



KS-1080

Installation Guide

(C) 2002 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 directive 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.

WARNING: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

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.

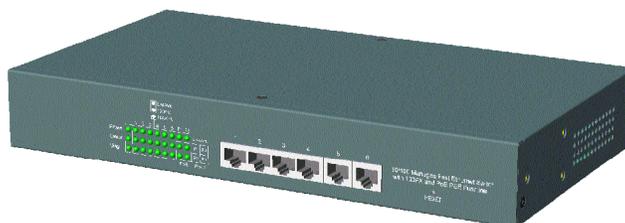
Table of Contents

1. Introduction	6
1.1 Features	7
1.2 Front and Rear Panels	7
1.3 Specifications	8
2. Installation	11
2.1 Unpacking	11
2.2 Safety Cautions	11
2.3 Mounting the Switch	11
2.4 AC Power Supply	12
2.5 Making UTP Connections	12
2.6 Making Power over Ethernet UTP Connections	12
2.7 Making Fiber Connections	13
2.8 Configuring IP Address and Access Settings for the Switch	14
2.9 Reset Button	14
2.10 LED Indicators	14
3. Advanced Functions	15
3.1 QoS Function	15
3.1.1 Priority Level	15
3.1.2 Egress Service Policy	15
3.1.3 Packet Priority Classification	15
3.1.3.1 Port-based Priority Setting (per port setting)	16
3.1.3.2 802.1p Classification (per port setting)	16
3.1.3.3 DSCP Classification (per port setting)	16
3.1.3.4 IP Network Address Classification	17
3.1.4 Other QoS Settings	17
3.2 VLAN Function	18
3.2.1 VLAN Operation	18
3.2.2 Ingress Rules	19
3.2.2.1 802.1Q Tag Aware VLAN Mode (global setting)	19
3.2.2.2 Ingress Member Filtering (global setting)	19
3.2.2.3 Unmatched VID Filtering (per port setting)	19
3.2.3 VLAN Group Mapping	20
3.2.4 Packet Forwarding under VLAN	20
3.2.5 Egress Tagging Rules	20
3.2.5.1 Egress Tag Rule (per port setting)	20
3.2.5.2 Null VID Replacement (per port setting)	21
3.2.6 Summary of VLAN Function	21
3.3 Power over Ethernet Function	22
3.3.1 PoE Specifications	22
3.3.2 PoE PSE Capabilities	22
3.3.3 PoE Management functions	23
3.3.4 Notices for PoE Installation	23
4. Software Management	24
4.1 Telnet Management Interface	24

4.2 IP Menu	25
4.3 SNMP Menu	26
4.4 Port Config	27
4.5 Administrator	28
4.5.1 Administrator -> VLAN Settings	28
4.5.2 Administrator -> QoS Settings	32
4.5.3 Administrator -> PoE Settings	35
4.6 Restore Default Values	36
4.7 Security Manager	36
4.8 Update Firmware	36
4.9 Reboot System	37
4.10 Exit	37
5. Web Management	38
5.1 Start Browser Software and Making Connection	38
5.2 Login to the Switch Unit	38
5.3 Port Status Menu	40
5.4 Administrator	41
5.4.1 Basic Menu	41
5.4.2 Port Controls	44
5.4.3 VLAN Controls	45
5.4.4 QoS Controls	48
5.4.5 PoE Controls	51
5.4.6 Security Manager	52
5.4.7 Image Refresh Time	52
5.4.8 Update Firmware	53
5.4.9 Restore Default	53
5.4.10 Reboot System	53
6. SNMP Management	54
6.1 MIB Objects	54
6.2 SNMP Traps	54
Appendix. Factory Default Settings	55

1. Introduction

The switch provides six 10/100Mbps Fast Ethernet switched copper ports and two 100Mbps fiber port slots. The copper ports support auto-negotiation and auto MDI/MDI-X for easy making connections to Fast Ethernet devices.



The switch also provides the following advantages:

Fiber Connections

The 100Mbps fiber port slots can accommodate a variety of optional fiber modules for multimode and single mode fiber connections.

Power over Ethernet (PoE)

Four of the copper ports are equipped with IEEE standard Power over Ethernet (PoE) function. The PoE function enables the ports to deliver DC power to the remote connected devices which are capable to receive operating power from the network cable. This allows to extend the network connections to a locations where the power line is difficult to reach.

Quality of Service (QoS)

For more multimedia applications over IP such as voice and video, the switch provides a very powerful QoS function which allows high priority data to be forwarded with best performance. The provided packet priority classifications are powerful and flexible to meet different application needs. The classifications can be port-based, 802.1p-based, IP-DSCP-based, or IP network address based.

Virtual LAN (VLAN)

For VLAN environments, the switch provides a flexible VLAN mechanism to support eight different VLANs at the same time. Each VLAN can be identified by full 12-bit VLAN ID value. Together with powerful ingress filtering rules and egress tagging rules, the switch allows LAN administrators to build a VLAN network easily.

Management

For configuration and management purpose, the switch is featured with the following management interfaces:

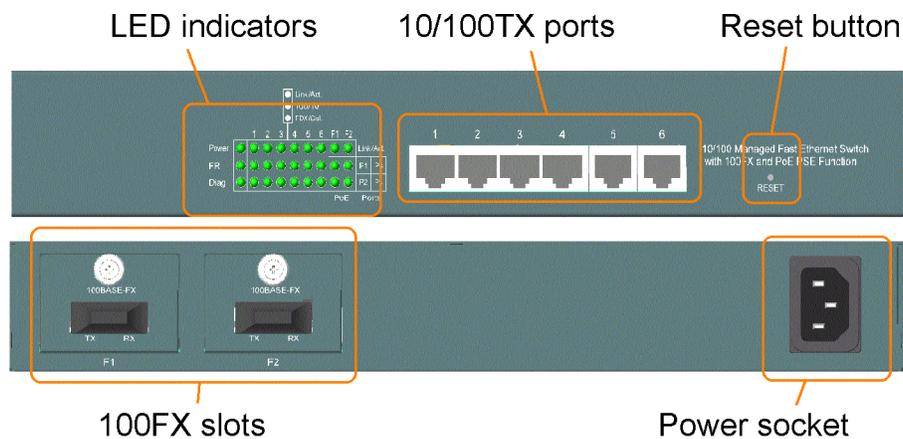
- Telnet software over TCP/IP network
- SNMP manager software over TCP/IP network
- Web browser software from Internet or Intranet over TCP/IP network
- SNMP trap hosts from Internet or Intranet over TCP/IP network

1.1 Features

- Fast Ethernet switch with 6 10/100TX TP ports and 2 100FX slots
- Auto MDI/MDI-X detection on all TP ports
- Auto-negotiation capable on all TP ports
- Port configuration control function
- IEEE 802.3af PoE PSE function on 4 TP ports
- 100FX slots support wide range of fiber options
 - ST, SC, MT-RJ, VF-45, LC, single WDM SC
 - Multi-mode fiber, Single mode duplex fiber, Single fiber
 - Short reach, medium reach, and long reach fiber connections
- Far End Fault function on FX ports
- Back pressure flow control for half duplex operation
- IEEE 802.3x flow control for full duplex operation
- Broadcast storm protection function
- Software management : Web, SNMP, telnet, SNMP trap
- QoS function
- VLAN function
- Provides comprehensive LED indication
- Support desktop, wall, and 19-inch rack mounting

1.2 Front and Rear Panels

The front panel and rear panel of the switch are shown as follows:



1.3 Specifications

Network Ports

TP Copper Ports	6 fixed 10/100TX Twisted Pair Ports (P1 - P6)
PoE Function Ports	4 of the 6 10/100TX ports with configurable PoE PSE function (P1 - P4)
FX Ports	2 100FX fiber slots

10/100TX Twisted Pair Port (TP Port P1 ~ P6)

Compliance	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX
Connectors	Shielded RJ-45 jacks
Pin assignments	Auto MDI/MDI-X detection
Configuration	Auto-negotiation capable or forced mode
Transmission rate	10Mbps, 100Mbps
Duplex support	Full/Half duplex
Flow control	IEEE 802.3x pause frame base for full duplex operation Back pressure for half duplex operation
Network cable	Cat.5 UTP
PoE function	P1 ~ P4 with optional PoE PSE function

100FX Fiber Slots (FX Ports)

Compliance	IEEE 802.3u 100BASE-FX
Configuration	Forced 100Mbps, Full duplex (factory default)
Transmission rate	100Mbps
Far end fault function	Capable to receive FEFI (far end fault indication) signal Capable to send FEFI signal when Rx link failure detected
Flow control	IEEE 802.3x pause frame base for full duplex operation Back pressure for half duplex operation
Optional modules	Refer to Installation guide for optional fiber modules
Network cables	MMF 50/125mm 60/125mm, SMF 9/125mm
Eye safety	IEC 825 compliant

PoE Function

Compliance	IEEE 802.3af
PoE PSE ports	P1 ~ P4
PSE Pinout	Alternative B RJ-45 Pin 4,5 - Positive Vport RJ-45 Pin 7,8 - Negative Vport
PSE level	Class 0 for all ports
Maximum output	15.4W per PoE port
Port Output voltage	Vport = 48VDC

Control	Enable/Disable via software control
Monitor	Power status, power voltage, power current, watts

