Intelligent 8-port Gigabit Switch
User's Manual

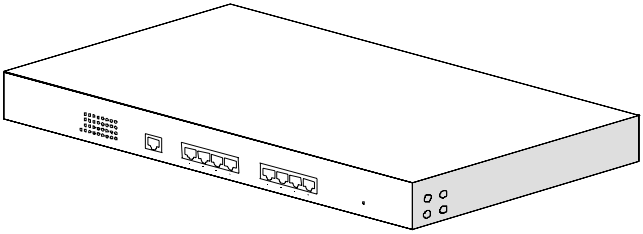
We make no warranties with respect to this documentation and disclaim any implied warranties of merchantability, quality, or fitness for any particular purpose. The information in this document is subject to change without notice. We reserve the right to make revisions to this publication without obligation to notify any person or entity of any such changes.

About this manual . . .

This manual is a general manual for different models of our Intelligent 8G Ethernet Switch. *They are similar in operation but have different hardware configuration.*

These models are

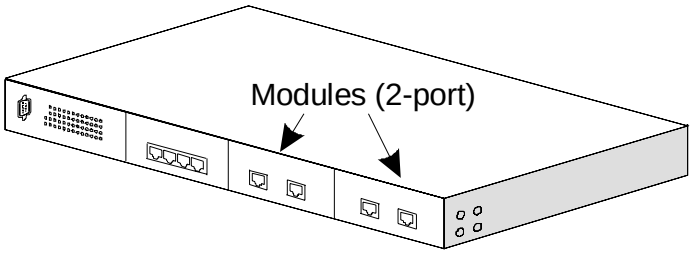
1. Non-modularized model



It has eight 10/100/1000Mbps fixed UTP ports.

2. Modularized model

It has four fixed UTP ports and two 2-port module slots at front panel. These 2-port modules could be 2* 10/100/1000M TX ports or 2* 1000M SX/LX ports or some other 2-port module. It has flexible design for hardware configuration.



Content

CHAPTER 1 INTRODUCTION 1

1.1 PACKAGE CONTENTS 1
1.2 INSTALLATION PROCEDURE 1

CHAPTER 2 WHERE TO PLACE THE SWITCH 2

2.1 PLACING THE INTELLIGENT SWITCH ON A DESK OR SHELF 2
2.2 MOUNTING THE INTELLIGENT SWITCH ONTO A RACK 2

CHAPTER 3 CONFIGURE THE SWITCH 3

3.1 INTRODUCTION 3
[1] Overview 3
[2] Manage the switch 3
3.2 CONFIGURE THE SWITCH BY CONSOLE 5
3.2.1 Logging on to the Intelligent Switch 5
3.2.2 Performing Basic Management Activities 7
3.2.2.1 General : 7
3.2.2.2 LAN Port : 8
3.2.2.3 Console Port : 8
3.2.3 Performing Advanced Management Activities 10
3.2.3.1 L2 Switching DataBase 11
3.2.3.2 IP Networking 19
3.2.3.3 Bridging 25
3.2.3.4 Static Filtering 26
3.2.3.5 Spanning Tree 27
3.2.3.6 SNMP 30
3.2.3.7 Other Protocols 31
3.2.3.8 QoS Setup 33
3.2.3.9 File Transfer 39
3.2.4 Other Functions in the Main Menu 41
3.3 CONFIGURE THE SWITCH BY WEB BROWSER 42
3.3.1 Logging on to the Switch 42
3.3.2 Performing Basic Management Activities 42
3.3.3 Performing Advanced Management Activities 43
3.3.4 File Transfer, Reboot, Logout and Save Setting 43

CHAPTER 4 SNMP AND RMON MANAGEMENT 44

4.1 OVERVIEW 44
4.2 SNMP AGENT AND MIB-2 (RFC1213) 44
4.3 RMON MIB (RFC 1757) AND BRIDGE MIB (RFC 1493) 45
4.3.1 RMON Group Supported 45
4.3.2 Bridge Group Supported 45

CHAPTER 5 CONFIGURE THE NETWORK CONNECTION 47

5.1 CONNECTING DEVICES TO THE SWITCH 47
5.2 CONNECTING TO ANOTHER ETHERNET SWITCH/HUB (NON-TRUNKING) 47
5.3 APPLICATION 47

CHAPTER 6 LEDS CONDITIONS DEFINED 49

CHAPTER 7 ADD/REMOVE MODULE 50

7.1 FOR MODULARIZED MODEL 50

CHAPTER 8 FAQ 51

A. PRODUCT FEATURES/SPECIFICATION 54

B. COMPLIANCES 56

C. WARRANTY 57

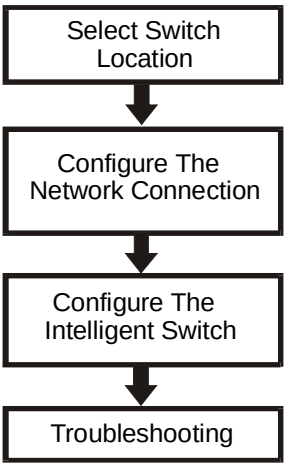
Chapter 1 Introduction

The Intelligent Gigabit Switch is a high performance Ethernet/ Fast Ethernet/ Gigabit Ethernet switch with SNMP/RMON web-based management function. From a departmental backbone switches to high-speed switch-to-switch and switch-to-server links, this switch delivers outstanding performance in every environment. With IGMP and VLAN functions, this Intelligent Switch ensures maximum bandwidth by reducing multicast transmissions and distributing data over the most efficient media and pathway. With Quality of Service (QoS) supports, this Intelligent Switch provides the capability to prioritize certain tasks on the network and this is particularly useful for sending voice or video over the switched network. This Intelligent Switch is a powerful management Ethernet switch for network administrator.

1.1 Package Contents

- One Intelligent 8GE Switch
- One AC power cord
- Rack-mount kits and screws
- This user's manual
- One console cable

1.2 Installation Procedure



Chapter 2

Chapter 5

Chapter 3

Chapter 6, 8

Chapter 2 Where To Place the Switch

The Intelligent Switch can be place on a flat surface (your desk, shelf or table) or mounted onto a rack. Place the Intelligent Switch at a location with these connection considerations in mind:

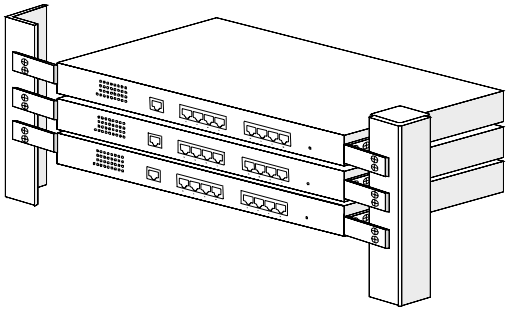
- The switch configuration does not break the rules as specified in Chapter 5.
- The switch is accessible and cables can be connected easily to it.
- The cables connected to the switch are away from sources of electrical interference such as radio, computer monitor, and light fixtures.
- There is sufficient space surrounding the hub to allow for proper ventilation (the switch may not function according to specifications beyond the temperature range of 0 to 50 degrees C).

2.1 Placing the Intelligent Switch on a Desk or Shelf

1. Place the Intelligent Switch on a firm flat surface where you want to install the switch.
2. If you want to configure the Intelligent Switch, please refer to Chapter 3.
3. Connect network cables to the Intelligent Switch. Please refer to Chapter 5 for network connection.

2.2 Mounting the Intelligent Switch Onto a Rack

1. Use the brackets and screws supplied in the rack mounting kit.
2. Use a crosshead screwdriver to attach the brackets to the side of the intelligent Switch.
3. Position the Intelligent Switch in the rack by lining up the holes in the brackets with the appropriate holes on the rack, and then use the supplied screws to mount the hub onto the standard EIA 19-inch rack.



Chapter 3 Configure the Switch

3.1 Introduction

[1] Overview

The Intelligent Switch provides a user-friendly, menu driven console interface. Using this interface, you can perform various switch configuration and management activities, including:

- Configuring system and port parameters.
- Assigning an IP address.
- Configuring DHCP relay.
- Setting up VLAN policy.
- Setting up packet filters.
- Configuring STP and SNMP parameters.
- Upgrading software.

[2] Manage the switch

There are three ways to manage the Intelligent Switch:

- Local Console Management via the Intelligent Switch serial port.
- Remote Management via a network connection with Telnet/http.
- Using an SNMP Network Management Station.

1. Local Console Management :

You can manage the Intelligent Switch locally by connecting a VT100 terminal, or a personal computer or workstation with terminal emulation software, to the Intelligent Switch serial port. The terminal or workstation connects to the Intelligent Switch serial port using a console cable that has the appropriate connectors on each end. This management method is ideal when:

- The network is unreliable.
- The switch has not been assigned an IP address.
- The Network Manager does not have direct network connection.

The default setting of the Intelligent Switch's serial port is [**Baud Rate : 115200, Data Bits : 8, Parity Bits : None, Stop Bit : 1, Flow Control : None**]. Therefore, configure the terminal or workstation to use these settings before you log on to the Intelligent Switch. You can change this default setting, if desired, after you log on.

Here is the example for terminal setup in Windows.
(Example of using *Hyper Terminal* of Windows95/98/2000)

1. Select Accessories → Communication → Hyper Terminal.
2. Execute HYPERTERM.EXE.
3. Set Name and Icon in Connection Description.
4. Set, in Connect To, a PC COM port through which the console and the modem are connected.
5. Set the followings in COMx Properties:

Bit per second: 115200, Data bits: 8, Parity bit: None, Stop bits: 1, and Flow control: None.

2. Remote Management :

You can manage the Intelligent Switch remotely by having a remote host establish a Telnet connection to the Intelligent Switch via an Ethernet or modem link. Using this management method, the Intelligent Switch must have an IP address. The Remote Console Management interface is identical in appearance and functionality to the Local Console Management interface described in the previous section.
You can manage the Intelligent Switch from remote site across a LAN using

a. SNMP Network Management Station
b. Web Browser interface
c. Telnet program

This management method lets you monitor statistical counters and set switch parameters from the remote Network Management Station. Using this management method:
. The network must run the IP protocol.
. The Intelligent Switch must have an IP address

Here is the quick guide for IP setting.

1. Complete the console connection with PC and start the terminal program.
2. Assign IP address in the main operation menu. .
   [Advanced Management] -> [IP Networking] -> [IP & RIP Settings] -> Select the VLAN -> [IP Address:]
3. Assign gateway address in the main operation menu. .
   [Advanced Management] -> [IP Networking] -> [Routing Table] -> “+” key -> [Default Gateway] -> [Default Gateway:]

3. Logging on to the Intelligent Switch

When you log on to the Intelligent Switch console port for the first time, a sign-on string appears and you are prompted for a console login name and password. The factory default login name is **admin** and password is **123456**. If you desire, you can change this password after you log on.

3.2 Configure the Switch by Console

The Intelligent Switch provides a menu-driven console interface for configuration purposes. The switch can be configured either locally through its console port or remotely via a Telnet/Http/SNMP session.

Note: The settings will take effect immediate. If you want to save them, please select "Save Settings" before leaving the setup.

3.2.1 Logging on to the Intelligent Switch

At the screen prompt:

```
------------------------------
Intelligent Switch
System Name:

Console Login:
------------------------------
```

Enter the console interface factory default console name "**admin**" and password "**123456**" or user-defined password if you changed the default password. The Switch Management screen will appear.

Switch Management
Basic Management
Advanced Management
Logout
Save Settings
Restore Default Settings
Reboot

Operating in the console interface, here is the direction about the keyboard :
Move the highlight up - **Up-arrow** or **K**
Move the highlight down - **Down-arrow** or **J**
Move the highlight between screens - **Tab**
Select the highlight option - **Enter**
Move to the previous menu - **Esc**

Operation Notes:

1. In the operation of the console configuration/management, you have to *highlight the item and press Enter* if you want to select or change it.
2. For some terminal program, the "Up-arrow" and "Down-arrow" can not be used to move cursor bar. In this situation, please use key "K" and "J" instead.
3. Only one console and three telnet users can log on to the Intelligent Switch concurrently. However, it is not recommended that multiple users modify the configuration at the same time.

