3.3.8.1 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.

3.3.9 Summary of VLAN Function

VLAN Modes

Port-based VLAN Mode : simple port-based 2-VLAN-groups mode

Port-based VLAN ISP Mode : simple port-based 5-VLAN-groups mode

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

Advanced VLAN Mode

Egress Settings (per port) : [Tag Aware], [Keep Tag], [Drop Untag], [Drop Tag]

Ingress Default Tag (per port) : [PVID], [CFI], [User Priority]

VLAN Groups (global) : 8 VLAN groups

VLAN Group Settings (per group) : [VID], [Member Ports], [Source Port Check]

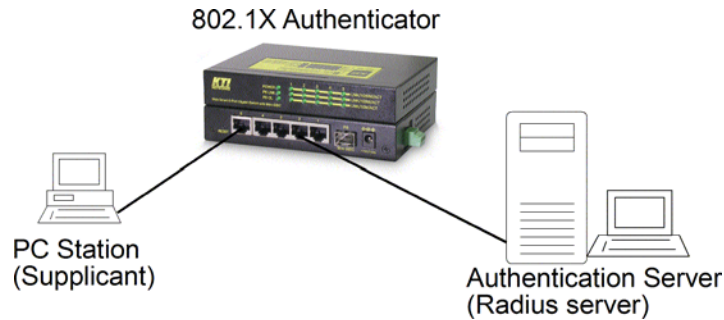
Egress Settings : [Insert Tag], [Untagging Specific VID], [Untagged VID]

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

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

3.4 802.1X Authentication Port Access Control

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:



- **An 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.
- **An 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.
- **An 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.

The 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. Web Management

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

Web Browser

Compatible web browser software with JAVA script support

Microsoft Internet Explorer 4.0 or later

Netscape Communicator 4.x or later

Set IP Address for the System Unit

Before the switch can be managed from a 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 follows:



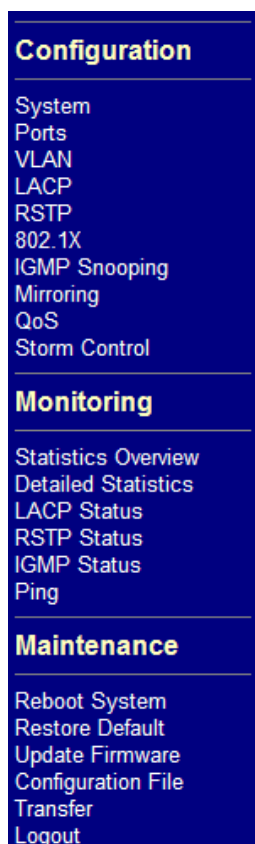
The switch will accept only one successful management connection at the same time. The other connection attempts will be prompted with a warning message.

Duplicated Administrator
This device is managed by 192.168.0.102
currently!!

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 3 minutes.

System Configuration is displayed after a successful login.

4.3 Main Management Menu



The following information describes the basic functions of the main 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 configuration |
| Mirroring | Port mirroring related configuration |
| QoS | Quality of Service related configuration |
| Storm Control | Packet Storm protection control 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 |
| 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 | Upload and save configuration file |
| Logout | Command to logout from the switch management |

4.4 System

System Configuration

| | |
|--------------------|-------------------|
| MAC Address | 00-40-F6-F1-03-43 |
| S/W Version | 1.0 |
| H/W Version | 1.0 |
| Active IP Address | 192.168.0.211 |
| Active Subnet Mask | 255.255.255.0 |
| Active Gateway | 192.168.0.1 |
| DHCP Server | 0.0.0.0 |
| Lease Time Left | 0 secs |

| | | | | | | | |
|--------------------------------|--|--------------------------------|-----|---------------|--------------------------------|--------------------------------|--------------------------------|
| DHCP Enabled | <input type="checkbox"/> | | | | | | |
| Fallback IP Address | <input type="text" value="192.168.0.38"/> | | | | | | |
| Fallback Subnet Mask | <input type="text" value="255.255.255.0"/> | | | | | | |
| Fallback Gateway | <input type="text" value="192.168.0.1"/> | | | | | | |
| Management VLAN | <table><tr><td>VID</td><td>CFI</td><td>User Priority</td></tr><tr><td><input type="text" value="0"/></td><td><input type="text" value="0"/></td><td><input type="text" value="0"/></td></tr></table> | VID | CFI | User Priority | <input type="text" value="0"/> | <input type="text" value="0"/> | <input type="text" value="0"/> |
| VID | CFI | User Priority | | | | | |
| <input type="text" value="0"/> | <input type="text" value="0"/> | <input type="text" value="0"/> | | | | | |
| Name | <input type="text"/> | | | | | | |
| Password | <input type="password" value="..."/> | | | | | | |
| Inactivity Timeout (secs) | <input type="text" value="300"/> | | | | | | |
| 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"/> | | | | | | |