Switch Functions

Forwarding & filtering	Non-blocking, full wire speed
Switching technology	Store and forward
Maximum packet length	1536 bytes
Broadcast storm	64 consecutive broadcast packets in 800ms Protection by dropping broadcast storm packets
VLAN function	Port-based VLAN & IEEE 802.1Q Tag-based VLAN
QoS function	Port-based, 802.1p-based, IP DSCP-based, IP address-based
Port control	Port configuration control via software management

Software Management Functions

Interfaces	Web, telnet, SNMP MIB-II & private MIB, Traps
Management objects	Port configuration control and status Username and password settings IP, SNMP related settings VLAN function settings QoS function setting PoE function setting and status

Port Configuration Control Function

Configuration	P1 ~ P6
Port control function	Port TX/RX - enable, disable Port mode - Auto (auto-negotiation), Forced Port speed - 100Mbps, 10Mbps Port duplex - full, half
Port Status	Port mode, link, speed, duplex

VLAN Function

VLAN groups	8 groups
Global Settings	VLAN Mode - Port-based, 802.1Q Tag Aware VLAN Ingress member port filtering mode
VLAN Group Settings	12-bit VLAN ID Member ports
Per Port Settings	Default VLAN group index Unmatched VID packet ingress filtering mode Egress Tagging Rules

Null VID replacement mode (Egress)

QoS Function

Priority level	2, High priority and Low priority
Priority classifications	Port-based priority mode (per port setting) 802.1p classification (per port setting) Default IP DSCP classification (per port setting) 2 user defined DSCP match classification (global) 2 user defined IP network address match classification (global)
802.1p priority tag	Threshold tag value setting for high priority (0 ~ 7)
Egress service policy	Weighted round robin ratio : 16:1, always high first, 8:1, 4:1

LED Indicators

System	Power status
Diag	Diagnostic status
Per 10/100TX port	TP port link status, 100M/10M status, duplex status
Per 100FX port	FX port link status
Per PoE port	PoE power status

Power Characteristics

Power supply	Rating AC input : 100~240V / 50-60Hz
Input voltage range	90VAC ~ 264VAC
Input frequency range	47 ~ 63Hz
Power consumption	100W max. @AC110V (All PoE ports output maximum power.)

Environmental

Operating temperature	-5°C ~ 40°C
Storage temperature	-20°C ~ 85°C
Relative humidity	5% ~ 95% noncondensing

Physical Characteristics

Dimension	295 x 160 x 43 mm (L x D x H)
Weight	1.5 Kg
Mounting	Desktop, Wall mountable, 19-inch rack mountable

Electrical Approvals

FCC	Part 15 rule Class A
CE	EMC, CISPR22 Class A

2. Installation

2.1 Unpacking

The product package contains:

- The switch unit
- One power cord
- One 19-inch rack mounting kit
- One product CD-ROM

2.2 Safety Cautions

To reduce the risk of bodily injury, electrical shock, fire, and damage to the equipment, 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.

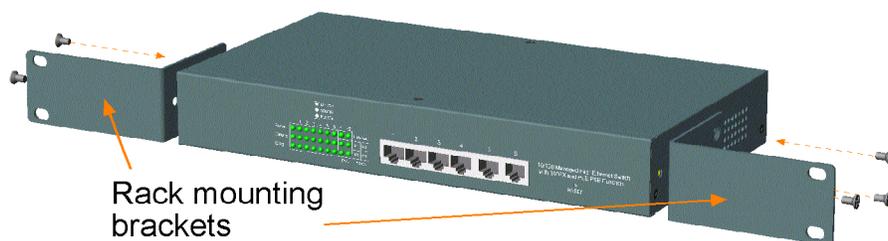
2.3 Mounting the Switch

Desktop Mounting

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

Rack Mounting

Two 19-inch rack mounting brackets are supplied with the switch for 19-inch rack mounting.



The steps to mount the switch onto a 19-inch rack are:

1. Turn the power to the switch off.
2. Install two brackets with supplied screws onto the switch as shown in above figure.
2. Mount the switch onto 19-inch rack with rack screws securely.
3. Turn the power to the switch on.

2.4 AC Power Supply

One AC power cord which meets the specification of your country of origin was supplied with the switch unit. Before installing AC power cord to the switch, make sure the AC power switch is in OFF position and the AC power to the power cord is turned off.

The switch supports wide range of AC power input specifications as follows:

Power Rating : 100 ~ 240VAC, 50/60Hz, 100W max.
Voltage Range : 90 ~ 264VAC
Frequency : 47 ~ 63 Hz

2.5 Making UTP Connections

The 10/100TX ports supports the following connection types and distances:

<u>Speed</u>	<u>Compliance</u>	<u>UTP Cables</u>	<u>Distance</u>
10Mbps	IEEE 802.3 10BASE-T	Cat. 3, 4, 5, 5e	100 meters
100Mbps	IEEE 802.3u 100BASE-TX	Cat. 5, 5e	100 meters

The ports can be configured to one of the following operating modes:

Auto mode : The port is auto-negotiation enabled and uses the speed and duplex settings as the highest port capability for negotiation with the auto-negotiation capable link partner.

Forced mode : The port is auto-negotiation disabled and uses the speed and duplex settings as the connection configuration.

2.6 Making Power over Ethernet UTP Connections

To deliver power and network signals to a remote device by using PoE function, make sure the following conditions are properly checked before making connection:

1. The connected device is an IEEE 802.3af complaint Powered Device (PD).
2. The PoE PD port of the connected device should comply with the pin out as follows:

RJ-45 Definitions

Pin 4	Positive received power voltage
Pin 5	Positive received power voltage
Pin 7	Negative received power voltage
Pin 8	Negative received power voltage

3. The network cable used should meet the definition below:

Straight Cat.5	<u>PoE PSE RJ-45 end</u>	<u>PoE PD RJ-45 MDI-X</u>
	Pin 1 -----	Pin 1
	Pin 2 -----	Pin 2
	Pin 3 -----	Pin 3
	Pin 4 -----	Pin 4
	Pin 5 -----	Pin 5
	Pin 6 -----	Pin 6
	Pin 7 -----	Pin 7
	Pin 8 -----	Pin 8

Crossover Cat.5	<u>PoE PSE RJ-45</u>	<u>PoE PD RJ-45 MDI-X</u>
	Pin 1 -----	Pin 3
	Pin 2 -----	Pin 6
	Pin 3 -----	Pin 1
	Pin 4 -----	Pin 4
	Pin 5 -----	Pin 5
	Pin 6 -----	Pin 2
	Pin 7 -----	Pin 7
	Pin 8 -----	Pin 8

The PoE function is disabled with factory default settings. Use software management interface to enable the PoE function for the switch and the PoE ports. Refer to the PoE function described in next chapter for further information.

2.7 Making Fiber Connections

Before making the connection, properly install the fiber module into an available 100FX slot as follows:

1. Turn off the power to the switch.
2. Remove the cover of the slot.
3. Insert the fiber module into the slot until it is seated properly.
4. Screw the module on the switch securely.
5. Turn on the power to the switch.

After module installation, follow the steps below to make a proper connection:

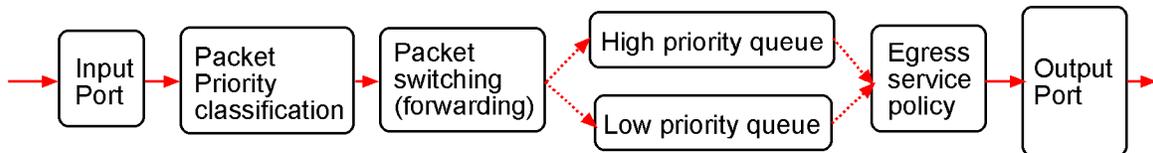
1. Use an appropriate fiber cable, multimode fiber or single mode fiber for the connection.
2. Make sure Tx-to-Rx connection rule is followed between both ends of the cable.
3. Configure the port via software management interface to : forced, 100Mbps, full duplex.

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 QoS Function

The switch provides a powerful Quality of Service (QoS) function to guide the packet forwarding in two priority levels. 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 input port until it is transmitted out from the output port:



3.1.1 Priority Level

Each output (egress) port in the switch is equipped with two transmission priority queues to store the packets for transmission. The high priority queue stores the high priority packets and low priority queue stores the low priority packets.

3.1.2 Egress Service Policy

The packets in high priority queue and low priority queue are transmitted out from a port based on a user configured round robin ratio, called egress service policy between high priority queue and low priority queue. The switch provides four ratio options for the service policy:

- [4:1] : 4 high priority packets then 1 low priority packet
- [8:1] : 8 high priority packets then 1 low priority packet
- [16:1] : 16 high priority packets then 1 low priority packet
- [Always high priority first] : Packets in high priority queue are sent first until the queue is empty

3.1.3 Packet Priority Classification

Each received packet is determined and classified into one of two priority levels, high priority and low priority upon reception. The switch provides many classification methods including:

- Port based
- 802.1p based
- IP DSCP based
- IP network address based

They all can be configured to be activated or not. Some are per port configuration and some are global configuration for the switch. More than one classification method can be enabled at the same time. If a packet is classified as high priority in any one of the enabled (applied) classifications, the packet is forwarded to the high priority queue of the output port. Otherwise, it is classified as low priority.

3.1.3.1 Port-based Priority Setting (per port setting)

As one port is configured to be enabled for port-based priority, all received packets on the port will be classified as high priority. The options are:

Enable - All packets received on the port are classified as high priority

Disable - Port-based classification is not applied.