Here we show the map of setting in the next page for quick reference.

Map of Functions in Menu :

<table>
<tr><td rowspan="13">Basic Management</td><td rowspan="3">General</td><td colspan="2">System Name, Software Version, Password, Http Enable/Disable, . . .</td></tr>
<tr><td colspan="2">LAN Port</td><td>Port Physical Configuration, Mac ID</td></tr>
<tr><td colspan="2">Console Port</td><td>Console Port Settings</td></tr>
<tr><td rowspan="10">Advances Management</td><td rowspan="4">L2 Switching Database</td><td>VLAN & PVID Perspective</td><td>VLAN Settings / Status</td></tr>
<tr><td>IP Multicast Group Perspective</td><td>IP Multicast Groups Operation Status</td></tr>
<tr><td>Mac Address Perspective</td><td>Mac ID Activity in the switch</td></tr>
<tr><td>Port Perspective</td><td>Port Status/Statistics, Mac Limit Setting</td></tr>
<tr><td>IP Networking</td><td colspan="2">IP Address, ARP Table, Routing Table, DHCP Gateway, Ping</td></tr>
<tr><td>Bridging</td><td colspan="2">Aging Time, Flooding Limit</td></tr>
<tr><td>Static Filtering</td><td colspan="2">Static Mac ID Filter-in, Filter-out</td></tr>
<tr><td>Spanning Tree</td><td colspan="2">Spanning Tree Status / Configuration</td></tr>
<tr><td>SNMP</td><td colspan="2">SNMP Configuration</td></tr>
<tr><td>Other Protocols</td><td colspan="2">GVRP / IGMP Protocols Enable/Disable and Configuration</td></tr>
<tr><td>QoS Setup</td><td colspan="2">Configure the QoS operation of the switch.
1. Enable / Disable
2. VLAN Tag / ToS / Logical Port QoS Configuration
3. Priority queues QoS Policy configuration</td></tr>
<tr><td>File Transfer</td><td colspan="2">Software / Firmware upload & download</td></tr>
<tr><td>Logout</td><td colspan="3">Logout the management interface.</td></tr>
<tr><td>Save Settings</td><td colspan="3">Save current settings.</td></tr>
<tr><td>Restore Default Settings</td><td colspan="3">Restore the factory default settings.</td></tr>
<tr><td>Reboot</td><td colspan="3">Reboot the switch.</td></tr>
</table>

3.2.2 Performing Basic Management Activities

Basic management activities consist of **General**, **LAN port**, and **Console port** tasks. To perform basic management activities:

1. Select "**Basic Management**" and the function table will appear in the screen.
2. Select a function and press Enter.

```
Basic Management
General
LAN Port
Console Port
```

Menu	Description
General	For system general information and settings.
LAN Port	1. For LAN port configuration and connection status 2. Get Mac address of the switch
Console Port	For console port configuration and settings

3.2.2.1 General :

```
General
Hardware Revision: 300023 Rev. 1
Hardware Configuration: 0800gh1.rom
Software Revision: v3.1e (Aug 22 2003 16:56:14)
Firmware Revision: No Firmware
    ----------
System Name:
Location:
admin Password: ******
guest Password: ******
Reboot-On-Error: Enabled
Remote Telnet Login: Enabled
Remote HTTP Login: Disabled
```

You can change the system name, location, administration/guest passwords, statistics collection, reboot-on-error, and remote Telnet login and other system settings.

There is some system information in the option. You can change the following items in this option.

1. **System Name** : The name of the system.
2. **Location** : Location of the system.
3. **Administration Password** : You have to enter the old password first before change the administration password. And the system will ask user to re-type the new password after the new password being entered. If the new password has been confirmed by the system, the "Password changed" message appears. Please press "Enter" to remove the message and return to the General screen.

Otherwise, there must be something wrong in the new password entering and the new password did not take effect. Please repeat this procedure to change the password.

4. **Guest Password** : Change the password of "Guest" account.
5. **Reboot-On-Error** : If it is enable in this option, the Intelligent Switch will automatically reset when a fatal error is detected.
6. **Telnet Login** : Enable or disable remote Telnet logins to the Switch.
7. **Remote HTTP Login** : Enable or disable remote HTTP login function.

3.2.2.2 LAN Port :

```
LAN Port Configurations
Speed & Flow Control
Physical Address
```

You can change the connection configuration on each port of the Intelligent Switch with this option.

1. Speed & Flow Control :

```
                    Line Speed & Flow Control
  Port  1 (1000M): Speed-Auto  FC-On     (Down)
  Port  2 (1000M): Speed-Auto  FC-On     (Down)
  Port  3 (1000M): Speed-Auto  FC-On     (Down)
  Port  4 (1000M): Speed-Auto  FC-On     (Down)
  Port  5 (1000M): Speed-Auto  FC-On     (Down)
  Port  6 (1000M): Speed-Auto  FC-On     (Down)
  Port  7 (1000M): Speed-Auto  FC-On     (Down)
  Port  8 (1000M): Speed-Auto  FC-On     (Down)
<UpArrow><DownArror>Move <Enter>Modify <L>Switch     <ESC>Previous
```

User can change the connection speed (10Mbps or 100Mbps), full duplex mode or half duplex mode, and the flow control function on each connection port with this function.

2. **Physical Address** :

```
Physical Port Address
  Port  1 (1000M): 00C0F660017B
  Port  2 (1000M): 00C0F660017B
  Port  3 (1000M): 00C0F660017B
  Port  4 (1000M): 00C0F660017B
  Port  5 (1000M): 00C0F660017B
  Port  6 (1000M): 00C0F660017B
  Port  7 (1000M): 00C0F660017B
  Port  8 (1000M): 00C0F660017B
```

This function can display the physical port address.

3.2.2.3 Console Port :

Console Port Configurations
Baud Rate: 115200
Flow Control: Disabled
Modem Control: Disabled
Modem Setup String: AT&F E0 L1 &C1 S0=1 &D2

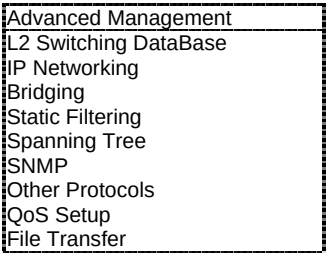
You can change the console baud rate, flow control method, modem control, and setup string; enable or disable SLIP; and configure the SLIP address and SLIP subnet mask.

1. **Baud Rate** : Select the baud rate of the Intelligent Switch console port. If the "Auto" option is selected, press the "Enter" key one or more times until the prompt of the Intelligent Switch Login Password appears on your computer screen when you exit the configuration program.
2. **Flow Control** : Select the flow control method of the Intelligent Switch console port.
3. **Modem Control** : Enable or disable the modem control function on the Intelligent Switch console port. If the modem control function is enable, proceed to "Specify a Modem Setup String" to specify the appropriate modem setup string.
4. **Modem Setup String** : If you enabled a modem connection to the console port, use this function to specify a modem setup string. You can select the "Default Setup String" and that will configure the modem to auto answer. It works for all Hayes compatible modems. Or, you may select the "Custom Setup String" to specify the modem initializing string by yourself.

3.2.3 Performing Advanced Management Activities

Advanced management activities consist of the L2 switching database, L3 IP networking, bridging, static filtering, spanning tree, SNMP, other protocols (GVRP and IGMP), and software upgrade. To perform advanced management activities:

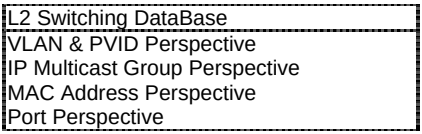
1. Select "**Advanced Management**" and the following screen will appear.



2. Select a function and press Enter.

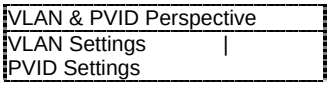
Menu	Description
L2 Switching DataBase	1. VLAN & PVID setting, VLAN activity status 2. IP multicast group activity status 3. Mac addresses activity status 4. Statistics on port, VLAN activity on port and Mac address learning configuration on port
IP Networking	1. IP address and RIP configuration of the switch 2. ARP Table of the switch 3. Routing Table of the switch 4. DHCP Gateway setting 5. Ping operation
Bridging	1. Aging Time setting 2. Flooding/Broadcast Strom Control setting
Static Filtering	1. Static Filter-out Mac Address (DA or SA) 2. Static Filter-in Mac Address (SA) on port
Spanning Tree	Spanning Tree Configuration on Switch / Ports
SNMP	SNMP Configuration of the switch
Other Protocols	Enable/Disable IGMP and GVRP protocols
QoS Setup	Configure the QoS operation of the switch

3.2.3.1 L2 Switching DataBase



You can view and configure the switch from VLAN, MAC address, IP multicast group, and port perspectives. If you select **L2 Switching DataBase** from the Advanced Management screen, the screen will appear.
The Intelligent Switch can be viewed from the four perspectives in the L2 Switching DataBase screen. These four views allow a network administrator to manage and monitor VLANs and their associated MAC addresses and ports status effectively.

- **VLAN & PVID Perspective :**



If you select "VLAN & PVID Perspective", the screen will appear.
You can select "VLAN Settings" to create VLAN groups first. Then use "PVID Settings" function to assign VLAN ID to ports for untagged packets.

*** Default VLAN** : The IEEE 802.1Q standard defines VLAN ID #1 as the default VLAN. The default VLAN includes all the ports as the factory default. The default VLAN's egress rule restricts the ports to be all untagged, so it can, by default, be easily used as a simple 802.1D bridging domain. The default VLAN's domain shrinks as untagged ports are defined in other VLANs.

*** Tagged/Untagged Port** : Tag is a four bytes packet information added in a packet for VLAN and priority information of the packet. We call the packets with tag as ***tagged packets*** and the packets without tag as ***untagged packets***. For the ports on the switch, we also set them as tagged or untagged port when we configure the VLAN.
For *untagged ports*, they should be connected to untagged devices and the network administrator should assign the ***PVID*** (Port VLAN ID) to these ports as their VLAN ID. If these untagged packets are forwarded to tagged ports, tags will be added to the packets with the PVID as their VLAN ID in the tag.
For *tagged port*, they should be connected to tagged devices. If these tagged packets are forwarded to untagged ports, the tag will be removed from the packets.

*If "**VLAN Settings**" is selected*, the following screen will appear.

VLAN ID	Name
1 (0x001)	Default

You can do the following operations from this screen.
1. Create a new VLAN
2. Delete a VLAN
3. View VLAN activity
4. View and change VLAN configuration

1. Create a new VLAN :

a). Use "+" (Shift key & + key) to add a VLAN. Move the highlight and press Enter to assign VLAN ID and VLAN name to the new VLAN. The ID is a 12-bit decimal or hexadecimal ID value. (Notes: "Remote" will be appended to the VLAN ID automatically if the VLAN is learned from a remote switch.)

New VLAN Settings
VLAN ID:
VLAN Name:

b). After a new VLAN is created, you can add switching ports to the VLAN in the following screen.

Switch Ports	Properties

Use "**+**" (Shift key & + key) to add a switch port to the VLAN. Select Tagged or Untagged port first. Then select the port number. Repeat these steps to add switch ports to the VLAN.

To delete a switch port in the screen, highlight the port and press "-" (- key) to remove the port from the VLAN.

2. Delete a VLAN :

Highlight the VLAN you want to delete and press "-" (- key). A message will ask whether you are sure you want to delete the VLAN ID. Select "Yes" and the VLAN will be deleted.

