WATERS NETWORK SYSTEMS™

INSTALLATION GUIDE

AND

OPERATING MANUAL

ProSwitch®FlexPort- 2600M
Managed Modular Copper and Fiber Switch

CORPORATE HEADQUATERS
5001 American Blvd. W., Suite 605
Bloomington, MN 55437
Phone: 800.441.5319
Phone: 952.831.5603

MANUFACTURING/CUSTOMER SERVICE
945 37th Avenue, NW
Rochester, MN 55901
Phone: 800.328.2275
Phone: 507.285.1951

Web site: http://www.watersnet.com

TABLE OF CONTENTS

1.0 Specifications

OPERATIONAL CHARACTERISTICS:

MAC Address Table: Up to 2K
Switching Mode: Store-and-forward
Memory Buffer Size: 2 MB
Filtering/Forwarding Rate Performance
- 10Mbps: 14,880 pps
- 100Mbps: 148,800 pps
- 1000Mbps: 1,488,000 pps

MANAGEMENT OPTIONS:

In-band: Web Based, SNMP, Telnet
Out-band: Console
SNMP Agent:
- MIB-II (RFC1213)
- Bridge MIB (RFC1493)
- RMON MIB (RFC1757, Group 1, 2, 3, 9)
- VLAN MIB (802.1Q)

IEEE 802.1D
VLAN: Port-based/802.1Q, Tagged, 128 VLANs
Trunking: 3 groups
IGMP: IP Multicast filtering
QoS:
- Port-based
- Tag-based
- DS/TOS-based

Security:
- Limit number of MAC addresses per port
- Static MAC address filter
- Static/dynamic MAC address limit

Internal Routing
RIP/RIP-2DHCP-Relay
Software Update: TFTP/Kermit software upgrade capability

LED INDICATORS:

Power/Link/Activity/HDX/FDX
System LED Power

NETWORK STANDARDS:

IEEE 802.3 10BASE-T Ethernet
IEEE 802.3u 100BASE-TX/FX Fast Ethernet
IEEE 802.3z 1000BASE-X Gigabit Ethernet
IEEE 802.3x Flow Control
IEEE 802.1P/Q Tagged VLAN
IEEE 802.1D Spanning Tree

EMI/SAFETY COMPLIANCE:

UL 1950, CSA 22.2 No. 950
EN60950 (TUV), VCCI, FCC Class A, CE
EN50082-1, CE

COPPER CABLE/CONNECTORS:

Twisted Pair
Shielded RJ45
Console Port:
4RS232 Cable/DB9 connector

FIBER CABLE/CONNECTORS:

Multimode FX port: 50/125um, 62.5/125mm
Multimode FX port: 50/125um, 62.5/125mm
Singlemode FX port: 9/125um
Multimode SX/LX port: 50/125um, 62.5/125mm
Singlemode SX/LX port: 9/125um, 62.5/125mm
SC or ST connectors

FIBER DISTANCE:
100Mbps Fiber
- Multimode: 2km
- Singlemode: 15km

1000Mbps Fiber
- Singlemode: 10km
- Multimode: 220m

MANAGEMENT CONSOLE CABLE CONNECTOR:

DB9 male, accepts industry standard null-modem cable

POWER SUPPLY:

Input Voltage: 100-240VAC/50/60Hz
Power Consumption: 47 watts, depending on modules installed

OPERATING ENVIRONMENT:

Ambient Temperature: 32° to 122°F (0° to 50°C)
Storage: -40° to 158°F (-40° to 70°C)
Ambient relative humidity: 5% to 95% (non-condensing)

MECHANICAL:

Enclosure: Rugged high-strength sheet metal suitable for stand-alone or rack-mounting
Cooling Method: Fan cooled

PHYSICAL CHARACTERISTICS:

Dimensions:
- 17.25” W x 10” D x 1.75” H
- 438mm x 254mm x 44mm

Weight:
- Switch Chassis: 6.12 lbs (2.8 kg)
- Copper Module: 0.41 lbs (18.4 kg)
- Fiber Module: 0.59 lbs (.27 kg)
- GIG Module: 0.11 lbs (.05 kg)

WARRANTY:
Limited Lifetime Made in U.S.A.

2.0 Package Contents - ProSwitch®- 2600M

- ProSwitch®- 2600M
- Two rack-mount kits and screws
- Console cable
- Installation manual

2.1 Product Description

The ProSwitch®- 2600M is a high performance 10/100/1000Mbps auto-negotiation switch with SNMP/RMON web-based management capability. From a departmental backbone managing lower-level switches, hubs and workstations to high-speed switch-to-switch and switch-to-server links, the 2600M delivers outstanding performance in every environment. With IGMP and VLAN functions, the 2600M ensures maximum bandwidth by reducing multicast transmissions and distributing data over the most efficient media and pathway. With Quality of Service (QoS) supports, the 2600M provides the capability to prioritize certain tasks on the network. This is particularly useful for sending voice or video over a switched network. The modular design of the 2600M provides increased flexibility so you can customize up to 26 usable ports to meet your network requirements.

2.2 Uplink Modules

The following module configurations are available for the 2600M.

2600-8TX	8-port 10/100Base-TX module with RJ45 connectors
2600-8FXSC	8-port 100Base-FX multimode fiber module with SC connectors
2600-8FXST	8-port 100Base-FX multimode fiber module with ST connectors
2600-8SMSC	8-port 100Base-FX singlemode (15km) fiber module with SC connectors
2600-1GigTX	1-port 1000Base-TX with RJ45 connector
2600-1GigSX	1-port 1000Base-SX multimode fiber module with SC connector
2600-1GigLX	1-port 1000Base-LX singlemode (10km) fiber module with SC connector

3.0 Installation of the ProSwitch®- 2600M

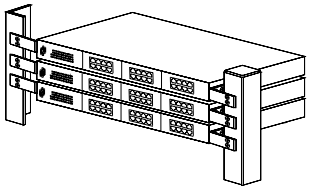
This section provides instructions for installing the ProSwitch®- 2600M

3.1 Location of the ProSwitch®- 2600M

The 2600M can be place on a flat surface (your desk, shelf or table) or mounted onto a rack. As you consider the location for the 2600M, consider the following connection issues: he rules

- The switch is accessible and the cables can be easily be connected to the switch.
- 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 switch to allow for proper ventilation (the switch may not function according to specifications beyond the temperature range of 0 to 50 degrees C).

3.2 Rack Mounting the ProSwitch®- 2600M



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 2600M on 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.

3.3 Powering the 2600M

The 2600M switch is equipped with a universal power supply that accepts AC input voltages from 100 to 240VAC and 50 to 60 Hz.

To supply power to your switch:

1. Plug the connector of the power cord into the power port on the rear panel of your switch.
2. Plug the other end of the power cord into an AC wall outlet.

Note: Network cable segments can be connected or disconnected from the switch while the power is on, without interrupting the operation of the switch.

3.4 The Modules

Warning: Before installing a module into the 2600M, you must disconnect the switch from the main power supply. The 2600M does not support the hot-swap function. There are three choices of modules for long distance fiber optic cable connection.

Handling Modules

The module can be easily damaged by electrostatic discharge. To prevent damage, please observe the following:

- Do not remove modules from their packaging until you are ready to install it into a switch.
- Do not touch any of the pins, connections or components on the modules.
- Handle the modules only by its edges and front panel.
- Always wear an anti-static wristband connected to a suitable grounding point.
- Always store or transport modules in appropriate anti-static packaging.

