

KS-2300/KS-2600
Intelligent Switch
User's Guide

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.

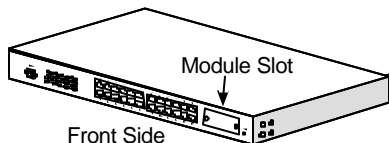
Trademarks or brand names mentioned herein are trademarks or registered trademarks of their respective companies.

About this manual . . .

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

These models are

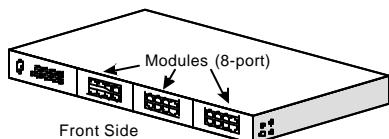
1. Non-fully-modularized model (24-only or 24+2G models)



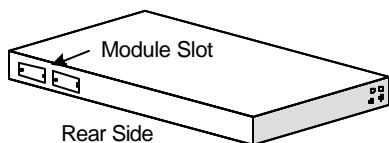
It has 24 10/100Mbps RJ45 MDIX ports and one module slot on front panel for 100BaseFX extension. Because the 100BaseFX extension ports will share Port 23/24 of TX ports, it is 24 ports totally on front panel.

2. Fully- modularized model

It has three 8-port module slots at front panel. These 8-port modules could be 8* 10/100M TX ports or 8* 100M FX ports or some other 8-port module. It has flexible design for hardware configuration.



If 24+2G, there are two gigabit module slots at rear panel for gigabit extension for both models.



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	4
3.1 INTRODUCTION.....	4
[1] Overview.....	4
[2] Manage the switch	4
3.2 CONFIGURE THE SWITCH BY CONSOLE.....	7
3.2.1 Logging on to the Intelligent Switch.....	7
3.2.2 Performing Basic Management Activities.....	10
General :.....	10
LAN Port :.....	11
Console Port :.....	12
3.2.3 Performing Advanced Management Activities.....	14
L2 Switching DataBase	16
VLAN & PVID Perspective :.....	16
IP Multicast Group Perspective :.....	19
MAC Address Perspective :.....	20
Port Perspective :	20
IP Networking	24
IP & RIP Setting :.....	24
ARP Table :.....	25
Routing Table :.....	26
DHCP Gateway Setting :.....	28
Ping :.....	30
Bridging	31

Static Filtering	32
Spanning Tree	33
Spanning Tree Configurations.....	33
Spanning Tree Port States	34
Spanning Tree Path Cost.....	34
Spanning Tree Port Priorities	35
SNMP	37
Other Protocols	38
Port Trunking	40
Port Mirroring	41
QoS Setup	42
Global Setting	43
Logical Port	45
VLAN.....	46
ToS.....	46
Profile	46
Port Configuration	49
Rate Control.....	50
File Transfer	51
3.2.3 <i>Other Functions in the Main Menu</i>	53
Logout :	53
Save Setting	53
Restore Default Settings	53
Reboot	53
3.3 CONFIGURE THE INTELLIGENT SWITCH BY WEB BROWSER ..	54
3.3.1 <i>Logging on to the Intelligent Switch</i>	54
3.3.2 <i>Performing Basic Management Activities</i>	54
3.3.3 <i>Performing Advanced Management Activities</i>	55
3.3.4 <i>File Transfer, Reboot, Logout and Save Setting</i>	55
CHAPTER 4 SNMP AND RMON MANAGEMENT	57
4.1 OVERVIEW	57
4.2 SNMP AGENT AND MIB-2 (RFC1213)	57

4.3 RMON MIB (RFC 1757) AND BRIDGE MIB (RFC 1493)	58
4.3.1 RMON Group Supported.....	58
4.3.2 Bridge Group Supported.....	59
CHAPTER 5 CONFIGURE THE NETWORK CONNECTION.....	60
5.1 CONNECTING DEVICES TO INTELLIGENT SWITCH	60
5.2 TRUNKING TO ANOTHER ETHERNET SWITCH	60
5.3 CONNECTING TO ANOTHER ETHERNET SWITCH/HUB (NON- TRUNKING).....	61
5.4 APPLICATION	62
CHAPTER 6 LEDS CONDITIONS DEFINED	64
CHAPTER 7 ADD/REMOVE MODULE.....	65
7.1 FOR NON-FULLY MODULARIZED MODELS	65
7.2 FOR FULLY MODULARIZED MODELS.....	68
CHAPTER 8 FAQ.....	71
A. PRODUCT FEATURES/SPECIFICATION.....	75
B. COMPLIANCES	78
C. WARRANTY.....	79

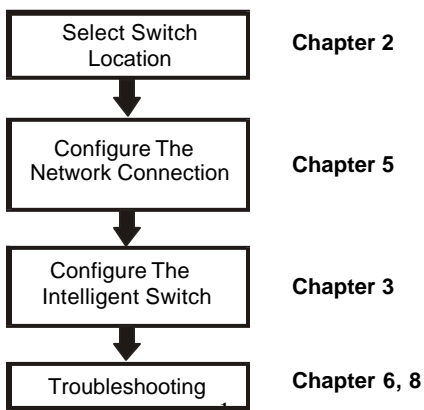
Chapter 1 Introduction

The Intelligent Switch is a high performance Ethernet/ Fast Ethernet NWay auto-negotiation switch with SNMP/RMON web-based management function. From a departmental backbone managing lower-level switches, hubs and workstations to high-speed switch-to-switch and switch-to-server links, this Intelligent 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 Switch
- One AC power cord
- Two rack-mount kits and screws
- This installation guide
- One console cable

1.2 Installation Procedure



Chapter 2 Where To Place the Switch

The Intelligent Switch can be placed 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:

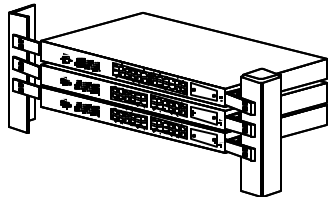
- The switch configuration does not break the rules as specified in Chapter 5.
- The switch is accessible and cables can be connected easily to it.
- The cables connected to the switch are away from sources of electrical interference such as radio, computer monitor, and light fixtures.
- There is sufficient 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 Section 3.
3. Connect network cables to the Intelligent Switch. Please refer to Section 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 cross-head 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 ARP.
- 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 Console Management via a network connection.
- 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.

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

3. Assigning an IP Address to the Intelligent Switch

To manage the Intelligent Switch remotely through the console port or with an SNMP Management Station, you must assign an IP address to the Intelligent Switch. You assign IP address through the IP Settings screen. This procedure is described in next section. Please refer to the "Advanced Management" function in the Local Console Management interface to set the IP address. We recommend you assign an IP address to the default VLAN (VLAN ID = 1) for Remote Console Management and SNMP Network Management.

4. 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. (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:

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.