3. View VLAN activities :

You can view active ports associated with a VLAN here.

a). Highlight an existing VLAN and press Enter. Then select the "VLAN Activities". The screen will appear.

VLAN 10 (0x00A) test
Port Count: 1

VLAN Domain
Port 7

This screen shows all active ports for the VLAN you selected. Active ports are those ports that have been sending frames from this VLAN to the switch.

4). View or change a VLAN configuration.

a). Highlight an existing VLAN and press Enter. Then select the "VLAN Settings". The following screen will appear.

Switch Ports	Properties
Port 4	untagged
Port 5	untagged
Port 6	untagged

b). To add ports to VLAN, use "+" (Shift key & + key) to add a switch port to the VLAN. Select Tagged or Untagged port first. Then select the port number. Repeat these steps to add switch ports to the VLAN.

c). To delete ports from VLAN, highlight the port and press "-" (- key) to remove the port from the VLAN. Repeat these steps to remove switch ports from the VLAN.

*If "**PVID Settings**" is selected*, the following screen will appear.

PVID Settings	
Port 1:	1 (0x001)
Port 2:	1 (0x001)
Port 3:	1 (0x001)
Port 4:	1 (0x001)
Port 5:	1 (0x001)
Port 6:	1 (0x001)
Port 7:	1 (0x001)
Port 8:	1 (0x001)

Select the port and then you can modify its PVID.

About PVID:

After VLAN setting complete, you can go to "**PVID Settings**" function to assign PVID to connection ports.

Because there is no VLAN information in untagged packets for untagged ports, you can assign VLAN ID to untagged ports with this function. But it is not necessary for tagged ports because there is already VLAN information in the packets. (Tagged ports only for tagged network devices only. Don't use tagged ports for untagged devices.)

- **IP Multicast Group Perspective :**

The IP multicast group perspective provides information associated with an IP multicast group. To obtain an IP multicast group perspective:

a). Highlight "**IP Multicast Group Perspective**" and press the Enter key. The following screen appears.

IP Multicast Group Address	
224.0.1.1	VLAN 1 (0x001)
224.0.1.24	VLAN 1 (001)

Notes: If the IGMP protocol is disable, the “IGMP Currently Disabled” message will appear.
Because the IP multicast groups are generated from the IGMP snooping operation of the switch, please enable the IGMP protocol in "Other Protocols" of "Advanced Management" first.

b). To obtain an IP multicast group perspective for one of the addresses in the screen, highlight an address and press the Enter key.

IP Multicast Group 224.0.1.1 VLAN 1 (0x001)
No. of Ports in Multicast Group: 1 No. of Hosts in Multicast Group: 1

Hosts
00C0F6B03729

Multicast Domain
Port 5

c). To view the VLAN and IP multicast group addresses associated with the MAC address, highlight a host in the Hosts screen and press Enter. A VLAN/IP Multicast Group Membership screen will appear.

- **MAC Address Perspective :**

The MAC address perspective lets you view all characteristics associated with a MAC address, corresponding VLANs, and corresponding ports in the switching database. To obtain a MAC address perspective . . .

a). Highlight "**MAC Address Perspective**" and press Enter key. You are prompted for a MAC address. Enter a MAC address, and a screen similar to the one appears.

Mac Address 00C0F6B03729
Member of IP Multicast Group(s) : Yes Filtering : No Port : 5

VLAN/IP Multicast Group Membership
VLAN 1 (0x001) IP Group 224.0.1.1

b). Use the Up and Down Arrow keys to scroll through the VLAN/IP Multicast Group Membership screen.

- **Port Perspective :**

The port perspective lets you view VLAN activities and RMON statistics for each port. You can also configure Mac address learning function of each port from this function. Highlight "**Port Perspective**" and press the Enter key. The Port Perspective screen appears.

Port Perspective
Per Port VLAN Activities
Per Port Statistics
Per Port MAC Limit
Port Access Type

1. Per Port VLAN Activities

If you select “Per Port VLAN Activities” from the Port Perspective screen, a screen similar to the Per Port VLAN Activities appears.

Per Port VLAN Activities
Port 1 (1000M)
Port 2 (1000M)
Port 3 (1000M)
Port 4 (1000M)
Port 5 (1000M)
Port 6 (1000M)
Port 7 (1000M)
Port 8 (1000M)

Highlight the port number whose corresponding VLANs activities you want to view. Press the Enter key. A screen with a list of the MAC addresses for the selected VLAN and the corresponding VLAN memberships will appear.

Port 7
VLAN Count: 2
Total MAC Address Count: 6

MAC Addresses
0000E2617504
0000E2921DAD
0000E294F6C8
0000E83641BA
0000E836528E
0000E84272D1

VLAN Membership
VLAN 1 (0x001)
VLAN 10 (0x00A)

Operation of the table:

1). Use **Tab** key to switch to the MAC Addresses screen if it is the current screen. Then Use the Up Arrow and Down Arrow key to scroll through the list of active MAC addresses for the selected port.

2). To search for a MAC address, press **S**. When the search prompt appears, enter a MAC address in the "Enter MAC Addr to Search" screen and press the Enter key. If the address is found, it is highlighted in the "Port MAC Addresses" screen.

3). To obtain additional information about a particular MAC address, scroll to the address in the "Port MAC Address" screen and press Enter key. The same screen as result in **MAC Address Perspective** will be prompted.

2. Per Port Statistics

If you select “Per Port Statistics” from the Port Perspective screen, you can also get a port list screen.

Select one of the ports, you can get the statistics counters for the port. For example, Port 7 is selected.

Port 7 Statistics
Total No. of Bytes Received: 1,096,656
Total No. of Packets Received: 9,076
Total No. of Broadcast Packets Received: 4,439
Total No. of CRC/Alignment Errors Received: 0
Total No. of Undersize Packets Received: 0
Total No. of Oversize Packets Received: 0
Total No. of Collisions: 0
Total No. of 64-byte Packets Received: 5,034
Total No. of 65 to 127-byte Packets Received: 1,657
Total No. of 128 to 255-byte Packets Received: 2,005
Total No. of 256 to 511-byte Packets Received: 380
Total No. of 512 to 1023-byte Packets Received: 0
Total No. of 1.0 to 1.5-kbyte Packets Received: 0
VTotal No. of Bytes Transmitted: 384

To reset counters for the port in the screen above, press **R**. Then select Yes in the confirm screen to reset the counters.

Note: If the counters are always zero, please check [Basic Management] -> [General] -> Statistics Collection. If it is disable, please enable it.

3. Per Port MAC Limit

You can configure Mac address learning function of each port with this function to

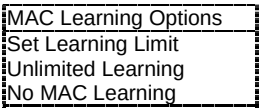
1. Limited Learning
2. Unlimited Learning
3. No Learning

for Mac address limit application on port.

If you select this function, the screen will appear.

Per Port MAC Limit
Port 1 (10/100M): Unlimited
Port 2 (10/100M): Unlimited
Port 3 (10/100M): Unlimited
Port 4 (10/100M): Unlimited
Port 5 (10/100M): Unlimited
Port 6 (10/100M): Unlimited
Port 7 (10/100M): Unlimited
Port 8 (10/100M): Unlimited

Then you highlight the port number and press Enter. The following screen will appear.



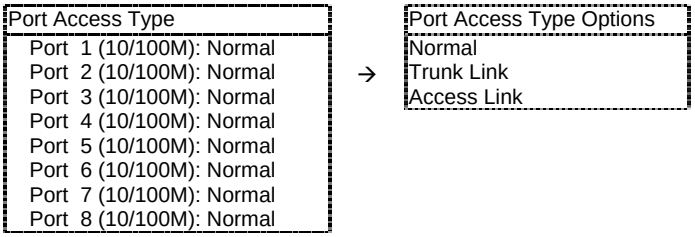
a). *Set Learning Limi*t : You can set a number to limit the PC number that can share this connection at the same time.
b). *Unlimited Learning* : You can remove the PC connecting number limit if you select this item. And the PC connecting number on the port will become no limit. (It's the normal state of a normal switch.)
c). *No MAC Learning* : You can disable the MAC learning function on this port if you select this item. The MAC addresses that can connect to this port will be assigned by the operator from the "Static Filtering" function.

The "Set Learning Limit" function can set a limit on the number of PC that can share this connection. The "No MAC Learning" function can set a static Mac address table (manual assigned) to allow only these PC can use this connection. This function allows the network administrator or the service provider to limit the users that can access network through the connected ports.
"No MAC Learning" is a static user limit function - only these Mac addresses are allowed. "Set Learning Limit" is a dynamic user number limit function – any Mac addresses in the limited number are allowed to access network through the ports.

Note: If you select "Set Learning Limit" on the connection port and also assign some MAC addresses on the port in the "MAC Address In-Filters" of "Static Filtering" function, these MAC addresses will always be allowed to use this connection and these MAC addresses are not included in the limit number of PC.

4. Port Access Type

You can configure the port access type for tagged/untagged operation. There are three options for each port of the switch.



1. Normal : the packet transmitted from the port will be tagged or untagged – depending on the packet and setting. But the packets will be always untagged if the PVID of the port is the same as its VLAN ID.
2. Trunk Link : the packets transmitted from the port will be always tagged.
3. Access Link : the packets transmitted from the port will be always untagged.

If the port is uplink to another switch/device with applications that needs tag in packet (for example, 802.1Q VLAN), users can configure it as “Trunk” and all the packets from the port will always be tagged.

If the port is connected to an untagged device (for example, normal network adapter), users can configure it as ”Access” for untagged packets.

The Normal option will tag or untag packet according to the packet and port setting. But if PVID of port is equal to its VLAN ID, the network device should be untagged and the port will always send untagged packets.

Here is the table about the setting.

Port setting	Direction	Operation	About PVID
Trunk Link	Receive	Tagged packet only	Don’t care PVID.
	Transmit	Always tagged packet	
Access Link	Receive	Untagged packet only	PVID must be equal to VLAN ID.
	Transmit	Always untagged packet	
Normal	Receive	Tagged packet	Don’t care PVID.
		Untagged packet	PVID must be equal to VLAN ID.
	Transmit	Tagged packet	If PVID is not equal to VLAN ID and the port is tagged port.
		Untagged packet	If PVID is equal to VLAN ID or the port is untagged port.

3.2.3.2 IP Networking

In this function, you can view or change IP settings, ARP and routing table parameters, RIP parameters, DHCP gateway settings, and ping settings.

If you select **IP Networking** from the Advanced Management screen, the IP Networking screen appears.

IP Networking
IP & RIP Settings
ARP Table
Routing Table
DHCP Gateway Settings
Ping

- **IP & RIP Setting :**

  If this function is selected, an "IP Settings" screen similar to the following appears, with a list of the VLAN IDs, IP addresses, subnet masks, and frame types currently defined.

VLAN ID	IP Address	Subnet Mask	Proxy ARP	RIP
1 (0x001)	192.168.1.9	255.255.255.0	Disabled	Disabled
10 (0x00A)				

The IP and its subnet setting of the switch are assigned based on VLAN. Different VLAN could be different IP subnets. For normal application, uses just need to assign IP address to the default VLAN for remote management.

To modify the settings shown:

a). Highlight the row that contains the parameters you want to change, then press Enter. The following screen appears.

VLAN 1 (0x001) IP Settings
IP Address: 192.168.1.9
IP Subnet Mask: 255.255.255.0
Frame Type: Ethernet_II
BOOTP: Disabled
Proxy ARP: Disabled
RIP Setting: Disabled
Use Broadcast/Multicast:
Advertise Routes:
Advertise Default Route:
Accept RIP V1/V2 Updates:
Accept Default Route Updates:
Use Split Horizon:
Use Poisoned Reverse:
Send Triggered Responses:

To change a setting, highlight it and press the Enter key.

To delete a setting, highlight the setting and press the "-" key.