3.1.3.2 802.1p Classification (per port setting)

For a received 802.1Q VLAN tagged packet, the switch will check the 3-bit User Priority value in TCI (Tag Control Information) field of packet tag data. If the priority value is equal or larger than a configured **802.1p High Priority Tag Setting**, the packet is classified as high priority.

Enable - Tagged packets received on the port are classified by comparing the packet's User Priority value and 802.1p High Priority Tag Threshold Setting.

Disable - 802.1p classification is not applied.

3.1.3.3 DSCP Classification (per port setting)

As a port is enabled for IP DSCP classification, the switch will check the DiffServ Code Point (DSCP) value of the IP packets received on the port.

Enable - IP packets received on the port are classified by checking the packet's DSCP value.

Disable - DSCP classification is not applied.

The following checks are performed to classify the packet priority:

1. **Default DSCP** : If the packet's DSCP value is one the default code point listed below, the packet is classified as high priority. EF - <101110>, AF - <001010> <010010> <011010> <100010> and Network Control - <111000> <110000>.
2. **User Defined DSCP** : If the packet's DSCP value matches the user defined DSCP(A) and DSCP(B) settings, the packet is classified as high priority. DSCP(A) and DSCP(B) settings will be described later.

User defined DSCP(A) and DSCP(B) can be enabled respectively.

User Defined DSCP(A) Classification (Global)

User can configure a specific DSCP value in **DSCP(A) setting** as high priority beside default DSCPs.

Enable - Enable DSCP(A) checking

Disable - DSCP(A) classification is not applied.

User Defined DSCP(B) Classification (Global)

User can configure a specific DSCP value in **DSCP(B) setting** as high priority beside default DSCPs.

Enable - Enable DSCP(B) checking

Disable - DSCP(B) classification is not applied.

3.1.3.4 IP Network Address Classification

User can configured two IP network address settings, IP(A) and IP(B). If a received IP packet's source address or destination address belongs to the user defined IP network addresses. The packet is classified as high priority.

User Defined IP(A) Classification (Global)

Enable - Enable IP(A) checking

Disable - IP(A) classification is not applied.

User Defined IP(B) Classification (Global)

Enable - Enable IP(B) checking

Disable - IP(B) classification is not applied.

3.1.4 Other QoS Settings

- 802.1p High Priority Tag Setting for 802.1p classification
- User Defined DSCP(A) Setting for DSCP classification
- User Defined DSCP(B) Setting for DSCP classification
- User Defined IP(A) Settings for IP network address classification
 - IP(A) IP address setting
 - IP(A) IP subnet mask setting
- User Defined IP(B) Settings for IP network address classification
 - IP(B) IP address setting
 - IP(B) IP subnet mask setting

3.2 VLAN Function

The switch supports port-based VLAN, 802.1Q Tag Aware VLAN and eight VLAN groups. Some VLAN related terminologies are described as follows:

VLAN Group

VLAN group specifies a VLAN information that can be referred by the switch in performing VLAN mapping and packet forwarding for ingress port and the received packets. The information includes:

- **Group Number** : index number of the VLAN group (1 ~ 8)
- **VID (VLAN ID)** : 12-bit value to indicate a VLAN to which the group is associated (1 ~ 4095)
- **Member Ports** : the ports belong to this VLAN group for egress

Ingress Port

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

Default VLAN Group Index (Port VLAN index)

Each port has this index, which points to a default VLAN group. It is used for mapping a VLAN group for the ingress port under Port-based VLAN mode. It is also used for mapping to a VLAN group for an untagged received packet under 802.1Q Tag Aware VLAN mode.

PVID (Port VID)

PVID is the default VID of an ingress port. It is obtained from the VID of the indexed default VLAN group by the ingress port. It is often used in ingress packet filtering and egress tagging operation.

Egress Port

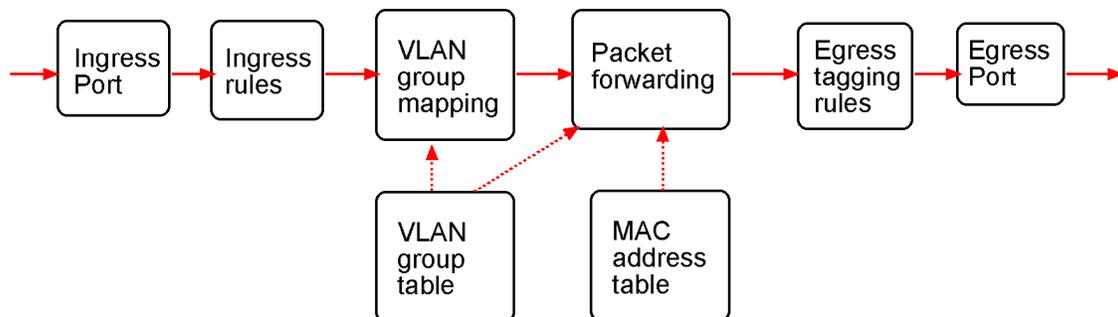
Egress port is the output port from which a packet is sent out after VLAN operation.

Null VID Packet

A tagged packet is called Null VID packet if the packet 's VID is equal to 0. Sometimes, it is also called priority tag packet.

3.2.1 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 related 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.

3.2.2 Ingress Rules

When a packet is received on an ingress port, the ingress rules are applied for packet filtering and mapping a VLAN group. The first rule is :

3.2.2.1 802.1Q Tag Aware VLAN Mode (global setting)

Enable - 802.1Q Tag Aware VLAN mode is used

Disable - Port-based VLAN mode is used

802.1Q Tag Aware VLAN Mode

Under this mode, the switch will check the content of every received packets. For 802.1Q tagged packets, the tagged VID on the packet is used to look up the VLAN group table and find the group whose VID matches the packet tagged VID.

<u>Received packet type</u>	<u>VLAN group mapping</u>	<u>Final VLAN group used</u>
802.1Q Tagged packets	Tagged VID	Matched - use the matched VLAN group No matched - drop the packet
Untagged packets	Port VLAN index	Default VLAN group of the ingress port

Port-based VLAN Mode

Under this mode, the switch does not check the contents of the received packets. The default VLAN group indexed by the ingress port is used directly for further VLAN operation.

3.2.2.2 Ingress Member Filtering (global setting)

As this rule is enabled, the received packet is dropped if the ingress port is not the member port of the mapped VLAN group.

Enable - Drop packet if the ingress port is not the member port of the VLAN group

Disable - No ingress member filtering is applied

3.2.2.3 Unmatched VID Filtering (per port setting)

A tagged received packet will be dropped if the tagged VID does not match the PVID of the ingress port. PVID is the VID of ingress port's default VLAN group.

Enable - Drop the tagged packet if the packet's VID does not match the ingress port's PVID

Disable - No Unmatched VID filtering is applied to the port

3.2.3 VLAN Group Mapping

The VLAN group mapping is the switch's decision process to find a right VLAN group for the received packet when it is not filtered by ingress rules. The group mapping depends on the VLAN mode and the packet type. The following table lists the decision rules:

<u>VLAN Mode</u>	<u>Packet Type</u>	<u>Mapping Method</u>
802.1Q Tag Aware	Tagged & non-Null	Use packet's VID to loop up VLAN group table Matched - use the group matched Unmatched - drop the packet
802.1Q Tag Aware	Null VID	Use ingress port's default VLAN group directly
802.1Q Tag Aware	Untagged	Use ingress port's default VLAN group directly
Port-based VLAN	Tagged	Use ingress port's default VLAN group directly
Port-based VLAN	Untagged	Use ingress port's default VLAN group directly

3.2.4 Packet Forwarding under VLAN

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

- The mapped VLAN group's member ports : the port range for forwarding
- The packet's destination MAC address : for MAC address table loop up
- The switch's MAC address table : to find the associated input port for a learned MAC address

If the MAC address table lookup is matched and the associated port is the VLAN member port, the packet is forwarded to the port (egress port). If the lookup is not matched, the switch will broadcast the packet to all member ports.

3.2.5 Egress Tagging Rules

Egress Tagging rules are used to make change to the packet before it is transmitted out from an egress port. Two egress tagging settings are provided for each port and are described as follows:

3.2.5.1 Egress Tag Rule (per port setting)

Four basic options are provided for egress tagging :

1. Tagging with PVID for all packets

Untagged packet : the packet is inserted with the associated ingress port's PVID as tag VID

Tagged packet : the packet's tag VID is replaced with ingress port's PVID as new tag VID

2. Untagging for all packets

Untagged packet : the packet is not modified

Tagged packet : the packet's tag VID is removed and becomes an untagged packet

Null VID packet : depending on Null VID Replacement setting in next section

3. PVID insertion for untagged packets only

Untagged packet : the packet is inserted with the associated ingress port's PVID as tag VID

Tagged packet : the packet is not modified

4. No tag insertion and tag removal

The packet is not modified at all. No tag insertion or tag removal are performed for all packets.

3.2.5.2 Null VID Replacement (per port setting)

The null VID of a Null VID packet will be replaced with the associated ingress port's PVID. This setting still works even Egress Tag rule : [*PVID insertion for untagged packets only*] is selected.