Apply

Refresh

| Configuration | Description |
|---------------------------|--|
| MAC Address | The MAC address factory configured for the switch It can not be changed in any cases. |
| S/W Version | The firmware version currently running |
| H/W Version | The hardware version currently operating |
| Active IP Address | Currently used IP address for the switch management |
| Active Subnet Mask | Currently used subnet mask for IP address for the switch management |
| Active Gateway | Currently used 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 not enabled |
| 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 |
| Management VLAN | Set management VLAN information |
| - VID | VLAN ID configured for web management to the switch |
| - CFI | CFI value for web reply packets from the switch |
| - User priority | Priority value for web reply packets from the switch |
| Name * | Set the system name for this switch unit |
| Password | Set new password |
| Inactivity Timeout (secs) | Set timerout for auto-logout timer |
| SNMP enabled | Enable SNMP agent |
| SNMP Trap destination | The IP address of the SNMP trap manager |
| SNMP Read community | The community allowed for the SNMP [get] message |
| SNMP Write community | The community allowed for the SNMP [set] message |
| SNMP Trap community | The community used for the SNMP trap messages sent by the switch |
| [Apply] | Click to apply the configuration change |
| [Refresh] | Click to refresh current configuration |

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 bootup.

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 the VLAN function is disabled, Management VLAN settings are ignored and no VLAN limitation is applied in accessing the switch web management interface. The switch web (http) server only accepts untagged management packets and replies untagged packets to the management host.
2. If [Management VLAN - VID] settings is zero, no VLAN limitation is applied in accessing the switch web management interface. The switch web (http) server only accepts untagged management packets and replies untagged packets to the management host.
3. If [Management VLAN - VID] settings is not zero, The switch web (http) server only accepts tagged management packets matched [Management VLAN -VID] and replies tagged packets with tag composed of [Management VLAN] VID, CFI and User Priority settings to the management host. The egress port will also be limited in the member ports of the matched VLAN group.

Summary of the rules:

| <u>VLAN Function</u> | <u>Management VID</u> | <u>Switch Embedded Web Server operation</u> |
|----------------------|-----------------------|--|
| VLAN disabled | Ignore | Accept untagged web packets Reply untagged packets No VLAN group member checking |
| VLAN enabled | VID=0 | Accept untagged web packets Reply untagged packets No VLAN group member checking |
| VLAN enabled | VID<>0 (1 ~ 4095) | Accept matched tagged web packets only Reply tagged packets with the configured tag Matched VLAN group member checking |

Notes:

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

4.5 Ports

Port Configuration

| Enable Jumbo Frames | <input checked="" type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|-------------------------------------|------------|-------------------------------------|--------------|---|---------|------------|-------------------------------------|---|------|------------|-------------------------------------|---|---------|------------|-------------------------------------|---|------|------------|-------------------------------------|---|------|------------|-------------------------------------|---|------|------------|-------------------------------------|--|
| Power Saving Mode: | Full | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <table border="1"><thead><tr><th>Port</th><th>Link</th><th>Mode</th><th>Flow Control</th></tr></thead><tbody><tr><td>1</td><td>1000FDX</td><td>Auto Speed</td><td><input checked="" type="checkbox"/></td></tr><tr><td>2</td><td>Down</td><td>Auto Speed</td><td><input checked="" type="checkbox"/></td></tr><tr><td>3</td><td>1000FDX</td><td>Auto Speed</td><td><input checked="" type="checkbox"/></td></tr><tr><td>4</td><td>Down</td><td>Auto Speed</td><td><input checked="" type="checkbox"/></td></tr><tr><td>5</td><td>Down</td><td>Auto Speed</td><td><input checked="" type="checkbox"/></td></tr><tr><td>6</td><td>Down</td><td>Auto Speed</td><td><input checked="" type="checkbox"/></td></tr></tbody></table> | Port | Link | Mode | Flow Control | 1 | 1000FDX | Auto Speed | <input checked="" type="checkbox"/> | 2 | Down | Auto Speed | <input checked="" type="checkbox"/> | 3 | 1000FDX | Auto Speed | <input checked="" type="checkbox"/> | 4 | Down | Auto Speed | <input checked="" type="checkbox"/> | 5 | Down | Auto Speed | <input checked="" type="checkbox"/> | 6 | Down | Auto Speed | <input checked="" type="checkbox"/> | |
| Port | Link | Mode | Flow Control | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1000FDX | Auto Speed | <input checked="" type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | Down | Auto Speed | <input checked="" type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | 1000FDX | Auto Speed | <input checked="" type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | Down | Auto Speed | <input checked="" type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | Down | Auto Speed | <input checked="" type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6 | Down | Auto Speed | <input checked="" type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Drop frames after excessive collisions | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Apply | Refresh | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Configuration

Function

Enable Jumbo Frames Select to enable jumbo frame support

Power Saving Mode *Full* - all the time
Link-up - saving when link up
Link-dwon - saving when link down
Disable - disable power saving