Notes:

1. The IP and its subnet setting of the switch are assigned based on VLAN.
2. This switch allows user to assign different IP subnet on different VLANs.
3. The RIP operation of the switch is for internal routing between the IP subnet assigned on different VLANs. It is not a real L3 switch high-speed routing operation.
4. For normal case, assign the switch's IP address on the default VLAN for remote management is OK.
5. If you expect the switch to get IP from DHCP server, please set "BOOTP" item to DHCP.

- **ARP Table :**

If you select **ARP Table** from the "IP Networking" screen, an ARP Table screen appears with the ARP table entries that have been already defined or learned by the switch.

Internet Address	Physical Address	VLAN ID	Type
210.63.246.25	0000E8503807	1 (0x001)	dynamic

You can *add*, *delete* and *search* static entries in the ARP table in the screen.

1). Adding static entries to the ARP table

a). From the ARP Table screen, hold down the Shift key and press +. The Static ARP Specifications screen appears.

b). Highlight the Internet Address and press Enter. A "Enter Internet Address" screen will appear.

c). Type an Internet address (IP address). When you finish, press Enter. The Internet address you typed appears next to Internet Address in the Static ARP Specifications screen.

d). Highlight the Physical Address and press Enter. A "Enter Physical Address" screen will appear.

e). Type the corresponding physical address and press Enter. The physical address you typed appears next to Physical Address in the Static ARP Specifications screen.

f). Press Esc. The Internet and physical addresses you typed appear in the ARP Table screen.

g). To add more static ARP table entries, repeat these steps. When you finish, press Esc to return to the ARP Table screen.

2). Deleting Static ARP Table Entries

If you no longer need a static entry in the ARP table, use the following procedure to delete it. There is no precautionary message that appears before you delete a static ARP table entry. Therefore, be sure you want to delete the entry before doing so.

- Highlight the ARP entry that you want to delete and press "-". The entry will be deleted.

3). Searching for ARP Table Entries

a). From the ARP Table screen, press S. The Search Options screen prompts you to select an Internet Address or a Physical Address.

b). Select the "Internet Address" or "Physical Address" and then enter the IP or physical address you are searching and press Enter. The address you want to view is highlighted.

Note: The ARP (Address Resolution Protocol) table is a mapping table of IP address and its Ethernet Mac addresses. The ARP table in the switch is similar to the ARP table in a PC.

- **Routing Table :**

If you select **Routing Table** from the IP Networking screen, a Routing Table screen appears.

Network	Mask	Gateway	Metric	VLAN	Type	Protocol
0.0.0.0	255.0.0.0	0.0.0.0	1		Martian	Local
127.0.0.0	255.0.0.0	0.0.0.0	1		Martian	Local
192.168.1.0	255.255.255.0	192.168.1.9	16	0x001	Direct	Local
192.168.1.0	255.255.255.255	192.168.1.255	16	0x001	Martian	Local
192.168.1.9	255.255.255.255	192.168.1.9	16	0x001	Other	Other
192.168.1.9	255.255.255.255	192.168.1.9	16	0x001	Myself	Local
192.168.1.255	255.255.255.255	192.168.1.255	16	0x001	Bcast	Local
224.0.0.0	224.0.0.0	0.0.0.0	1		Martian	Local
224.0.0.0	240.0.0.0	0.0.0.0	1		Mcast	Local
224.0.0.9	255.255.255.255	0.0.0.0	1		Mcast	Local
255.255.255.255	255.255.255.255	255.255.255.255	1		Bcast	Local

The Routing Table allows you to view, add, delete, or search a particular routing path. The following table identifies the columns in this screen.

Item	Description
Network	The IP sub-network address to which the switch can route packets.
Mask	The related IP sub-network mask to which the switch can route packets.
Gateway	The IP address of the router at the next hop.
Metric	The number of hops needed between the switch and the destination network.
VLAN	The VLAN within which the gateway or destination resides.
Type	The IP route type for the IP subnetwork. There are six IP route types: **Direct -** A directly connected subnetwork. **Remote -** A remote IP subnetwork or host address. **Myself -** A switch IP address on a specific IP subnetwork. **Bcast -** A subnetwork broadcast address. **Mcast -** An IP multicast address. **Martian -** An illegal IP address to be filtered.
Protocol	**Local -** A manually configured routing entry. **NetMgmt -** A routing entry set via SNMP. **ICMP -** A routing entry obtained via ICMP redirect. **RIP -** A routing entry learned via the RIP protocol.

	Other - A protocol other than one of the other four listed above.

1). Adding Routing Table Entries

a). From the Routing Table screen, hold down the Shift key and press +. The "Route Options" screen appears. Select "Default Gateway" or "Static Route" and press Enter.

Route Options
Default Gateway Static Route

b). If you select "Default Gateway", the following screen appears. Press Enter and type an IP address for the default gateway.

Default Route Specifications
Default Gateway: 0.0.0.0 Metric: 1

c). If you select "Static Route", the following screen appears. At each field, press Enter, type the appropriate parameter, and press Enter again.

Static Route Specifications
Network: Mask: Gateway: Metric: 1

2). Deleting Routing Table Entries

If you no longer need an entry in the routing table, use the following procedure to delete it. There is no precautionary message that appears before you delete an entry in the routing table. Therefore, be sure you want to delete the entry before doing so.

- Highlight the Routing table entry you want to delete and press "-". The entry will be deleted.

3). Searching for Routing Table Entries

To search for entries in the Routing table, press S in the Routing Table screen. Then "Enter Network Address" screen appears. Type the network address you want to search for, then press Enter.

Note: You can assign the gateway IP address of the switch with the “Default Gateway” in Adding Routing Table Entries operation for management through Internet.

■ DHCP Gateway Setting :

If you highlight **DHCP Gateway Settings** from the "IP Networking" screen and press the Enter key, a DHCP Gateway Settings screen appears.
In this screen:

VLAN ID	IP Address	DHCP Gateway	Max Hops	Delay	Servers	Relays
1 (0x001)	192.168.1.9	Disabled				

- **VLAN ID** shows the IDs of the VLANs that have been defined.
- **IP Address** shows the corresponding IP addresses of the VLANs.
- **DHCP Relay** shows whether the DHCP relay is enabled or disabled.
- **Max Hops** shows the maximum number of hops that a DHCP request broadcast can be relayed along the DHCP relay path from the DHCP client to the DHCP server.
- **Delay** shows the number of seconds that must elapse before a DHCP request broadcast is relayed to the next IP subnetwork.
- **Servers** shows any preferred servers that have been defined.
- **Relays** shows the outbound IP subnetwork for relaying a DHCP request broadcast.

Notes: To specify DHCP gateway settings, you must first create a VLAN with an assigned IP address as described in "**VLAN Perspective**" of "**L2 Switching DataBase**".

The following procedure describes how to change the DHCP gateway settings. As part of this procedure, you can specify up to three preferred servers and/or an outbound relay interface.

a). Highlight the appropriate VLAN ID and press Enter. A screen similar to the following appears.

```
DHCP Gateway Settings
VLAN ID: 1 (0x001)
IP Address: 192.168.1.9
    ----------
DHCP Gateway: Disabled
Maximum Hops: 0
Delay (sec): 0
Preferred Server:
Preferred Server:
Preferred Server:
Preferred Server:
```

b). To add a relay IP, hold down the Shift key and press +. A setup screen will appear. Highlight the appropriate interface and press Enter.

c). You can enable/disable DHCP Gateway, set Maximum Hops number, set the Delay time (in seconds) and specify up to three more preferred servers in the screen. Please move the highlight and press Enter to setup these items.

This DHCP relay function allows the DHCP request being routed to the DHCP server that is in different IP subnet on another VLAN.

Notes: About DHCP Protocol

Dynamic Host Configuration Protocol (DHCP), described in RFC 1541, is an extension of the Bootstrap Protocol (BOOTP). DHCP allows hosts on a TCP/IP network to dynamically obtain basic configuration information. When a DHCP client starts, it broadcasts a DHCP Request packet, looking for DHCP servers.

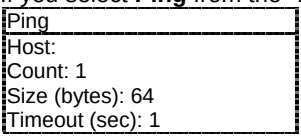
DHCP servers respond to this packet with a DHCP Response packet. The client then chooses a server to obtain TCP/IP configuration information, such as its own IP address. Since DHCP uses broadcast mechanism, a DHCP server and its client must physically reside on the same subnet. However, it's not practical to have one DHCP server on every subnet; in fact in many cases, DHCP/BOOTP clients and their associated DHCP/BOOTP server(s) do not reside on the same IP network or subnet. In such cases, a third-party agent is required to transfer BOOTP messages between clients and servers. BOOTP/DHCP Relay, described in RFC 1542, enables a host to use a BOOTP or DHCP server to obtain basic TCP/IP configuration information, even if the servers do not reside on the local subnet. When a Intelligent Switch with BOOTP/DHCP Relay Agent receives a DHCP Request packet destined for a BOOTP/DHCP server, it inserts its own IP address into the DHCP Request packet so the server knows the subnet where the client is located. Then, depending on the configuration setup, the switch either:

- Forwards the packet to a specific server as defined in the switch' configuration using unicast routing, or
- Broadcasts the DHCP Request again to another directly attached IP subnet specified in the switch configuration for the receiving IP subnet.

When the DHCP server receives the DHCP request, it allocates a free IP address for the DHCP client from its scope in the DHCP client's subnet, and sends a DHCP Response back to the DHCP Relay Agent. The DHCP Relay Agent then broadcasts this DHCP Response packet received from the DHCP server to the appropriate client.

- **Ping :**

If you select **Ping** from the "IP Networking" screen, a Ping screen appears.



You can set the following items for the ping operation:

- The IP address of the host you want to ping
- The packet count number (from 1 to 999, or 0 for an infinite packet count)
- The packet size (from 0 to 1500)
- The timeout value (from 0 to 999)

Highlight the items and press Enter, then you set each item in the screen. After all the items are set, you can press Esc to start the ping operation.

3.2.3.3 Bridging

If you select [Bridging] from the [Advanced Management], the Bridging Parameters screen appears.

Bridging Parameters
Aging Time (seconds): 300
Flood Limit for All ports (pkt/s): Unlimited

1. Aging Time

   Aging is an operation for switch to maintain its learning table. If a network device does not send any packet in the aging time, its Mac address entry in the learning table will be removed. This operation is called aging.

   To change the aging time, highlight **Aging Time (seconds)** and press Enter. A prompt will ask you to enter a bridge aging period, in seconds. Enter a new aging period and press the Enter key. Enter **0** for no aging.

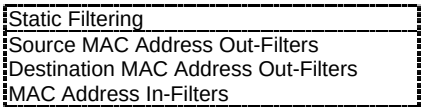
2. Flood Limit

   Whenever a packet is sent to a switch, the switch will try to find the destination port of the packet through looking it up in the learning table. Then forward it. If the DA (destination Mac address) of the packet cannot be found in the learning table, the switch will forward it to every port. This operation of a switch is called flooding. These flooding packets may cause unnecessary network traffic in the network.

   To change the flood limit for all ports, highlight **Flood Limit for All ports (pkts/sec)**, the following prompt asks you to set flood limit (packets per second) or unlimited. Select [Set Flood Limit] and enter a new flood limit. Or, you may select [Unlimited] to disable the flooding limit function for unknown Mac address packets.

3.2.3.4 Static Filtering

User can view, add, delete, or search all source or destination addresses to be filtered. If you select [Static Filtering] from the [Advanced Management] screen, the Static Filtering screen appears.



1. Mac Address Out-Filter:
The "Out-Filters" function will filter out these packets with the source/destination addresses in the out-filters table, i.e. these packets will not be forwarded by the switch.