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 :

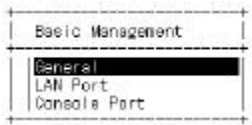
Basic Management	General	System Name, Software Version, Password, Http Enable/Disable, . . .	
	LAN Port	Port Physical Configuration, Mac ID	
	Console Port	Console Port Settings	
Advances Management	L2 Switching Database	VLAN & PVID Perspective	VLAN Settings / Status
		IP Multicast Group Perspective	IP Multicast Groups Operation Status
		Mac Address Perspective	Mac ID Activity in the switch
		Port Perspective	Port Status/Statistics, Mac Limit Setting
	IP Networking	IP Address, ARP Table, Routing Table, DHCP Gateway, Ping	
	Bridging	Aging Time, Flooding Limit	
	Static Filtering	Static Mac ID Filter-in, Filter-out	
	Spanning Tree	Spanning Tree Status / Configuration	
	SNMP	SNMP Configuration	
	Other Protocols	GVRP / IGMP Protocols Enable/Disable.	
	Port Trunking	Port Trunking Configuration	
	Port Mirroring	Port Mirroring Setting	
	QoS Setup	Configure the QoS operation of the switch. 1. Enable / Disable 2. Transmit priority / Drop priority mapping and configuration 3. Frame Scheduling configuration with profile setting. 4. Rate Control	
	File Transfer	Software / Firmware upload & download	
Logout	Logout the management interface.		
Save Settings	Save current settings.		

Restore Default Settings	Restore the factory default settings.
Reboot	Reboot the switch.

3.2.2 Performing Basic Management Activities

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

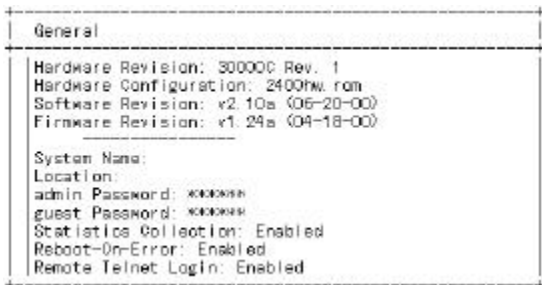
1. Select "**Basic Management**" and the function table will appear in the screen.
2. Select a function and press Enter.



Menu	Description
General	For system general information and settings.
LAN Port	<ol style="list-style-type: none">1. For LAN port configuration and connection status2. Get Mac address of the switch
Console Port	For console port configuration and settings

■ General :

Lets you 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. **Statistic Collection** : Enable or disable the statistic collection to the Intelligent Switch.
6. **Reboot-On-Error** : If it is enable in this option, the Intelligent Switch will automatically reset when a fatal error is detected.
7. **Telnet Login** : Enable or disable remote Telnet logins to the Switch.
8. **Remote HTTP Login** : Enable or disable remote HTTP login function.

■ **LAN Port :**

Lets you configure speed and flow control, link type, and physical address.

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



1. **Speed & Flow Control** : User can change the connection speed (10Mbps or 100Mbps), full duplex mode or half duplex mode, and the

Line Speed & Flow Control				
All Ports: Speed-Auto FC-On				
Part 1	(10/100M)	Speed-Auto	FC-On	<Down>
Part 2	(10/100M)	Speed-Auto	FC-On	<Down>
Part 3	(10/100M)	Speed-Auto	FC-On	<Down>
Part 4	(10/100M)	Speed-Auto	FC-On	<10M/HD >
Part 5	(10/100M)	Speed-Auto	FC-On	<Down>
Part 6	(10/100M)	Speed-Auto	FC-On	<Down>
Part 7	(10/100M)	Speed-Auto	FC-On	<Down>
Part 8	(10/100M)	Speed-Auto	FC-On	<Down>
Part 9	(10/100M)	Speed-Auto	FC-On	<Down>
Part 10	(10/100M)	Speed-Auto	FC-On	<Down>
Part 11	(10/100M)	Speed-Auto	FC-On	<Down>
Part 12	(10/100M)	Speed-Auto	FC-On	<Down>
Part 13	(10/100M)	Speed-Auto	FC-On	<Down>

flow control function on each connection port with this function.

! Notes: If there are **100BaseFX** ports on the switch, please always set the operation speed and operation mode of the FX ports to **100Mbps, Full Duplex** mode. The FX ports will fail to work if they are set to 10Mbps or half duplex or Auto.

2. **Physical Address** : This function can display the physical port

Physical Port Address		
Port 1	(10/100M)	0000F90D0001
Port 2	(10/100M)	0000F90D0001
Port 3	(10/100M)	0000F90D0001
Port 4	(10/100M)	0000F90D0001
Port 5	(10/100M)	0000F90D0001
Port 6	(10/100M)	0000F90D0001
Port 7	(10/100M)	0000F90D0001
Port 8	(10/100M)	0000F90D0001
Port 9	(10/100M)	0000F90D0001
Port 10	(10/100M)	0000F90D0001
Port 11	(10/100M)	0000F90D0001
Port 12	(10/100M)	0000F90D0001
Port 13	(10/100M)	0000F90D0001
Port 14	(10/100M)	0000F90D0001

address.

■ Console Port :

Lets you change the console baud rate, flow control method, modem control, and setup string; enable or disable SLIP; and configure the SLIP address and

Console Port Configurations	
Baud Rate:	115200
Flow Control:	Disabled
Modem Control:	Disabled
Modem Setup String:	AT&F E0 L1 &01 S0=1 &02
SLIP:	Disabled
SLIP Address:	
SLIP Subnet Mask:	

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.

5. **SLIP** : Enable or disable the SLIP function of the Intelligent Switch console port. If you enable SLIP, a message tells you that the console port becomes accessible only through the SLIP protocol after you logout from the current console screen. If you enable SLIP, please also specify a SLIP address and SLIP subnet mask.
6. **SLIP Address** : If you enabled SLIP, use this function to enter an address that has a network part different than the network address of the Intelligent Switch. (For more information, contact your network administrator.)
7. **SLIP Subnet Mask** : If you are using SLIP, enter a suitable SLIP subnet mask with this function.

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), port trunking, port mirroring, and software upgrade. To perform advanced management activities:

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



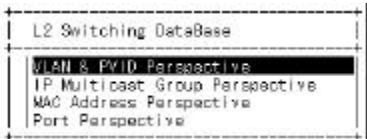
2. Select a function and press Enter.

Menu	Description
L2 Switching DataBase	<ol style="list-style-type: none">1. VLAN & PVID setting, VLAN activity status2. IP multicast group activity status3. Mac addresses activity status4. Statistics on port, VLAN activity on port and Mac address learning configuration on port
IP Networking	<ol style="list-style-type: none">1. IP address and RIP configuration of the switch2. ARP Table of the switch3. Routing Table of the switch4. DHCP Gateway setting5. Ping operation
Bridging	<ol style="list-style-type: none">1. Aging Time setting2. Flooding Control setting
Static Filtering	<ol style="list-style-type: none">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

<i>SNMP</i>	SNMP Configuration of the switch
<i>Other Protocols</i>	Enable/Disable IGMP and GVRP protocols
<i>Port Trunking</i>	Configure Port Trunking for Trunking Connection
<i>Port Mirroring</i>	Port Mirroring Configuration
<i>QoS Setup</i>	Configure the QoS operation of the switch
<i>File Transfer</i>	For Software upload/download operation

■ L2 Switching DataBase

Lets you 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.

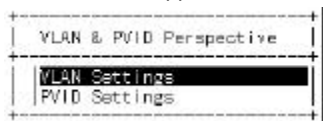


The Intelligent Switch can be viewed from the four perspectives in the L2 Switching DataBase screen. These four views allow a network administrator to manage and monitor VLANs and their associated MAC addresses and ports status effectively.