Port The port number

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

Port 1 - Port 5

| <u>Mode</u> | <u>Auto-negotiation</u> | <u>Speed capability</u> | <u>Duplex capability</u> |
|-------------------|-------------------------|-------------------------|--------------------------|
| <i>Auto Speed</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> |

Port 6

| <u>Mode</u> | <u>Auto-negotiation</u> | <u>Speed capability</u> | <u>Duplex capability</u> |
|-------------------|-------------------------|-------------------------|--------------------------|
| <i>Auto speed</i> | <i>Enable</i> | <i>1000M</i> | <i>Full</i> |
| <i>1000 Full</i> | <i>Disable</i> | <i>1000M</i> | <i>Full</i> |

Flow Control

Set port flow control function

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

[Apply]

Click to apply the configuration change

[Refresh]

Click to refresh current configuration

4.6 VLANs

VLAN Configuration

- ☒ VLAN Disable
- ☐ Port-based VLAN Mode > [Setting](#)
- ☐ Port-based VLAN ISP Mode > [Setting](#)
- ☐ Advanced VLAN Mode > [Setting](#)

Remark

Click [Apply] will make your selection effect immediately.
Any improper configuration might cause network connection problem.
Refer to operation manual before making VLAN configuration.

Note

All members of a trunk group if configured must be in same VLAN group and have same all per-port VLAN settings.

| 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 5 port-based VLAN groups |
| Advance 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 Port-based VLAN Mode

VLAN Configuration

Port-based VLAN Mode

| Group | Member ports | | | | | |
|-------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| 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"/> |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Remark

1. Two port-based VLAN groups are created.
2. The member ports in group can communicate with each other.
3. No packet modification from ingress to egress.
4. Member port overlap is allowed.

| 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.

4.6.2 Port-based VLAN ISP Mode

VLAN Configuration

Port-based VLAN ISP Mode

Joint port

Remark

1. 5 port-based VLAN groups are created. Each includes 2 member ports.
2. Joint port is the overlap among all 5 groups.
3. The member ports in group can communicate with each other.
4. No packet modification from ingress to egress.

Example

P6 is joint port.
Groups : [P1,P6] [P2,P6] [P3,P6] [P4,P6] [P5,P6] are created.

| Configuration | Description |
|---------------|--|
| Joint port | Select a port as the joint port for all 5 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 6 is selected as the joint port, the 5 port-based VLAN groups are configured as follows automatically:

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

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.

4.6.3 Advanced VLAN Mode

Advanced VLAN Mode

| | | | |
|---------------------|------------------|-----------------|-------------|
| Ingress Default Tag | Ingress Settings | Egress Settings | VLAN Groups |
|---------------------|------------------|-----------------|-------------|

Ingress Default Tag

| Port | PVID | CFI | User Priority |
|------|--------------------------------|--------------------------------|--------------------------------|
| 1 | <input type="text" value="1"/> | <input type="text" value="0"/> | <input type="text" value="0"/> |
| 2 | <input type="text" value="1"/> | <input type="text" value="0"/> | <input type="text" value="0"/> |
| 3 | <input type="text" value="1"/> | <input type="text" value="0"/> | <input type="text" value="0"/> |
| 4 | <input type="text" value="1"/> | <input type="text" value="0"/> | <input type="text" value="0"/> |
| 5 | <input type="text" value="1"/> | <input type="text" value="0"/> | <input type="text" value="0"/> |
| 6 | <input type="text" value="1"/> | <input type="text" value="0"/> | <input type="text" value="0"/> |

| | | |
|-------|---------|------|
| Apply | Refresh | Back |
|-------|---------|------|

Remark

1. Port's Ingress Default Tag = PVID+CFI+User-priority
This tag is used for egress tagging in port-based mode.
2. PVID is used as index for VLAN group table lookup when
[Tag Aware]=Tag-ignore (port-based mode).
3. PVID is also used as index for VLAN group table lookup when
[Tag Aware]=Tag-aware for untagged and priority-tagged packets.

| 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 |

4.6.3.1 Ingress Default Tag

| 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

4.6.3.2 Ingress Settings

Ingress Settings

| Port | Tag Aware | Keep Tag | Drop Untag | Drop Tag |
|------|--------------|----------|------------|-----------|
| 1 | Tag-ignore ▼ | Enable ▼ | Disable ▼ | Disable ▼ |
| 2 | Tag-ignore ▼ | Enable ▼ | Disable ▼ | Disable ▼ |
| 3 | Tag-ignore ▼ | Enable ▼ | Disable ▼ | Disable ▼ |
| 4 | Tag-ignore ▼ | Enable ▼ | Disable ▼ | Disable ▼ |
| 5 | Tag-ignore ▼ | Enable ▼ | Disable ▼ | Disable ▼ |
| 6 | Tag-ignore ▼ | Enable ▼ | Disable ▼ | Disable ▼ |

Apply Refresh Back

Remark

1. [Tag Aware]

