

**LevelOne**

**GSW-2600TXM**

**Intelligent Switch**

**User's Guide**

Multilayer 24-Port Intelligent  
Fast Ethernet Switch with 24 10BASE-T / 100BASE-TX (RJ-45) Ports,  
and 2 Slots for Optional Gigabit Uplink Modules (RJ-45 / FIBER)

## Before Using this Manual:

This manual is suitable for the user of the management or intelligent switch. There are some shadow parts remarking in this manual, meaning only the display of the intelligent switch.

Note: Intelligent switch can work in Layer 2 mode or Multilayer mode, but Management switch only works in layer 2 mode.

**LevelOne GSW-2600TXM should be treated as an intelligent switch.**

Pls follow all the instruction of intelligent switch for configuring LevelOne GSW-2600TXM, 24-port 10/100Mbps + 2-slide in Layer3 Switch.

# Table Of Contents

1. Switch Management.....	9
1.1. Configuration Options .....	9
1.2. Required Connections.....	9
1.2.1. Console Port (Out-of-Band) Connections.....	9
1.2.2. Remote Management Via the Console Port.....	10
1.2.2.1. Configuring the Switch Site .....	10
1.2.2.2. Configuring the Remote Site .....	10
1.2.3. In-Band Connections.....	10
2. Console Interface .....	12
2.1. Log-in Screen.....	12
2.2. Main Menu .....	14
2.3. System Information Menu .....	16
2.3.1. Displaying System Information.....	16
2.3.2. Displaying Switch Version Information .....	17
2.4. Management Setup Menu .....	17
2.4.1. Changing the Network Configuration .....	18
2.4.1.1. IP Configuration (Layer 2 Mode).....	19
2.4.1.2. IP Connectivity Test (Ping).....	21
2.4.1.3. HTTP Configuration .....	21
2.4.2. Configuring the Serial Port.....	22
2.4.3. Assigning SNMP Parameters.....	23
2.4.3.1. Configuring Community Names .....	24

2.4.3.2. Configuring IP Trap Managers .....	24
2.4.4. User Log-in Configuration .....	25
2.4.5. Downloading System Software .....	27
2.4.6. Saving or Restoring the System Configuration .....	28
2.5. Device Control Menu.....	29
2.5.1. Setting the System Operation Mode .....	30
2.5.2. Layer 2 Menu .....	30
2.5.2.1. Configuring Port Parameters.....	31
2.5.2.2. Using a Mirror Port for Analysis.....	34
2.5.2.3. Configuring Port Trunks .....	35
2.5.2.4. Configuring the Static Unicast Address Table.....	37
2.5.2.5. Configuring the Static Multicast Address Table .....	38
2.5.3. Using the Bridge Menu.....	39
2.5.3.1. Configuring Global Bridge Settings.....	39
2.5.3.2. Configuring STA for Ports.....	41
2.5.4. Configuring Virtual LANs.....	43
2.5.4.1. VLAN Port Configuration.....	43
2.5.4.2. VLAN Table Configuration.....	46
2.5.5. Configuring IGMP Snooping .....	47
2.5.6. Configuring IP Settings .....	48
2.5.6.1. Subnet Configuration .....	49
2.5.6.2. Protocol Configuration .....	57
2.5.6.3. Static ARP Configuration.....	68
2.5.6.4. Static Route Configuration .....	68
2.5.6.5. Configuring the Default Route.....	70
2.5.7. Configuring Security Filters .....	71
2.5.7.1. Configuring MAC Address Filters .....	71
2.5.7.2. Configuring Security Mode.....	72
2.5.7.3. Configuring IP Address Filters.....	73
2.6. Monitoring the Switch.....	73
2.6.1. Displaying Port Statistics.....	74
2.6.1.1. Displaying Ethernet Port Statistics .....	75
2.6.1.2. Displaying RMON Statistics .....	78
2.6.2. Layer 2 Address Table.....	79
2.6.2.1. Displaying the Unicast Address Table .....	80
2.6.3. Displaying Bridge Information .....	81
2.6.3.1. Viewing the Current Spanning Tree Information.....	81
2.6.3.2. Displaying the Current STA for Ports .....	83

2.6.4. Displaying VLAN Information .....	84
2.6.4.1. VLAN Dynamic Registration Information.....	85
2.6.4.2. VLAN Forwarding Information.....	86
2.6.5. IP Multicast Registration Table .....	86
2.6.6. IP Menu.....	87
2.6.6.1. Displaying Subnet Information .....	88
2.6.6.2. ARP Table .....	89
2.6.6.3. Routing Table .....	90
2.6.6.4. Multicast Table .....	92
2.6.6.5. OSPF Table.....	97
2.7. Resetting the System .....	104
2.8. Logging Off the System.....	105
3. Web Interface .....	106
3.1. Web-Based Configuration and Monitoring.....	106
3.2. Navigating the Web Browser Interface .....	108
3.2.1. Home Page .....	108
3.2.2. Configuration Options .....	108
3.2.3. Panel Display .....	109
3.2.4. Port State Display.....	109
3.2.5. Configuring the Serial Port .....	110
3.3. Main Menu .....	111
3.4. System Information Menu .....	113
3.4.1. Displaying System Information.....	113
3.4.2. Displaying Switch Version Information .....	114
3.5. Management Setup Menu .....	114
3.5.1. Changing the Network Configuration (Layer 2 Mode) .....	115
3.5.2. Assigning SNMP Parameters.....	116
3.5.2.1. Configuring Community Names .....	116
3.5.2.2. Configuring IP Trap Managers .....	117
3.5.3. User Login Configuration .....	117
3.5.4. Downloading System Software .....	118
3.5.5. Saving or Restoring the System Configuration .....	119
3.6. Device Control Menu.....	119
3.6.1. Setting the System Operation Mode .....	120
3.6.2. Layer 2 Menu .....	121
3.6.2.1. Configuring Port Parameters.....	121
3.6.2.2. Using a Port Mirror for Analysis.....	123
3.6.2.3. Configuring Port Trunks .....	124