◆ 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

VLAN ID	Name
1	<0x001>
11	<0x009>

New VLAN Settings

VLAN ID: []
VLAN Name: []

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.)

- 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.

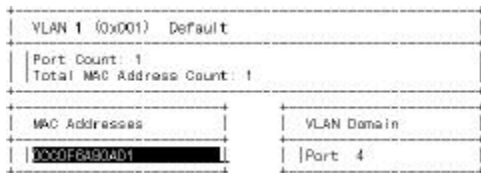
2. Delete a VLAN :

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 :

The following procedure describes how to use the VLAN Perspective screen to view activities for a particular VLAN. Using this procedure, you can view active ports, active MAC addresses associated with a VLAN, a transient address (if any), filtering and port information.

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



show all active MAC addresses and VLAN domains for the VLAN you selected. *MAC addresses* are those that have been sending frames from this VLAN to the switch within the last aging period. *VLAN domain* shows the domains in this VLAN from which active MAC addresses have been learned within the last aging period. You can use the **Tab** key to move between the MAC Addresses and VLAN Domain screens.

- b). In the *MAC addresses* Screen . . .

Searching for MAC Addresses :

In the VLAN MAC Address screen, press **S**. The "Enter MAC Addr To Search" screen 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 MAC Addresses screen.

Obtaining Additional Information :

To obtain additional information about an active MAC address, you can scroll to the address about which you want more information in the MAC Addresses screen. Press the Enter key. A VLAN/IP Multicast Group Membership screen will appear.

- c). In the *VLAN domain* Screen . . .

When the VLAN Domain screen is active, you can use the Up Arrow and Down Arrow keys to scroll through the list of domains associated with the selected VLAN.

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.



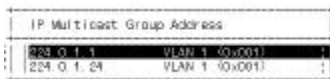
- b). To add ports to VLAN, use "+" (Shift key & + key) to add a switch port to the VLAN. Select Tagged or Untagged port first. Then select the port number. Repeat these steps to add switch ports to the VLAN.
- c). To delete ports from VLAN, highlight the port and press "-" (- key) to remove the port from the VLAN. Repeat these steps to remove switch ports from the VLAN.

After you complete the VLAN setting, you can go to the "**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 :

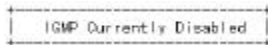
The IP multicast group perspective provides information associated with an IP multicast group. To obtain an IP multicast group perspective:

- a). Highlight "**IP Multicast Group Perspective**" and press the Enter key.



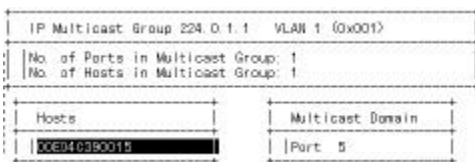
The following screen appears.

Notes: If the IGMP protocol is disabled, the following screen will appear. Please enable the IGMP protocol in "Other Protocols" function of the



"Advanced Management" first because the IP multicast groups are generated from the IGMP snooping operation of the switch.

- b). To obtain an IP multicast group perspective for one of the addresses in



the screen, highlight an address and press the Enter key.

- 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 . . .



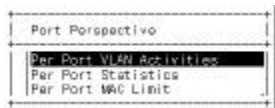
- a). Highlight **"MAC Address Perspective"** and press Enter key.

You are prompted for a MAC address. Enter the MAC address whose characteristics, corresponding VLANs, and corresponding ports you want to view. Then press Enter and a screen similar to the one appears.

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

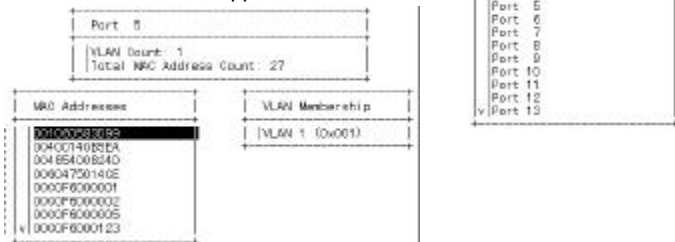
◆ **Port Perspective :**

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



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.



- a). 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.
- b). 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.
- c). 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.
- d). To obtain additional information about a particular MAC address, scroll to the address in the "Port MAC Address" screen and press Enter key. The following screen appears, showing detailed information about the

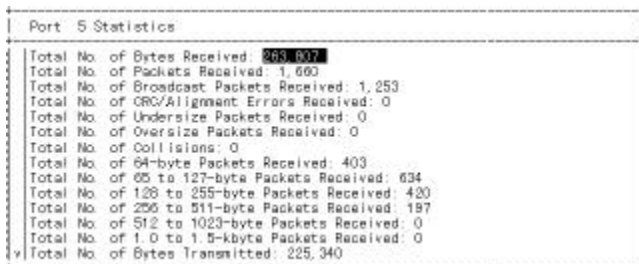


selected MAC address.

2). Per Port Statistics

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

- a). To reset counters for all ports, press R. Then select Yes in the



confirm screen to reset the counters. Or, select No to not reset them.

b). To view statistics for a port, highlight the desired port and press the Enter key. A screen similar to the one appears, showing the statistics for the port you selected.

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

3). Per Port MAC Limit

You can configure Mac address learning function of each port to

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

with this function for "Mac address limit" application on port. If you select this function, the screen will appear.

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

MAC Learning Options	
Set Learning Limit	
Unlimited Learning	
No MAC Learning	

Per Port MAC Limit	
Port 1 :	Unlimited
Port 2 :	Unlimited
Port 3 :	Unlimited
Port 4 :	Unlimited
Port 5 :	Unlimited
Port 6 :	Unlimited
Port 7 :	Unlimited
Port 8 :	Unlimited
Port 9 :	Unlimited
Port 10 :	Unlimited
Port 11 :	Unlimited
Port 12 :	Unlimited
Port 13 :	Unlimited

a). **Set Learning Limit** : 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.

■ IP Networking

Lets you 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 & RIP Setting :

If you select **IP & RIP Settings** from the "IP Networking" screen, 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)	210.63.246.50	255.255.255.0	Disabled	Disabled

Notes: Before you can define a VLAN's IP settings, you must first create a VLAN as described in the "**VLAN Perspective**" of "**L2 Switching DataBase**".

To modify the settings shown:

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



b). Review the settings. To change a setting, highlight it, press the Enter key, select the desired setting, and press Esc.
c). To delete a setting, highlight the setting and press the "-" key. Then select Yes in the confirm screen to delete it.

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 routing operation.
4. For normal case, assign the switch's IP address on the default VLAN for remote management is OK.
5. If you want 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.

Internet Address	Physical Address	VLAN ID	Type
210.63.246.25	0000EB503807	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

- From the ARP Table screen, press S. The Search Options screen prompts you to select an Internet Address or a Physical Address.
- 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
210 63 246 0	255 255 255 0	210 63 246 50	1	0x001	Direct	Local
210 63 246 0	255 255 255 255	210 63 246 255	1	0x001	Martian	Local
210 63 246 50	255 255 255 255	210 63 246 50	1	0x001	Myself	Local
210 63 246 255	255 255 255 255	210 63 246 255	1	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.
- b). If you select "Default Gateway", the following screen appears. Press

```

+-----+
| Default Route Specifications |
+-----+
| Default Gateway: [REDACTED] |
| Metric: 1 |
+-----+

```

Enter and type an IP address for the default gateway.