Tag-aware : Use packet's tag VID (if exists and VID>0) for VLAN lookup

Tag-ignore : Use ingress default tag PVID for VLAN lookup

2. [Keep Tag]

Disable : Packet's tag is removed (if exists and VID>0)

Enable : Packet's tag is not removed

| 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:

| <u>Received packet type</u> | <u>Ingress [Tag Aware] setting</u> | |
|-----------------------------|------------------------------------|------------------|
| | <u>Tag-ignore</u> | <u>Tag-aware</u> |
| Untagged | PVID | PVID |
| Priority-tagged (VID=0) | PVID | PVID |
| VLAN-tagged (VID>0) | PVID | Packet tag VID |

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

4.6.3.3 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 |

Apply Refresh Back

Remark

[Insert Tag] - egress tagging
Disable : no tag insertion
Enable : Insert tag to packet when egress

Source of Tag inserted:

Ingress Default Tag when [Tag Aware]=Tag-ignore

Received packet's Tag when [Tag Aware]=Tag-aware and VID>0

Note

If Ingress [Keep Tag] and egress [Insert Tag] are enabled,
Priority-tagged and VLAN-tagged packets will be double-tagged when egress.

| 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 VID of 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:

| <u>Received packet type</u> | <u>[Tag Aware]=Tag-ignore</u> | <u>[Tag Aware]=Tag-aware</u> |
|-----------------------------|-------------------------------|------------------------------|
| 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 |

4.6.3.4 VLAN Groups

VLAN Groups

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

Remark

[Source Port Check] - ingress port must be member port of the VLAN
Otherwise, packet is dropped.

Configuration

Description

Group

Group number

VID

VID of the VLAN to which this group is associated
1 ~ 4095 - decimal 12-bit VID value

Member Ports

Select the admitted egress ports for the packets belong to the VLAN
Port 1 ~ 6 - click to select

Source Port Check

Check whether the ingress port is the member port of the VLAN
Enable - set to enable this check, the packet is dropped if ingress port is not member port of the VLAN.
Disable - 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

4.6.4 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:

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

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. <i>Auto</i> - 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 with same key value are in same LACP aggregate group.
3. The ports with Auto key are in same LACP aggregate group.

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 |

| 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. |
| Max Age | When the switch is the root bridge, the whole LAN will apply this setting as their maximum age time. |
| 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. |
| 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 | <p>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 <i>Auto</i>. <i>Auto</i> means a default cost is automatically calculated in RSTP operation based on the port link speed.</p> <p>The default costs are :</p> <table> <tr> <td><u>Link Speed</u></td><td><u>Auto Default Cost</u></td></tr> <tr> <td>10Mbps</td><td>2000000</td></tr> <tr> <td>100Mbps</td><td>200000</td></tr> <tr> <td>1000Mbps</td><td>20000</td></tr> </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 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 |
| | | | Re-authenticate All | Force Reinitialize All | |

Parameters

| 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 <i>Authorized</i> (green color) - the port is in 802.1X authorized state <i>Unauthorized</i> (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. |
| [Statistics] | Click to show 802.1X related counters for the port. See Section 4.9.1. |
| [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. See Section 4.9.2. |
| [Apply] | Click to apply the configuration change. |
| [Refresh] | Click to refresh current configuration. |

4.9.1 802.1X Statistics

802.1X Statistics for Port 1

Refresh

Port 1

Port 2

Port 3

Port 4

Port 5

Port 6

| Authenticator counters | | | |
|--------------------------------------|---|--------------------------------------|---|
| authEntersConnecting | 0 | authEapLogoffsWhileConnecting | 0 |
| authEntersAuthenticating | 0 | authAuthSuccessesWhileAuthenticating | 0 |
| authAuthTimeoutsWhileAuthenticating | 0 | authAuthFailWhileAuthenticating | 0 |
| authAuthEapStartsWhileAuthenticating | 0 | authAuthEapLogoffWhileAuthenticating | 0 |
| authAuthReauthsWhileAuthenticated | 0 | authAuthEapStartsWhileAuthenticated | 0 |
| authAuthEapLogoffWhileAuthenticated | 0 | | |
| Backend Authenticator counters | | | |
| backendResponses | 0 | backendAccessChallenges | 0 |
| backendOtherRequestsToSupplicant | 0 | backendAuthSuccesses | 0 |
| backendAuthFails | 0 | | |
| dot1x MIB counters | | | |
| dot1xAuthEapolFramesRx | 0 | dot1xAuthEapolFramesTx | 0 |
| dot1xAuthEapolStartFramesRx | 0 | dot1xAuthEapolLogoffFramesRx | 0 |
| dot1xAuthEapolRespIdFramesRx | 0 | dot1xAuthEapolRespFramesRx | 0 |
| dot1xAuthEapolReqIdFramesTx | 0 | dot1xAuthEapolReqFramesTx | 0 |
| dot1xAuthInvalidEapolFramesRx | 0 | dot1xAuthEapLengthErrorFramesRx | 0 |
| dot1xAuthLastEapolFrameVersion | 0 | dot1xAuthLastEapolFrameSource | |
| Other statistics | | | |
| Last Supplicant identity | | | |