Module Installation

1. Ensure that the switch is disconnected from the main power supply and that you are wearing an anti-static wristband connected to a suitable grounding point.
2. Place the switch on a flat surface.
3. Using a small cross-bladed screwdriver, remove the module cover from the switch. Do not remove any other screws from the switch.
4. Keep the blank module cover and screws in a safe place. If you remove the module at any time, you must replace the blank module cover to prevent dust and debris from entering the switch and to aid the circulation of cooling air.
5. Follow the rails on both sides of the module slot to slide the module in slowly.
6. Push the module firmly to ensure connection with the module and the connector in the switch.
7. Tighten the screws to firmly connect the module to the switch.
8. Power ON the switch.

Connecting Modules

1. Turn off the switch.

2. Remove the protective plastic covers from the fiber connectors on the module.
3. Plug the connector on the fiber cable into the fiber socket on the module.
4. Connect the other end of the fiber optic segment to an appropriate device fitted with a 100Mbps adapter.
5. Power on the switch.
6. Check the LED indicators on the front of the switch to ensure that the module is operating correctly.

Removing Modules

1. Ensure that the power supply and the backbone connection cables are disconnected from the switch.
2. Place the switch on a flat surface. Undo the two captive thumbscrews securing the module into the switch. Do not remove any other screws from the switch.
3. If you are not installing another module immediately, you must replace the blank module cover to ensure that dust and debris do not enter the switch, as well as to aid circulation of cooling air.
4. Loosen the screws on the module.
5. Remove the module slowly from the module slot.
6. Install the blank module cover.
7. Power on the switch.

3.5 Connecting the ProSwitch® – 2600M

Any of the modules for the 2600M can be used to:

- Connect the switch to the backbone of your network
- Connect the switch to a classroom/workgroup hub or switch
- Connect the switch to a server or workstation with a fiber NIC

The 2600M switch has been designed to support all standard Ethernet media types within a single switch unit. The various media types supported along with the corresponding IEEE 802.3 and 802.3u standards and connector types are as follows:

Fiber:

IEEE Standard	Media Type	Max. Distance	Connector Type
100Base-FX	multimode fiber	2km (6,562 ft)	SC or ST
1000Base-SX	multimode fiber	550m (1,804 ft)	SC
1000Base-LX	singlemode fiber	10km (32,810 ft)	SC
Copper:			
10Base-T	CAT3 or 5	100m (328 ft)	RJ45
100Base-TX	CAT5 or 5E	100m (328 ft)	RJ45
1000Base-TX	CAT5 or 5E	100M (328 ft)	RJ45

Note: Since dual-speed ports are auto-sensing for both 10 and 100Mbps, it is recommended that high quality CAT5E or better cables (which work for both 10Mbps and 100Mbps) be used whenever possible in order to provide flexibility in a mixed-speed network. Because the switch supports auto MDI/MDI-X detection, normal straight through cables for both workstation connection and hub or switch connection can be used. All ports are auto MDI/MDI-X, so you can use any of the ports to connect a port on another hub or switch with straight through or crossover cables.

3.6 Configuration of ProSwitch®- 2600M

The 2600M 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

3.7 Status of LEDs

LED	STATUS	CONDITION
Power	ON	Switch is receiving power.
Fault	ON	ON when switch is booting and OFF when running. If it is steady ON when running, the switch is faulty.
Link / Act	ON	Port has established a valid link.
	Blinking	Data packets received or sent.
	Green	The connection speed is 100Mbps.
	Yellow	The connection speed is 10Mbps.
FDX / Col	ON	The connection is Full Duplex.
	Blinking	Packet collisions occurring.

Note: The Link/Act LED is green. The speed display on the TX module is Green for 100Mbps and Yellow for 10Mbps. If 100Base-FX ports are installed, the operation speed must be set to 100Mbps and the operation mode must be set to full duplex. The 100Base-FX ports will not work if they are set to 10Mbps, half duplex or Auto.

4.0 Managing the Switch

There are three ways to manage the 2600M switch:

- Local Console Management interface (CMI) via the console port.
- Remote Console Management via a network connection.
- Using an SNMP Network Management Station.

Note: The 2600M does not have a default IP address. Remote management cannot be used until an IP address has been set.

4.1 Console Management Interface (CMI)

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.

Equipment Required

- Null modem cable, 9 position D-Sub, female to female
- Computer with function RS-232C port (COMx)
- Terminal emulation program (HyperTerminal in Windows, Minicom in Linux or any other emulation software).

To use the Hyper Terminal Program with Windows, follow these instructions.

Hardware setup

1. Connect the console port on the switch to the COM port on the PC using a standard 9-pin console cable.

Using HyperTerminal

1. Boot PC with MS Windows.
2. Load the **HyperTerminal** program from the Start menu. Select **Programs – Accessories – Communications – HyperTerminal**.
3. If the connection file has not been created, follow the instructions on the screen to create a new connection named "2600M" (or something similar).
4. Select the COM1 port in the **connect using** field.
5. Set COM port parameters:
    a. "Bits per second: ***115200***
    b. Data Bits: ***8***
    c. Parity Check: ***None***
    d. Stop Bit: ***1***
    e. Flow Control: ***None***
6. Select OK.
7. Power on the switch and a login screen will be displayed on your screen.

Using Remote Management

You can manage the 2600M remotely by establishing a remote host using a Telnet connection VIA a modem link or a network connection. Before using this management method, the 2600M must have an assigned IP address. The Remote Console Management interface is identical in appearance and functionality to the Local Console Management interface described in the previous section.

Management can be done from a remote site across a LAN using:

- SNMP Network Management Station

- Web Browser interface
- 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

Assigning an IP Address

To manage the 2600M remotely through the console port or with an SNMP Management Station, you must assign an IP address to the switch. The IP address is assigned through the IP Settings screen. This procedure is described in **IP Networking** in Section 6.0. Use 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.

Logging Into the Management Functions

Once a CMI session has begun, the login screen should be displayed. You will be required to enter a valid username and password combination to gain access to the menu functions through the CMI. The following are the two predefined user names and passwords created by default:

- Login name – **admin**
- Password – **123456**

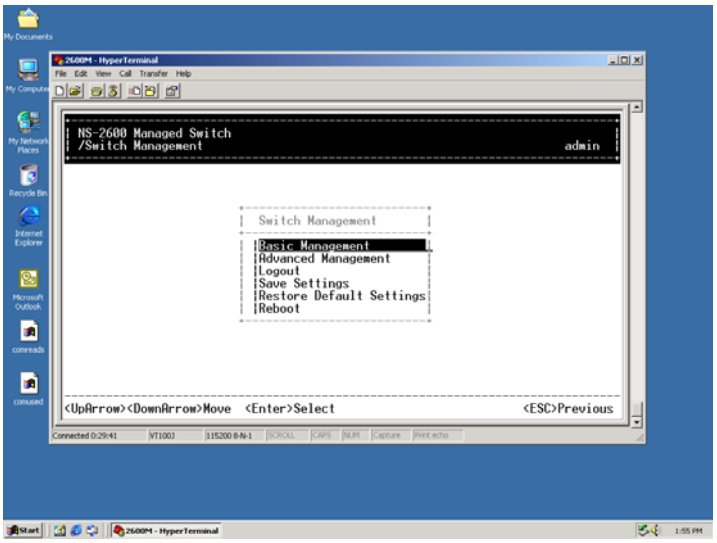
Once you have logged in, you can change this password.

5.0 Using the Management Functions

Navigation through the console menu options is very simple. Notice the menu options listed at the bottom of the screen.

The **UP Arrow** and **Down Arrow** are used to move the highlight the menu option. **Enter** is used to select the menu. The menu keys will always be listed at the bottom of the screen as you use the Management options. So depending on the option you are configuring, different menu keys will be available.

Some terminal programs will not work with the arrow keys. If your arrow keys do not move the cursor through the management menus, use the **K key for the up arrow** and the **J key for the down arrow**.