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

```

+-----+
| Static Route Specifications |
+-----+
| Network: [REDACTED] |
| Mask: [REDACTED] |
| Gateway: [REDACTED] |
| Metric: 1 |
+-----+

```

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
<0x00>	210.23.240.50	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.



- 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 which 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)



```
Ping
-----
Host: ██████████
Count: 1
Size (bytes): 64
Timeout (sec): 1
-----
```

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.

■ Bridging

Lets you view and change the aging period for a MAC address. If you select **Bridging** from the Advanced Management screen, the Bridging Parameters screen appears.



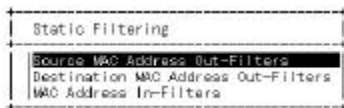
- a). To change the aging time, highlight **Aging Time (seconds)** and press Enter. A prompt will ask you to enter a bridge aging period, in seconds. Enter a new aging period and press the Enter key. Enter **0** for no aging.
- b). To change the flood limit for all ports, highlight **Flood Limit for All ports (packets/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.

Notes:

1. Aging : 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.
2. Flooding : 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.

■ Static Filtering

Lets you 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.

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.

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

You can highlight one of these items and press Enter. A MAC address table will appear.

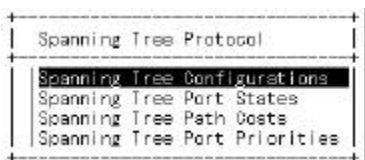
- a). Add a MAC address : Hold down the Shift key and press + to add a specific MAC address to be filtered.
- b). Delete a MAC address : Press "-" to delete a specific MAC address from being filtered. There is no precautionary message that appears before you delete a MAC address. Therefore, be sure you 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.

■ Spanning Tree

The Spanning Tree function can be used to prevent network loops, and to provide backup links with another network device. It can ensure that only one route exists between any two stations on 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.

```

Spanning Tree Protocol Configurations
-----
Bridge ID: 8000:0000F60D0001
Designated Root: 8000:0000F60D0001
Root Port:
Root Path Cost: 0
Current Max Age (sec): 20
Current Hello Time (sec): 2
Current Forward Delay (sec): 15
Hold Time (sec): 1
Topology Change Count: 1
Time Since Last Topology Change (sec): 7, 658

Spanning Tree Protocol: Enabled
Bridge Priority: 32,768
v Hello Time (sec): 2

```

```

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: Forwarding
Port 6: Disabled (Link Down)
Port 7: Disabled (Link Down)
Port 8: Disabled (Link Down)
Port 9: Disabled (Link Down)
Port 10: Disabled (Link Down)
Port 11: Disabled (Link Down)
Port 12: Disabled (Link Down)
v Port 13: Disabled (Link Down)

```

Note:

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.

◆ **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.

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

```
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
Port 9: 19
Port 10: 19
Port 11: 19
Port 12: 19
v
```

appears.

```
Spanning Tree Path 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
Port 9: 128
Port 10: 128
Port 11: 128
Port 12: 128
v
```

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**

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.

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.

■ SNMP

```
SNMP Configurations
SNMP: Disabled
Get Community Name: public
Set Community Name: public
Trap Community Name 1: public
Trap Community Name 2: public
Trap Community Name 3: public
Trap Community Name 4: public
Trap Host 1 IP Address:
Trap Host 2 IP Address:
Trap Host 3 IP Address:
Trap Host 4 IP Address:
Cold Start Trap: Enabled
Warm Start Trap: Enabled
Link Down Trap: Enabled
```

Let you view and change all SNMP-related information. If you select **SNMP** from the Advanced Management screen, the SNMP Configurations screen appears.

This switch supports 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.

■ Other Protocols

You can enable / disable *GVRP* and *IGMP* protocols here. 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 : 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*

Concentration – For *IGMP snooping* operation in concentration *VLAN* configuration (every port is *VLAN* grouped with some common port and not *VLAN* grouped with the other ports.)

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

Notes: *GVRP* Protocol

In addition to network management tools that allow network administrators to statically add and delete *VLAN* member ports, the Intelligent 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 Intelligent Switch register and propagate *VLAN* membership to all ports that are part of the active topology of the *VLAN*.

Notes: 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 Intelligent 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 Intelligent 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 subnetworks, an external IP multicast router is needed if IP multicast packets have to be routed across different subnetworks.

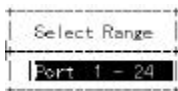
■ Port Trunking

This switch supports two/three trunking connections maximum – two trunking connections for 10/100M ports, one trunking connection for gigabit ports if your model has gigabit ports. It is port-based manually setting.

Here is the configuration screen. The switch treats these trunking connection ports as one connection. You can select one of the trunking and then select the ports for the trunking connection.

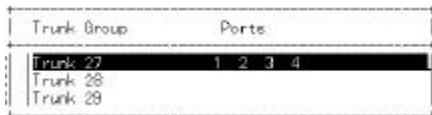
Here is an example for trunking configuration for 24+2G model.

1. Select one of the trunk connection and the following screen will appear.



Select Range
Port 1 - 24

2. Select the port range and select/remove the port to/from the trunk with Enter key. Four 10/100Mbps ports for a trunking connection maximum.
3. The following screen is an example after configuration.



Trunk Group	Ports
Trunk 27	1 2 3 4
Trunk 28	
Trunk 29	

If your switch is 24+2G model and you want to use the two gigabit ports for trunking connection, please select “Trunk 29”. Then select Port 25, 26 for this trunking connection. Its bandwidth is up to 4Gbps for the gigabit ports trunking.

■ Port Mirroring

Using **Port Mirroring** from the Advanced Management screen, you can mirror one port to another port for network traffic monitoring. From the Advanced Management screen, highlight **Port Mirroring** and press the Enter key. The screen appears.

Mirror Index	Mirror To	Mirror From	Mode
1			
2			

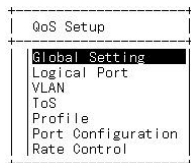
- Highlight one index and press Enter. The screen will appear.
- Highlight the "Mirror To" and press Enter. Select the port that will be mirrored to.
- Highlight the "Mirror From" and press Enter. Select the mirrored port from the port list and press Enter.
- Highlight the "Mirror Mode" and press Enter. Select the mirror mode (Receive / Transmit) and press Enter. (You can mirror the receive or transmit packets only but not both in the switch.)

Port Mirroring Options	
Mirror To:	
Mirror From:	
Mirror Mode:	

Notes: The mirror port number that you see in your console may be different from the screen shown in the manual. Please do it according to the port number shown on your screen.

■ 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.



This switch supports 4 priority queues on each 10/100Mbps ports and 8 priority queues on gigabit port if your model has it. This switch also support 2 classes of drop rates with WRED (Weighted Random Early Detection) logic that you can configure. You can configure the priority and drop rate for the priority values in VLAN tag and ToS of IP packet. You can also configure the priority and drop rate for TCP/UDP logical service ports. You can configure the packet scheduling operation on each priority queue and the traffic rate on each port with the QoS function of the switch.

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.