Configuration

Description

| | |
|-----------|--|
| [Port X] | Click to select Port X for the statistics. |
| [Refresh] | Click to refresh current counters. |

4.9.2 802.1X Re-authentication Parameters

802.1X Parameters

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

| 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 checked="" type="checkbox"/> |
| Router Ports | 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> |
| 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 IGMP snooping. |
| Router Ports | The ports which have multicast routers connected and require forwarding of all IPMC packets unconditionally |
| Unregistered IPMC Flooding | Enable to flooding unregistered IPMC |
| VLAN ID | The VID of an existing VLAN |
| IGMP Snooping Enabled | Check to enable IGMP snooping function on the associated VID. |
| IGMP Querying Enabled | Check to enable IGMP querying function on the associated VID. |
| [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"/> |

| | |
|-------------|-----|
| Mirror Port | 1 ▾ |
|-------------|-----|

| | |
|-------|---------|
| Apply | Refresh |
|-------|---------|

| Configuration | Description |
|---------------|--|
| Mirror Port | The port is 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

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 |

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

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

Remark

1. 802.1p mode uses L2 packet's User Priority tag for priority classification.
2. DSCP mode uses L3 IP packet's DSCP value for priority classification.
3. 802.1p mode is superior over DSCP mode when both are enabled.
4. Port Priority is used when 802.1p and DSCP failed in classification.
5. Priority level : Class 3 > Class 2 > Class 1 > Class 0

| 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.

4.12.1 802.1p 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 ▾ |

Remark

1. Per port table : per User Priority tag value (0~7) maps to one priority class
2. Used to classify priority-tagged and VLAN-tagged packets

| 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 <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 |
|--------|--------------------------------|

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

4.12.2 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 ▾ |

Remark

1. Table : per DSCP value (0~63) maps to one priority class
2. Used to classify L3 IP packets
3. All ports share same table.

| Configuration | Description |
|---------------|--|
| DSCP [0-63] | Seven user-defined DSCP values which are configured with a priority class <i>0 ~ 63 - 6-bit DSCP value in decimal</i> |
| 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.

4.12.3 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 |

Remark

1. Strict priority : high class is always served first till it is empty
2. Weighted ratio : 4 classes are served in round robin weighted ratio
3. Four classes are served with weighted guaranteed bandwidth on an egress port.

| 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 Statistics Overview

Statistics Overview for all ports

[Clear](#)[Refresh](#)

| Port | Tx Bytes | Tx Frames | Rx Bytes | Rx Frames | Tx Errors | Rx Errors |
|------|----------|-----------|-----------|-----------|-----------|-----------|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 235077 | 975 | 115729236 | 476580 | 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 |

| 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. |
|-----------|--|

4.15 Detailed Statistics

Statistics for Port 1

Clear

Refresh

Port 1

Port 2

Port 3

Port 4

Port 5

Port 6

| Receive Total | | | Transmit Total | | |
|--------------------------|--|---|--------------------------|--|---|
| Rx Packets | | 0 | Tx Packets | | 0 |
| Rx Octets | | 0 | Tx Octets | | 0 |
| 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 | | 0 | Tx Broad- and Multicast | | 0 |
| Rx Error Packets | | 0 | 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/Alligment | | - | 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. |
|-----------|--|

4.16 LACP Status

LACP Aggregation Overview

| Group/Port | 1 | 2 | 3 | 4 | 5 | 6 |
|------------|---|---|---|---|---|---|
| Normal | | | | | | |
| Group 1 | 1 | 2 | | | | |
| Group 2 | | | 1 | 2 | | |

| Aggregation Group 1 | |
|---------------------------|-------------------|
| Partner MAC Address | 00-40-F6-EC-2E-2F |
| Local Ports Aggregated | 1,2 |
| Seconds since last change | 803 |
| Aggregation Group 2 | |
| Partner MAC Address | 00-40-F6-EC-2D-87 |
| Local Ports Aggregated | 3,4 |
| Seconds since last change | 1042 |

| Legend | |
|---|------------|
|  | Down |
|  | Blocked |
|  | Learning |
|  | Forwarding |
|  | Forwarding |