3.2.6 Summary of VLAN Function

Number of VLAN groups : 8 groups at the same time

VLAN ID supported : 1 ~ 4095 (12-bit VID)

VLAN mode options : 802.1Q Tag Aware VLAN, Port-based

Ingress rules : Ingress Member Filtering (global setting)
Unmatched VID Filtering (per port setting)

Egress Tagging rules : Egress Tag Rule (per port setting)

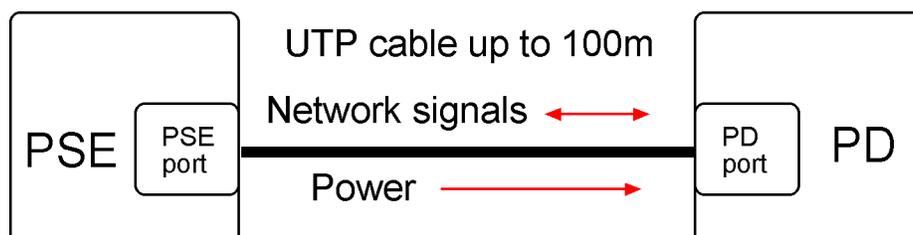
- Tagging with PVID for all packets
- Untagging for all packets
- PVID insertion for untagged packets only
- No tag insertion and tag removal

Null VID Replacement (per port setting)

3.3 Power over Ethernet Function

Power over Ethernet (PoE) is a technology that DC power can be delivered over a twisted pair network cable to a remote connected device which has no other power supply input. The power is delivered together with bidirectional Ethernet network signals over the network cable. The advantage of the PoE technology is delivering power to a network device located in a place where power line is unable to reach.

The following figure illustrates a simple PoE connection model :



PSE : Power Source Equipment - the device capable to deliver power over an Ethernet cable

PD : Powered Device - the device capable to receive power from an Ethernet cable

PSE Port : The Ethernet port equipped with PoE function as power source for a connected PD

PD Port : The Ethernet port equipped with PoE function to receive power from a connected PSE

3.3.1 PoE Specifications

The switch provides IEEE 802.3af compliant PoE PSE function on Port 1, Port 2, Port 3 and Port 4 with the following specifications (PSE port):

Power Output Voltage delivered : 48VDC

Maximum Power delivered : 15.4Watts (Class 0)

PSE Pinout on RJ-45 : Pin 4 and Pin 5 - Positive 48VDC
Pin 7 and Pin 8 - negative 48VDC

Maximum Cable Length : UTP cable up to 100 meters

3.3.2 PoE PSE Capabilities

The PSE ports are equipped with the following capabilities:

1. Detection for an IEEE 802.3af compliant PD.
2. No power is supplied to a device which is classified non-IEEE802.3af compliant PD.
3. No power is supplied when no connection exists on the port.
4. The power is cut off immediately from powering condition when a disconnection occurs.
5. The power is cut off immediately from powering condition when overload occurs.
6. The power is cut off immediately from powering condition when over-current occurs.
7. The power is cut off immediately from powering condition when short circuit condition occurs.

3.3.3.3 PoE Management functions

The switch provides the following management function via software interfaces:

1. Enable or disable the switch 's PoE function.
2. Enable or disable port PoE function in per port basis.
3. Monitor the power up / down status on the PoE ports
4. Monitor the power output voltage, current and watts of each PoE port

3.3.4 Notices for PoE Installation

1. Do not connect the PSE port to an non-IEEE 802.3af compliant PD Ethernet port.
2. Disable PoE function of the port when it connects to a non-PoE 100BASE-TX or 10BASE-T Ethernet port.
3. Disable PoE of the port when it connects to a 1000BASE-T Gigabit Ethernet copper port.
4. Disable the PoE function when no PoE installation is required.

4. Software Management

The switch provides the following in-band management interfaces for configuring the switch to meet requirements for different applications:

- Telnet over TCP/IP
- Http web-based over TCP/IP
- SNMP over TCP/IP

4.1 Telnet Management Interface

Use Telnet software to perform the management operation. The most convenient solution is using the built-in Telnet function in your Windows PC. Execute Telnet command as follows:

```
>tel net xxx. xxx. xxx. xxx
```

The specified xxx.xxx.xxx.xxx is the IP address of the switch. Factory default IP address is 192.168.0.2.

A welcome message and login prompt are displayed if the connection is established properly.

```
Wel come to Tel net Server
```

```
Logi n: xxxxx  
password: xxx  
Wel come xxxxx
```

```
Factory default login name : admin
```

```
Factory default password : 123
```

It is suggested to change the user name and password first before performing other configuration. To change the user name and password, select [6] *Security Manager* for configuration.

Main Menu

```
INET>  
Setup Menu  
TCP/IP stack v1.0  
[0] Print this menu  
[1] IP Menu  
[2] SNMP Menu  
[3] Port Config  
[4] Administrator  
[5] Restore Default Values  
[6] Security Manager  
[7] Update firmware  
[8] Reboot System  
[Q] Exit  
Please Select (0-9)....
```

4.2 IP Menu

Select [1] *IP Menu* to configure the switchs IP related settings.

```
IP Menu:
[0] Print this menu
[1] Set IP Address
[2] View IP status
[Q] Back Menu
Please Select(0-3)....
INET>1
```

Enter Esc to abort..

```
Please Input IP Address(xxx.xxx.xxx.xxx): 192.168.0.232
replacing net[0] IP address192.168.0.232 with 192.168.0.232
Please Input Subnet Mask(xxx.xxx.xxx.xxx): 255.255.255.0
replacing subnet mask[0]255.255.255.0 with 255.255.255.0
Please Input Gateway IP(xxx.xxx.xxx.xxx): 192.168.0.1
replacing gateway IP addr[0] 192.168.0.1 with 192.168.0.1
Do you want to Change IP setting?(Y/N):
```

IP Settings	Description
IP Address :	IP address assigned to the switch
Subnet Mask :	IP subnet mask of the switch
Gateway IP :	IP address of the default gateway of the switch

To view current IP settings of the switch, select [2] *View IP status*.

```
IP Menu:
[0] Print this menu
[1] Set IP Address
[2] View IP status
[Q] Back Menu
Please Select(0-3)....
INET> 2
```

```
IP Addr: 192.168.0.232 Submask: 255.255.255.0 Gateway: 192.168.0.1
```

```
INET>
```

4.3 SNMP Menu

This menu is used for configuring SNMP related settings.

Snmp Menu:

```
[0] Print this menu
[1] View Snmp Setting
[2] Set Snmp Name
[3] Set Snmp Location
[4] Set Snmp Contact
[5] Set Snmp Community
[6] Set Snmp Trap Manager
[7] Set Port Link Trap Function
[8] Set Login Failure Trap Function
[Q] Back Menu
Please Select (0-9)....
INET>
```

SNMP Settings	Description
System Name	Name of the switch for SNMP management
System Location	Location of the switch for SNMP management
System Contact	Contact person for the switch
Community Name	Community Name allowed for SNMP access to the switch Up to 4 communities can be configured.
Community Access Right	Access Right associated to the community name, options <i>R(read-only)</i> - only read operation is allowed <i>W(read-write)</i> - both read and write operations are allowed.
Trap Manager	IP Address of the SNMP station which can receives trap Up to 3 trap stations can be configured.
Trap Community Name	Community string sent with a trap message
Port Link Trap Function	Enable or disable SNMP trap for port link change events
Login Failure Trap Function	Enable or disable SNMP trap for login failure events

4.4 Port Config

Select [3] *Port Config* to configure port configuration.

Port Config Menu:

[0] Print this menu

[1] Port Status

[2] Port Config

[Q] Back Menu

Please Select (0-3)

Select [1] *Port Status* to view current port status for all ports as example below:

INET> Port Status:

Port No.	Link Status	Auto Negotia.	Speed Status	Duplex Status	Port Control	Auto_No Control	Speed Control	Duplex Control
1	Down	--	--	--	Enable	Enable	100 M	Full
2	Down	--	--	--	Enable	Enable	100 M	Full
3	Down	--	--	--	Enable	Enable	100 M	Full
4	Up	Enable	100 M	Full	Enable	Enable	100 M	Full
5	Down	--	--	--	Enable	Enable	100 M	Full
6	Down	--	--	--	Enable	Enable	100 M	Full
7	Down	--	--	--	Enable	Enable	100 M	Full
8	Down	--	--	--	Enable	Enable	100 M	Full

INET>

Status

Description

Port No.	The port number
Link Status	Port link status <i>Down</i> - port link down (no status is displayed.) <i>Up</i> - port link up
Auto Negotia.	Auto-negotiation configuration <i>Enable</i> - auto-negotiation is enabled <i>Disable</i> - auto-negotiation is disabled (forced mode is used)
Speed Status	Port speed status <i>100M</i> - 100Mbps is used <i>10M</i> - 10Mbps is used
Duplex Status	Port duplex status <i>Full</i> - full duplex is used <i>Half</i> - half duplex is used
Port Control	Port function configuration <i>Enable</i> - Port function (Tx/Rx) is enabled <i>Disable</i> - Port function (Tx/Rx) is disabled
Auto-No Control	Port auto-negotiation function <i>Enable</i> - enable port auto-negotiation <i>Disable</i> - disable port auto-negotiation (use forced mode)
Speed Control	Speed configuration when auto-negotiation is disabled

	<i>100M</i> - 100Mbps
	<i>10M</i> - 10Mbps
Duplex Control	Duplex configuration when auto-negotiation is disabled
	<i>Full</i> - full duplex
	<i>Half</i> - half duplex

Select [2] *Port Config* to view current port status for all ports as example below:

Port Setting	Description
Ports	Select port range to be configured. More than one group can be configured at the same time. Examples: 123 - Port 1, Port 2, Port 3 1 2 3 - Port 1, Port 2, Port 3 1,2,3 - Port 1, Port 2, Port 3
Port Control	Enable / disable port function (Tx/Rx)
Auto Negotiation	Enable / disable port auto-negotiation function
Speed	Configure speed when port auto-negotiation function is disabled
Duplex	Configure duplex when port auto-negotiation function is disabled

4.5 Administrator

Select [4] *Administrator* to configure advanced settings including VLAN, QoS, and PoE settings:

```

Administrator:
[0] Print this menu
[1] VLAN Settings
[2] QoS Settings
[3] PoE Settings
[Q] Back Menu
Please Select (0-4)

```

4.5.1 Administrator -> VLAN Settings

Select [1] *VLAN Settings* to configure VLAN function related settings:

```

VLAN Settings Menu:
[0] Print this menu
[1] VLAN Group Information
[2] VLAN Select
[3] VLAN Global Settings
[4] VLAN Group Member Settings
[5] VLAN Group VID Settings
[6] VLAN Per Port Settings
[Q] Back Administrator
Please Select (0-7)

```

Select [1] VLAN Group Information to view all groups.