2. Mac Address In-Filter:
The "In-Filters" function will filter in these packets with the MAC addresses in the in-filters table, i.e. the port of the switch will always forward these packets. This filter-in function is binding on port. If you set the MAC address learning function of the port to "No MAC Learning" in [Port Perspective] of [L2 Switching Database] of [Advanced Management], only these MAC addresses in the in-filters table for the port will be forwarded by the switch.

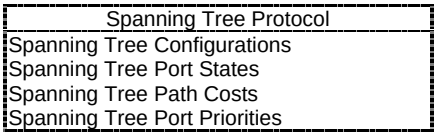
Mac Address Out-Filter/In-Filter Operation:
You can highlight one of these items and press Enter. A MAC address table will appear.

a). Add a MAC address : Hold down the Shift key and press + to add a specific MAC address to be filtered.
b). Delete a MAC address : Press "-" to delete a specific MAC address from being filtered. There is no precautionary message that appears before you delete a MAC address. Therefore, be sure you want to delete the address before doing so.
c). Search a MAC address : Press S to search through the list of MAC addresses in the static filtering database.

3.2.3.5 Spanning Tree

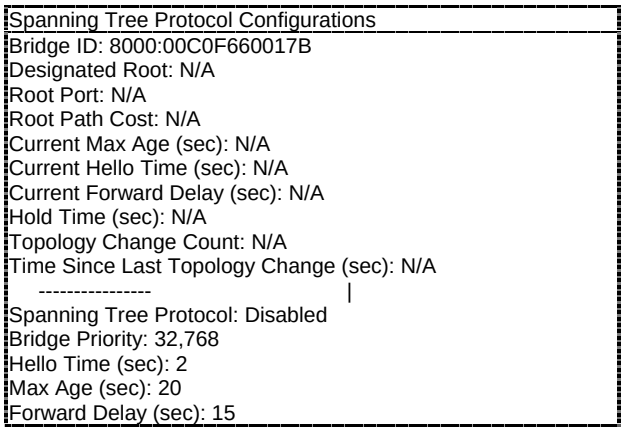
The Spanning Tree function can be used to prevent network loops, or to provide backup links with another network device. It can ensure that only one route exists between any two stations in the network.
(Note: Whenever any network connection configuration is changed, the new connection will start to work after about 30 seconds later if spanning tree is enable. That is the spanning tree re-configuration time.)

This function lets you view and change parameters relating to the spanning tree protocol. If you select [Spanning Tree] from the [Advanced Management] screen, the Spanning Tree Protocol screen appears.



- **Spanning Tree Configurations**

If you highlight [Spanning Tree Configurations] in the [Spanning Tree Protocol] screen and press the Enter key, a “Spanning Tree Protocol Configuration” screen appears.
The top half of this screen displays read-only values. The bottom half, starting with Spanning Tree Protocol, is user configurable. Highlight a field, then press Enter to change the value. When you finish, press the Esc key until you return to the desired screen.



1. Bridge Priority: Bridge priority is for selecting the root device, root port, and designated port. The device with the highest priority (lowest value) becomes

the STA root device. If all devices have the same priority, the device with the lowest MAC address will then become the root device.

2. Hello Time: The time interval for root device to transmits spanning tree configuration message.
3. Max Age: The maximum time for a device to start spanning tree reconfiguration without receiving STP configuration message. (All device ports should receive STP configuration messages at regular intervals.)
   The minimum value is the higher of 6 or [2 x (Hello Time + 1)].
   The maximum value is the lower of 40 or [2 x (Forward Delay - 1)].
4. Forward Delay: The maximum time for root device to wait before changing states (for example, listening to learning to forwarding). Every device must receive information about topology changes before it starts to forward frames and each port needs time to listen for conflicting. The delay time is needed for the STP operation request.
   The maximum value is 30.
   The minimum value is the higher of 4 or [(Max. Message Age / 2) + 1].

- **Spanning Tree Port States**

If you highlight [Spanning Tree Port States] in the Spanning Tree Protocol screen and press the Enter key, a Spanning Tree Port States screen appears. This screen displays read-only values. When you finish, press the Esc key until you return to the desired screen.

Spanning Tree Port States
Port 1: Disabled (Link Down)
Port 2: Disabled (Link Down)
Port 3: Disabled (Link Down)
Port 4: Disabled (Link Down)
Port 5: Disabled (Link Down)
Port 6: Disabled (Link Down)
Port 7: Disabled (Link Down)
Port 8: Disabled (Link Down)

If you want to change the administration status, highlight the port that you want to change and press Enter. You can enable or disable the selected port - Up for enable and Down for disable.

- **Spanning Tree Path Cost**

If you highlight [Spanning Tree Path Costs] in the Spanning Tree Protocol screen and press the Enter key, a Spanning Tree Path Costs screen appears.

Spanning Tree Path Costs
All Ports: 19
Port 1: 19
Port 2: 19
Port 3: 19
Port 4: 19
Port 5: 19
Port 6: 19
Port 7: 19

Port 8: 19

If you want to change the spanning tree path cost, highlight the port that you want to change and press Enter. Enter the new path cost in the prompt screen and press Enter. After completing the modification, press Esc to back to last screen.

Path Cost (0 – 65535): It is used to determine the best path between devices if looping happens. Lower values will be forwarded and should be assigned to ports with fast connections. Higher values will be blocked and should be assigned to ports with slow connections. The suggestion values are 100(50~600) for 10M, 19(10~60) for 100M and 4(3~10) for 1000M connections.

- **Spanning Tree Port Priorities**

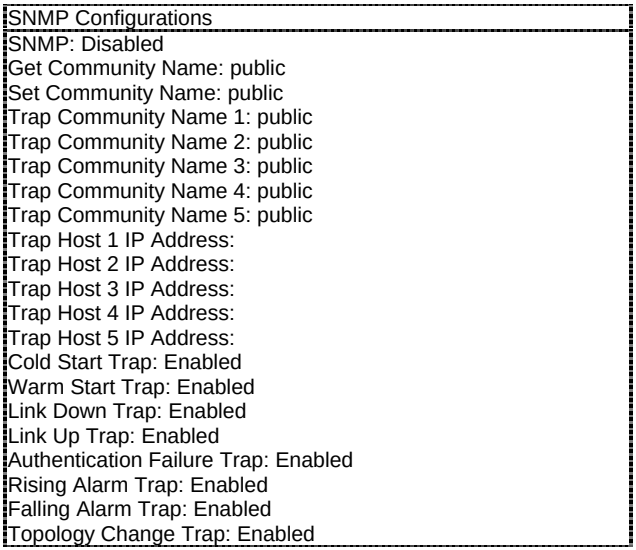
Spanning Tree Port Priorities
All Ports: 128
Port 1: 128
Port 2: 128
Port 3: 128
Port 4: 128
Port 5: 128
Port 6: 128
Port 7: 128
Port 8: 128

If you highlight [Spanning Tree Port Priorities] in the Spanning Tree Protocol screen and press the Enter key, a Spanning Tree Port Priorities screen appears.
If you want to change the spanning tree path priorities, highlight the port that you want to change and press Enter. Enter the new path priorities in the prompt screen and press Enter. The value is from 0 to 255 and a low value gives the port a greater likelihood of becoming a Root port. After completing the modification, press Esc to back to last screen.

About Port Priority (0-255) :
If the path cost for all ports on a switch are the same, the port with the highest priority (lowest value) will be forwarded when looping happens. If more than one port have the same highest priority, the port with lowest port number will be forwarded.

3.2.3.6 SNMP

You can view and change all SNMP-related information here. If you select [SNMP] from [Advanced Management] screen, the SNMP Configurations screen appears.



This switch support SNMP agent function and you can configure SNMP settings (community name, trap host, trap events…) here.

If you want to change the configuration, highlight the item that you want to change and press Enter. Enter the new setting for the item in prompt screen and press Enter. After completing the change, press Esc to leave.

3.2.3.7 Other Protocols

In this function, you can enable/disable GVRP and IGMP protocols of the switch.

Other Protocol Settings
GVRP: Disabled
IGMP: Disabled

The GVRP (GARP VLAN Registration Protocol) protocol can handle the VLAN activity inside the switch and between switches.
The IGMP (Internet Group Management Protocol) protocol can handle IP multicast activity in the network. This switch supports IGMP Snooping operation for IP multicast packets filtering and forwarding.

If you want to change the configuration, highlight the item that you want to change and press Enter.

GVRP : Enable - enable GVRP operation
Disable - disable GVRP operation

IGMP : Mode [Disable/Passive/Active]:
Disable - disable IGMP operation
Passive – Passively snooping on the IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to learn IP Multicast group members.
Active – Actively sending IGMP Query messages to solicit IP Multicast group members.
Query interval (sec): The query interval for IGMP operation in active mode.
Query timeout (sec) [Auto/Set Value]: The query timeout for IGMP operation in passive mode.

(If IGMP function is enabled and IP multicast happens in the switch, users can find the IP multicast groups at [IP Multicast Group Perspective] of [L2 Switching DataBase] in [Advanced management].)

Select the new setting for the item from prompt screen and press Enter. After completing the change, press Esc to leave.

About GVRP Protocol
In addition to network management tools that allow network administrators to statically add and delete VLAN member ports, the switch supports GARP VLAN Registration Protocol (GVRP). GVRP supports the dynamic registration of VLAN port members within a switch and across multiple switches. In addition to dynamically updating registration entries within a switch, GVRP is used to communicate VLAN registration information to other VLAN-aware switches, so that members of a VLAN can cover a wide span of switches in a network. GVRP allows both VLAN-aware workstations and the Intelligent Switch to issue and revoke VLAN

memberships. VLAN-aware the switch register and propagate VLAN membership to all ports that are part of the active topology of the VLAN.

About IGMP Protocol (IGMP Snooping and IP Multicast Filtering)

The Internet Group Management Protocol (IGMP) runs between hosts and their immediately neighboring multicast routers. The protocol's mechanisms allow a host to inform its local router that it wants to receive transmissions addressed to a specific multicast group. Routers periodically query the LAN to determine if known group members are still active. If there is more than one router on the LAN performing IP multicasting, one of the routers is elected "querier" and assumes the responsibility of querying the LAN for group members. Based on the group membership information learned from the IGMP, a router can determine which (if any) multicast traffic needs to be forwarded to each of its "leaf" subnetworks. Multicast routers use this information, along with a multicast routing protocol, to support IP multicasting across the Internet. IGMP provides the final step in an IP multicast packet delivery service since it is only concerned with the forwarding of multicast traffic from the local router to group members on directly attached subnetworks. The switch support IP Multicast Filtering by:

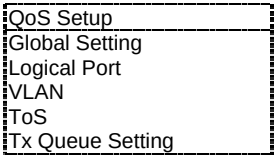
- Passively snooping on the IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to learn IP Multicast group members, and
- Actively sending IGMP Query messages to solicit IP Multicast group members.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts members and routers instead of flooding to all ports in the subnet (VLAN). The switch with IP multicast filtering/switching capability not only passively monitor IGMP Query and Report messages, DVMRP Probe messages, PIM, and MOSPF Hello messages; they also actively send IGMP Query messages to learn locations of multicast routers and member hosts in multicast groups within each VLAN. Note, however, IGMP neither alters nor routes any IP multicast packets. Since IGMP is not concerned with the delivery of IP multicast packets across sub-networks, an external IP multicast router is needed if IP multicast packets have to be routed across different sub-networks.

3.2.3.8 QoS Setup

QoS (Quality of Service) is a quite important issue for network devices now because there are so many different data are transferred in the network – phone call, audio, video, web business, email, file transfer, web access and so on. Different data types have different requests about delay, throughput and reliability on packet transfer. The network administrators should know about their network applications and the requests for these applications. Then they can configure this switch to meet these requests. When congestion happens on some ports of the switch, the QoS operation can transfer packets with different priorities, different drop rates, different bandwidth allocations for different requests of packets.