Refresh

| Status | Description |
|-----------------------|---|
| Port | The port number |
| Normal | Display the ports not LACP enabled. |
| Group # | The LACP group |
| Status | <p>The LACP port status presented with color and a number</p> <p><Down> - the port is link down</p> <p><Blocked & #> - the port is blocked by RSTP and the # is the port number of LACP link partner</p> <p><Learning> - the port is learning by RSTP</p> <p><Forwarding> - the port is link up and forwarding frames</p> <p><Forwarding & #> - the port is link up and forwarding frames and the # is the port number of LACP link partner</p> |
| 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

| Port | Protocol Active | Partner Port Number | Operational Port Key |
|------|-----------------|---------------------|----------------------|
| 1 | yes | 1 | 3 |
| 2 | yes | 2 | 3 |
| 3 | yes | 1 | 515 |
| 4 | yes | 2 | 515 |
| 5 | no | | |
| 6 | no | | |

| 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 |

4.17 RSTP Status

RSTP VLAN Bridge Overview

| VLAN Id | Bridge Id | Hello Time | Max Age | Fwd Delay | Topology | Root Id |
|---------|-------------------------|------------|---------|-----------|----------|--------------------------------------|
| 1 | 32769:00-40-F6-EC-31-F6 | 2 | 20 | 1 | Steady | 32768:50-67-F0-53-53-6E via port : 1 |

Refresh

RSTP Port Status

| Port/Group | Vlan Id | Path Cost | Edge Port | P2p Port | Protocol | Port State |
|------------|---------|-----------|-----------|----------|----------|------------|
| Port 1 | 1 | 20000 | no | yes | STP | Forwarding |
| Port 2 | | | | | | Disabled |
| Port 3 | | | | | | Non-STP |
| Port 4 | | | | | | Non-STP |
| Port 5 | | | | | | Non-STP |
| Port 6 | | | | | | Non-STP |

| Status | Description |
|---------------|--|
| VLAN ID | The RSTP status on the VLAN is displayed. |
| Bridge ID | The Bridge ID of this Bridge instance. |
| 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. |
| Max Age | When the switch is the root bridge, the whole LAN will apply this setting as their maximum age time. |
| 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. |
| Topology | The current state of the Topology Change Flag for this Bridge instance. |
| Root ID | The Bridge ID of the currently elected root bridge. |

| | |
|-----------|------------------------------|
| [Refresh] | Click to refresh the status. |
|-----------|------------------------------|

| Port Status | Description |
|-------------|--|
| Port/Group | The port ID or aggregation group ID |
| Vlan ID | The RSTP port status on the VLAN is displayed. |
| Path Cost | The current STP port path cost. This will either be a value computed from the Auto setting, or any explicitly configured value. |
| Edge Port | The current STP port (operational) Edge Flag. An Edge Port is a switch port to which no Bridges are attached. The flag may be automatically computed or explicitly configured. Each Edge Port transits directly to the Forwarding Port State, since there is no possibility of it participating in a loop. |
| P2P Port | The current STP port point-to-point flag. A point-to-point port connects to a non-shared LAN media. The flag may be automatically computed or explicitly configured. The point-to-point properties of a port affect how fast it can transition STP state. |
| Protocol | STP or RSTP is applied on the port. |
| Port State | The current STP port state. The port state can be one of the following values: <i>Blocking</i> , <i>Learning</i> , <i>Forwarding</i> , <i>Non-STP</i> , <i>Disabled</i> . |

4.18 IGMP Status

IGMP Status

| VLAN ID | Querier | Queries transmitted | Queries received | v1 Reports | v2 Reports | v3 Reports | v2 Leaves |
|---------|---------|---------------------|------------------|------------|------------|------------|-----------|
| 1 | Idle | 14 | 10 | 0 | 134 | 22 | 5 |

Refresh

Member Groups

| VLAN ID | Groups | Port Members |
|---------|-----------------|--------------|
| 1 | 224.0.0.251 | 5 |
| 1 | 239.255.255.250 | 5 |
| 1 | 224.0.1.60 | 5 |
| 1 | 224.0.1.22 | 5 |
| 1 | 224.0.0.252 | 5 |

| Status | Description |
|---------------------|--|
| VLAN ID | The IGMP status on the VLAN is displayed. |
| Querier | Show the Querier status is Active or Idle? |
| Queries transmitted | The number of Transmitted Querier |
| Queries received | The number of Received Querier |
| 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 Leaves | The number of received v2 Leave s |
| [Refresh] | Click to refresh the current status. |

| | |
|--------------|--|
| VLAN ID | The VLAN where the multicast group is found |
| Groups | The IP multicast group found |
| Port Members | The port members of the IP multicast group found |

4.19 Ping

Ping Parameters

| | |
|--------------------|------------------------------------|
| Target IP address | <input type="text"/> |
| Count | 1 <input type="button" value="v"/> |
| Time Out (in secs) | 1 <input type="button" value="v"/> |

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

| 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 |
| 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 reponse time of a ping request (in mini-seconds) |

4.20 Reboot System

Warm Restart

Are you sure you want to perform a Warm Restart?

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.

4.21 Restore Default

Restore Default

Are you sure you want to restore factory default?

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.

4.22 Update Firmware

Software Upload

This page facilitates an update of the firmware controlling the switch. Enter the path and file name of a software image file for uploading.

| | |
|----------|---|
| [Browse] | Click to the location of a software image |
| [Upload] | Click to start uploading. |

After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and the switch reboots.