VLAN Select: Disable VLAN

Member Ports (0 : member, - : not member):

G\P	1	2	3	4	5	6	7	8
1	0	0	0	0	0	0	0	0
2	-	0	-	-	-	-	-	-
3	-	-	0	-	-	-	-	-
4	-	-	-	0	-	-	-	-
5	-	-	-	-	0	-	-	-
6	-	-	-	-	-	0	-	-
7	-	-	-	-	-	-	0	-
8	-	-	-	-	-	-	-	0

VLAN ID:

Group	1	2	3	4	5	6	7	8
VLAN ID	1	2	3	4	5	6	7	8

INET>

VLAN Information	Description
VLAN Select	VLAN function of the switch is enabled or disabled.
Member ports	Table list for member ports : X axis - port number Y axis - group number
VLAN ID	VLAN ID configuration of each group

Select [2] VLAN Select to enable or disable VLAN function of the switch.

Select [3] VLAN Global Settings to configure 802.1Q Tag Aware Mode and Ingress Member Filtering Mode:

VLAN Other Settings:

- [0] Print this menu
 - [1] View VLAN Global Settings
 - [2] 802.1Q Tag Aware Mode
 - [3] Ingress Member Filtering Mode
 - [Q] Back VLAN
- Please Select (0-4)

VLAN Global Settings	Description
802.1Q Tag Aware Mode	<p><i>Enable</i> - Under this mode, the switch will check the content of every received packets. For 802.1Q tagged packets, the tagged VID on the packet is used to look up the VLAN group table and find the group whose VID matches the packet tagged VID.</p> <p><i>Disable</i> - Under this mode, the switch does not check the contents of the received packets. The default VLAN group indexed by the ingress port is used directly for further VLAN operation.</p>
Ingress Member Filtering Mode	<p><i>Enable</i> - Drop packet if the ingress port is not the member port of the VLAN group</p> <p><i>Disable</i> - No ingress member filtering is applied</p>

Select [4] *VLAN Group Member Settings* to configure member ports for VLAN groups.

Input	Description
Groups	<p>Specify group list to be configured. More than one group can be configured at the same time. Examples:</p> <p>123 - Group 1, Group 2, Group 3</p> <p>1 2 3 - Group 1, Group 2, Group 3</p> <p>1,2,3 - Group 1, Group 2, Group 3</p>
Ports	<p>Enter port list for the selected groups</p> <p>Examples:</p> <p>123 - Port 1, Port 2, Port 3</p> <p>1 2 3 - Port 1, Port 2, Port 3</p> <p>1,2,3 - Port 1, Port 2, Port 3</p>

Select [5] *VLAN Group VID Settings* to configure VLAN ID for VLAN groups.

VID Setting	Description
Groups	Select group list to be configured.
VLAN ID	<p>Enter VLAN ID for the selected groups</p> <p>Valid values : 1 - 4095</p>

Select [6] *VLAN Per Port Settings* to configure VLAN ID for VLAN groups.

VLAN Per Port Settings:

Port No.	Default Group	Unmatched VID	Egress tag rule	Null VID
1	1	Disabled	4	Disabled
2	1	Disabled	4	Disabled
3	1	Disabled	4	Disabled
4	1	Disabled	4	Disabled
5	1	Disabled	4	Disabled
6	1	Disabled	4	Disabled
7	1	Disabled	4	Disabled
8	1	Disabled	4	Disabled

Enter Esc to abort..
Please Input Ports (1~8):

Per Port Settings	Description
Ports	Input port list for configuration.
Default Group	Index to the default group of the selected ports
Unmatched VID	<p><i>Enable</i> - Drop the tagged packet if the packet's VID does not match the ingress port's PVID</p> <p><i>Disable</i> - No Unmatched VID filtering is applied to the port</p>
Egress tag rule	<p>Egress Tagging rules are used to make change to the packet before it is transmitted out from an egress port. Options are:</p> <p>(1) <i>Tagging with ingress PVID for all packets</i> -</p> <p>Untagged packet : the packet is inserted with the associated ingress port's PVID as tag VID</p> <p>Tagged packet : the packet's tag VID is replaced with ingress port's PVID as new tag VID</p> <p>(2) <i>Untagging for all packets</i> -</p> <p>Untagged packet : the packet is not modified</p> <p>Tagged packet : the packet's tag VID is removed and becomes an untagged packet</p> <p>Null VID packet : depending on next Null VID Replacement setting</p> <p>(3) <i>Ingress PVID insertion for untagged packets only</i> -</p> <p>Untagged packet : the packet is inserted with the associated ingress port's PVID as tag VID</p> <p>Tagged packet : the packet is not modified</p> <p>(4) <i>No tag insertion and tag removal</i> -</p> <p>The packet is not modified at all. No tag insertion or tag removal are performed for all packets.</p>

Null VID The null VID of a Null VID packet will be replaced with the associated ingress port's PVID. This setting still works even Egress Tag rule : [PVID insertion for untagged packets only] is selected.

Enable - Null VID is replaced with Port's PVID for Null VID packets
Disable - Null VID replacement rule is not applied.

4.5.2 Administrator -> QoS Settings

Select [4] Administrator -> [2] QoS Settings to configure QoS function related settings for the switch.

QoS Settings Menu:
 [0] Print this menu
 [1] QoS Per Port Settings
 [2] QoS Other Settings
 [Q] Back Administrator
 Please Select (0-3)

Select [1] QoS Per Port Settings to configure port related QoS settings:

QoS Per Port Settings:

Port No.	Port based priority	802.1p classification	Default TOS/DS classification
1	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled

Enter Esc to abort..
 Please Input Ports (1~8):

Per Port Settings	Description
Ports	Input port list for configuration.
Port based priority	<i>Enable</i> - All packets received on the port are classified as high priority <i>Disable</i> - Port-based classification is not applied.
802.1p classification	<i>Enable</i> - Tagged packets received on the port are classified by comparing the packet's User Priority value and 802.1p High Priority Tag Setting. <i>Disable</i> - 802.1p classification is not applied.
Default TOS/DS classification	<i>Enable</i> - If the packets DSCP value is one the default code point listed below, the packet is classified as high priority. EF - <101110>.

AF - <001010> <010010> <011010> <100010> and Network Control - <111000> <110000>
Disable - Default DSCP classification is not applied.

Select [2] *QoS Other Settings* to configure QoS global settings:

QoS Other Settings:
 [0] Print this menu
 [1] Show QoS Other Status
 [2] 802.1p priority tag
 [3] Egress service policy
 [4] Specific DS Settings
 [5] Specific IP Settings
 [Q] Back QoS
 Please Select (0-6)

Select [1] *Show QoS Other Status* to view other settings (global):

```
802.1p priority tag      : 4
Egress service policy   : 16 : 1
Specific DS(A) Setting  : Disabled
Specific DS(A) Value    : 111111
Specific DS(B) Setting  : Disabled
Specific DS(B) Value    : 111111
Specific IP(A) Setting  : Disabled
Specific IP(A) Value    : 255.255.255.255
Specific IP(A) Mask Value : 255.255.255.255
Specific IP(B) Setting  : Disabled
Specific IP(B) Value    : 255.255.255.255
Specific IP(B) Mask Value : 255.255.255.255
INET>
```

Select [2] - [5] to configure other settings as follows:

QoS Other Settings	Description
802.1p priority tag	802.1p High Priority Tag Threshold Setting for 802.1p classification Valid values : 0 - 7
Egress service policy	Weighted Round Robin ratio: (1) 4:1 - 4 high priority packets then 1 low priority packet (2) 8:1 - 8 high priority packets then 1 low priority packet (3) 16:1 - 16 high priority packets then 1 low priority packet (4) <i>Always high first</i> - Packets in high priority queue are sent first until the queue is empty
Specific DS(A) Setting	<i>Enable</i> - Enable user defined DSCP(A) checking <i>Disable</i> - User defined DSCP(A) classification is not applied.
Specific DS(A) Value	Enter user defined DSCP(A) value for classification.
Specific DS(B) Setting	<i>Enable</i> - Enable user defined DSCP(B) checking <i>Disable</i> - User defined DSCP(B) classification is not applied.
Specific DS(B) Value	Enter user defined DSCP(B) value for classification.