3.6.2.4. Static Unicast Address Table.....	126
3.6.2.5. Configuring the Static Multicast Address Table .....	126
3.6.3. Using the Bridge Menu.....	127
3.6.3.1. Configuring Global Bridge Settings.....	128
3.6.3.2. Configuring STA for Ports.....	130
3.6.4. Configuring Virtual LANs.....	131
3.6.4.1. VLAN Port Configuration.....	131
3.6.4.2. VLAN Table Configuration.....	134
3.6.5. Configuring IGMP Snooping .....	135
3.6.6. Configuring IP Settings .....	136
3.6.6.1. Subnet Configuration .....	136
3.6.6.2. Protocol Configuration .....	141
3.6.6.3. Static ARP Configuration.....	148
3.6.6.4. Static Route Configuration .....	149
3.6.6.5. Configuring the Default Route.....	150
3.6.7. Configuring Security Filters .....	150
3.6.7.1. Configuring MAC Address Filters .....	150
3.6.7.2. Configuring IP Address Filters.....	151
3.6.7.3. Configuring Security Mode.....	151
3.7. Monitoring the Switch.....	152
3.7.1. Displaying Port Statistics.....	152
3.7.1.1. Displaying Ethernet Port Statistics .....	153
3.7.1.2. Displaying RMON Statistics .....	155
3.7.2. Layer 2 Address Table.....	156
3.7.2.1. Displaying the Unicast Address Table .....	156
3.7.3. Displaying Bridge Information .....	157
3.7.3.1. Viewing the Current Spanning Tree Information.....	157
3.7.3.2. Displaying the Current STA for Ports .....	158
3.7.4. Displaying VLAN Information .....	159
3.7.4.1. VLAN Dynamic Registration Information.....	159
3.7.4.2. VLAN Forwarding Information.....	160
3.7.5. IP Multicast Registration Table .....	160
3.7.6. IP Menu.....	160
3.7.6.1. Displaying Subnet Information .....	161
3.7.6.2. ARP Table .....	161
3.7.6.3. Routing Table .....	162
3.7.6.4. Multicast Table .....	163
3.7.6.5. OSPF Table.....	165

3.8. Resetting the System .....	170
4. Chapter 4: Advanced Topics.....	172
4.1. Layer 2 Switching.....	172
4.1.1. Unicast Switching.....	172
4.1.2. Multicast Switching.....	173
4.1.3. Spanning Tree Algorithm .....	173
4.2. Layer 3 Switching.....	175
4.2.1. Initial Configuration .....	175
4.2.2. IP Switching .....	176
4.2.3. Routing Path Management .....	177
4.2.4. ICMP Router Discovery.....	177
4.2.5. Proxy ARP.....	178
4.2.6. Routing Protocols.....	178
4.2.6.1. RIP and RIP-2 Dynamic Routing Protocols.....	178
4.2.6.2. OSPFv2 Dynamic Routing Protocol .....	179
4.2.7. Non-IP Protocol Routing .....	182
4.3. Virtual LANs .....	182
4.3.1. Assigning Ports to VLANs .....	183
4.3.1.1. VLAN Classification .....	183
4.3.1.2. Port Overlapping .....	184
4.3.1.3. Port-based VLANs .....	184
4.3.1.4. Automatic VLAN Registration (GVRP) .....	184
4.3.2. Forwarding Tagged / Untagged Frames.....	184
4.3.3. Connecting VLAN Groups.....	185
4.4. Multicast Filtering .....	186
4.4.1. IGMP Snooping.....	186
4.4.2. IGMP Protocol.....	187
4.4.3. GMRP Protocol .....	187
4.4.4. DVMRP Routing Protocol.....	188
4.5. Class-of-Service (CoS) Support .....	188
4.6. BOOTP / DHCP Relay .....	188
4.7. Security Features .....	189
4.7.1. SNMP Community Strings.....	189
4.7.2. User Name and Passwords .....	190
4.7.3. MAC Address Filters .....	190
4.7.4. IP Address Filters .....	190
4.8. SNMP Management Software.....	190
4.9. Remote Monitoring (RMON).....	190

5. Appendix A: Troubleshooting .....	192
5.1. Troubleshooting Chart .....	192
5.2. Upgrading Firmware via the Serial Port .....	192
6. Appendix B: Pin Assignments .....	195
6.1. Console Port Pin Assignments .....	195
6.1.1. DB-9 Port Pin Assignments .....	195
6.1.2. Console Port to 9-Pin COM Port on PC .....	196
6.1.3. Console Port to 25-Pin DCE Port on Modem .....	196
6.1.4. Console Port to 25-Pin DTE Port on PC .....	196
7. Glossary .....	197
7.1.1. Bandwidth Utilization .....	197
7.1.2. BOOTP .....	197
7.1.3. Distance Vector Multicast Routing Protocol (DVMRP) .....	197
7.1.4. GARP VLAN Registration Protocol (GVRP) .....	197
7.1.5. Generic Attribute Registration Protocol (GARP) .....	197
7.1.6. Group Attribute Registration Protocol .....	197
7.1.7. Generic Multicast Registration Protocol (GMRP) .....	197
7.1.8. ICMP Router Discovery .....	197
7.1.9. Internet Control Message Protocol (ICMP) .....	198
7.1.10. IEEE 802.1D .....	198
7.1.11. IEEE 802.1Q .....	198
7.1.12. IEEE 802.3ac .....	198
7.1.13. Internet Group Management Protocol (IGMP) .....	198
7.1.14. IGMP Snooping .....	198
7.1.15. In-Band Management .....	198
7.1.16. IP Multicast Filtering .....	198
7.1.17. Layer 2 .....	198
7.1.18. Layer 3 .....	199
7.1.19. Link Aggregation .....	199
7.1.20. Management Information Base (MIB) .....	199
7.1.21. Multicast Switching .....	199
7.1.22. Open Shortest Path First (OSPF) .....	199
7.1.23. Out-of-Band Management .....	199
7.1.24. Port Mirroring .....	199
7.1.25. Port Trunk .....	199
7.1.26. Remote Monitoring (RMON) .....	199
7.1.27. Routing Information Protocol (RIP) .....	200
7.1.28. Simple Network Management Protocol (SNMP) .....	200