5.1 Management Functions

Basic Management	General	System Name, Software Version, Password, HTTP Enable/Disable, . . .	
	LAN Port	Port Physical Configuration, MAC ID	
	Console Port	Console Port Settings	
Advanced 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.		

5.2 Performing Basic Management Functions

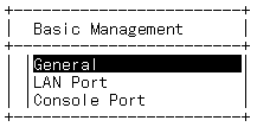
Basic management functions consist of the following functions:

- System name and location
- Set password

- Configuration of LAN ports
- Configuration of console port
- Learn MAC address of switch

5.3 System Management

1. Login to the 2600M switch.
2. Select **Basic Management**.
3. The following menu will be displayed:



4. Select **General**.
5. The **General Menu** screen will display the current information about the 2600M switch. You can set or modify the:
   - System Name
   - Location of the switch
   - Administrator's and guest password
6. The following tasks can also be performed from this menu: (These tasks are all enabled by default.)
   - **Statistics Collection** – Collects information about the operation of the switch
   - **Reboot-On-Error** – If this option is enabled, the switch will automatically reset if a fatal error is detected.
   - **Telnet Login** – Enable or disable remote Telnet logins to the switch.
   - **Remote HTTP Login** – Enable or disable remote HTTP login to the switch.

   Note: All of the options are enabled by default.
7. Use the **Esc** key to return to the **Basic Management Menu**.

Changing the Password

Before you can enter a new password, you must enter the old password. You will be asked to re-type the new password to confirm that you have entered the password correctly. The system will confirm the password and the "Password Changed" message will be displayed.

You may also use this menu to change the "guest password."

5.4 Configuring the LAN Ports

This management function allows you to configure speed and flow control, link type and physical address. You can change the connection configuration on each port of the switch with this option.

Speed and Flow Control

1. Access the **Basic Management Menu**.

2. Select **LAN Port**.
3. Select **Speed & Flow Control**.
4. Select the appropriate port and make the desired changes. Use the **Arrow** keys and the **Enter** key to make your selections.
5. Press **Esc** to return to the Main Menu.

Note: Changes are automatically saved in flash memory, so they take place immediately. So, as long as the switch is on, the settings will be saved. However, if the switch is powered down, the settings will be lost. When you logout of the management menu, you will be prompted to save your settings. Settings can be saved from the **Switch Management** menu in case you don't want to wait until you log out.

Note: If 100Base-FX ports are installed, the operation speed must be set to 100Mbps and the operation mode must be set to full duplex. The 100Base-FX ports will not work if they are set to 10Mbps, half duplex or Auto. If you have installed an uplink in your 2600M switch (port 25 and/or port 26), make sure the LAN port is configured to reflect the type of installed uplink. For example, if you installed a 2600-1GigSX (fiber Gigabit port), make sure the port is configured for 1000Mbps with full duplex.

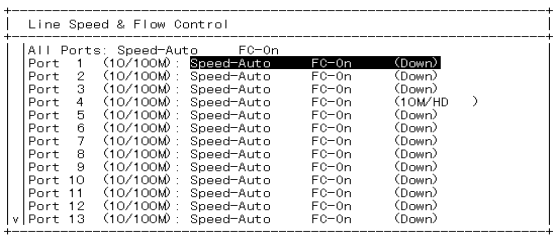
The **Physical Address** on the **LAN Port Configuration** menu displays the MAC address of the switch for informational purposes only. You cannot make any changes to this physical address.

5.5 Configuring the Console Port

This option allows you to change settings for the console port.

Console Port

1. Access the **Basic Management Menu**.
2. Select **Console Port**.
3. The following settings can be made with this menu.
   a. **Baud Rate** – Select the baud rate for the console port (115200 is recommended). If "Auto" option is selected, press the **Enter** key one or more times until the prompt for the **Login Password** appears on



   the screen when you exit the configuration menu.

   b. **Flow Control** – Flow control can be enabled or disabled from this menu. The default is **disabled**.

   c. **Modem Control** – Modem control can be enabled or disabled from this menu. The default is **disabled**. If the modem control is enabled, you must proceed to **Modem Setup String** to specify the appropriate modem setup string.

   d. **Modem Setup String** – If you enabled a modem connection to the console port, use this function to specify a modem setup string. The "default setup string" configures the model to **auto answer**. This will work for all Hayes compatible modems. Or, select **Custom Setup String** to specify your modem type.

   e. **SLIP** – (Serial Line Internet Protocol) Enable or disable the SLIP function of the console port. If you enable SLIP, a message tells you that the console port is accessible only through the SLIP protocol after you logout from the current session. If you enable SLIP, you must specify a SLIP address and SLIP subnet mask. **SLIP** is disabled by default.

   f. **SLIP Address** – If you enabled SLIP, use this function to enter an address that has a network location

that is different than the network address of the switch.

g. **SLIP Subnet Mask** – If you are using SLIP, enter a suitable SLIP subnet mask.

6.0 Advanced Management Functions

VLANS

1. Login to the switch and select **Advanced Management**.

   Select **L2 Switching DataBase**. This menu option allows you to view and configure the switch from four perspectives: VLAN, MAC address, IP multicast group, and port. These four views allow a network administrator to manage and monitor VLANs and their associated MAC addresses and ports status effectively.

2. Select **VLAN & PVID** (Port VLAN ID) **Perspective**. This option allows to you to create VLAN groups. Once VLANs are created, you can then use **PVID Settings** 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: A **tag** is a four bytes of packet information added in a packet for VLAN and priority information of the packet. Packets that include the four byte of packet information are referred to as ***tagged packets*** and the packets without tag as ***untagged packets***. You can set the switch ports as tagged or untagged when configuring VLANs.

Untagged ports should be connected to untagged devices, and the ***PVID*** should be assigned 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. If tagged packets are forwarded to untagged ports, the tag will be removed from the packet.

The following operations can be done from **VLAN Settings**:

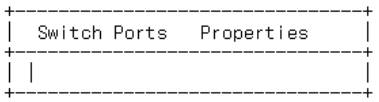
- ❑ Create a new VLAN
- ❑ Delete a VLAN
- ❑ View VLAN activity
- ❑ View and change VLAN configuration

Creating a VLAN

1. Login to the switch.
2. From the **Switch Management Menu**, select **Advanced Management**.
3. Select **L2 Switching DataBase**.
4. Select **VLAN & PVID Perspective**.
5. Select **VLAN Settings**.
6. Press **Shift** and **+** to add a VLAN.
7. Press **Enter** to assign a VLAN ID and VLAN name. The ID can be a 12-bit decimal or hexadecimal ID value.

Note: "Remote" will be appended to the VLAN ID automatically if the VLAN is learned from a remote switch.

8. The following screen is used to add switch ports to the VLAN. Press **Shift** and **+** to add a switch port number.



9. Select **Tagged** or **Untagged**.
10. Select the **port number** and press **Enter**.
11. Repeat these steps to add ports to the VLAN.
12. To remove a switch port number, highlight the port and press **–** (the minus key).
13. Press **Esc** to return to the desired menu.

Deleting a VLAN

1. From the **Switch Management Menu**, select **Advanced Management**.
2. Select **L2 Switching DataBase**.
3. Access the **VLAN & PVID Perspective** menu.
4. Select **VLAN Settings**.
5. Highlight the VLAN you want to delete.
6. Press the **–** key.
7. A message will be displayed to make sure you want to delete the VLAN. Select **Yes** and the VLAN will be deleted.
8. Press **Esc** to return to the desired menu.

VLAN Activities

This option allows you to view activities for a particular VLAN. You can view active ports, active MAC addresses associated with a VLAN, a transient address (if any) and filtering and port information.