With delay bounded, strict priority, and/or WFQ transmission scheduling, and WRED dropping schemes, this switch provides powerful QoS functions for various multimedia and mission critical applications. Each port provides 8 transmission priorities and 2 levels of dropping precedence. Each packet is assigned a transmission priority and dropping precedence based on the VLAN priority field in a VLAN tagged frame, or the DS/TOS field, and UDP/TCP logical port fields in IP packets.



This section is a description about the QoS setting of the switch.

You can follow the entry for QoS setting. [Advanced Management] -> [QoS]. And here is the main menu of QoS setting.

Menu	Description
Global Setting	For general settings of the QoS functions in the switch
Logical Port	Define the TCP/IP service logical ports operation – enable/disable, transmit priority, drop rate.
VLAN	Define the transmit priority and drop rate operation in the switch for each priority value in VLAN tag.
ToS	Define the transmit priority and drop rate operation in the switch for each priority value in ToS.
Tx Queue Setting	Define and configure the QoS policy for the priority queues.

■ Global Setting

Set the general configuration for the QoS operation.

Global Setting
QoS Status: Enabled
DiffServ Expedite Forwarding: Enabled
ToS/VLAN Tag Preference: VLAN Tag
ToS for Xmit: From Bit[4:2] of ToS
ToS for Drop: From Bit[4:2] of ToS
WRED Drop Priority Setting...

1. **QoS Status** : Enable / Disable. This function can enable or disable the QoS function of the switch.

2. **DiffServ Expedite Forwarding** : Enable / Disable. This function can enable or disable the DiffServ EF function on the switch. This switch can map IETF DifferServ classes to its priority classes and transfer DiffServ packets with the following queue mapping.

Tx Queues	P7,P6	P5,P4	P3,P2	P1,P0
IETF	NM+EF	AF0	AF1	BE0

Note: DiffServ" is the abbreviation of "*Differentiated Service*". Differentiated Services provides a simple and coarse method of classifying services of various applications. And *Expedited Forwarding* (EF) has a single *codepoint* (DiffServ value). EF minimizes delay and jitter and provides the highest level of aggregate quality of service. Any traffic that exceeds some traffic limit may be discarded. The simplicity of DiffServ to prioritize traffic belies its flexibility and power. When DiffServ uses specific application types to identify and classify constant-bit-rate traffic, it will be possible to establish well-defined aggregate flows that may be directed to fixed bandwidth pipes. As a result, you could share resources efficiently and still provide guaranteed service.

3. **ToS/VLAN Tag Preference** : Select the preference priority information in packets – priority in ToS or priority in VLAN tag. ToS is the abbreviation of "*Type of Service*" and it is an 8-bit field in IP packet. Here is its definition.
   Bit 0-2 : Precedence. This 3 bits (value 0~7) indicate the priority of the IP packet.
   Bit 3 : Delay. If this bit is set (1), it requires low delay.
   Bit 4 : Throughput. If this bit is set (1), it requires high throughput.
   Bit 5 : Reliability. If this bit is set (1), it requires high reliability.
   Bit 6-7 : Unused.
   The content of ToS is set by the application on the network.

4. **ToS for Xmit** : You can select the bit field in ToS for transmit priority mapping. [7:5] is Bit 0-2 (Precedence) of ToS. [4:2] is Bit 3-5 (Delay/ Throughput/Reliability) of ToS.

5. **ToS for Drop** : You can select the bit field in ToS for drop priority mapping. [7:5] uses Bit 0-2 (Precedence) of ToS. [4:2] uses Bit 3-5 (Delay / Throughput / Reliability) of ToS.

6. **WRED Drop Priority Setting** : WRED is the abbreviation of "*Weighted Random Early Detection/Discard*". WRED is a congestion avoidance mechanism. When a packet belonging to a queue for which WRED is enabled arrives, some actions take place. The Average Queue Size (AQS) is calculated. If the AQS is less than the minimum WRED threshold, the packet is enqueued. Otherwise, the packet is dropped or enqueued accordingly to the Drop Percentage of the packet within a WRED class. The setting of WRED parameters can influence this behavior. It is possible to set WRED parameters for each aggregate of packets (Class).
   You can define two WRED drop rates (*Low Drop Rate* and *High Drop Rate*) here and there are three levels for each drop rate setting.

Low Drop Percentage
Level 1: 0%
Level 2: 25.0%
Level 3: 100%

   The drop levels *Level 1* and *Level 2* define the packet drop rates when queue buffer usage is up to different levels (depends on the QoS policy setting in [Tx Queue Setting] of the switch). *Level 3* is 100% dropping because the queue buffer is almost full.

■ **Logical Port**

You can configure the QoS operation of different TCP/IP logical (service) ports in the switch with this function. There are three types of logical ports can be configured in the function.

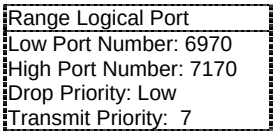
Logical Port
User-Defined Port
Range Port

1. **User-Defined Port** : This switch allows 15 user-defined TCP/IP logical ports for QoS operation.
   Select one of them (for example, 0) and assign a TCP/IP port number, you can do the following QoS settings on this TCP/IP logical port.

User-Defined Port 0
Port Number: 80
Drop Priority: Low
Transmit Priority: 7
Port Status: Enabled

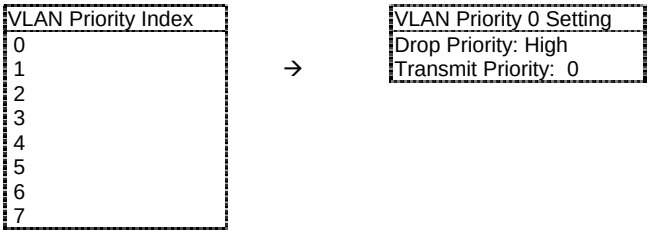
   1). Enable / Disable this QoS setting.
   2). Configure its drop rate to high drop rate or low drop rate.
   3). Configure its transmit priority to 0 ~ 7.

2. **Range Port** : In "*Range Logical Port*", you can define the drop priority and transmit priority for some range of TCP/IP logical ports.



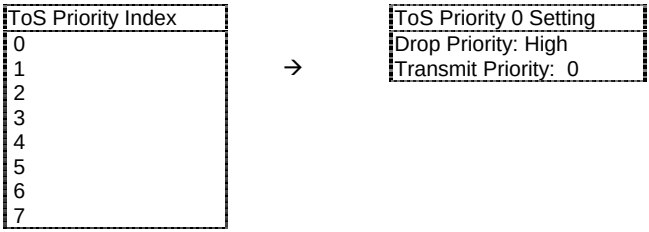
- **VLAN**

In this function, you can configure the drop priority and transmit priority of QoS operation for each priority value in VLAN tag.
Select one of them and you can configure the QoS configuration of this priority.



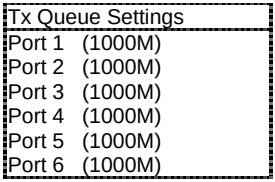
- **ToS**

You can configure the QoS operation – drop priority and transmit priority for each priority value in ToS.
Select one of them and you can configure the QoS configuration of this priority. You can select using Bit0-2 or Bit3-5 of ToS for the transmit priority and drop priority setting with “General” of QoS configuration.



- **Tx Queue Setting**

Users can define and configure the QoS policy of the switch in this function. Select the function and the following screen appears.



Port 7 (1000M)
Port 8 (1000M)

There are four basic QoS scheduling operations for this switch.

1. Strict Priority (SP) : SP is for the highest priority queue only in the switch. If there is only even one frame in the queue with SP, it will be transmitted first. The SP class is used for IETF expedited forwarding (EF), where performance guarantees are required. The SP traffic should be either policed or implicitly bounded (e.g. if the traffic of the queue with SP is very light and predictable patterned).
2. Delay Bound : It is a delay assurance algorithm of the switch. It can dynamically adjusts its scheduling and dropping criteria, guide by the queue occupancies and the due dates of their head-of-line(HOL) frames. As a result, we assure latency bounds for all admitted frames with high confidence.
3. Weighted Fair Queuing (WFQ) : You can weight the priority queues for different transmit bandwidth allocation for these queues. In WFQ mode, we do not assure frame latency as delay bound.
4. Best Effort (BE) : In BE mode, a queue only receives bandwidth when none of the other classes have any traffic to offer. It is used for non-essential traffic because we provide no assurances about BE performance.

This switch supports four scheduling configurations for each physical port on different priority queues (8 priority queues on each gigabit port).

	P7	P6	P5	P4	P3	P2	P1	P0
Delay Bound	Delay Bound						Best Effort	
SP + Delay Bound	Strict Priority		Delay Bound				Best Effort	
SP + WFQ	Strict Priority		Weighted Fair Queuing					
Weighted Fair Queuing	Weighted Fair Queuing							

Users can define and configure the QoS policy for the gigabit ports (Port 25,26).

Port 1 Transmit Queue
QoS Policy: SP + Delay Bound Bandwidth Partitions... Shaper Configuration... QoS with Flow Control: Disabled

1). QoS Policy :
Users can define the traffic scheduling policy of the eight priority queues in gigabit ports.

2). Bandwidth Partitions...
Users can configure the bandwidth partition for the eight priority queues in the gigabit ports for WFQ operation.

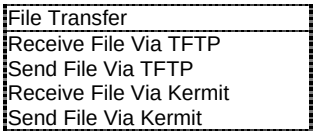
3). Shaper Configuration
The shaper function is used to control the peak and average rate for traffic with transmit priority 6 (queue P6). It is for the Gigabits ports, and only to queue P6

(the second highest priority) when it is in strict priority. It is design for expedited forwarding (EF) traffic.
Users can configure the peak and average rate for the traffic with transmit priority 6 (queue P6) here when it is in strict priority.

4). QoS with Flow Control
The flow control operation on port may conflict with the QoS operation because the flow control operation will pause the packets sending from the connected device to prevent packet lost when the port is busy. But this operation will break the QoS request from the application running on that device.
The switch also treats the packets from flow-control-enable port as lowest priority during transmission scheduling so that those packets are not exposed to the WRED dropping operation. What this means is that if flow control is enabled for a given source port, then we can guarantee that no packet originating from that port will be lost, but at the possible expense of minimum bandwidth or maximum delay assurances.
This option provides a function of permitting normal QoS scheduling for frames originating from flow control enabled port. But it is possible that some packets may be dropped because of QoS operation, even though its flow control is on.

3.2.3.9 File Transfer

You can upload/download the software and system configuration running in the switch here. If you select [File Transfer] from the [Advanced Management] screen, the Software Upgrade screen appears.



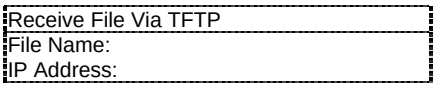
You can do the files transfer with *TFTP* (through network connection) or *Kermit* (through console connection) protocols. Highlight the item and press Enter to start file transfer.

Note: The software in the switch is module design and you can download or upload them by some of the module files instead of the whole software.
There are five module files could be transferred to or from the switch.

1. Software configuration file : This file contains the software configuration (VLAN, IP, Spanning Tree, …) settings of the switch.
2. Hardware configuration file : This file contains the hardware configuration of the switch. If wrong hardware configuration is used, that may cause the switch fail to work.
3. Debug monitor file : This is for engineer debugging. Please ignore it.
4. Runtime file : This is the main code of the switch. It controls the software version of the switch.
5. Web browser file : This file contains the http interface html code.