Specific IP(A) Setting	<p>If a received IP packet's source address or destination address belongs to the user defined IP network addresses. The packet is classified as high priority.</p> <p><i>Enable</i> - Enable user defined IP(A) network address checking <i>Disable</i> - IP(A) classification is not applied.</p>
Specific IP(A) Value	Set user defined IP(A) address for classification.
Specific IP(A) Mask Value	<p>Set user defined IP(A) subnet mask for classification.</p> <p>IP(A) address and IP(A) subnet mask specify IP(A) user defined IP network address for IP packet classification.</p>
Specific IP(B) Setting	<p>If a received IP packet's source address or destination address belongs to the user defined IP network addresses. The packet is classified as high priority.</p> <p><i>Enable</i> - Enable user defined IP(B) network address checking <i>Disable</i> - IP(B) classification is not applied.</p>
Specific IP(B) Value	Set user defined IP(B) address for classification.
Specific IP(B) Mask Value	<p>Set user defined IP(B) subnet mask for classification.</p> <p>IP(B) address and IP(B) subnet mask specify IP(B) user defined IP network address for IP packet classification.</p>

4.5.3 Administrator -> PoE Settings

Select [4] Administrator -> [3] PoE Settings to configure PoE function related settings:

```
PoE Settings:
[0] Print this menu
[1] PoE Status
[2] PoE Master Enable
[3] PoE Port Enable
[Q] Back Administrator
Please Select(0-4)....
INET>
```

Select [1] PoE Status to view PoE status:

```
PoE Master Enable : Enable
Port PoE Enable Power Status Current(mA) Voltage(V) Power(W)
+-----+-----+-----+-----+-----+-----+
1   Enable   Down      0.00      1.33      0.00
2   Enable   Down      0.00      1.49      0.00
3   Enable   Down      0.00      1.33      0.00
4   Enable   Down      0.00      0.19      0.00
+-----+-----+-----+-----+-----+-----+
INET>
```

The PoE status are:

Status	Description
PoE Master Enable	PoE function of the switch is enabled or disabled.
Port	Port number
PoE Enable	PoE function of the port is enabled or disabled.
Power Status	Power is supplied from the port. <i>Down</i> - the power is not supplied on the port <i>Up</i> - the power is supplied
Current(mA)	The power current currently supplied on the port. Unit: mA
Voltage(V)	The power voltage currently supplied on the port. Unit: V
Power(W)	The power currently supplied on the port. Unit: Watts

Select [2] PoE Master Enable to enable or disable PoE function of the switch.
Select [3] PoE Port Enable to enable or disable PoE function of the PSE ports individually.

Setting	Description
Ports	Select port list for the configuration.
PoE Port Control	<i>Enable</i> - enable Port PoE function for the selected ports <i>Disable</i> - disable Port PoE function for the selected ports

4.6 Restore Default Values

Select [6] *Restore Default Values* to restore all settings of the switch back to factory default values.

Do you want to restore system default settings?(Y/N):

Refer to Appendix for factory default values.

4.7 Security Manager

Select [7] *Security Manager* to change user name and password. The user name and password are used for login into the switch in telnet management and web management.

Current username: admin
Current password: *****

Press ESC to abort ...

Change username[admin]: admin
Enter password(1-8): ***
Confirm password: ***
Password updating
Password updated.

User is requested to enter new password again for confirmation. A new password is accepted only two passwords are identical.

It is suggested to change the factory default user name and password before installing the switch into your network.

4.8 Update Firmware

Select [7] *Update Firmware* to update the firmware of the switch. A new firmware may be released by the factory due to function enhancement. The update method is via TFTP protocol.

The steps are:

1. A TFTP server must be available in the network before updating the firmware.
2. Place the new firmware on the TFTP server with filename [image.bin].
3. Use [7] *Update firmware* to specify the IP address of the TFTP server and start downloading of the new firmware as follows:

Enter Esc to abort..
Please Input TFTP Server IP Address(xxx. xxx. xxx. xxx): yyy. yyy. yyy. yyy
TFTP Server : yyy. yyy. yyy. yyy
Do you want to start download new image? (Y/N)

Setting	Description
TFTP IP Address	IP address of the TFTP server from where a new firmware is downloaded.

4.9 Reboot System

Select *[7] Reboot System* to reboot the switch.

```
Do you want to reboot system?(Y/N):y
Start rebooting.....
```

Press *[Y]* to confirm to reboot the switch with current configuration settings. Note that the current telnet connection will be disconnected after confirmation.

You must restart your telnet and login into the switch again.

4.10 Exit

Select *[Q] Exit* to stop telnet connection with the switch.

5. Web Management

The switch features an http server which can serve the management requests coming from any web browser software over internet or intranet network.

Web Browser

Compatible web browser software with JAVA 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.

5.1 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

5.2 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:



Login

Factory default Username : Admin

Factory default Password : 123

The following screen shows welcome screen when a successful login is performed.



In addition to the device image, the screen supports the following menus on the right side:

1. Home : home page and device image
2. Port Status : view all switched port status
3. Administrator : other management functions

5.3 Port Status Menu

Click >*Port Status Menu* to display the port status for all switched ports. The pop-up port status list is as follows:

Port Status				
Port	Link Status	Auto Negotiation	Speed Status	Duplex Status
1	Down	--	--	--
2	Down	--	--	--
3	Down	--	--	--
4	Up	Enabled	100 M	Full
5	Down	--	--	--
6	Down	--	--	--
7	Down	--	--	--
8	Down	--	--	--

Port Status	Description
Port Number	1 - 6 : 10/100TX ports - P1 ~ P2 7 - 8 : 100FX ports - F1 F2
Link Status	Port link status <i>Up</i> - port link up (an active link is established with a link partner) <i>Down</i> - port link down
Auto Negotiation	Auto negotiation mode status <i>Enabled</i> - auto negotiation mode is enabled <i>Disabled</i> - auto negotiation mode is disabled (forced mode)
Speed Status	Port speed status <i>100M</i> - 100Mbps <i>10M</i> - 10Mbps
Duplex Status	Port duplex status <i>Full</i> - full duplex <i>Half</i> - half duplex

Clicking the port icons on the product image in web page also will pop-up the port status.

5.4 Administrator

Click *>Administrator* to perform more advanced management functions as follows:



Menu	Function
Basic	Configure IP and SNMP settings for the switch
Port Control	Change port configuration including auto-negotiation, speed, duplex
VLAN Controls	Configure VLAN related settings
QoS Controls	Configure QoS related settings
PoE Controls	Configure Power over Ethernet (PoE) settings
Security Manager	Change user name and password
Image Refresh Time	Set the image refresh time for the web device image
Update Firmware	Update firmware of the switch
Restore Default	Restore the switch back to factory default settings
Reboot System	Reboot the switch

5.4.1 Basic Menu

Click *Basic* menu to configure IP settings and SNMP settings for the switch:

[IP Address | SNMP Entries]

The following menu options provide some basic functions to allow a user to view and modify:

IP Address, and
SNMP Entries (Various Settings).

IP Address

[\[IP Address | SNMP Entries \]](#)

IP Address Settings

IP Address:	<input type="text" value="192.168.0.232"/>
Submask:	<input type="text" value="255.255.255.0"/>
Gateway:	<input type="text" value="192.168.0.1"/>

IP Address Setting	Description
IP Address	IP address for the switch
Submask	Subnet mask of the IP address
Gateway	IP address of the default gateway

SNMP Entries

SNMP settings include system settings, community settings and Snmp trap settings as follows:

[\[IP Address | SNMP Entries \]](#)

SNMP Management

System Options

Name:	<input type="text"/>
Location:	<input type="text"/>
Contact:	<input type="text"/>

System Settings	Description
Name	Set a system name for the switch
Location	Set the location where the switch unit is installed
Contact	Set the contact person for the switch unit

Community Strings

Current Strings	Action	New Community String
public	<input type="button" value=" << Add << "/> <input style="margin-top: 5px;" type="button" value=" Remove "/>	String: <input type="text"/> <input checked="" type="radio"/> RO <input type="radio"/> RW

Community Settings	Description
--------------------	-------------

Community String	Community strings which are allowed to access the switch unit via SNMP protocol
Access Right	The access right assigned to the community string, options are: <i>RO</i> - read only <i>RW</i> - read / write
<<Add>>	Add one new community string specified in String box. Up to 4 community strings are allowed.
Remove	Remove the specified community string from list.