1. From the **Switch Management Menu**, select **Advanced Management**.
2. Select **L2 Switching DataBase**.
3. Access the **VLAN & PVID Perspective** menu.
4. Select **VLAN Settings**.
5. Highlight an existing VLAN and press **Enter**.
6. Select **VLAN Activities**.
7. This screens displays the VLAN domain for the selected VLAN. The VLAN domain shows the ports included in this domain.

Changing a VLAN Configuration

1. From the **Switch Management Menu**, select **Advanced Management**.
2. Select **L2 Switching DataBase**.
3. Access the **VLAN & PVID Perspective** menu.
4. Select **VLAN Settings**.
5. Highlight an existing VLAN and press **Enter**.

6. Select **VLAN Settings**.
7. To add a port , press **+** (the plus key).
8. Select **Tagged** or **Untagged**.
9. Select the **port number**.
10. Repeat these steps to add additional ports.
11. Press **Esc** to return to the desired menu.

Deleting Ports from a VLAN

1. From the **Switch Management Menu**, select **Advanced Management**.
2. Select **L2 Switching DataBase**.
3. Access the **VLAN & PVID Perspective** menu.
4. Select **VLAN Settings**.
5. Highlight an existing VLAN and press **Enter**.
6. Select **VLAN Settings**.
7. To delete a port, highlight the port and press **–** (the minus key).
8. Repeat **Step 5** to remove additional ports from the VLAN.

Assigning PVID

1. From the **Switch Management Menu**, select **Advanced Management**.
2. Select **L2 Switching DataBase**.
3. Access the **VLAN & PVID Perspective** menu.
4. Select **PVID Settings**.
5. Select the appropriate port number and press **Enter**.
6. Enter the **PVID**.
7. Press **Esc** when finished.

Note: Because there is no VLAN information in untagged packets for untagged ports, you can assign a VLAN ID to untagged ports with this function. 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 this information:

1. Select **L2 Switching DataBase** from the **Advanced Management** menu.
2. Select **IP Multicast Group Perspective** and press **Enter**.

Note: If the IGMP protocol is disabled, a message will be displayed that says “IGMP Currently Disabled.” To enable IGMP:

a. Return to the **Advanced Management** menu.
b. Select **Other Protocols**.
c. Press **Enter** for **IGMP**.
d. Select **IGMP** and press **Enter**.
e. Press **Enter**.

f. Select **Active**.

Passive mode: Passively snooping on the IGMP Query and IGMP Report. Packets are transferred between IP Multicast Routers and IP Multicast host groups to learn IP Multicast group members.

Active mode: Actively sending IGMP Query messages to solicit IP Multicast group members.

So, in a**ctive mode**, the switch will automatically send the IGMP query messages to the network and check IGMP members. But in **passive mode**, the switch will not send IGMP query messages.

g. Press **Esc** to return to the **Advanced Management Menu**.

h. Return to the **IP Multicast Group Perspective** menu.

3. Highlight an **address** and press **Enter**.
4. To view the VLAN and IP multicast group addresses associated with the MAC address, highlight a **host** in the Hosts screen and press **Enter**. The VLAN/IP Multicast Group Membership screen will appear.

MAC Address Perspective

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

1. Select **L2 Switching DataBase** from the **Advanced Management** menu.
2. Select **MAC Address Perspective** and press **Enter**.
3. You will be prompted for a MAC address. Enter the appropriate MAC address and press **Enter**.
4. Use the **Up** and **Down** arrows to scroll through the VLAN/IP Multicast Group Membership screen.

Port Perspective

The Port Perspective allows you view VLAN activities and RMON statistics. You can also configure the MAC address learning function of each port with this function. To obtain a port perspective:

1. Select **L2 Switching DataBase** from the **Advanced Management** menu.
2. Select **Port Perspective** and press **Enter**.
3. Select **Per Port VLAN Activities**.
4. Select the appropriate port number and press **Enter**. A screen with a list of the MAC addresses for the selected VLAN and the corresponding VLAN memberships will appear.
5. Use **Tab** to switch to the **VLAN Membership** screen.
6. Use the **Up** and **Down** arrow keys to scroll through the list of active MAC addresses for the selected port.
7. To search for a MAC address, press **S**.
8. When the search prompt appears, enter a **MAC address** in the "Enter MAC Addr to Search" screen and press **Enter**.
9. If the address is found, it will be highlighted in the **Port MAC Addresses** screen.
10. To obtain additional information about a particular MAC address, scroll to the address in the **Port MAC Address** screen and press **Enter**. Detailed information about the selected MAC address will be displayed.

Per Port Statistics.

1. Select **L2 Switching DataBase** from the **Advanced Management** menu.
2. Select **Port Perspective** and press **Enter**.
3. Select **Per Port Statistics**.
4. To reset counters for all ports, press **R**.
5. Select **Yes** to confirm the reset of the counters.

6. To view statistics for a port, **highlight** the desired port and press **Enter**. The statistics for the port you selected will be displayed.

7. Return to the **Port Perspective** menu.

Per Port MAC Limit

You can configure the MAC address learning function of each port to:

- **Limited Learning** – set a number to limit the PCs that can share this connection at the same time.
- **Unlimited Learning** – remove the PC connecting number limit. The PC connecting number on the port will become no limit. This is the normal state for a switch.
- **No Learning** – Disable the MAC learning function. The MAC addresses that can connect to this port will be assigned from the **Static Filtering** function. This function allows the network administrator to limit the users that can access the network through the connected ports.

Note: If you select **Learning Limit** on the connection port and also assign MAC addresses on the port in the **MAC Address In-Filters** of **Static Filtering** function (this option is on the **Advanced Management Menu**), these MAC addresses will always be allowed to use this connection. These MAC addresses are not included in the limit number of PC.

IP Networking

IP Networking allows you view or change IP settings, ARP and routing table parameters, RIP parameters, DHCP gateway settings and ping settings. Before you can define IP settings, a VLAN must be created as described in a previous section.

1. Select **IP Networking** from the **Advanced Management** menu.
2. Select **IP & RIP Settings**.
3. Displayed is the following information:
    a. VLAN ID
    b. IP Address
    c. Subnet Mask
    d. Proxy ARP
    e. RIP
4. Highlight the appropriate VLAN and press **Enter**.
5. Review the settings and make the appropriate changes. To enter information, highlight the setting, press **Enter**.
6. Enter the information and press **Esc**.
7. Once you have configured all IP Settings, press **Esc** to return to the **Advanced Management** menu.

Note: The IP and its subnet setting of the switch are assigned based on VLAN. This switch allows users to assign different IP subnets on different VLANs. 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. For normal cases, assigning the switch's IP address on the default VLAN for remote management is OK.

Using DHCP to Set the IP Address of the Switch

1. Select **IP Networking** from the **Advanced Management** menu.
2. Select **IP & RIP Settings**.
3. Select **VLAN 1**.
4. Select **BOOTP**.
5. Press **Enter**.
6. Select **DHCP**.
7. Write down the IP address of the Switch.

ARP Table

If you select **ARP Table** (Address Resolution Protocol) from the "IP Networking" screen, an ARP Table screen appears with the ARP table entries that have been already defined or learned.

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

Adding Static ARP Table Entries

1. From the **ARP Table screen**, press **Shift** and press **+**. The Static ARP Specifications screen will be displayed.
2. Highlight the **Internet Address** and press **Enter**. The **Enter Internet Address** screen will be displayed.
3. Type an **Internet Address** (IP address). When you finish, press **Enter**. The Internet address you typed will be displayed next to Internet Address in the Static ARP Specifications screen.
4. Highlight the **Physical Address** and press **Enter**. The **Enter Physical Address** screen will be displayed.
5. Type the **corresponding physical address** and press **Enter**. The physical address you typed will be displayed next to **Physical Address** in the **Static ARP Specifications** screen.
6. Press **Esc**. The Internet and physical addresses you entered will be displayed in the ARP Table screen.
7. To add more static ARP table entries, repeat these steps. When you finish, press **Esc** to return to the ARP Table screen.