1. Receive File Via TFTP

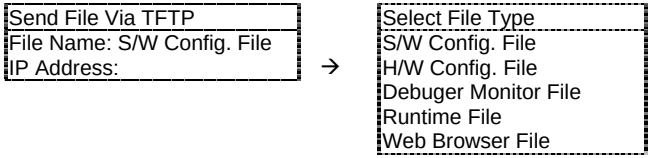
Before doing this operation, you have to put the file to the TFTP server and check the connection between the switch and the TFTP server by ping operation first. Highlight [Receive File Via TFTP] and press Enter. The following screen will appear.



a). Highlight the "File Name" option and press Enter. Enter the file name and press Enter.
b). Highlight the "IP Address" option and press Enter. Enter the IP address of the TFTP server and press Enter.
c). Press Esc and confirm the file transfer (Yes or No).

2. Send File Via TFTP

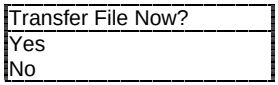
Before doing this operation, you have to check the connection between the switch and the TFTP server by ping operation first.
Highlight [Send File Via TFTP] and press Enter. Then select the file name and set the IP address of the TFTP server. Press Esc to confirm the file transfer (Yes or No). This operation can get the file from switch to TFTP server.



3. Receive File Via Kermit

Before doing this operation, you have to start the terminal program and complete the console connection first.

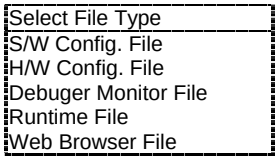
1. Highlight [Receive File Via Kermit] and press Enter. Then select Yes or No to confirm the file transfer via Kermit.
2. Start the file transfer (send) operation in the terminal program with Kermit protocol.



4. Send File Via Kermit

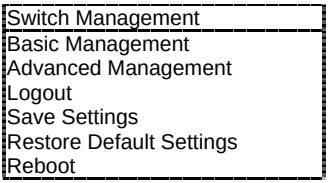
Before doing this operation, you have to start the terminal program and complete the console connection first.

1. Highlight [Send File Via Kermit] and press Enter. The following screen will appear.
2. Select the file you want to transfer and press Enter. Then select Yes or No to confirm the file transfer via Kermit.
3. Start the file transfer (receive) operation in the terminal program with Kermit protocol.



3.2.4 Other Functions in the Main Menu

Here is the content of the Main Menu.



- **Logout :**

You can logout from the switch with this function.

- **Save Setting**

You can save the settings to flash chip with this function.
All the settings in the configuring process will take effect immediately. But they will be lost after power off. If you want to save them, please come to this function and save them to flash.

- **Restore Default Settings**

If you want to go back to the default settings of the switch, you may use this function to do it. It will clear current settings and restore them to the default factory settings. After restoring default settings, the switch will reboot.

- **Reboot**

You can reboot the switch with this function.

3.3 Configure the Switch by Web Browser

This switch offers web browser interface for its configuration/administration. You have to assign an IP address to the switch with console interface first. (See the **Section 3.2.3.2** IP Networking).

3.3.1 Logging on to the Switch

Follow the procedures below for the configuration/management of the switch on web browser.

1. Start a web browser (MS IE 4.0 / Netscape 4.7 or higher /w 800x600 recommendable).
2. Input http://xxx.xxx.xxx.xxx/ as URL (xxx.xxx.xxx.xxx is the IP address of the switch).

A login screen will be prompted for user name/password. (Users may try to ping to the switch first to confirm their network connection.)

If the correct user name/password (default is **admin/123456**) is entered, the following home page will be prompted. The general system is shown in this page.

3.3.2 Performing Basic Management Activities

Click “Basic Setup” item in the homepage. The function list including [General], [LAN Ports], [Console Port] will be shown.

Users can select one of them and start the selected function. These functions are the same as you do in console. You may check the description in **Section 3.2.2** about them.

Basic Setup → General
LAN Ports
Console Port

3.3.3 Performing Advanced Management Activities

Click "Advanced Setup" item in the homepage. The function list including [Mac Address Management], [IP Networking], [Per Port Statistics], . . . will be shown.
Users can select one of them and start the selected function. These functions are the same as you do in console. You may check the description in **Section 3.2.3** about them.

Advanced Setup → Mac Address Management
IP Networking
Per Port Statistics
. . .
. . .
SNMP
Other Protocols
QoS

3.3.4 File Transfer, Reboot, Logout and Save Setting

Click "File" item in the homepage. The function list including [Save Setting], [Receive File Via TFTP], [Reboot], [Logout] will be shown.
Users can select one of them and start the selected function. These functions are the same as you do in console. You may check the description in **Section 3.2.4** about them.

File → Save Setting
Receive File Via TFTP
Send file Via TFTP
Reboot
Logout

Chapter 4 SNMP and RMON Management

4.1 Overview

RMON is an abbreviation for the **Remote Monitoring MIB** (Management Information Base). RMON is a system defined by the Internet Engineering Task Force (IETF) document RFC 1757, which defines how networks can be monitored remotely.

RMONs typically consist of two components: an RMON probe and a management workstation:
- The RMON probe is an intelligent device or software agent that continually collects statistics about a LAN segment or VLAN. The RMON probe transfers the collected data to a management workstation on request or when a predefined threshold is reached.
- The management workstation collects the statistics that the RMON probe gathers. The workstation can reside on the same network as the probe, or it can have an in-band or out-of-band connection to the probe.

This switch provides RMON capabilities that allow network administrators to set parameters and view statistical counters defined in MIB-II, Bridge MIB, and RMON MIB. RMON activities are performed at a Network Management Station running an SNMP network management application with graphical user interface.

4.2 SNMP Agent and MIB-2 (RFC1213)

The SNMP Agent running on the switch manager CPU is responsible for:

- Retrieving MIB counters from various layers of software modules according to the SNMP GET / GET NEXT frame messages.
- Setting MIB variables according to the SNMP SET frame message.
- Generating an SNMP TRAP frame message to the Network Management Station if the threshold of a certain MIB counter is reached or if other trap conditions (such as the following) are met:
  - Warm start
  - Cold start
  - Link up
  - Link down
  - Authentication failure
  - Rising alarm
  - Falling alarm
  - Topology change

MIB-2 defines a set of manageable objects in various layers of the TCP/IP protocol suites. MIB-2 covers all manageable objects from layer 1 to layer 4 and, as a result, is the major SNMP MIB supported by all vendors in the networking industry. The Intelligent Switch supports a complete implementation of SNMP Agent and MIB-2.

4.3 RMON MIB (RFC 1757) and Bridge MIB (RFC 1493)

The Intelligent Switch provides hardware-based RMON counters in the switch chipset. The switch manager CPU polls these counters periodically to collect the statistics in a format that complies with the RMON MIB definition.

4.3.1 RMON Group Supported

The Intelligent Switch supports the following RMON MIB groups defined in RFC1757:

- RMON Statistics Group - maintains utilization and error statistics for the switch port being monitored.

- RMON History Group - gathers and stores periodic statistical samples from the previous Statistics Group.

- RMON Alarm Group - allows a network administrator to define alarm thresholds for any MIB variable. An alarm can be associated with Low Threshold, High Threshold, or both. A trigger can trigger an alarm when the value of a specific MIB variable exceeds a threshold, falls below a threshold, or exceeds or falls below a threshold.

- RMON Event Group - allows a network administrator to define actions based on alarms. SNMP Traps are generated when RMON Alarms are triggered. The action taken in the Network Management Station depends on the specific network management application.

4.3.2 Bridge Group Supported

The Intelligent Switch supports the following four groups of Bridge MIB (RFC1493):

- The dot1dBase Group - a mandatory group that contains the objects applicable to all types of bridges.

- The dot1dStp Group - contains the objects that denote the bridge's state with respect to the Spanning Tree Protocol. If a node does not implement the Spanning Tree Protocol, this group will not be implemented. This group is applicable to any transparent only, source route, or SRT bridge that implements the Spanning Tree Protocol.

- The dot1dTp Group - contains objects that describe the entity's transparent bridging status. This group is applicable to transparent operation only and SRT bridges.

- The dot1dStatic Group - contains objects that describe the entity's destination-address filtering status. This group is applicable to any type of bridge which performs destination-address filtering.

Chapter 5 Configure the Network Connection

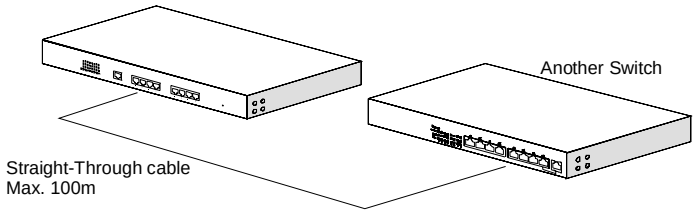
5.1 Connecting Devices to the switch

[Connection Guidelines:]

Connection Type	Max. Distance	Cable
10BaseT	100 meters	Category 3 or 5 UTP cable
100BaseTX	100 meters	Category 5 UTP cable
1000BaseTX	100 meters	Category 5, 5e, 6 UTP cable
1000BaseSX	550 meters	Multi-mode optical fiber
1000BaseLX	8 ~ 10 KM	Single mode optical fiber

5.2 Connecting to Another Ethernet Switch/Hub (Non-Trunking)

This switch can be connected to existing 10Mbps/100Mbps/1000Mbps hubs/ switches. The TX ports of the switch support Auto-MDIX function, you can use straight-through cables for this connection.



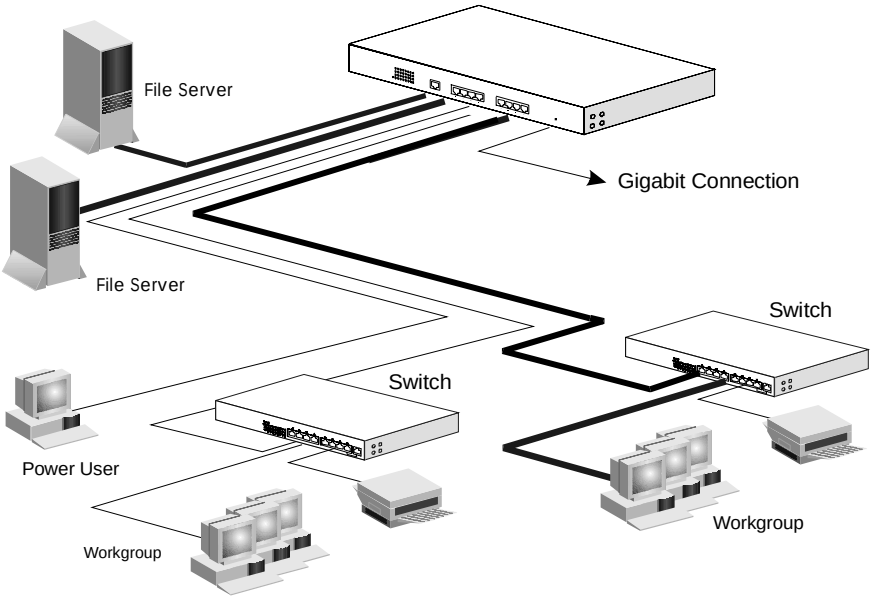
5.3 Application

An Ethernet switch can be used to overcome the hub to hub connectivity limitations as well as improve overall network performance. Switch makes intelligent decisions about where to send network traffic based on the destination address of the packet. As a result, the switch can significantly reduce unnecessary traffic.

The example below demonstrates the switch ability to segment the network. The number of nodes on each segment is reduced thereby minimizing network contention (collisions) and boosting the available bandwidth per port.

User can setup VLAN of the Intelligent Switch for network management. The gigabit throughput provides wide bandwidth between network connections. The

administrator can manage the network connection by Telnet / Console / Web-Browser / NMS to the Intelligent Switch to monitor the network



Chapter 6 LEDs Conditions Defined

LEDs of the switch provide useful information about the switch and the status of all individual ports.