Warning: While the firmware is being updated, Web access appears to be defunct. Do not reset or power off the device at this time or the switch may fail to function afterwards.

4.23 Configuration File Transfer

You can upload or download the switch configuration.

Configuration Upload



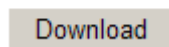
The interface for uploading a configuration file. It features a text input field for the file path and name, followed by a button labeled '瀏覽...' (Browse...). Below the input field is an 'Upload' button.

Enter the path and file name of a configuration file for uploading.

[Browse] Click to the location of a configuration file

[Upload] Click to start uploading configuration.

Configuration Download



The interface for downloading a configuration file. It features a single 'Download' button.

[Download] Click to start download of the configuration.

4.24 Logout

Please enter password to login



The interface for logging out, which prompts the user to enter a password. It includes a label 'Password:' followed by a text input field. Below the input field is an 'Apply' button.

Logout menu is used to perform a logout from the switch management immediately. For convenience, a login page to the same switch is prompted.

5. SNMP Support

| | | |
|----------------------|---|------------------------------------|
| SNMP version support | Snmv 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 } |
| 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 | |
| SNMP Trap Support | RFC 1573 - Evolution of the Interfaces Group of MIB-II | |
| | TRAP_COLDSTART - the device boot up trap | |
| | TRAP_LINKUP - the port link recovery trap | |
| | TRAP_LINKDOWN - port link down trap | |

Appendix. Factory Default Settings

System Configuration

| | |
|---------------------------------|------------------------------|
| DHCP Enabled | <i>Not select (disabled)</i> |
| Fallback IP Address | <i>192.168.0.2</i> |
| Fallback IP Subnet mask | <i>255.255.255.0</i> |
| Fallback Gateway IP | <i>192.168.0.1</i> |
| Management VLAN - VID | <i>0</i> |
| Management VLAN - CFI | <i>0</i> |
| Management VLAN - User priority | <i>0</i> |
| Name | <i>Null</i> |
| Inactivity timeout | <i>300 seconds</i> |
| Password | <i>123</i> |
| SNMP enabled | <i>Not select (disabled)</i> |
| SNMP Trap destination | <i>0.0.0.0</i> |
| SNMP Read community | <i>public</i> |
| SNMP Write community | <i>private</i> |
| SNMP Trap community | <i>public</i> |

Ports Configuration

| | |
|---------------------|---------------------------------|
| Enable Jumbo Frames | <i>Not select (disabled)</i> |
| Power Saving Mode | <i>Full</i> |
| Port Mode | <i>Auto for all ports</i> |
| Flow Control | <i>v : Enable for all ports</i> |

VLAN Configuration

| | |
|-----------|---------------------|
| Main Mode | <i>VLAN Disable</i> |
|-----------|---------------------|

Port-based VLAN Mode setting

| | |
|--------------|---|
| Member Ports | <i>Port 1, 2, 3, 4, 5, 6 for Group 1</i> <i>None for Group 2</i> |
|--------------|---|

Port-based VLAN ISP Mode setting

| | |
|------------|---------------|
| Joint Port | <i>Port 6</i> |
|------------|---------------|

Advanced VLAN Mode Settings

| | |
|----------------------------|------------------------|
| Ingress Default Tag - PVID | <i>1 for all ports</i> |
| Ingress Default Tag - CFI | <i>0 for all ports</i> |

| | |
|-------------------------------------|--------------------------|
| Ingress Default Tag - User Priority | 0 for all ports |
| Ingress Setting - Tag Aware | Tag-ignore for all ports |
| Ingress Setting - Keep Tag | Enable for all ports |
| Ingress Setting - Drop Untag | Disable for all ports |
| Ingress Setting - Drop Tag | Disable for all ports |
| Egress Setting - Insert Tag | Disable for all ports |
| Egress Setting - Untagging VID | Disable for all ports |
| Egress Setting - Untagged VID | 1 for all ports |
| VLAN Group 1 - VID | 1 |
| VLAN Group 1 - Member Ports | Port 1, 2, 3, 4, 5, 6 |
| VLAN Group 1 - Source Port Check | Disable |
| VLAN Group 2 - VID | 2 |
| VLAN Group 2 - Member Ports | None |
| VLAN Group 2 - Source Port Check | Disable |
| VLAN Group 3 - VID | 3 |
| VLAN Group 3 - Member Ports | None |
| VLAN Group 3 - Source Port Check | Disable |
| VLAN Group 4 - VID | 4 |
| VLAN Group 4 - Member Ports | None |
| VLAN Group 4 - Source Port Check | Disable |
| VLAN Group 5 - VID | 5 |
| VLAN Group 5 - Member Ports | None |
| VLAN Group 5 - Source Port Check | Disable |
| VLAN Group 6 - VID | 6 |
| VLAN Group 6 - Member Ports | None |
| VLAN Group 6 - Source Port Check | Disable |
| VLAN Group 7 - VID | 7 |
| VLAN Group 7 - Member Ports | None |
| VLAN Group 7 - Source Port Check | Disable |
| VLAN Group 8 - VID | 8 |
| VLAN Group 8 - Member Ports | None |
| VLAN Group 8 - Source Port Check | Disable |