Deleting Static ARP Table Entries

There is no precautionary message that appears before you delete a static ARP table entry, so be sure you want to delete the entry before proceeding.

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

Searching ARP Table Entries

1. From the **ARP Table screen**, press **S.** The Search Options screen prompts you to select an **Internet Address** or a **Physical Address**.
2. 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 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

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.

Adding Routing Table Entries

1. From the **Routing Table** screen, press **Shift** and press **+**. The **Route Options** screen will be displayed. Select **Default Gateway** or **Static Route** and press **Enter**.
2. If you select **Default Gateway**, the **Default Route Specification** screen will be displayed. Press **Enter** and type an **IP address** for the default gateway.
3. If you select **Static Route**, the **Static Route Specification** screen will be displayed. At each field, press **Enter**, type the **appropriate parameter** and press **Enter** again.

Deleting Routing Table Entries

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

1. Highlight the **Routing Table Entry** you want to delete and press **-**. The entry will be deleted.
2. Searching for **Routing Table Entries**.
3. To search for entries in the Routing table, press **S** in the **Routing Table screen**. The **Enter Network Address** screen will be displayed. Type the **network address** you want to search for and 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

The **DHCP Gateway Settings** screen provides the following information:

- **VLAN ID** - lists the IDs of the VLANs that have been defined.
- **IP Address** - displays the corresponding IP addresses of the VLANs.
- **DHCP Relay** – shows whether the DHCP relay is enabled or disabled.
- **Max Hops** - displays 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** – displays the number of seconds that must elapse before a DHCP request broadcast is relayed to the next IP subnetwork.
- **Servers** - lists any preferred servers that have been defined.
- **Relays** - shows the outbound IP subnetwork for relaying a DHCP request broadcast.

Note: To specify DHCP gateway settings, you must first create a VLAN with an assigned IP address as described in **VLAN & PVID Perspective** Section 6.0.

The following procedure describes how to change the **DHCP Gateway Settings**. You can specify up to three preferred servers and/or an outbound relay interface.

1. Select **IP Networking** from the **Advanced Management** menu.
2. Select **DHCP Gateway Settings**.
3. Highlight the appropriate VLAN ID and press **Enter**.
4. To add a relay **IP**, press **Shift** and press **+**.
5. A setup screen will be displayed. Highlight the **appropriate interface** and press **Enter**.
6. You can **enable/disable DHCP Gateway**, set **Maximum Hops**, set the **Delay time** (in seconds) and specify up to **three more preferred servers** in this screen. The DHCP gateway is disabled by default. Highlight **Disabled** and press **Enter**.
7. Select **Enabled** and press **Enter**.
8. Set the **Maximum hops** and **Delay** time.
9. Press **Esc** to return to the appropriate menu.

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

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 logs in, 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 the 2600M 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 will either:

- Forward the packet to a specific server as defined in the switch configuration using Unicast routing
- Broadcast 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.

Pinging

The following options can be set for pinging:

- 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).

To set the ping options:

1. Select **IP Networking** from the **Advanced Management Menu**.
2. Select **Ping**.
3. Highlight each item one at a time and press **Enter**.
4. Set each option in the screen.
5. Press **Esc** to start the ping operation.

Bridging

Bridging allows you view and change the aging period.

1. Select **Bridging** from the **Advanced Management Menu**
2. To change the aging time, highlight **Aging Time (seconds)** and press Enter.
3. Press **Enter** for **Set Aging Time**.
4. 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.
5. To change the flood limit for all ports, highlight **Flood Limit for All ports (pkts/sec)** and press **Enter**.
6. The next 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.
7. Follow the same steps for **Broadcast Limit** and **Multicast Limit.**
8. When you are finished, return to the **Advanced Management** Menu.

Note: To remove these settings, return to the option for **Aging**. Choose **No Aging**. Set the other parameters to **unlimited** to remove the settings.

Aging - Aging is an operation used so a switch can maintain its learning table. If a network device does not send any packets in the aging time, its MAC address entry in the learning table will be removed. This operation is called aging.

Flooding - Whenever a packet is sent to a switch, the switch will try to find the destination port of the packet by looking it up in the learning table. It will 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. **Multicast limit**s work like broadcast, but the packet is only sent to the member client, not all ports.

Static Filtering

Static Filtering allows you view, add, delete, or search all source or destination addresses to be filtered.

The **Out-Filters** function will filter out 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 always be forwarded by the switch. 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 will be forwarded by the switch.

1. Select **Static Filtering** from the **Advanced Management** menu.
2. Select **Source MAC Address Out-Filters**.
3. To add a MAC address to be filtered, press **Shift** and **+**.
4. To delete a MAC address from being filtered., press **-**. There is no precautionary message that appears before you delete a MAC address, so be sure you want to delete the address before doing so.
5. To search a MAC address, press **S** to search through the list of MAC addresses in the static filtering database.
6. Follow the same procedure to enter **Destination MAC Address Out-filters** and **MAC Address In-Filters**.
7. Return to the **Advanced Management** menu.

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 if spanning tree is enabled. Thirty seconds is the spanning tree re-configuration time.

The **Spanning Tree** menu from the **Advanced Management** screen provides the following options:

- Spanning Tree Configurations
- Spanning Tree Port States
- Spanning Tree Path Costs
- Spanning Tree Port Priorities

Spanning Tree Configurations

1. Highlight **Spanning Tree Configurations** in the **Spanning Tree Protocol** screen and press the **Enter** key.
2. The top half of this screen displays read-only values. The bottom half, starting with **Spanning Tree Protocol**, is user configurable.
3. Highlight a field, then press **Enter** to change the value.
4. Press the **Esc** key until you return to the desired screen.

Note: The **Spanning Tree** protocol is disabled by default. **Bridge priority** is used to select 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. **Hello Time** is the time interval for the root device to transmit the spanning tree configuration message.

Spanning Tree Port States

If you highlight **Spanning Tree Port States** from the **Spanning Tree Protocol** menu and press the **Enter** key, a Spanning Tree Port States screen appears. When you finish, press the Esc key until you return to the desired screen.

If you want to change the **Port 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. You can also enable the STP Protocol from this screen.

Spanning Tree Path Cost

This option will allow you to change the **spanning tree path cost**.

1. Select **Spanning Tree** from the **Advanced Management** menu.
2. Select **Spanning Tree Path Costs**.
3. Select the port that you want to change.
4. Enter the **new path cost** in the prompt screen and press **Enter**.
5. Press **Esc** to return to the desired screen.

Path Cost (0 – 65535) - It is used to determine the best path between devices when there is looping. 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

This option will allow you to change the spanning tree path priorities.

1. Select **Spanning Tree** from the **Advanced Management** menu.
2. Select **Spanning Tree Port Priorities**.
3. Highlight the port that you want to change and press **Enter**.
4. Enter the new path priorities in the prompt screen and press **Enter**. The value is from 0 to 255. A low value gives the port a greater likelihood of becoming a Root port.
5. Press Esc to return to the desired screen.

Port Priority (0-255) - If the path cost for all ports on a switch is the same, the port with the highest priority (lowest value) will be forwarded when there is looping. If more than one port has the same high priority, the port with lowest port number will be forwarded.

SNMP

SNMP allows you to view and change all SNMP-related information. The 2600M supports the SNMP agent function and you can configure SNMP settings (community name, trap host, trap events, etc). SNMP is enabled by default. To change the configuration:

1. Select **SNMP** from the **Advanced Management** menu.
2. Highlight the item that you want to change and press **Enter**.
3. Enter the new setting for the item in prompt screen and press **Enter**.
4. Press **Esc** to return to the menu.