7.1.29. Spanning Tree Protocol (STP) .....	200
7.1.30. Telnet .....	200
7.1.31. Trivial File Transfer Protocol (TFTP) .....	200
7.1.32. Virtual LAN (VLAN) .....	200
7.1.33. XModem.....	200

# 1. Switch Management

## 1.1. Configuration Options

For advanced management capability, the onboard management agent provides a menu-driven system configuration program. This program can be accessed by a direct or modem connection to the serial port on the rear panel (out-of-band), or by a Telnet connection over the network (in-band).

The management agent is based on SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any PC in the network using in-band management software.

The management agent also includes an embedded HTTP Web agent. This Web agent can be accessed using a standard Web browser from any computer attached to the network.

The system configuration program and the SNMP agent support management functions such as:

- Enable / disable any port.
- Set the communication mode for any port.
- Configure SNMP parameters.
- Add ports to network VLANs.
- Configure IP routing and multicast VLANs.
- Display system information or statistics.
- Configure the switch to join a Spanning Tree.
- Download system firmware.

## 1.2. Required Connections

### 1.2.1. Console Port (Out-of-Band) Connections

Attach a VT100 compatible terminal or a PC running a terminal emulation program to the serial port on the switch's rear panel. Use the null-modem cable provided with this package, or use a null-modem connection that complies with the wiring assignments shown in Appendix B of this guide.

When attaching to a PC, set terminal emulation type to VT100, specify the port used by your PC (i.e., COM 1~4), and then set communications to 8 data bits, 1 stop bit, no parity, and 19200 bps (for initial configuration). Also be sure to set flow control to "none." (Refer to "Configuring the Serial Port" on chapter 2 for a complete description of configuration options.)

**Note:**

If the default settings for the management agent's serial port have been modified and you are having difficulty making a console connection, you can display or modify the current settings using a Web browser as described under "Configuring the Serial Port" on chapter 3.

## 1.2.2.Remote Management Via the Console Port

### 1.2.2.1.Configuring the Switch Site

Connect the switch's DB9 serial port to the modem's serial port uses standard cabling. For most modems which use a 25-pin port, you will have to provide an RS-232 cable with a 9-pin connector on one end and a 25-pin connector on the other end. Set the modem at the switch's site to force auto-answer mode. The following is a sample initialization string: "ATQ1S0=1&D0&K0&W" as defined below:

Q1 : Inhibit result codes to DTE  
S0=1 : Auto answer on first ring  
D0 : Don't care DTR  
K0 : Disables DTE / DCE flow control  
W : Write command to modem memory

### 1.2.2.2.Configuring the Remote Site

At the remote site, connect the PC's COM port (COM 1~4) to the modem's serial port. Set terminal emulation type to VT100, specify the port used by your PC (i.e., COM 1~4), and then set communications to 8 data bits, 1 stop bit, no parity, 19200 bps, and no flow control.

## 1.2.3.In-Band Connections

Prior to accessing the switch's onboard agent via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway (for Layer 2 mode) using an out-of-band connection or the BOOTP protocol.

After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere within the attached network. The onboard configuration program can be accessed using Telnet from any computer attached to the network. The switch can also be managed by any computer using a Web browser (Internet Explorer 4.0 or above, or Netscape Navigator 4.0 or above), or from a network computer using network management software.

### Notes:

1. By default BOOTP is disabled. To enable BOOTP, see "IP Configuration (Layer 2 Mode)" on chapter 2.

2. Each VLAN group can be assigned its own IP interface address (chapter 2 “IP Configuration (Layer 2 Mode)”). Therefore, if the port connected to the management station has joined several VLANs, you can manage the switch via any of these IP addresses.
3. This switch supports four concurrent Telnet sessions.
4. The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP- based network management software.

## 2. Console Interface

### 2.1. Log-in Screen

Once a direct connection to the serial port or a Telnet connection is established, the log-in screen for the onboard configuration program appears as shown below.

```
V1.00          10-19-2001 (c) Copyright communications Corp.
                Intelligent Switch1
                User Name:
                Password :
```

1. For Management Model, it will display “Management Switch”.

If this is your first time to log into the configuration program, then the default user names are “admin” and “guest,” with no password. The administrator has Read / Write access to all configuration parameters and statistics, while the guest has Read Only access to the management program.