LACP Port Configuration

| | |
|------------------|-------------------------------------|
| Protocol Enabled | Not select (disabled) for all ports |
| Key Value | auto for all ports |

RSTP System Configuration

| | |
|-----------------|--------|
| System Priority | 32768 |
| Hello Time | 2 |
| Max Age | 20 |
| Forward Delay | 15 |
| Force Version | Normal |

RSTP Port Configuration

| | |
|------------------|--|
| Protocol enabled | <i>Not select (disabled) for all ports</i> |
| Edge | <i>v: Select for all ports</i> |
| Max Age | 20 |
| Forward Delay | 15 |
| Force Version | Normal |

802.1X Configuration

| | |
|--------------------------|---------------------------------------|
| Mode | <i>Disabled</i> |
| RADIUS IP | <i>0.0.0.0</i> |
| RADIUS UDP Port | <i>1812</i> |
| RADIUS Secret | <i>None</i> |
| Admin State | <i>Force Authorized for all ports</i> |
| Reauthentication Enabled | <i>No</i> |
| Reauthentication Period | <i>3600</i> |
| EAPTimeout | <i>30</i> |
| Port 1~Port 6 - tag 1 | <i>Class 0</i> |
| Port 1~Port 6 - tag 2 | <i>Class 1</i> |
| Port 1~Port 6 - tag 3 | <i>Class 1</i> |
| Port 1~Port 6 - tag 4 | <i>Class 2</i> |
| Port 1~Port 6 - tag 5 | <i>Class 2</i> |
| Port 1~Port 6 - tag 6 | <i>Class 3</i> |
| Port 1~Port 6 - tag 7 | <i>Class 3</i> |

IGMP Snooping Configuration

| | |
|----------------------------|------------------------------|
| IGMP Snooping | <i>Enabled for all ports</i> |
| Router Ports | <i>None</i> |
| Inregistered IPMC Flooding | <i>Disabled</i> |
| IGMP Snooping | <i>Enabled for all VLANs</i> |

IGMP Querying *Enabled for all VLANs*

Mirroring Configuration

Mirror source *Not select for all ports*
Mirror Port *1 (Port 1)*

Quality of Service Configuration

802.1p Classification *Disable for all ports*
DSCP Classification *Disable for all ports*
Port Priority *Class 3 for all ports*

QoS 802.1p Mapping

Port 1~Port 6 - tag 0 *Class 0*
Port 1~Port 6 - tag 1 *Class 0*
Port 1~Port 6 - tag 2 *Class 1*
Port 1~Port 6 - tag 3 *Class 1*
Port 1~Port 6 - tag 4 *Class 2*
Port 1~Port 6 - tag 5 *Class 2*
Port 1~Port 6 - tag 6 *Class 3*
Port 1~Port 6 - tag 7 *Class 3*

QoS DSCP Mapping

DSCP 1 / Priority *0, Class 0*
DSCP 2 / Priority *0, Class 0*
DSCP 3 / Priority *0, Class 0*
DSCP 4 / Priority *0, Class 0*
DSCP 5 / Priority *0, Class 0*
DSCP 6 / Priority *0, Class 0*
DSCP 7 / Priority *0, Class 0*
All others DSCP *Class 0*

QoS Service Policy

Port 1 *Strict priority*
Port 2 *Strict priority*
Port 3 *Strict priority*
Port 4 *Strict priority*
Port 5 *Strict priority*
Port 6 *Strict priority*

QoS DSCP Mapping

| | |
|-------------------|-------------------|
| DSCP 1 / Priority | <i>0, Class 0</i> |
| DSCP 2 / Priority | <i>0, Class 0</i> |
| DSCP 3 / Priority | <i>0, Class 0</i> |
| DSCP 4 / Priority | <i>0, Class 0</i> |
| DSCP 5 / Priority | <i>0, Class 0</i> |
| DSCP 6 / Priority | <i>0, Class 0</i> |
| DSCP 7 / Priority | <i>0, Class 0</i> |
| All others DSCP | <i>Class 0</i> |

QoS Service Policy

| | |
|--------|------------------------|
| Port 1 | <i>Strict priority</i> |
| Port 2 | <i>Strict priority</i> |
| Port 3 | <i>Strict priority</i> |
| Port 4 | <i>Strict priority</i> |
| Port 5 | <i>Strict priority</i> |
| Port 6 | <i>Strict priority</i> |

Storm Control Configuration

| | |
|----------------------|-----------------|
| Broadcast Rate | <i>No limit</i> |
| Multicast Rate | <i>No limit</i> |
| Flooded Unicast Rate | <i>No limit</i> |