Profile Define the QoS operation profiles for packet transmit scheduling of each priority queue on ports



Port Configuration Assign the operation profile for each physical port

Rate Control Setup the traffic rate allowed on each port

◆ Global Setting

Set the general configuration for the QoS operation.

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 DiffServ classes to its priority classes and transfer DiffServ packets with the following queue mapping.

Tx Queues	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.

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

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.

Level 1 defines the drop percentage when the queue is 75% full.

Level 2 defines the drop percentage when the queue is 87.5% full.

Level 3 defines the drop percentage when the queue is 100% full. It is always 100% drop because the queue is already 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.

1. User-Defined Port : This switch allows 8 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.

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

2. Well-Known Port : In "Well-Known Port", you can do QoS configuration for some well-known TCP/IP ports. There are 8 well-known ports could be set in the switch. Select one of them. (For example, 0) you can do the following QoS settings on this TCP/IP logical port.

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

Well-Known Port	Service	Well-Known Port	Service
23	Telnet	111	SUN rpc
512	TCP/UDP	22555	IP phone call
6000	XWIN	22	SSH
443	HTTP	554	RTSP

Logical Port			
User-Defined Port			
Well-Known Port			
Range Port			

User-Defined Port 0			
Port Number: 00			
Drop Priority: Low			
Transmit Priority: 7			
Port Status: Enabled			

Well-Known Port 0			
Port Number: 23			
Drop Priority: Low			
Transmit Priority: 0			
Port Status: Enabled			

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

◆ VLAN

You can configure the QoS operation – drop priority and transmit priority for each priority value in VLAN tag.

Select one of them and you can configure the QoS configuration of this priority.

Range Logical Port	
Low Port Number:	2970
High Port Number:	7170
Drop Priority:	Low
Transmit Priority:	7

◆ ToS

You can configure the QoS operation – drop priority and transmit priority for each priority value in ToS.

VLAN Priority 0 Setting	
Drop Priority:	High
Transmit Priority:	0

Select one of them and you can configure the

VLAN Priority Index	
0	
1	
2	
3	
4	
5	
6	
7	

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..

ToS Priority 0 Setting	
Drop Priority:	High
Transmit Priority:	0

ToS Priority Index	
0	
1	
2	
3	
4	
5	
6	
7	

◆ Profile

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 adjust 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 (4 priority queues on 10/100M ports, 8 priority queues on gigabit port for 24+2G models).

10/100M Port	P3		P2		P1		P0	
Gigabit Port	P7	P6	P5	P4	P3	P2	P1	P0
Option 1	Delay Bound						Best Effort	
Option 2	Strict Priority		Delay Bound				Best Effort	
Option 3	Strict Priority		Weighted Fair Queuing					
Option 4	Weighted Fair Queuing							

There are 10 profiles in the configuration menu. The following is the mapping between the 10 profiles and the four scheduling configurations.

	Strict Priority	Delay Bound	WFQ Setting (default)	
Profile 1	Disable	Enable	50%, 25%, 25%, 0%	Option 1
Profile 2	Enable	Enable	50%, 25%, 25%, 0%	Option 2
Profile 3	Enable	Disable	50%, 25%, 12.5%, 12.5%	Option 3
Profile 4	Disable	Disable	50%, 25%, 12.5%, 12.5%	Option 4
Profile 5	Disable	Enable	75%, 12.5%, 12.5%, 0%	Option 1
Profile 6	Enable	Enable	75%, 12.5%, 12.5%, 0%	Option 2
Profile 7	Enable	Disable	75%, 12.5%, 6.25%, 6.25%	Option 3
Profile 8	Disable	Disable	75%, 12.5%, 6.25%, 6.25%	Option 4
Profile 9	Enable	Enable	25%, 50%, 25%, 0%	Option 2

Profile Setting
Megabit Profile
Gigabit Profile

Megabit Profile Attributes
Parts Using This Profile: 1, 2, 3, 4, 5, 6,
Strict Priority: Disabled
Delay Sensitive Application: Enabled
Profile Name: Default Name 01
Profile Status: Active Profile #1
Bandwidth Partitions...
QoS with Flow Control: Disabled

Megabit Profile
Default Name 01: A1
Default Name 02: A2
Default Name 03: A3
Default Name 04: A4
Default Name 05: NA
Default Name 06: NA
Default Name 07: NA
Default Name 08: NA
Default Name 09: NA
Default Name 10: NA

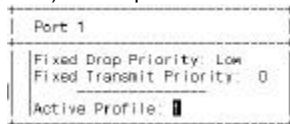
Profile 10	Enable	Disable	25%, 50%, 12.5%, 12.5%	Option 3
------------	--------	---------	------------------------	----------

You can configure the WFQ setting in each profile and select four of the ten profiles to be the active profiles for the scheduling operation on each port of the switch.

For the profile setting, you have to select Megabit Ports Profile or Gigabit Ports Profile first.

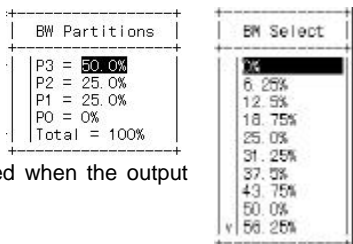
We select the Megabit Profile here. You can define the content of QoS profiles for megabit ports here. There are 10 different profiles and only four of them could be the active profiles for QoS control in the switch. Now, we open the 01 profile.

1. **Port Using This Profile** : Show the ports using this profile.
2. **Strict Priority** : Show the Strict Priority setting of this profile.
3. **Delay Sensitive Application** : Show the Delay Bound setting of the profile.
4. **Profile Name** : The name of this profile. You can modify it.
5. **Profile Status** : The status (active / non-active) of this profile. You can modify it. Because this switch support four active profiles only. If you enable this profile, that may cause some other active profile being disable by the switch.
6. **Bandwidth Partition** : In "Bandwidth Partitions" you can set the bandwidth allocation for the four transmit queues on ports for Weight Fair Queue operation.



7. **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. In this case, the packets from ports whose flow control function is enable will always be forwarded with the lowest priority during scheduling so that they will not exposed to the WRED dropping scheme to prevent any packet dropping in the QoS operation. It can guarantee that no packets will be lost, but at the possible expense of minimum bandwidth or maximum delay assurance.

If this function is enable, it will force the QoS function still works when the flow control is enabled. However, only the best effort traffics are not dropped. The high priority traffics are still transmitted first, but the packet may be dropped when the output port is highly congested.



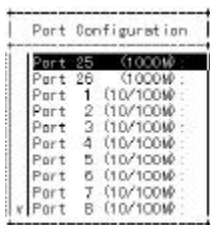
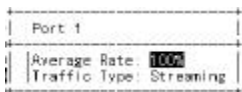
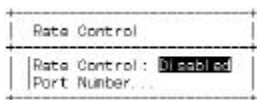
◆ Port Configuration

With this function, you can select the QoS operation profile for each physical port from the four active profiles. And you can see the fixed drop and transmit priority settings of the port here. If the QoS operation is set to port-based mode, these settings will be the QoS settings for the port.

◆ Rate Control

With this function, you can set the traffic rate control for each physical port. (You can set the rate control for 10/100M ports only.) This switch supports 10 levels rate control from line speed. You select one of the ten levels to limit the traffic rate allowed on ports. You can also select the traffic type for rate control is streaming or burst.