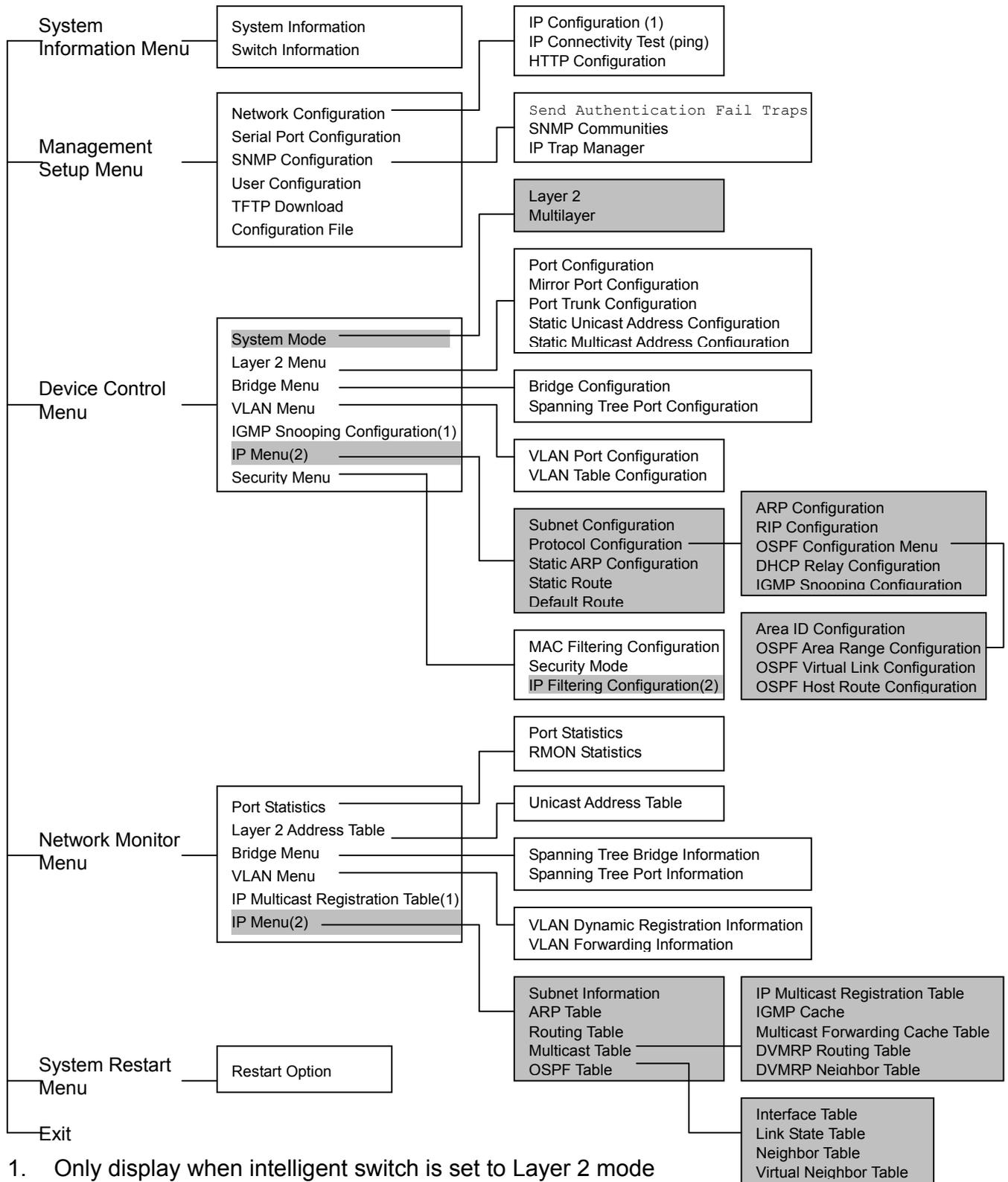
You should define a new administrator password, record it and put it in a safe place.

Select User Configuration from the Management Setup Menu and enter a new password for the administrator. Note that passwords can consist of up to 15 alphanumeric characters and are not case sensitive.

**Note:**

You are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

After you enter the user name and password, you will have access to the system configuration program illustrated by the following menu map:



1. Only display when intelligent switch is set to Layer 2 mode or the switch is management model.
2. Only display when intelligent switch is set to multilayer mode.

## 2.2.Main Menu

With the system configuration program you can define system parameters, manage and control the switch and all its ports, or monitor network conditions. The screen below of the Main Menu and the table following it briefly describe the selections available from this program.

**Note:**

Options for the currently selected item are displayed in the highlighted area at the bottom of the interface screen.

```

Intelligent Layer3 Switch1
Multilayer Mode*

Main Menu
=====

System Information Menu...
Management Setup Menu...
Device Control Menu...
Network Monitor Menu...
System Restart Menu...
Exit

Display or change system information.
Use <TAB> or arrow keys to move. <Enter> to select.

```

1.For Management Model, it will display “Management Switch”.

\*.The operation mode is only display on intelligent switch.

Menu	Description
(Operation Mode) <sup>3</sup>	The text string in the top right corner of the screen shows if the switch is operating as a Layer 2 switch or as a multilayer routing switch. (See chapter 2 “setting the system operation mode”.)
<i>System Information Menu</i>	
System Information	Provides basic system description, including contact information.
Switch Information	Shows hardware / firmware version numbers, power status, and expansion modules used in the switch.
<i>Management Setup Menu</i>	
Network Configuration	Includes IP setup <sup>1</sup> , Ping facility, and HTTP (Web agent) setup.
Serial Port Configuration	Sets communication parameters for the serial port, including baud rate, console timeout, and screen data refresh interval.

SNMP Configuration	Activates authentication failure traps; configures community access strings, and trap managers.
User Configuration	Sets the user names and passwords for system access.
TFTP Download	Downloads new version of firmware to update your system (in-band).
Configuration File	Saves or restores configuration data based on the specified file.
<i>Device Control Menu</i>	
System Mode <sup>3</sup>	Sets the switch to operate as a Layer 2 switch or as a multilayer routing switch.
Layer 2 Menu	Configures port communication mode, mirror ports, port trunking, and static addresses.
Bridge Menu	Configures GMRP and GVRP for the bridge, as well as Spanning Tree settings for the global bridge or for specific ports.
VLAN Menu	Configures VLAN settings for specific ports, and defines the port membership for VLAN groups.
IGMP Snooping Configuration <sup>1</sup>	Configures IGMP multicast filtering.
IP Menu <sup>2</sup>	Configures the subnets for each VLAN group, global configuration for ARP and ARP proxy, unicast and multicast protocols, BOOTP / DHCP relay, static ARP table entries, static routes and the default route.
Security Menu	Configures MAC and IP address filtering. And configures the learning function and Uplink port.
<i>Network Monitor Menu</i>	
Port Statistics	Displays statistics on port traffic, including information from the Interfaces Group, Ethernet-like MIB, and RMON MIB.
Layer 2 Address Table	Contains the unicast address table.
Bridge Menu	Displays Spanning Tree information for the overall bridge and for specified ports.
VLAN Menu	Displays dynamic port registration information for VLANs as well as VLAN forwarding information for static and dynamic assignment.
IP Multicast Registration Table <sup>1</sup>	Displays all the multicast groups active on this switch, including the multicast IP addresses and corresponding VLANs.
IP Menu <sup>2</sup>	Displays all the IP subnets used on this switch, as well as the corresponding VLANs and ports. Also contains the ARP table, routing table, multicast table, and OSPF table.
Restart System	Restarts the system with options to restore factory defaults.
Exit	Exits the configuration program.