Trap Managers

Current Managers	Action	New Manager
192.168.0.2	<input type="button" value=" << Add << "/> <input style="margin-top: 5px;" type="button" value=" Remove "/>	IP Address: <input type="text"/> Community: <input type="text"/>

Enable Link Change Trap
 Enable Login Failure Trap

Trap Manager Settings	Description
-----------------------	-------------

IP Address	Specify the IP address of the trap manager to which the switch will send Snmp traps when predefined events occur.
Community	Community string used together with the trap messages sent to the trap manager
<<Add>>	Button to add a new trap manager (specified by an IP and Community) into manager list
Remove	Button to remove the trap manager
Enable Link Change Trap	Button to enable the switch to send a trap when any port link

changes

Enable Login Failure Trap Button to enable the switch to send a trap when any login failure is detected

5.4.2 Port Controls

Port Controls

Port	Port Function	Auto Negotiation	Speed Control	Duplex Control
Port 1	Null	Null	Null	Null
Port 2				
Port 3				
Port 4				
<input type="button" value="Apply"/>				

Port	Link Status	Port Function	Auto Negotiation	Speed Status	Duplex Status
1	Down	Enabled	Enabled	100 M	Full
2	Down	Enabled	Enabled	100 M	Full
3	Down	Enabled	Enabled	100 M	Full
4	Up	Enabled	Enabled	100 M	Full
5	Down	Enabled	Enabled	100 M	Full
6	Down	Enabled	Enabled	100 M	Full
7	Down	Enabled	Enabled	100 M	Full
8	Down	Enabled	Enabled	100 M	Full

Port Settings

Description

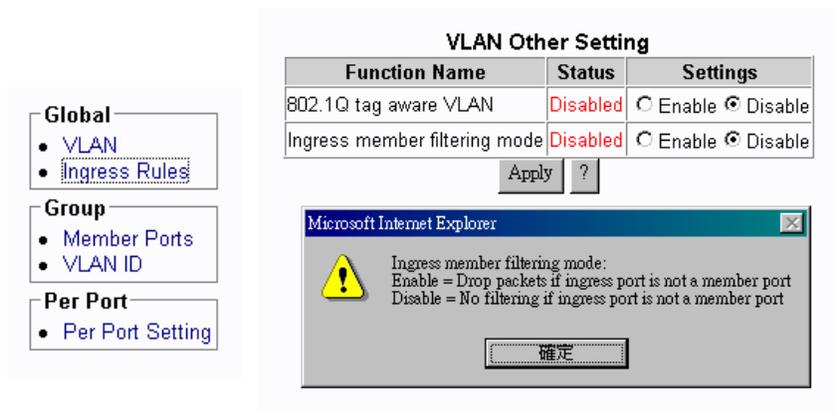
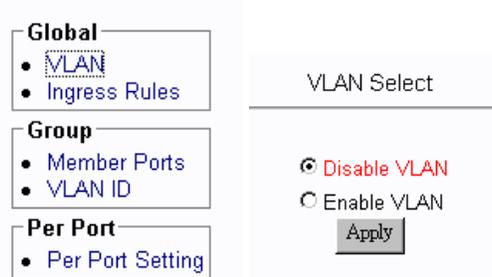
Port	Specify the ports for the new settings. More than one port can be configured at the same time. Use <Shift> key and <Ctrl> key to specify multiple ports.
Port Function	Enable port transmission function, options: <i>Null</i> - unchanged <i>Enable</i> - enable the port function <i>Disable</i> - disable the port function
Auto Negotiation	Enable auto negotiation function, options: <i>Null</i> - unchanged <i>Enable</i> - enable the port auto-negotiation function <i>Disable</i> - disable the port auto-negotiation function and use forced mode
Speed Control	Select port speed when auto-negotiation is disabled, options: <i>Null</i> - unchanged <i>100M</i> - 100Mbps <i>10M</i> - 10Mbps
Duplex Control	Select port duplex when auto-negotiation is disabled, options: <i>Null</i> - unchanged <i>Full</i> - full duplex <i>Half</i> - half duplex
Apply	Button to confirm the settings

The current port settings for all ports are also listed below the control dialog window.

5.4.3 VLAN Controls

VLAN settings are divided into three categories:

1. Global - Settings which are applied for the switch and not for specific ports
2. Group - Settings for VLAN groups
3. Per Port - Settings applied to each port



Global Settings	Description
VLAN	
VLAN Select	<i>Enable VLAN</i> - Enable switch VLAN function <i>Disable VLAN</i> - disable switch VLAN function
Ingress Rules	
802.1Q tag aware VLAN	<i>Enable</i> - Under this mode, the switch will check the content of every received packets. For 802.1Q tagged packets, the tagged VID on the packet is used to look up the VLAN group table and find the group whose VID matches the packet's tagged VID. <i>Disable</i> - Under this mode, the switch does not check the contents of the received packets. The default VLAN group indexed by the ingress port is used directly for further VLAN operation.
Ingress member filtering Mode	<i>Enable</i> - Drop packet if the ingress port is not the member port of the found VLAN group <i>Disable</i> - ingress member filtering rule is not applied

VLAN Group Configuration

VLAN Member Port Setting

Groups	Ports							
	1	2	3	4	5	6	7	8
Group 1	Null	Null	Null	Null	Null	Null	Null	Null
Group 2	Null	Null	Null	Null	Null	Null	Null	Null
Group 3	Null	Null	Null	Null	Null	Null	Null	Null
Group 4	Null	Null	Null	Null	Null	Null	Null	Null

Groups	Ports							
	1	2	3	4	5	6	7	8
1								
2								
3								
4								
5								
6								
7								
8								

Group Settings Description

Groups	Specify the VLAN group for member port configuration
Port	Specify the port to be added into or deleted from the specified group. <i>Null</i> - unchanged <i>Add</i> - add the port into member port list of the group <i>Del</i> - delete the port from member list of the group
Apply	Button to confirm the settings

Global

- VLAN
- Ingress Rules

Group

- Member Ports
- VLAN ID

Per Port

- Per Port Setting

VLAN ID Setting

Group	1	2	3	4	5	6	7	8
VLAN ID	1	2	3	4	5	6	7	0
Settings	<input type="text" value="1"/>	<input type="text" value="2"/>	<input type="text" value="3"/>	<input type="text" value="4"/>	<input type="text" value="5"/>	<input type="text" value="6"/>	<input type="text" value="7"/>	<input type="text" value="0"/>

Microsoft Internet Explorer

Set VLAN ID for each VLAN groups.
The VLAN ID of an indexed group is also used as PVID for the ingress port which is index to.

Group Settings Description

VLAN ID	Current VLAN ID of each VLAN group
Settings	Set new VLAN ID of VLAN group, valid values : 1 ~ 4095
?	Button to view information about VLAN ID
Apply	Button to confirm the settings

Per Port Settings

VLAN Per Port Setting

Port	Ingress		Egress	
	Default Group	Unmatched VID	Egress tag rule	Null VID
Port 1	Null	Null ?	Null ?	Null ?
Port 2		Null		
Port 3		Enable		
Port 4		Disable		

Port	Ingress		Egress	
	Default Group	Unmatched VID	Egress tag rule	Null VID
1	1	Disabled	4	Disabled
2	1	Disabled	4	Disabled
3	1	Disabled	4	Disabled
4	1	Disabled	4	Disabled
5	1	Disabled	4	Disabled
6	1	Disabled	4	Disabled
7	1	Disabled	4	Disabled
8	1	Disabled	4	Disabled

Per Port Settings

Description

Port

Select port list for configuration.

Ingress Rules

Default Group

Index to the default VLAN group of the selected ports, group 1 ~ 8

Unmatched VID

Null - unchanged

Enable - Drop the tagged packet if the packet VID does not match the ingress port PVID

Disable - No Unmatched VID filtering is applied to the port

Egress Rules

Egress tag rule

This tagging rule is used to make change to the packet before it is transmitted out from an egress port. Options are:

Null - unchanged

1 Tagging with ingress PVID for all packets -

Untagged packet : the packet is inserted with the associated ingress port PVID as tag VID

Tagged packet : the packet tag VID is replaced with ingress port PVID as new tag VID

2 Untagging for all packets -

Untagged packet : the packet is not modified

Tagged packet : the packet tag VID is removed and becomes an untagged packet

Null VID packet : depending on next Null VID Replacement setting

3 Ingress PVID insertion for untagged packets only -

Untagged packet : the packet is inserted with the associated ingress port PVID as tag VID

Tagged packet : the packet is not modified

4 No tag insertion and tag removal -

The packet is not modified at all. No tag insertion or tag removal are performed for all packets.

Null VID

The null VID of a Null VID packet will be replaced with the associated ingress port's PVID. This setting still works even Egress Tag rule : [*PVID insertion for untagged packets only*] is selected.

Enable - Null VID is replaced with Port's PVID for Null VID packets

Disable - Null VID replacement rule is not applied.

?

Button to view more information about the associated setting

Apply

Button to confirm the settings

5.4.4 QoS Controls

QoS settings are divided into two categories:

1. Per Port Settings - QoS settings for each port
2. Other Settings - Some global QoS settings

QoS Functions

- Per Port Settings
- Other Settings

QoS Per Port Settings

Port	Port based priority	802.1p classification	TOS/DS classification
Port 1	Null	Null	Null
Port 2			
Port 3			
Port 4			

Port	Port based priority	802.1p classification	TOS/DS classification
1	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled

QoS Per Port Settings Description

Port	Select port list for the per port QoS configuration.
Port based priority	Port based priority classification <i>Enable</i> - All packets received on the port are classified as high priority <i>Disable</i> - Port-based classification is not applied.
802.1p classification	<i>Enable</i> - Tagged packets received on the port are classified by comparing the packet's User Priority value and 802.1p High Priority Tag Setting. <i>Disable</i> - 802.1p classification is not applied.
TOS/DS classification	<i>Enable</i> - If the packets DSCP value is one the default code point listed

below, the packet is classified as high priority. EF - <101110>, AF - <001010> <010010> <011010> <100010> and Network Control - <111000> <110000>

Disable - Default DSCP classification is not applied.

Apply

Button to confirm settings.