Other Protocols

The **Other Protocols** Menu allows you to enable and disable *GVRP* and *IGMP* protocols. 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. GVRP and IGMP are disabled by default.

- **GVRP** - Enable or disable GVRP operation
- **IGMP** - Enable or 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** – IGMP snooping operation in a concentration VLAN configuration sets multicast group

as part of VLAN group and not VLAN grouped with the other ports.

GVRP Protocol

In addition to network management tools that allow network administrators to statically add and delete VLAN member ports, the 2600M 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 2600M to issue and revoke VLAN memberships. VLAN-aware, the 2600M register and propagate VLAN membership to all ports that are part of the active topology of the VLAN.

IGMP Protocol (IGMP Snooping and IP Multicast Filtering)

The Internet Group Management Protocol (IGMP) runs between hosts and their immediate 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 2600M supports 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.
- 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 2600M with IP multicast filtering/switching capability not only passively monitors 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.

To enable or disable GVRP and IGMP:

1. Select **Other Protocols** from the **Advanced Management** menu.
2. Highlight the item that you want to change and press **Enter**.
3. Select the new setting for the item from the prompt screen and press **Enter**.
4. Press **Esc** to return to the Main Menu.

Port Trunking

This switch supports three trunking connections:

- Two trunking connections for 10/100Mbps ports
- One trunking connection for Gigabit ports.

Trunking connections are manually set by port. The configuration screen lists the ports. The switch treats these trunking connection ports as one connection. Select one of the trunking numbers, and then select the ports for the trunking connection.

To use the two Gigabit ports for trunking connection, use **Trunk 29**. Then select **Port 25** and **26**. The maximum bandwidth is 4Gbps for the Gigabit trunk ports.

1. Select **Port Trunking** from the **Advanced Management** menu.

2. Select a trunk group and press **Enter**.
3. Pres **Enter** to select the range.
4. Use the **Enter** key to mark each port.
5. Press **Esc** to return to the menu when you are finished.

Port Mirroring

Port Mirroring allows you to mirror one port to another port for network traffic monitoring.

1. From the **Advanced Management** menu, highlight **Port Mirroring** and press **Enter**.
2. Highlight **one index** and press **Enter**.
3. Highlight **Mirror To** and press **Enter**. Select the appropriate port.
4. Highlight **Mirror From** and press **Enter**. Select the mirrored port from the port list and press **Enter**.
5. Highlight **Mirror Mode** and press **Enter**. Select the mirror mode (Receive / Transmit) and press **Enter**. You can mirror the receive or transmit packets, but not both.

QoS Setup

QoS (Quality of Service) is an important issue for network devices now because there are so many different types of data transmitted across the network – phone call, audio, video, web business, email, file transfer, web access, etc. Different types of data have different requests about delay, throughput and reliability on packet transfer. Network administrators should consider the type of network applications and the requests for these applications. You can then configure this switch to meet these requests. When congestion occurs 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.

The 2600M supports four priority queues on each 10/100Mbps ports and eight priority queues on the Gigabit ports. The 2600M also supports two classes of drop rates with WRED (Weighted Random Early Detection) logic that can be configured. 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.

To configure QoS for your switch, use the **Advanced Management** menus to select **QoS**. The following chart provides an overview of the settings for QoS.

Menu	Description
Global Setting	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 from the **QoS Setup** menu allows you to set the general configuration for the QoS operation.

- **QoS Status** – Use this function to enable or disable QoS. QoS is enabled by default.
- **DiffServ Expedite Forwarding** – Use this function to enable or disable DiffServ EF. This switch can map IETF DifferServ 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 for "*Differentiated Service*". Differentiated Services provides a simple method of classifying services of various applications. *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 a set 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.

DiffServ is enabled by default.

- **ToS/VLAN Tag Preference –** Use this function to select the preference priority information in packets, priority in ToS or priority in VLAN tag. ToS is the abbreviation for *Type of Service* and it is an 8-bit field in an IP packet. Here is the explanation of the bits:

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.

- **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.
- **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.
- **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, actions take place. The Average Queue Size (AQS) is calculated. If the AQS is less than the minimum WRED threshold, the packet is enqueued. (Enqueued means the packet is waiting in the queue for its turn to be sent.) 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*). 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

The **Logical Port** function from the **QoS Setup** menu allows you to configure the QoS operation of different TCP/IP logical (service) ports. There are three types of logical ports can be configured:

- **User-Defined Port** - Eight user-defined TCP/IP logical ports can be set for the **User-Defined** Port QoS operation. Once you select a logical port and assigned a TCP/IP port number, you can configure the following:
    - Enable / Disable it.
    - Configure the drop rate to high drop rate or low drop rate.
    - Configure the transmit priority to 0 ~ 7.
- **Well-Known Port** – Eight well-known ports can be set for the **Well-Known Port** QoS. Once you select a port, you can configure the following:
    - Enable / Disable it.
    - Configure its drop rate to high drop rate or low drop rate.
    - Configure its transmit priority to 0 ~ 7.

The following chart shows an example of how well-known ports may be used:

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

- **Range Port** – The Range Port setting allows you to define the drop priority and transmit priority for some range of TCP/IP logical ports.

VLAN

The **VLAN Index** from the **QoS Setup** menu allows you to configure the drop priority and transmit priority for each priority value in VLAN tag. Select a priority index and configure the QoS setting for this priority.

ToS

The **ToS Index** from the **QoS Setup** allows you to configure the drop priority and transmit priority for each priority value in ToS. Select a ToS priority index and configure the QoS setting for this priority. You can set Bit 0-2 or Bit 3-5 of ToS for the transmit priority and drop priority setting with the **Global Setting** from the **QoS** Menu.

Profile

The 2600M supports eight scheduling configurations for each physical port on different priority queues (four priority queues on 10/100M ports and eight priority queues on gigabit port).

- **Strict Priority (SP)** - SP is the highest priority queue in the switch. If there is only 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).
- **Delay Bound** – Delay bound a delay assurance algorithm of the switch. It can dynamically adjust its scheduling and dropping criteria by the queue occupancies and the due dates of their head-of-line (HOL) frames. As a result, latency bounds for all admitted frames with high confidence is assured
- **Weighted Fair Queuing (WFQ)** - You can weight the priority queues for different transmit bandwidth

allocation for these queues. In WFQ mode, frame latency as delay bound is not assured.

- **Best Effort (BE)** - In BE mode, a queue only receives bandwidth when none of the other classes have any traffic. It is used for non-essential traffic because there are no assurances about BE performance.

10/100M Port	P3		P2		P1		P0	
Gigabit Port	P7	P6	P5	P4	P3	P2	P1	P0
Option 1	Delay Bound						BE	
Option 2	Strict Priority		Delay Bound				BE	
Option 3	Strict Priority		WFQ					
Option 4	WFQ							

There are ten profiles in the configuration menu. The following is the mapping between the ten 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 10	Enable	Disable	25%, 50%, 12.5%, 12.5%	Option 3

Note: If the **Delay Sensitive Application** option of any active profile is enabled, an error message will be displayed when you try to set the rate control. It is recommended to try to activate another profile with the **Delay Sensitive Application** option disabled because the **Delay Bound** scheduling operation conflicts with rate control operation of the switch. It is recommended to use Profiles 3, 4, 7 or 8 as the activity profiles for rate control operation because they are **Delay Sensitive Application** disabled.

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, first select either **Megabit Ports Profile** or **Gigabit Ports Profile**.