1. Only display when intelligent switch is set to Layer 2 mode or the switch is management model.
2. Only display when intelligent switch is set to multilayer mode.

3. Only displayed in intelligent switch.

## 2.3. System Information Menu

Use the System Information Menu to display a basic description of the switch, including contact information, and hardware / firmware versions.

```

System Information Menu
=====

System Information ...

Switch Information ...

                                <OK>
Display System Information.
Use <TAB> or arrow keys to move. <Enter> to select.

```

Menu	Description
System Information	Provides basic system description, including contact information.
Switch Information	Shows hardware / firmware version numbers, power status, and expansion modules used in the switch.

### 2.3.1. Displaying System Information

Use the System Information screen to display descriptive information about the switch, or for quick system identification as shown in the following screen and table.

```

System Information
=====

System Description      : Intelligent Switch
System Object ID       : 1.3.6.1.4.1
System Up Time         : 580430 (0 day 1 hr 36 min 44 sec)
System Name            :
System Contact         :
System Location        :

                                <Apply>                <OK>                <Cancel>
                                The name of this system.

| READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
System Description	System hardware description.
System Object ID	MIB II object identifier for switch's network management subsystem.
System Up Time	Length of time the current management agent has been running. (Note that the first value is in centiseconds.)
System Name*	Name assigned to the switch system.
System Contact*	Contact person for the system.
System Location*	Specifies the area or location where the system resides.

\* Maximum string length is 99, but the screen only displays 45 characters. You can use the arrow keys to browse the whole string.

## 2.3.2. Displaying Switch Version Information

Use the Switch Information screen to display hardware / firmware version numbers for the main board, as well as the power status.

Switch Information =====	
Hardware Version	: R01
Firmware Version	: V1.00
Serial Number	: 00-E8-00-34-00-00
Port Number	: 26
Internal Power Status	: Active
Expansion Slot 1	: 1GBASE-T
Expansion Slot 2	: 1GBASE-T
<OK> Return to previous panel. Use <Enter> to select.	

Parameter	Description
Hardware Version	Hardware version of the main board.
Firmware Version	System firmware version in ROM.
Serial Number	The serial number of the main board.
Port Number	Number of ports on this switch.
Internal Power Status	Shows if primary power is active or inactive.
Expansion Slot 1	Shows module type if inserted: 1GBase-SX/LX : 1000BASE-SX/LX (multimode/ single mode) 1GBase-T : 1000BASE-T

## 2.4. Management Setup Menu

After initially logging on to the system, adjust the communication parameters for your

console to ensure a reliable connection (Serial Port Configuration). Specify the IP addresses for the switch (Network Configuration / IP Configuration), and then set the Administrator and User passwords (User Configuration). Remember to record them in a safe place. Also set the community string which controls access to the onboard SNMP agent via in-band management software (SNMP Configuration). The items provided by the Management Setup Menu are described in the following sections.

```

Management Setup Menu
=====

Network Configuration ...
Serial Port Configuration ...
SNMP Configuration ...
User Configuration ...
TFTP Download ...
Configuration File

                                <OK>
Display or change network configuration.
Use <TAB> or arrow keys to move. <Enter> to select.

```

Menu	Description
Network Configuration	Includes IP setup, Ping facility, and HTTP setup for the onboard Web agent.
Serial Port Configuration	Sets communication parameters for the serial port, including baud rate, console timeout, and screen data refresh interval.
SNMP Configuration	Activates authentication failure traps and configures communities and trap managers.
User Configuration	Sets the user names and passwords for system access.
TFTP Download	Downloads new version of firmware to update your system (in-band).
Configuration File	Saves or restores configuration data based on the specified file.

## 2.4.1.Changing the Network Configuration

Use the Network Configuration menu to set the bootup option, configure the switch's Internet Protocol (IP) parameters, or enable the onboard Web agent. The screen shown below is described in the following table.

```

Network Configuration
=====

IP Configuration ...

IP Connectivity Test (Ping) ...

HTTP Configuration ...

                                <OK>
Display or change the IP configuration.
Use <TAB> or arrow keys to move. <Enter> to select.

```

Parameter	Description
IP Configuration*	Screen used to set the bootup option, or configure the switch's IP parameters.
IP Connectivity Test (Ping)	Screen used to test IP connectivity to a specified device.
HTTP Configuration	Screen used to enable the Web agent.

\* This menu does not appear if the switch is set to multilayer mode. In this case, you need to configure an IP interface for each VLAN that needs to connect to any device outside of its own VLAN group. (See "Subnet Configuration" on chapter 2.)

### 2.4.1.1.IP Configuration (Layer 2 Mode)

Use the IP Configuration screen to set the bootup option, or configure the switch's IP parameters. The screen shown below is described in the following table.