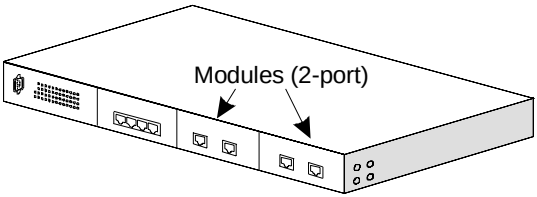
LED	STATUS	CONDITION
Power	ON	The Intelligent Switch is receiving power.
10	ON	Port has established a valid 10Mbps link.
	Flashing	Data packets being received or sent.
100	ON	Port has established a valid 100Mbps link.
	Flashing	Data packets being received or sent.
1000	ON	Port has established a valid 1000Mbps link.
	Flashing	Data packets being received or sent.
Full	ON	The connection is Full Duplex.
	OFF	The connection is Half Duplex.

Chapter 7 Add/Remove Module

7.1 For modularized model

This model supports two 2-port modules at front panel for Gigabit TX/SX/LX expansion.

Because this switch does not support hot-swap function, please turn off the switch before adding or removing module to/from the switch.



[Add Modules to the Switch at Front Panel]

1. Power OFF the switch first.
2. If the switch is rack-mounted, you have to remove the switch from rack first.
3. Loosen the screws of the cover on the module slot with screwdriver. Two at the front side, one at bottom side.
4. Remove the cover of the module slot.
5. Follow the rails on both sides of the module slot to slide in the module slowly.
6. Push the module firmly to make the module connecting well with the connector in the switch.
7. Drive the screws to fix the module to the switch firmly with screwdriver. Two at the front side, one at bottom side.
8. If the switch is rack-mounted, you can put the switch back to rack.
9. Power ON the switch.
10. Connect network cables to the connectors on the module. If the connected devices are working, the LED will be ON.

Note: We suggest you to keep these removed module slot covers. It can be use when these modules are removed in the future.

[Remove Modules from the Switch at Front Panel]

1. Power OFF the switch first.
2. If the switch is rack-mounted, you have to remove the switch from rack first.
3. Loosen the screws of the module with screwdriver. Two at the front side, one at bottom side.
4. Remove the module slowly from the module slot.
5. Put on the module cover and fix it to the switch by driving its screws with screwdriver. Two at the front side, one at bottom side.
6. If the switch is rack-mounted, you can put the switch back to rack.
7. Power ON the switch.

Chapter 8 FAQ

[Q1] How shall I configure the switch to allow the users on the switch to share an Internet connection, while preventing packet exchange between users?

[A] In this case, you can configure VLAN on the switch in "Concentration Mode". Supposing that users are connected on Port 1 ~ 7 and the Internet connection (or uplink) is on Port 8 (All the ports are untagged).

1. Create the following VLANs.

VLAN ID	VLAN name	VLAN port
2	V2	Port 1, 8
3	V3	Port 2, 8
4	V4	Port 3, 8
5	V5	Port 4, 8
6	V6	Port 5, 8
7	V7	Port 6, 8
8	V8	Port 7, 8
9	V9	Port 1, 2, 3, 4, 5, 6, 7, 8

2. PVID setting of each port.

Port 1	PVID=2	Port 2	PVID=3	Port 3	PVID=4
Port 4	PVID=5	Port 5	PVID=6	Port 6	PVID=7
Port 7	PVID=8	**Port 8**	**PVID=9**		

[Q2] How can I limit the number of users at each connection port?

[A] In order to limit the number of users, use the following procedure.

1. [Advanced Management] -> [L2 Switching DataBase] -> [Port Perspective] -> [Per Port Mac Limit] -> Select Port -> [Set Learning Limit] -> Set the number of users to limit the MAC learning.
2. Press the Esc key to return to the main menu.
3. The changed setting is applied immediately. In order to save the setting, press the ESC key to return to the main menu, and select [Save Setting].

[Q3] How can I limit the port for specific users to access the network?

[A] Use the following procedure.

1. [Advanced Management] -> [L2 Switching DataBase] -> [Port Perspective] -> [Per Port Mac Limit] -> Select Port -> Select [No Mac Learning] to disable Mac learning on the port.
2. Press the Esc key to return to the main menu.
3. [Advanced Management] -> [Static Filtering] -> [Mac Address In-Filter] -> Select -> Add the MAC address of the user to the list.
4. The changed setting is applied immediately. In order to save the setting, press the ESC key to return to the main menu, and select [Save Setting].

[Q4] Up/down arrow keys do not work for Telnet connection and console.
[A] It is because the terminal programs cannot transmit the correct codes for the two keys. In this case, you may use “J” and “K” for Up and Down key respectively.

[Q5] What is the difference between the tagged port and the untagged port in VLAN setting? What is PVID?
[A] Tag is a 4-byte data added to the packet. It includes the priority and VLADN ID for the packet. If a packet has a tag, it transfers information between the switches, so that the packet can be processed in other network device in accordance with the information. It is like GVRP operating between the network devices.
If a port in VLAN is set as the untagged port, all the packets transferred from the port do not have tags. If such packet arrives at the switch but with a tag, the tag is removed when the packet is transmitted from the port. Because most network devices do not support tag in the packet, they do not recognize the tagged packet. In this case, you should set the connection port to untagged.
If a port in VLAN is set as the tagged port, all the packets transferred from the port have the tags (tagged). If the packet arrives at the switch but without a tag, a tag is added when the packet is transmitted from the port. In this case, the PVID set in the ingress port is used, and VLAN ID is at the tag.
PVID (Port VLAN ID) is the VLAN ID setting at the untagged port. If a untagged packet arrives at a port, the switch checks if the VLAN ID and the PVID are identical, and determines whether to transmit or discard the packet.

[Q6] When network connection is added or changed at a switch, network connection is not performed conducted immediately.
[A] Check the spanning tree configuration first. If the spanning tree is enabled, the system checks the network configuration to prevent loop on the network. Therefore it takes about 30 seconds before a new connection is made. It is normal in the spanning tree operation.

[Q7] What is flooding?
[A] Flooding occurs when a packet arrives at the switch, and the switch fails to find DA (Rx MAC address) of the packets in the MAC learning table. In this case, the switch transfers the packet to all the ports to find the terminating network equipment. This action is called “flooding”.

[Q8] Will the switch support QoS?
[A] The switch provides QoS for various multimedia and important applications through limitation of delay, strict priority, WFQ transmit schedule and WRED discard. Each port supports 8 priority orders and discard sequence in 2 stages. Each packet has transmission priority order and discard order based on the physical port, the VLAN priority field of VLAN tagged frame, the DS/TOS field, and the UDP/TCP logical port field of IP packet.

If the traffic pattern is not known, if no policy or shaping is applied for the traffic, and if the network administrator knows the applications including voice/file transmission and web browsing and relative importance between the applications, the administrator can configure the switch to meet the QoS requirements of the applications.

[Q9] Why the tagged port send out untagged packets ?
[A] For a tagged port, please keep its PVID as default VLAN ID 1. It is not necessary to set the PVID for a tagged port. If you set the PVID of a tagged port to its VLAN ID, it will confuse the switch and cause the switch send out untagged packets from the tagged port. If the port is belonged to default VLAN, it will always send out untagged packets because default VLAN support untagged only.

[Q10] Why the connection is not stable when half duplex (e.g. 10M Hub) ?
[A] That is a compatibility problem. You may try to disable the flow control function of the port that connected with the half duplex devices.

[Q11] How to plan the QoS function of the switch ?
[A] Here is an example for your reference.

Class	Assured Bandwidth	Low drop subclass	High drop subclass
Highest transmission priority, P7	300Mbps	Control Information	
Highest transmission priority, P6	200Mbps	Phone Call, Circuit Emulation	Training Video Other Multimedia
Middle transmission priority, P5	125Mbps	Interactive Activity	Non-critical interactive activity
Middle transmission priority, P4	240Mbps	Web Business	
Low transmission priority, P3	80Mbps	File Backups	
Low transmission priority, P2	45Mbps	Email	Web Research
Best effort, P1-P0	10Mbps	Casual Web Browsing	
Total	1000Mbps		

The real QoS planning depends on the network applications of your environment.

A. Product Features/Specification

A.1 Features

- Prevents packet loss with back pressure and IEEE802.3x flow control
- Web-based management provides the ability to completely manage the switch from any web browser
- SNMP/Telnet interface deliver complete in-band management
- Supports IEEE 802.1D Spanning Tree Protocol
- Supports RMON agent
- Port-base/IEEE 802.1Q VLAN, with GVRP function
- Supports IP Multicasting through IGMP Snooping
- Provides 8-level transmit priorities, 2-level drop precedence on each port and different transmit scheduling schemes for QoS request. The QoS operation can refer to Tag-Base, DS/ToS or IP logical port settings of packets.
- Support flooding control
- Support static and dynamic MAC address limit function

A.2 Specification

[Basic Characteristics]

Access Method	CSMA/CD Ethernet operation
Communication Mode	Full / Half duplex
Ports	Support up to 8G ports
Console Port	RS-232 connection, with factory default [Baud Rate : 115200, Data Bits : 8, Parity Bits : None, Stop Bit : 1, Flow Control : None.]
Dimension	Non-Modularized Model: 440x172x44 (mm) Modularized Model: 440 x 254 x 44 (mm)
MDI / MDIX Select	Auto Detect
Input Power	100~240VAC, 50/60 Hz
Filter & Forwarding Rate	Full line speed
Transmission method	Store-and-forward
Flow Control	Back pressure for half duplex, IEEE802.3x for full duplex
LED Display	Per Port : 1000, 100, 10, Full Per Device : Power
Operation Temperature	Standard Operating: 0 to 50℃
Humidity	5% to 95% (Non-condensing)

[Management Support]

System Configuration	Out-band : console interface In-band : Telnet / Web Browser / SNMP interface
Management Agent	SNMP support: MIB II , Bridge MIB , RMON MIB
Spanning Tree Algorithm	IEEE 802.1D

VLAN Function	Port-Base/802.1Q-Tagged, with GVRP function
IGMP	IP Multicast Filtering by passively snooping on the IGMP Query
Quality of Service (QoS)	Provides 8-level transmit priorities, 2-level drop precedence on each port Supports Strict Priority, Delay Bound, Weighted Fair Queue and Best Effort – 4 different transmit scheduling schemes Refer to Tag-Base, DS/ToS or IP logical port settings of packets.
Port Security	Limit number of MAC addresses learned per port Static MAC addresses stay in the filtering table Static and dynamic MAC address limit
Internetworking Protocols	Bridging : 802.1D Spanning Tree 802.1P/Q - GARP/GVRP Internal Routing : RIP / RIP-2 / DHCP-Relay IP Multicast : IGMP Snooping IP Multicast Packet Filtering
Network Management	One RS232 port as local control console Telnet remote control console SNMP agent : MIB-2 (RFC 1213) Bridge MIB (RFC1493) RMON MIB (RFC1757) - statistics, history, alarms and events Private MIB Web browser support based on HTTP server and CGI parser
Software Update	TFTP/Kermit software-upgrade capability

B. Compliances

EMI Certification

FCC Class A Certification (USA)

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

CE Mark Declaration of Conformance for EMI and Safety (EEC)

This is to certify that this product complies with ISO/IEC Guide 22 and EN45014.
It conforms to the following specifications:

EMC:	EN55022(1988)/CISPR-22(1985)	class A
	EN60555-2(1995)	class A
	EN60555-3	
	IEC1000-4-2(1995)	4kV CD, 8kV AD
	IEC1000-4-3(1995)	3V/m
	IEC1000-4-4(1995)	1kV - (power line), 0.5kV - (signal line)

This product complies with the requirements of the Low Voltage Directive 73/23/EEC and the EMC Directive 89/336/EEC.

Warning! Do not plug a phone jack connector in the RJ-45 port. This may damage this device.

C. Warranty

We warrant to the original owner that the product delivered in this package will be free from defects in material and workmanship for a period of warranty time from the date of purchase from us or the authorized reseller. The warranty does not cover the product if it is damaged in the process of being installed. We recommend that you have the company from whom you purchased this product.