Megabit Profile

Use the **Megabit Profile** to define the content of QoS profiles. There are ten different profiles, but only four of them can be the active profiles for QoS control in the switch. The **01 profile** contains the following settings:

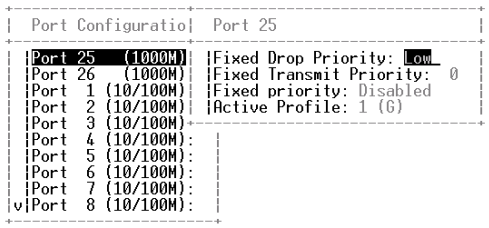
- **Port Using This Profile** – Lists the ports using this profile.
- **Strict Priority** - Displays the Strict Priority setting of this profile.
- **Delay Sensitive Application** - Displays the Delay Bound setting of the profile.
- **Profile Name** – Displays the name of this profile which can be modified.
- **Profile Status** – Displays status of this profile (active or non-active) which can be modified. The 2600M

support four active profiles, so if you enable this profile, other active profiles might be disabled by the switch.

- **Bandwidth Partition** – Allows you to set the bandwidth allocation for the four transmit queues on ports for Weight Fair Queue operation.
- **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 sent from the connected device to prevent packet loss when the port is busy. 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 enabled will always be forwarded with the lowest priority during scheduling so that they are not exposed to the WRED dropping scheme to prevent any packet dropping in the QoS operation. This can guarantee that no packets will be lost, but at the possible expense of minimum bandwidth or maximum delay assurance. If this function is enabled, it will force the QoS function to work when the flow control is enabled. However, only the best effort traffic is not dropped. The high priority traffic is still transmitted first, but the packet may be dropped when the output port is highly congested.

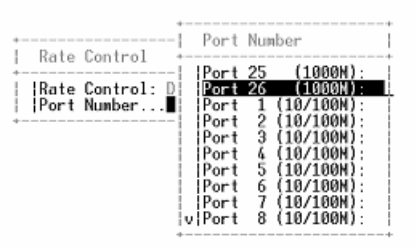
Port Configuration

With this function, you can select the QoS operation profile for each physical port from the four active profiles. The fixed drop and transmit priority settings of the port are set in this menu. 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.) The 2600M supports ten levels of 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 to either streaming or burst.



Note: If the **Delay Sensitive Application** option of any active profile is enabled, an error message will be displayed when you try to set the rate control. It is recommended to try to activate another profile with the **Delay Sensitive Application** option disabled because the **Delay Bound** scheduling operation conflicts with rate control operation of the switch. It is recommended to use Profiles 3, 4, 7 or 8 as the activity profiles for rate control operation because they are **Delay Sensitive Application** disabled.

7.0 File Transfer

Use this menu to download the software running in the switch. If you select **File Transfer** from the Advanced Management screen, the Software Upgrade screen appears. Files can be transferred with **TFTP** (through network connection) or **Kermit** (through console connection) protocols. Highlight the method of choice and press **Enter** to start file transfer.

Note: The software file in the switch is divided into five modules. So, download one module at a time instead of downloading the entire software file.

- **Software Configuration File** - This file contains the software configuration (VLAN, IP, Spanning Tree, …) settings of the switch.
- **Hardware Configuration File** - This file contains the hardware configuration of the switch. If the wrong hardware configuration is used, the switch may fail to work.
- **Debug Monitor File** - This file is used for debugging by an engineer. Please ignore it. It provides no network management functions.
- **Runtime File** - This file is the main code of the switch. It controls the software version of the switch.
- **Web Browser File** - This file contains the http interface html code.

Receive File Via TFTP

Before using this function, you must first download load the file to the TFTP server. Next, check the connection between the switch and the TFTP server by using the ping function.

1. Highlight **Receive File Via TFTP** and press **Enter**.
2. Highlight the **File Name** option and press **Enter**.
3. Type a file name and press **Enter**.
4. Highlight the **IP Address option** and press **Enter**.
5. Enter the **IP address** of the TFTP server and press **Enter**.
6. Press **Esc** and **confirm** the file transfer (Yes or No).

Send File Via TFTP

Before using this function, check the connection between the switch and the TFTP server by using the ping function.

1. Highlight **Send File Via TFTP** and press **Enter**.
2. Then select the file name and set the **IP address** of the TFTP server.
3. Press **Esc** to **confirm** the file transfer (Yes or No). This operation will transfer the file from the switch to the TFTP server.

Receive File Via Kermit

Before using this function, load the terminal program and complete the console connection.

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

Send File Via Kermit

Before using this function, load the terminal program and complete the console connection first.

1. Highlight **Send File Via Kermit** and press **Enter**.
2. Select the file you want to transfer and press **Enter**.

3. Then select **Yes or No** to confirm the file transfer via Kermit.

4. Start the **file transfer** (receive) operation in the terminal program with Kermit protocol.

Other Menu Functions

The remaining menu options provide the following functions:

- **Logout** – Use to logout of switch.
- **Save Settings** – All settings in the configuration process will take effect immediately. But, they will be lost once the power is turned off. To save them, use this function to save the settings to the flash chip.
- **Restore Default Settings** – Use this function to return to the factory default settings. This option clears current settings. After restoring the default settings, the switch will reboot.
- **Reboot** – Use this function to reboot the switch.

8.0 Use Web Browser to Configure 2600M

The 2600M provides a web-browser interface for configuration/ management purposes. Once the IP address of the switch has been assigned through the console interface, you can connect to the switch with your web-browser for configuration or management. Refer to the section: **Using DHCP to Set the IP Address of the Switch**. You must have your password to log into the switch from the Web. Web access provides the same features as connection through the console or Telnet, however, the menu options are slightly different.

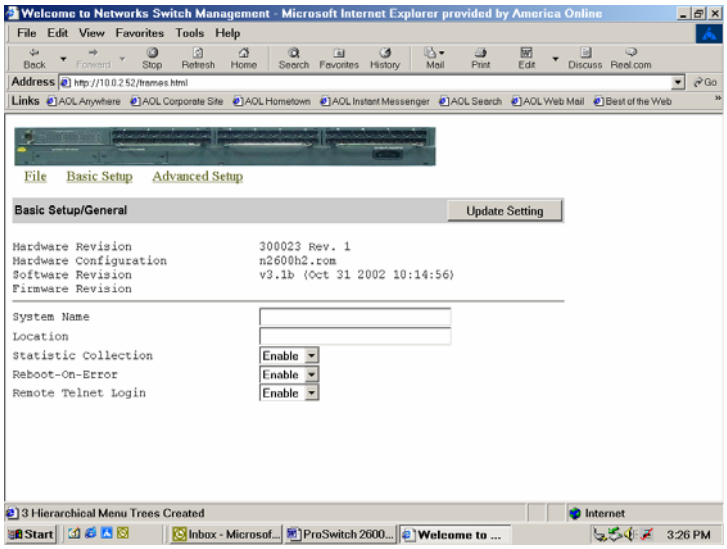
Logging into the 2600M

Follow these steps to use the load the management software from your web browser.

1. Load your **web browser**. (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 that you have set for the 2600M. There is no default IP for the 2600M.) The login screen will be displayed.
3. Input the password. The default password is **123456** for **admin**.

Note: You may change the password once your log into the switch.

4. The homepage of the 2600M will be displayed.



Performing Basic Management Activities

You can perform basic configuration/management with the **Basic Setup** button on the homepage. This function is very similar to the **Basic Management** function in the console interface. Refer to **Section 5.2** for the details of basic management.

Performing Advanced Management Activities

You can perform advanced configuration/management with the **Advanced Setup** button on the homepage. This function is very similar to the **Advanced Management** function in the console interface. Refer to **Section 6.0** for advanced management details.

File Transfer, Reboot, Logout and Save Setting

All of these functions can be done from the **File** button. Complete the operation step by step in the web-browser. These functions are very similar to those in the console interface. Refer to **Section 7.0** for the details of these functions.