Note : If the "Delay Sensitive Application" option of any active profile is enable, you will meet a error message when you try to set the rate control. Please try to activate another profile with the "Delay Sensitive Application" option disable because the Delay Bound scheduling operation conflict with rate control operation of the switch. We suggest that you may use Profiles 3,4,7,8 as the active profiles for rate control operation because they are "Delay Sensitive Application" disable.



■ File Transfer

You can upload or download the software 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 file in the switch is module design and you can download or upload them by one 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



```
Receive File Via TFTP
File Name: SW-Config-File
IP Address:
```

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.

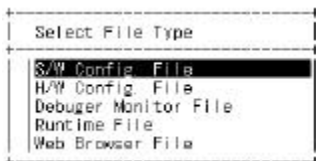
- a). Highlight the "File Name" option and press Enter. Enter the file name and press Enter.
- b). Highlight the "IP Address" option and press Enter. Enter the IP address of the TFTP server and press Enter.

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.

3.2.3 Other Functions in 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 State of the switch. After restoring default settings, the switch will reboot.

- **Reboot**

You can reboot the switch with this function.

3.3 Configure the Intelligent Switch by Web Browser

The Intelligent Switch provides a web-browser interface for configuration/management purposes. After the IP address of the Intelligent Switch has been assigned through the console interface, you can connect to the Intelligent Switch with web-browser for configuration or management. (Please refer to "**Assigning an IP Address to the Intelligent Switch**" in Section 3.1 for IP address assigning.)

3.3.1 Logging on to the Intelligent Switch

Follow the steps to start the web-browser configuration/management.

1. Start the Web-Browser first (MS IE 4.0 / Netscape 4.7 or above w/ 800x600 screen resolution is suggested,)
2. Enter "http://xxx.xxx.xxx.xxx/" as the web address. (xxx.xxx.xxx.xxx is the IP address of the Intelligent Switch) And the login screen will appear.



3. Input the password (the factory default is "123456" for "admin").
Note: You may change the password after you login to the Intelligent Switch.
4. If the password is accepted, the homepage of the Intelligent Switch will appear.

3.3.2 Performing Basic Management Activities

You can performance basic configuration/management with the "**Basic Setup**" button in the homepage. That is almost the same as the "Basic Management" function in console interface. Please refer to **Section 3.2.2** for the details of the basic management. (Here is a sample. Please refer to your Intelligent Switch. They are similar.)



3.3.3 Performing Advanced Management Activities

You can perform advanced configuration/management with the "Advanced Setup" button in the homepage. That is almost the same as the "Advanced Management" function in console interface. Please refer to **Section 3.2.2** for the details of the advanced management.



3.3.4 File Transfer, Reboot, Logout and Save Setting

You can do these functions in the "File" button. Please complete the operation step by step in the web-browser. That is almost the same as

these functions in console interface. Please refer to **Section 3.2.3** for the details of these functions.



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.

The Intelligent 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):

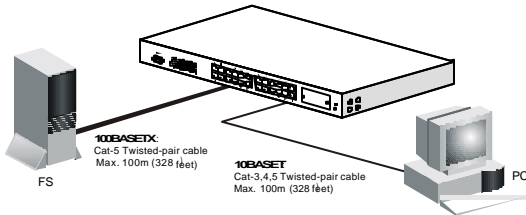
- The dot1dBase Group - a mandatory group that contains the objects applicable to all types of bridges.
- The dot1dStp Group - contains the objects that denote the bridge's state with respect to the Spanning Tree Protocol. If a node does not implement the Spanning Tree Protocol, this group will not be 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 Intelligent Switch

[Connection Guidelines:]

- Use Category 3 or 5 twisted-pair Ethernet cable when connecting 10BaseT devices to the Intelligent Switch and up to 100 meters.
- Use Category 5 twisted-pair Ethernet cable when connecting 100BaseTX devices to the Intelligent Switch and up to 100 meters.
- For 100BaseFX connection, it supports up to 2KM for multi-mode transceiver and up to 25~30KM for single-mode transceiver w/ single-mode cable.
- For 1000BaseSX connection, it supports up to 550 meters.
- For 1000BaseLX connection, it supports up to 8~10KM.
- For 1000BaseTX connection, it supports up to 100 meters with Cat 5 cable. (Cat.5e is suggested for 1000TX connection.)



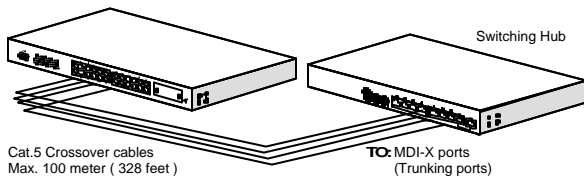
5.2 Trunking to Another Ethernet Switch

There could be two/three trunk connections on the Intelligent Switch.

1. Please setup the trunk configuration of the Intelligent Switch (refer to **Section 3**) from the Telnet/Console/Browser/SNMP management interface first.

2. Connect from the trunking ports of the Intelligent Switch to the trunking ports of another switch.

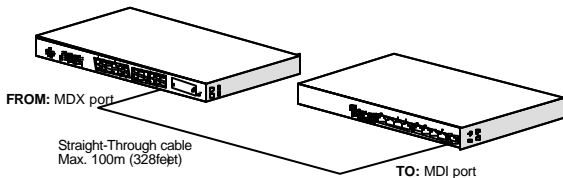
The following figure is an example of trunk connection from the Intelligent Switch. Because the UTP ports of the switch are MDIX ports, you may need to use "Crossover" Cable for trunking connection. (Notes: If the TX ports of your model support Auto-MDIX function, you can use straight-through cables for trunking connection. Please check the spec of your model.)



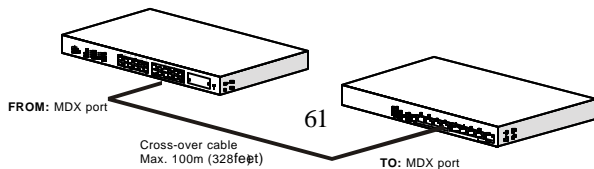
5.3 Connecting to Another Ethernet Switch/Hub (Non-Trunking)

The Intelligent Switch can be connected to existing 10 Mbps or 100 Mbps hubs/switches. The switch to switch/hub connection guidelines are shown as follow.

If connecting from MDIX port of the switch to MDI port of another hub/switch, Straight-Through cable is OK for this connection.



If connecting from MDIX port of the switch to MDIX port of another hub/switch, Crossover cable is needed for such a connection. (Notes: If the TX ports of your model support Auto-MDIX function, you can use straight-through cables for this connection. Please check the spec of your model.)