```

IP Configuration
=====

Interface Type : Ethernet
IP Address   : 192.168.1.254
Subnet Mask  : 255.255.255.0
Gateway IP   : 0.0.0.0
IP State     : USER-CONFIG

Mgt. Access : All

VLANs

<Apply>           <OK>           <Cancel>
IP address of this system for Ethernet. |
READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
Interface Type	Indicates IP over Ethernet.
IP Address	IP address of the switch you are managing. The system supports SNMP over UDP / IP transport protocol. In this environment, all systems on the Internet such as network interconnection devices and any PC accessing the agent module (or running network management software) must have an IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the configuration program.
Subnet Mask	Subnet mask of the switch. This mask identifies the host address bits used for routing to specific subnets.
Default Gateway	Gateway used to pass trap messages from the system's agent to the management station. Note that the gateway must be defined (when operating at Layer 2) if the management station is located in a different IP segment.
IP State	Specifies whether IP functionality is enabled via manual configuration, or set by Boot Protocol (BOOTP). Options include: USER-CONFIG IP functionality is enabled based on the default or user specified IP Configuration. (This is the default setting.) BOOTP Get IP IP is enabled but will not function until a BOOTP reply has been received. BOOTP requests will be broadcast periodically by the switch in an effort to learn its IP address. (BOOTP values can include the IP address, default gateway, and subnet mask.)
Mgt. Access	Allows management access of the switch from all VLANs or only

	from a specified VLAN. If you select “Mgmt VLAN,” then select Apply to display the VLAN ID field, select the required VLAN, and then select Apply or OK to save your changes.
--	---

### 2.4.1.2.IP Connectivity Test (Ping)

Use the IP Connectivity Test to see if another site on the Internet can be reached. The screen shown below is described in the following table.

```

Network Configuration: IP Connectivity Test (Ping)
=====
IP Address : 0.0.0.0
Test Times : 0
Success    : 0          Failure : 0

                [Start]                <CANCEL>
                IP address to test.      | READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
IP Address	IP address of the site you want to ping.
Test Times	The number of ICMP echo requests to send to the specified site. Range: 1~1000
Success / Failure	The number of times the specified site has responded (or not) to pinging.

**Note:**

The switch waits up to 10 seconds for a response to each ping.

### 2.4.1.3.HTTP Configuration

Use the HTTP Configuration screen to enable / disable the onboard Web agent.

```

Network Configuration: HTTP Configuration
=====

HTTP Server          : ENABLED

<Apply>              <OK>              <Cancel>
Administrative status of the HTTP server. | READ/SELECT
Use <TAB> or arrow keys to move, <Space> to scroll options.

```

**Note:**

Port 80 is used for HTTP service.

## 2.4.2. Configuring the Serial Port

You can access the onboard configuration program by attaching a VT100 compatible device to the switch’s serial port. (For more information on connecting to this port, see “Required Connections” on chapter 1.) The communication parameters for this port can be accessed from the Serial Port Configuration screen shown below and described in the following table.

```

Serial Port Configuration
=====

Management Mode      : CONSOLE MODE
Baud rate             : 19200
Data bits             : 8
Stop bits             : 1
Parity                : NONE
Time-Out (in minutes) : 0
Auto Refresh (in seconds) : 10

<Apply>              <OK>              <Cancel>
The connection mode of the serial port. |
READ/SELECT
Use <TAB> or arrow keys to move, <Space> to scroll options.

```

Parameter	Default	Description
Management Mode	Console Mode	Indicates that the port settings are for direct console connection.

Baud Rate	19200	The rate at which data is sent between devices. Options : 9600, 19200 and 38400 baud.
Data Bits	8 bits	Sets the data bits of the RS-232 port. Options : 7, 8
Stop Bits	1 bit	Sets the stop bits of the RS-232 port. Options : 1, 2
Parity	None	Sets the parity of the RS-232 port. Options : none, odd, even
Timeout	0 minutes	If no input is received from the attached device after this interval, the current session is automatically closed. Range : 0 - 100 minutes; where 0 indicates disabled
Auto Refresh	10 second	Sets the interval before a console session will auto-refresh the console information, such as Spanning Tree Information, Port Configuration, Port Statistics, and RMON Statistics. Range : 0-255 seconds; where 0 indicates disabled

### 2.4.3. Assigning SNMP Parameters

Use the SNMP Configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP). The switch includes an onboard SNMP agent which monitors the status of its hardware, as well as the traffic passing through its ports. A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the onboard agent are controlled by community strings. To communicate with the switch, the NMS must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following sections.

```

SNMP Configuration
=====

Send Authentication Fail Traps : ENABLED

SNMP Communities ...

IP Trap Manager ...

                                <OK>
Send a trap or not when SNMP authentication fails.      |
READ/SELECT
Use <TAB> or arrow keys to move, <Space> to scroll options.

```

Parameter	Description
Send Authentication Fail Traps	Issue a trap message to specified IP trap managers whenever authentication of an SNMP request fails. (The default is enabled.)
SNMP Communities	Assigns SNMP access based on specified strings.

IP Trap Managers	Specifies management stations that will receive authentication failure messages or other trap messages from the switch.
------------------	---

### 2.4.3.1. Configuring Community Names

The following figure and table describe how to configure the community strings authorized for management access. Up to 5 community names may be entered.

```

SNMP Configuration: SNMP Communities
=====

Community Name      Access      Status
1. public           READ/WRITE  ENABLED
2. private          READ ONLY   ENABLED
3.
4.
5.

<Apply>             <OK>             <Cancel>
The community name of entry 1. |
READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
Community Name	A community entry authorized for management access. Maximum string length: 19 characters
Access	Management access is restricted to Read Only or Read / Write.
Status	Sets administrative status of entry to enabled or disabled.

**Note:** The default community strings are displayed on the screen.

### 2.4.3.2. Configuring IP Trap Managers

The following figure and table describe how to specify management stations that will receive authentication failure messages or other trap messages from the switch. Up to 5 trap managers may be entered.

```

                                SNMP Configuration: IP Trap Manager
                                =====

                                IP Address           Community Name       Status
1.  192.168.1.254      public              ENABLED
2.  0.0.0.0
3.  0.0.0.0
4.  0.0.0.0
5.  0.0.0.0

                                <Apply>           <OK>
<Cancel>
                                The IP address of entry 1.      |
READ/WRITE
                                Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
IP Address	IP address of the trap manager.
Community Name	A community specified for trap management access.
Status	Sets administrative status of selected entry to enabled or disabled.

## 2.4.4. User Log-in Configuration

Use the User Configuration menu to restrict management access based on specified user names and passwords. There are two user types, Administrator and Guest. Only the Administrator has write access for parameters governing the SNMP agent. You should therefore assign a user name and password to the Administrator as soon as possible, and store it in a safe place. The parameters shown on this screen are indicated in the following figure and table.