QoS Functions

- [Per Port Settings](#)
- [Other Settings](#)

QoS Other Settings

Function Name	Status	Settings
802.1p priority tag high priority threshold	4	4
Egress service policy	16 : 1	16 : 1
Specific DSCP (A)	Disabled	<input type="radio"/> Enable <input checked="" type="radio"/> Disable 111111
Specific DSCP (B)	Disabled	<input type="radio"/> Enable <input checked="" type="radio"/> Disable 111111
Specific IP & Mask (A)	Disabled	<input type="radio"/> Enable <input checked="" type="radio"/> Disable IP: 255.255.255.255 Mask: 255.255.255.255
Specific IP & Mask (B)	Disabled	<input type="radio"/> Enable <input checked="" type="radio"/> Disable IP: 255.255.255.255 Mask: 255.255.255.255

QoS Global Settings

Description

802.1p high priority threshold	802.1p High Priority Tag Setting for 802.1p classification Valid values : 0 - 7
Egress service policy	Weighted Round Robin ratio: 4:1 - 4 high priority packets then 1 low priority packet 8:1 - 8 high priority packets then 1 low priority packet 16 :1 - 16 high priority packets then 1 low priority packet <i>Always high first</i> - Packets in high priority queue are sent first until the queue is empty
Specific DSCP(A)	<i>Enable</i> - Enable user defined DSCP(A) checking <i>Disable</i> - DSCP(A) classification is not applied.
Specific DSCP(A) Value	Enter user defined DSCP(A) value for classification.
Specific DSCP(B)	<i>Enable</i> - Enable user defined DSCP(B) checking <i>Disable</i> - DSCP(B) classification is not applied.
Specific DSCP(B) Value	Enter user defined DSCP(B) value for classification.
Specific IP & Mask (A)	If a received IP packet 's source address or destination address belongs to the user defined IP network addresses. The packet is classified as high priority. <i>Enable</i> - Enable user defined IP(A) network address checking <i>Disable</i> - IP(A) classification is not applied.
Specific IP Address (A)	Enter user defined IP(A) address for classification.
Specific Mask (A)	Enter user defined IP(A) subnet mask for classification. IP(A) address and IP(A) subnet mask specify IP(A) user defined

	IP network address for IP packet classification.
Specific IP & Mask (B)	If a received IP packet 's source address or destination address belongs to the user defined IP network addresses. The packet is classified as high priority. <i>Enable</i> - Enable user defined IP(B) network address checking <i>Disable</i> - IP(B) classification is not applied.
Specific IP Address (B)	Enter user defined IP(B) address for classification.
Specific Mask (B)	Enter user defined IP(B) subnet mask for classification. IP(B) address and IP(B) subnet mask specify IP(B) user defined IP network address for IP packet classification.
Apply	Button to confirm the settings

A received packet on an ingress port is classified as high priority if it meets one the following classifications:

1. The ingress port is enabled for port based high priority.
2. The ingress port is enabled for 802.1p classification and the packet is 802.1Q tagged with a tag value equal to or higher than **802.1p high priority tag threshold** setting.
3. The ingress port is enabled for Default TOS/DS classification and the packet is an IP packet with DSCP value <101110>, <001010>, <010010>, <011010>, <100010>, <111000> or <110000>.
4. Specific DSCP(A) classification is enabled and the packet is an IP packet with DSCP value matched **Specific DSCP(A)** setting.
5. Specific DSCP(B) classification is enabled and the packet is an IP packet with DSCP value matched **Specific DSCP(B)** setting.
6. Specific IP & Mask (A) classification is enabled and the packet is an IP packet whose source or destination address belong to the network address specified by **Specific IP & Mask (A)** settings.
7. Specific IP & Mask (B) classification is enabled and the packet is an IP packet whose source or destination address belong to the network address specified by **Specific IP & Mask (B)** settings.

If none of above classifications is matched, the received packet is classified as low priority. It is suggested to enable those classifications which are required for your application only and disable the rest.

5.4.5 PoE Controls

PoE Controls menu is used to configure the settings for PoE function as follows:

Master Enable

Enable

Disable

PoE Port Setting

Port	PoE Enable
Port 1	<input type="text" value="Enable"/>
Port 2	
Port 3	
Port 4	

Port	PoE Enable	Power Status	Current(mA)	Voltage(V)	Power(W)
1	Enabled	Down	0.00	1.53	0.00
2	Enabled	Down	0.00	1.39	0.00
3	Enabled	Down	0.00	1.36	0.00
4	Enabled	Down	0.00	0.26	0.00

PoE Settings

Description

Master Enable

Activate PoE function of the switch
Enable - enable PoE function for the switch
Disable - disable PoE function for the switch

Port

Select port list for Port PoE Enable setting

Port PoE Enable

Port PoE function status
Enable - enable PoE function for the selected ports
Disable - disable PoE function for the selected ports

PoE Status

Description

PoE Enable

Port PoE function status

Power Status

Port PoE power status
Up - power is up (Power is suppling from the port to the link partner.)
Down - power is down

Current (mA)

Port PoE power current status (unit : mA)

Voltage (V)

Port PoE power voltage status (unit : V)

Power (W)

Port PoE power delivered (unit : Watt)

5.4.6 Security Manager

This menu is used to change the user name and password. User name and password are used for access login in telnet and web management interfaces of the switch.

Security Manager

User Name:	<input type="text" value="admin"/>
Assign/Change password:	<input type="password" value="***"/>
Reconfirm password:	<input type="password" value="***"/>

Settings	Description
User Name	New user name
Assign/Change password	New password
Reconfirm password	Retype the new password

5.4.7 Image Refresh Time

Image Refresh Time

The switch image shown in web pages is updated periodically to present the latest status. The default time interval of refreshing the image is 20 seconds. It can be changed by clicking any of the time buttons displayed. This is a run time setting and not a permanent setting.

5.4.8 Update Firmware

This menu is used to perform firmware (switch software) upgrade via TFTP protocol. Before doing TFTP operation, one TFTP server must be available in the network to where this switch is connected and the new firmware file **image.bin** is placed in the server.

TFTP Download New Image

TFTP Server IP Address	192.168.0.3
Firmware File Name	image.bin

Settings	Description
TFTP Server IP Address	Specify the IP address of the TFTP server
Firmware File Name	Specify the file name of the new firmware
Apply	Button to confirm the settings

5.4.9 Restore Default

Do you want to restore system default settings?

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

5.4.10 Reboot System

Are you sure to reboot system?

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

6. SNMP Management

The switch supports SNMP v1 protocol for SNMP management. One device MIB file is provided in the product CD. The MIB file is used for SNMP management software to set or get the management information objects provided in the switch.

6.1 MIB Objects

The device private management objects provided by the SNMP agent in the switch are:

Objects	OID	Description
Enterprise	867	Manufacturer ID
Device	37	Device ID (Snmp agent)
Software	867.37.1.1	Device firmware version
	867.37.1.2	MIB version supported
Port Status	867.37.4.1	Port status information including: Link, Auto-negotiation, speed, duplex
Port Control	867.37.4.2	Port control information including: Port function, auto-negotiation, speed, duplex
VLAN	867.37.5	VLAN function related status and control objects
QoS	867.37.6	QoS function related status and control objects
PoE	867.37.7	PoE function related status and control objects

6.2 SNMP Traps

In addition to the MIB, the switch also provides SNMP trap function for sending associated trap messages to trap managers when the predefined events are detected. The following trap events are supported:

Trap Event	Description
Cold Start	The switch is powered on and complete initialization
Authentication failure	SNMP community authentication failure
Port link change	Any port link change among the switched ports - Port link down to link up - Port link up to link down

The *Authentication failure* trap and *port link change* trap can be disabled individually. The trap manager settings must also be properly configured to make the trap function works. Refer to *Trap Manager* menu in telnet management interface and *Administrator->Basic* menu in web management interface.

Appendix. Factory Default Settings

IP Settings

IP Address	192.168.0.2
IP Subnet mask	255.255.255.0
Gateway IP	192.168.0.1

Security Manager Settings

User name	admin
Password	123

SNMP Settings

System name	Null
System location	Null
System contact	Null
Community string 1	Public, Access right - read only
Community string 2-4	Null
Trap manager 1-3 IP	Null
Trap manager 1-3 Community	Null
Authentication failure trap	Enabled
Port link change trap	Enabled

Port Control Settings

Port 1 - 8 Port function	Enabled
Port 1 - 6 Auto-negotiation	Enabled
Port 1 - 8 Port speed	100Mbps
Port 1 - 8 Port duplex	Full

VLAN Settings

VLAN function	Disabled
802.1Q tag aware VLAN	Disabled
Ingress member filtering	Disabled
VLAN group 1	member : P1 - P8, VID : 1
VLAN group 2	member : P2, VID : 2
VLAN group 3	member : P3, VID : 3
VLAN group 4	member : P4, VID : 4
VLAN group 5	member : P5, VID : 5

VLAN group 6	member : P6, VID : 6
VLAN group 7	member : P7, VID : 7
VLAN group 8	member : P8, VID : 8
Default VLAN group index	1 (group 1) for Port 1 - Port 8
Unmatched VID	Disabled for Port 1 - Port 8
Egress tag rule	4 for Port 1 - Port 8
Null VID replacement	Disabled for Port 1 - Port 8

QoS Settings

Port based priority	Disabled for Port 1 - Port 8
802.1p classification	Disabled for Port 1 - Port 8
Default TOS/DS classification	Disabled for Port 1 - Port 8
802.1p high priority threshold	4
Egress service policy	16:1
Specific DSCP (A)	Disabled
Specific DSCP (A) setting	111111
Specific DSCP (B)	Disabled
Specific DSCP (B) setting	111111
Specific IP & Mask (A)	Disabled
Specific IP address (A)	255.255.255.255
Specific IP mask (A)	255.255.255.255
Specific IP & Mask (B)	Disabled
Specific IP address (B)	255.255.255.255
Specific IP mask (B)	255.255.255.255

PoE Settings

PoE Master Enable	Disabled
Port PoE	Disabled for Port 1 - Port 4