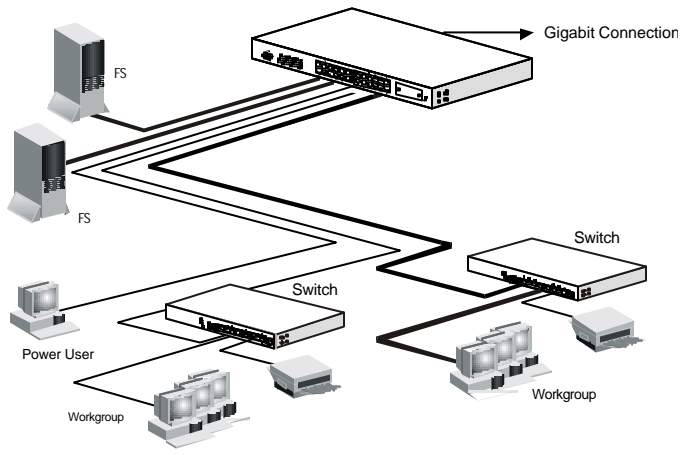
5.4 Application

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. User can also setup Trunk connection of the Intelligent Switch for faster trunk connection between switches. The administrator can manage the network connection by Telnet / Console / Web-Browser / NMS to the Intelligent Switch to monitor the network

The following figure is an application example of a 24+2G model Intelligent Switch.



Chapter 6 LEDs Conditions Defined

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

LED	STATUS	CONDITION
Power	ON	The Intelligent Switch is receiving power.
*Fault	ON	It will be ON when booting and go OFF when running. If it is steady ON when running, the switch is faulty. (*Some models do not have this LED.)
Link / Act	ON	Port has established a valid link.
	Flashing	Data packets being received or sent.
	Green	The connection is 100Mbps.
	Yellow	The connection is 10Mbps.
FDX /*Col.	ON	The connection is Full Duplex.
	Flashing	Packet collisions happen.

Note: For the Fully Modularized Model, the Link/Act LED is green color only. The speed display (Green:100M/Yellow:10M) is shown on the TX module.

! Important Note : *If there are 100BaseFX ports on the switch, please always set the operation speed and operation mode of the 100BaseFX ports to 100Mbps and full duplex mode. The 100BaseFX ports will fail to work if they are set to 10Mbps or half duplex or Auto.*

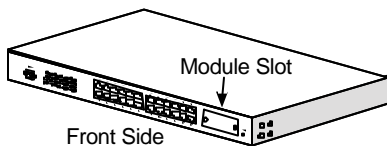
Chapter 7 Add/Remove Module

7.1 For non-fully modularized models

This model supports one 1/2-port 100BaseFX modules (at front panel) and two 1-port gigabit TX/SX/LX modules (at rear panel for 24+2G model).

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

-- Module at Front Side --



The adding 100BaseFX module at front side will disable Port 23/24 of UTP ports because they share the same port number. If one 100BaseFX port on the module, Port 24 of UTP port will be disabled and this 100BaseFX port become Port 24. If two 100BaseFX ports on the module, Port 23 and 24 of UTP ports will be disabled and these 100BaseFX ports become Port 23 and 24.

[Adding Modules to the Switch at Front Panel]

1. Turn off the switch first.
2. Loosen the screws of the cover of the module slot.
3. Remove the cover of the module slot.
4. Follow the rails on both sides of the module slot to slide in the module slowly.
5. Push the module firmly to make the module connecting well with the connector in the switch.
6. Drive the screws to fix the module to the switch firmly.
7. Power ON the switch.
8. If 100FX module are added, please configure these FX ports to *100/Full* in the following steps: [Basic Management] -> [LAN port] -> [Speed & Flow Control] -> Select the port -> Set it to 100/Full.

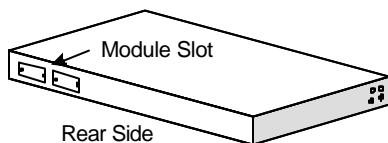
9. Connect network cables to the connectors on the module. If the connected devices are working, the Link/Act LED will be ON.

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. Turn off the switch first.
2. Loosen the screws of the module.
3. Remove the module slowly from the module slot.
4. Put on the module cover and fix it to the switch by driving its screws.
5. Power ON the switch.

-- Modules at Rear Side (for 24+2G model) --



[Adding Modules to the Switch at Rear Panel]

1. Turn off the switch first.
2. Loosen the screws of the cover on the module slot.
3. Remove the cover on the module slot.
4. Follow the rails on both sides of the module slot to slide in the module slowly.
5. Push the module firmly to make the module connecting well with the connector in the switch.
6. Drive the screws to fix the module to the switch firmly.
7. Power ON the switch.
8. Connect network cables to the connectors on the module. If the connected devices are working, the Link/Act 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. Turn off the switch first.
2. Loosen the screws of the module.
3. Remove the module slowly from the module slot.
4. Put on the module cover and fix it to the switch by driving its screws.

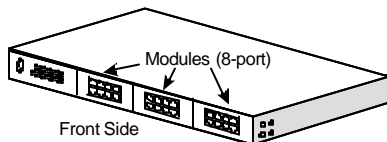
5. Power ON the switch.

7.2 For fully modularized models

This model supports three 8-port 10/100Mbps TX/FX modules (at front panel) and two 1-port gigabit TX/SX/LX modules (at rear panel for 24+2G model).

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

-- Modules at Front Side --



[Adding Modules to the Switch at Front Panel]

1. Turn 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. If 100FX module are added, please configure these FX ports to *100/Full* in the following steps: [Basic Management] -> [LAN port] -> [Speed & Flow Control] -> Select the port -> Set it to 100/Full.
11. Connect network cables to the connectors on the module. If the connected devices are working, the Link/Act LED will be ON.

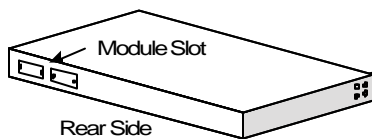
Note: We suggest you to keep these removed module slot covers. It can be use when these modules are removed in the future.

[Remove Modules from the Switch at Front Panel]

1. Turn 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.

-- Modules at Rear Side (for 24+2G model) --



[Adding Modules to the Switch at Rear Panel]

1. Turn off the switch first.
2. Loosen the screws of the cover on the module slot.
3. Remove the cover of the module slot.
4. Follow the rails on both sides of the module slot to slide in the module slowly.
5. Push the module firmly to make the module connecting well with the connector in the switch.
6. Drive the screws to fix the module to the switch firmly.
7. Power ON the switch.
8. Connect network cables to the connectors on the module. If the connected devices are working, the Link/Act 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. Turn off the switch first.
2. Loosen the screws of the module.
3. Remove the module slowly from the module slot.
4. Put on the module cover and fix it to the switch by driving its screws.
5. Power ON the switch.

Chapter 8 FAQ

[Q1] How to configure the switch to make the users connected on the switch cannot send/get packets to/from each other but all of them can share one Internet connection ?

[A] You can configure the VLAN on the switch to “Concentration Mode” for this application. Now we use the Intelligent Switch and the Internet connection is on Port 24 as an example. (All of the ports are untagged ports.)

1. Create the following VLANs first.

VLAN ID	VLAN Name	Ports in the VLAN
2	V2	Port 1, 24
3	V3	Port 2, 24
4	V4	Port 3, 24
.....		
23	V23	Port 22, 24
24	V24	Port 23, 24
25	V25	Port 1, 2, 3, 4, . . . , 22, 23, 24

2. Set the PVID of every port.

Port 1	PVID=2	Port 2	PVID=3	Port 3	PVID=4
Port 4	PVID=5	Port 5	PVID=2	Port 6	PVID=2
Port 7	PVID=8	Port 8	PVID=9	Port 9	PVID=10
.....					
Port 22	PVID=23	Port 23	PVID=24	Port 24	PVID=25

When a Port are forwarding packets, it will check its VLAN configuration (whose VLAN ID = its PVID). If the destination ports are in the same VLAN group, the packets will be forwarded. Otherwise, the packets will be dropped.