```

                                User Configuration
                                =====
User Name      Access Right Console  Telnet
HTTP
  guest        GUEST           DISABLED  DISABLED
ENABLED
  admin       ADMIN           ENABLED   ENABLED
ENABLED

                                <Add>                <OK>
                                Return to previous panel.
Use <TAB> or arrow keys to move. <Enter> to select.

```

Parameter	Description
User Name	Specifies a user authorized management access to the switch via the console, Telnet or HTTP.
Access Right	ADMIN: Read / Write for all screens. GUEST: Read Only for all screens.
Console	Authorizes management via the console.
Telnet	Authorizes management via Telnet.
HTTP	Authorizes management via HTTP (i.e., a Web browser).

To add a new user, select <Add>. When you add a user, the following screen displays.

```

                                User Configuration: Add User
                                =====
User Name      :
Password       :
Access Right   : GUEST
Console Access : DISABLED
Telnet Access  : DISABLED
HTTP Access    : ENABLED

                                <OK>                <Cancel>
                                User name.
| READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
User Name*	Specifies a user authorized management access to the switch via

	the console, Telnet or HTTP.
Password*	Password associated with this entry.
Access Right	ADMIN: Read / Write for all screens. GUEST: Read Only for all screens.
Console Access	Authorizes management via the console.
Telnet Access	Authorizes management via Telnet.
HTTP Access	Authorizes management via HTTP (i.e., a Web browser).

\*These entries can consist of up to 15 alphanumeric characters and are not case sensitive.

## 2.4.5. Downloading System Software

Use the TFTP Download menu to load software updates to permanent flash ROM in the switch. The download file should be a correct binary file for the switch; otherwise the agent will not accept it. The success of the download operation depends on the accessibility of the TFTP server and the quality of the network connection. After downloading the new software, the agent will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table.

```

                                TFTP Download
                                =====

Download Server IP : 0.0.0.0
Download Filename  :
Download Option   : Runtime Code

                                <Apply>                <OK>                <Cancel>
                                IP address of the TFTP server.

| READ/WRITE
  Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
Download Server IP	IP address of a TFTP server.
Download Filename	The binary file to download.
Download Option	Runtime Code Post Code

### Note:

You can also download firmware using the Web agent (see "Downloading system software" on chapter 3) or by a direct console connection after a restart (see "Upgrading Firmware via the Serial Port" on Appendix A).

## 2.4.6. Saving or Restoring the System Configuration

Use the Configuration File menu to save the switch configuration settings to a file on a TFTP client. The file can be later downloaded to the switch to restore the switch's settings. The success of the operation depends on the accessibility of the TFTP client and the quality of the network connection. Parameters shown on this screen are indicated in the following figure and table.

```

Configuration File
=====

Station IP :0.0.0.0

Operation :Download from switch

<START>                                     <Cancel>
      IP address of the TFTP client.
READ/WRITE
      Use <TAB> or arrow keys to move, other keys to make changes.
  
```

Parameter	Description
Station IP	IP address of a PC running TFTP client software.
Operation	Download from switch – Downloads the current switch configuration to a file on the client PC. Upload to switch – Uploads a configuration file to the switch from the client PC.

**Note:**

Saving and restoring switch configuration settings can then be initiated by using any TFTP client utility, such as the command line utility included in Windows NT. For example, using Windows NT, from a DOS window command prompt, enter the TFTP command in the form:

TFTP [-i] host [GET : PUT] source [destination]

To transfer a file –

*Switch:* Specify the IP address of the TFTP client, and select “Download from switch” or “Upload from Switch.”

*TFTP Client:* Set the mode to <binary>, specify the IP address of the target switch and the directory path / name of the file to transfer.

*Switch:* Select <START> from the Configuration File menu.

*TFTP Client:* Start transferring the configuration file from the TFTP client or the switch, and wait until the transfer completes.

## 2.5.Device Control Menu

The Device Control menu is used to control a broad range of functions, including port mode, port mirroring, port trunking, Spanning Tree, Virtual LANs, IP subnets, multicast filtering, and routing protocols. Each of the setup screens provided by these configuration menus is described in the following sections.

Device Control Menu ===== System Mode ... Layer 2 Menu ... Bridge Menu ... VLAN Menu ... IGMP Snooping Configuration ... IP Menu ... Security Menu ...  <OK> Change system operation mode. Use <TAB> or arrow keys to move. <Enter> to select.
--

Menu	Description
System Mode <sup>3</sup>	Sets the switch to operate as a Layer 2 switch or as a multilayer routing switch.
Layer 2	Menu Configures port communication mode, mirror ports, and port trunking.
Bridge Menu	Configures the Spanning Tree Protocol for the bridge or for specific ports, GMRP and GVRP for automatic registration of multicast and VLAN groups, traffic class priority threshold, and address aging time.
VLAN Menu	Configures VLAN settings for specific ports, and defines the port membership for VLAN groups.
IGMP Snooping Configuration <sup>1</sup>	Configures IGMP multicast filtering.
IP Menu <sup>2</sup>	Configures the subnets for each VLAN group, global configuration for ARP and Proxy ARP, unicast and multicast protocols, static ARP table entries, static routes and the default route.
Security Menu	Configures MAC and IP <sup>2</sup> address filtering and set the autolearn function.

1. Only display when intelligent switch is set to Layer 2 mode or the switch is management model.
2. Only display when intelligent switch is set to multilayer mode. (Note that this menu

includes IGMP Snooping Configuration.)

3. Only displayed in intelligent switch.

## 2.5.1. Setting the System Operation Mode

This switch can be set to operate as a Layer 2 switch, making all filtering and forwarding decisions based strictly on MAC addresses. Or, it can be set to operate as a multilayer routing switch, whereby it switches packets for all non-IP protocols (such as NetBUEI, NetWare or AppleTalk) based on MAC addresses (see “Virtual LANs” on chapter 4), and routes all IP packets based on the specified routing protocol. The System Mode menu is shown below. Note that the switch will be automatically rebooted whenever the system operation mode is changed.