9.0 Using Telnet

The 2600M provides access to the switch through Telnet for configuration/ management purposes. Once the IP address of the switch has been assigned through the console interface, you can connect to the switch with Telnet from any workstation on your LAN. Refer to the section: **Using DHCP to Set the IP Address of the Switch**.

The management functions will look the same and operate the same as they did from the Console screen. You must have your password to log into the switch.

1. Click on **Start**. - **Run**.
2. Type **cmd** and click **ok**.
3. Type **telnet** and press **Enter**.
4. Type **open** and the **IP address of the switch**.
5. Press **Enter**.
6. You must login with the user ID and password.
7. When you are finished using the management functions, logout from the **Switch Management** menu.
8. Once you have logged out, you will return to the **Command** screen. Type **quit** to exit Telnet.
9. Close the window to return to your desktop.

10.0 SNMP and RMON Management

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 RFC1757, which defines how networks can be monitored remotely.

RMONs typically consist of two components:

- **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 2600M 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.

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 2600M supports a complete implementation of SNMP Agent and MIB-2.

RMON MIB (RFC1757) and Bridge MIB (RFC1493)

The 2600M 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.

RMON Group Supported

The 2600M 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.

Bridge Group Supported

The 2600M 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.

11.0 Troubleshooting

All Waters' switching products are designed to provide reliability and consistently high performance in all network environments. The installation of Waters' ProSwitch®- 2600M switch is a straightforward procedure discussed in Section 3; the operation is also straightforward and is discussed in Section 4.

Should problems develop during installation or operation, this section is intended to help locate, identify and correct these types of problems. Please follow the suggestions listed below prior to contacting your supplier. However, if you are unsure of the procedures described in this section or if the ProSwitch®- 2600M switch is not performing as expected, do not attempt to repair the unit; instead contact your supplier for assistance or contact Waters Network Systems' Customer Support Center at **800.328.2275** or email carolynl@watersnet.com.

11.1 Before Calling for Assistance

1. If difficulty is encountered when installing or operating the unit, refer back to the Installation Section of the chapter of this manual. Also check to make sure that the various components of the network are inter-operable.
2. Check the cables and connectors to ensure that they have been properly connected and the cables/wires have not been crimped or in some way impaired during installation. (About 90% of network downtime can be attributed to wiring and connector problems.)
3. Make sure that an AC power cord is properly attached to the 2600M.
4. Be certain that each AC power cord is plugged into a functioning electrical outlet. Use the PWR LEDs to verify each unit is receiving power.
5. If the problem is isolated to a network device other than the Waters' ProSwitch®- 2600M switch, it is recommended that the problem device be replaced with a known good device. Verify whether or not the problem is corrected. If not, go to next step. If the problem is corrected, the Waters' ProSwitch®-2600M switch and its associated cables are functioning properly.
6. If the problem continues, contact Waters Network Systems Customer Service at 800.328.2275 or email carolynl@watersnet.com for assistance.

When Calling for Assistance

1. Please be prepared to provide the following information.
2. A complete description of the problem, including the following points:
3. The nature and duration of the problem
4. Situations when the problem occurs
5. The components involved in the problem
6. Any particular application that, when used, appears to create the problem
7. An accurate list of Waters Network Systems product model(s) involved. Include the date(s) that you purchased the products from your supplier.
8. It is useful to include other network equipment models and related hardware, including personal computers, workstations, terminals and printers; plus, the various network media types being used.
9. A record of changes that have been made to your network configuration prior to the occurrence of the problem. Any changes to system administration procedures should all be noted in this record.

11.2 Return Material Authorization (RMA) Procedure

All returns for repair must be accompanied by a Return Material Authorization (RMA) number. To obtain an RMA number, call Waters Network Systems Customer Service at 800.328.2275 during business hours from 8:00 am to 5:00 pm (CT) email carolynl@watersnet.com. When calling, please have the following information readily available:

- Name and phone number of your contact person
- Name of your company/institution
- Your shipping address
- Product name
- Packing List Number (or Sales Order Number)
- Failure symptoms, including a full description of the problem
- Waters Network Systems will carefully test and evaluate all returned products, will repair products that are under warranty at no charge, and will return the warranty-repaired units to the sender with shipping charges prepaid (see Warranty Information, Appendix A, for complete details). However, if Waters cannot duplicate the problem or condition causing the return, the unit will be returned as: **No Problem Found**.
- Waters Network Systems reserves the right to charge for the testing of non-defective units under warranty. Testing and repair of product that is not under warranty will result in a customer (user) charge.

11.3 Shipping and Packaging Information

Should you need to ship the unit back to Waters Network Systems, please follow these instructions: Package the unit carefully. It is recommended that you use the original container if available. Units should be wrapped in a "bubble-wrap" plastic sheet or bag for shipping protection. (You may retain all connectors and this Installation Guide.) CAUTION: Do not pack the unit in Styrofoam "popcorn" type packing material. This material may cause electro-static shock damage to the unit.

Clearly mark the Return Material Authorization (RMA) number on the outside of the shipping container. Waters Network Systems is not responsible for your return shipping charges.

Ship the package to:

Waters Network Systems

Attention: Customer Service

RMA Number:

945 37th Avenue, NW

Rochester, MN 55901

11.4 Warranty

Waters Network Systems'

Warranty Statement

Waters Network Systems' products are warranted against defects in materials and workmanship. The warranty period for each product will be provided upon request at the time of purchase. Unless otherwise stated, the warranty period is for the useable life of the product.

In the event of a malfunction or other indication of product failure attributable directly to faulty materials and/or workmanship, Waters Network Systems will, at its option, repair or replace the defective products or components at no additional charge as set for herein. This limited warranty does not include service to repair damage resulting from accident, disaster, misuse, neglect, lightning, acts of God, tampering or product modification.

Service under the warranty may be obtained by contacting Waters Network Systems and receiving a Return Material Authorization (RMA) number from Waters Network Systems. Returned product accompanied with the issued RMA number and prepaid shipping will be repaired or replaced by Waters Network Systems. Repaired or replaced products will be returned at no cost to the original Buyer and shipped via the carrier and method of delivery chosen by Waters Network Systems.

Specific warranty by product family is as follows:

ProSwitch-Secure:	Limited Lifetime (see note)
ProSwitch-SecureAir+:	Limited Lifetime
ProSwitch-Lite:	3 Years from date of manufacture (see note)
ProSwitch-Xpress:	Limited Lifetime
ProSwitch-Xtreme:	Limited Lifetime (see note)
ProSwitch-FlexPort:	Limited Lifetime
ProSwitch-FixPort:	Limited Lifetime
ProSwitch-CS and CSX:	3 Years from date of manufacture (see note)
ProMedia Converters	3 Years from date of manufacture (see note)

Note: Warranty period for any and all external power supplies is one (1) year from date of purchase.

EXCEPT FOR THE EXPRESS WARRANTY SET FORTH ABOVE, *WATERS NETWORK SYSTEMS* GRANTS NO OTHER WARRANTIES, EXPRESSED OR IMPLIED, BY STATUTE OR OTHERWISE, REGARDING THE PRODUCTS, THEIR FITNESS FOR ANY PURPOSE, THEIR QUALITY, THEIR MERCHANTABILITY, OR OTHERWISE.

WATERS NETWORK SYSTEMS' LIABILITY UNDER THE WARRANTY SHALL BE LIMITED TO PRODUCT REPAIR, OR REPLACEMENT OF THE BUYER'S PURCHASE PRICE. IN NO EVENT SHALL *WATERS NETWORK SYSTEMS* BE LIABLE FOR THE COST OF PROCUREMENT OF SUBSTITUTE GOODS BY THE CUSTOMER OR FOR ANY CONSEQENTIAL OR INCIDENTAL DAMAGES FOR BREACH OR WARRANTY.