[Q2] How to limit the user number on each connection port ?

[A] Please follow the steps to do it.

1. [Advanced Management] -> [L2 Switching DataBase] -> [Port Perspective] -> [Per Port Mac Limit] -> Select the port -> [Set Learning Limit] -> Set the user number to limit the Mac learning number on the port.

2. Go back to the main menu with Esc.
3. The setting will take effect immediately. If you want to save it, go back to the main menu with Esc and select [Save Setting].

[Q3] How to limit only some user can access network on some port ?

[A] Please follow the steps to do it.

1. [Advanced Management] -> [L2 Switching DataBase] -> [Port Perspective] -> [Per Port Mac Limit] -> Select the port -> [No Mac Learning] to disable the Mac learning function on the port.
2. Go back to the main menu with Esc.
3. [Advanced Management] -> [Static Filtering] -> [Mac Address In-Filter] -> Select the port -> Add the Mac address of the user to the list
4. The setting will take effect immediately. If you want to save it, go back to the main menu with Esc and select [Save Setting].

[Q4] Why the Up-Arrow key and Down-Arrow key fail to work on console and Telnet connection ?

[A] Because your terminal program fails to send the correct code of these two keys, the Intelligent Switch cannot get the correct input from keyboard. You may use "J" key instead of Down-Arrow key and use "K" key instead of Up-Arrow key in that case.

[Q5] The 100Base FX port fail to work after I adding a 100BaseFX module to my switch (some model support module expansion).

[A] This problem could be caused by the configuration of the 100BaseFX port because FX port does not support auto-negotiation function. You have to configure the FX port to 100/Full manual. Please follow the steps to do it. [Basic Management] -> [LAN Port] -> [Speed & Flow Control] -> Select the port -> Select 100/F. Then save it. Because the port is configured to full duplex mode, its FDX LED will be ON even no cable is connected. That is correct display because that port is already forced to full duplex mode.

[Q6] What is the difference between tagged port and untagged port in VLAN setting ? What is PVID ?

[A] Tag is a four-byte data added in the packet. It contains priority information and VLAN ID of the packet. If a packet has tag inside, it can carry these information from this switch to another switch and can be handled according the information in tag between different network devices. That is how GVRP working between network devices.

If a port in VLAN is set to untagged port, all the packets sent out from the port will be no tag inside (untagged). If these packets are tagged when they come to the switch, the tag will be removed when they are transferred from this port. Because lots of living network devices does not support tag in packet (untagged device), they cannot recognize tagged packets. In that case, you have to set their connection port to untagged.

If a port in VLAN is set to tagged port, all the packets sent out from the port will be tag inside (tagged). If these packets are untagged when they come to the switch, a tag will be added when they are transferred from this port. In this case, it will use the PVID set on the ingress port as the VLAN ID in the added tag.

PVID (Port VLAN ID) is the VLAN ID setting on an untagged port. When untagged packets come to the port, the switch will check the VLAN setting whose VLAN ID is the same as PVID and decide to drop or forward the packets.

[Q7] Why my network connection cannot work immediately when I add or change my network connection on the switch ? It always delays 30 seconds and then start to work.

[A] You can check the spanning tree configuration first. If spanning tree is enable, it will take about 30 seconds before any new connection starting to work because it will check the network configuration to prevent any looping happening in the network first. That is a correct for spanning tree operation.

[Q8] What is flooding ?

[A] Flooding happens when packets come to the switch and the switch cannot find their DA (Destination Mac Address) in its Mac learning table. In this case, the switch will forward these packets to every port to find the destination network devices. This operation is called flooding.

[Q9] Why the traffic in the trunk connection is not shared to every port when only several connections works between the switches ?

[A] For a DA-SA pair, its traffic are assigned to be transferred through one cable of the trunk only but not every cable. If only several connections works on the trunk connection, only part of the cables in the trunk are working. Because the traffic is not heavy in that case, part of the cables in the trunk is enough for the loading. If more DA-SA pairs are working in the trunk, they will be assigned to different cables to share the loading in the trunk. If there are many DA-SA connections in the trunk and their value are quite random, the traffic will be shared on every cable of the trunk smoothly.

That can meet the request for a trunking connection. If any cable in the trunk is broken, the traffic in that cable will be transferred to another cables in the trunk and their traffic will not stop.

[Q10] How does this switch support QoS function ?

[A] With delay bounded, strict priority, and/or WFQ transmission scheduling, and WRED dropping schemes, the switch provides powerful QoS functions for various multimedia and mission-critical applications. Each port provides 4 transmission priorities (8 priorities per Gigabit port) and 2 levels of dropping precedence. Each packet is assigned a transmission priority and dropping precedence based on the physical port, VLAN priority field in a VLAN tagged frame, or the DS/TOS field, and UDP/TCP logical port fields in IP packets.

In general, the approach to quality of service assumes the offered traffic pattern is unknown, the incoming traffic is not policed or shaped, and the network manager knows his applications, such as voice, file transfer, or web browsing, and their relative importance. Then he can configures the switch to meet the QoS request of his applications.

[Q11] 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.

[Q12] 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.

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
- VLAN (IEEE 802.1Q) with GVRP supports up to 128 groups
- Supports IP Multicasting through IGMP Snooping
- Provides 4-level transmit priorities, 2-level drop precedence on each port and different transmit scheduling schemes for QoS request. The QoS operation can refer to Port-Based, Tag-Base, DS/ToS or IP logical port settings of packets.
- Support port trunking and load sharing for high bandwidth links between switches
- Support flooding control
- Support static and dynamic MAC address limit function

A.2 Specification

[Basic Characteristics]

Access Method	CSMA/CD
Communication Mode	Full / Half duplex
Ports	Depending on your models – 24-only or 24+2G
Console Port	DB9 connector for RS-232 connection, with factory default [Baud Rate : 115200, Data Bits : 8, Parity Bits : None, Stop Bit : 1, Flow Control : None.]
Dimension	24+2G model : 440mm x 254mm x 44mm 24-only model : 440mm x 172mm x 44mm
MDI / MDIX Select	Fully Modularized Model : Auto Detect Non-Fully Modularized Model : MDIX only
Input Power	100~240VAC, 50/60 Hz
Filter & Forwarding Rate	Full line speed

Transmission method	Store-and-forward
Address Table	12K entries
Packet Buffer	2M bytes
Flow Control	Back pressure for half duplex, IEEE802.3x for full duplex
LED Display	Per Port : Link/Act, FDX/Col Per Device : Power, Fault
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, allowed up to 128 VLANs in one switch
Trunk Function	24+2G model : Three trunk connections allowed 24-only model : Two trunk connections allowed
IGMP	IP Multicast Filtering by passively snooping on the IGMP Query
Quality of Service (QoS)	Provides 4-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 Port-Based, 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 ICMP Router Discovery Message IP Multicast : IGMP Snooping IP Multicast Packet Filtering Maximum of 128 VLANs and IP multicast sessions

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
 VLAN MIB (802.1Q)
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.