```
System Mode
=====

Layer 2
Multilayer

                <OK>
                Multilayer operation.
                Use <TAB> or arrow keys to move. <Enter> to select.
```

Parameter	Description
Layer 2	Filtering and forwarding decision will be based on MAC addresses for all protocol traffic.
Multilayer	Switching based on MAC addresses will be used for all non-IP protocol traffic, and routing will be used for all IP protocol traffic.

**Note:**

When the switch is set to multilayer mode, the IP menus are enabled, and the “IP Configuration (Layer 2 Mode)” menu on chapter 2 is disabled. When operating in multilayer mode, you should configure an IP interface for each VLAN that needs to communicate with any device outside of the VLAN. (See “Subnet Configuration” on chapter 2.)

## 2.5.2. Layer 2 Menu

The Layer 2 menu contains options for port configuration, port mirroring, port trunking, static unicast address configuration and static multicast address configuration. These menu options are described in the following sections.

```

Layer 2 Menu
=====
Port Configuration ...
Mirror Port Configuration ...
Port Trunking Configuration ...
Static Unicast Address Configuration ...
Static Multicast Address Configuration ...

<OK>
Change the system port configuration.
Use <TAB> or arrow keys to move. <Enter> to select.

```

Menu	Description
Port Configuration	Enables any port, enables / disables flow control, and sets communication mode to auto-negotiation, full duplex or half duplex.
Mirror Port Configuration	Sets the source and target ports for mirroring.
Port Trunking Configuration	Specifies ports to group into aggregate trunks.
Static Unicast Address Table	Used to manually configure host MAC addresses in the unicast table.
Static Multicast Address Table	Used to manually configure host MAC addresses in the multicast table.

### 2.5.2.1. Configuring Port Parameters

Use the Port Configuration menu to display or set communication parameters for any port or module on the switch, including administrative status, auto-negotiation, default communication speed and duplex mode, as well as flow control in use.

```

Layer 2 Menu: Port Configuration (Port 1-12)
=====
Port  Link      Admin      Auto      Default      Current      Flow
Jack  Status      Status      Negotiate  Type          Type          Control
Control Type
-----
  1    Off        ENABLED    ENABLED    10HDX        10HDX        Off
      RJ-45
  2    Off        ENABLED    ENABLED    10HDX        10HDX        Off
      RJ-45
  3    Off        ENABLED    ENABLED    10HDX        10HDX        Off
      RJ-45
  4    Off        ENABLED    ENABLED    10HDX        10HDX        Off
      RJ-45
  5    Off        ENABLED    ENABLED    10HDX        10HDX        Off
      RJ-45
  6    Off        ENABLED    ENABLED    10HDX        10HDX        Off
      RJ-45
  7    Off        ENABLED    ENABLED    10HDX        10HDX        Off
      RJ-45
  8    Off        ENABLED    ENABLED    10HDX        10HDX        Off
      RJ-45
  9    On         ENABLED    ENABLED    10HDX        100TX-FDX    Off
      RJ-45
 10    Off        ENABLED    ENABLED    10HDX        10HDX        Off
      RJ-45
 11    Off        ENABLED    ENABLED    10HDX        10HDX        Off
      RJ-45
 12    On         ENABLED    DISABLED   100FDX       100FX-FDX    Off
      FIBER

Page>      <Apply>      <OK>      <Cancel>      <Prev Page> <Next
Administrative status for port 1.
READ/SELECT
Use <TAB> or arrow keys to move, <Space> to scroll options.

```

Parameter	Default	Description																				
Link Status		Indicates if the port has a valid connection to an external device.																				
Admin Status	Enabled	Allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then enable it after the problem has been resolved. You may also disable a port for security reasons.																				
Auto Negotiate	Enabled (except 100FX)	Enables or disables auto-negotiation for the following features <table border="1"> <thead> <tr> <th>Port Type</th> <th>Speed</th> <th>Duplex Mode</th> <th>Flow Control</th> </tr> </thead> <tbody> <tr> <td>10/100BASE-T</td> <td>auto</td> <td>auto</td> <td>auto</td> </tr> <tr> <td>100BASE-FX</td> <td>100M-</td> <td>full duplex</td> <td>auto</td> </tr> <tr> <td>1000BASE-SX/ LX</td> <td>1000M</td> <td>full duplex</td> <td>auto</td> </tr> <tr> <td>1000BASE-T</td> <td>1000M</td> <td>full duplex</td> <td>auto</td> </tr> </tbody> </table> The 10/100BASE-TX ports can auto negotiate the speed to 10/100 Mbps, and the transmission mode to half / full duplex.	Port Type	Speed	Duplex Mode	Flow Control	10/100BASE-T	auto	auto	auto	100BASE-FX	100M-	full duplex	auto	1000BASE-SX/ LX	1000M	full duplex	auto	1000BASE-T	1000M	full duplex	auto
Port Type	Speed	Duplex Mode	Flow Control																			
10/100BASE-T	auto	auto	auto																			
100BASE-FX	100M-	full duplex	auto																			
1000BASE-SX/ LX	1000M	full duplex	auto																			
1000BASE-T	1000M	full duplex	auto																			

		The 100BASE-FX, 1000BASE-SX/LX and 1000BASE-T modules are all fixed at the indicated speed and duplex mode. All media types can auto-negotiate flow control.									
Default Type	10HDX (except 100FX)	If auto-negotiation is disabled, the port will be set to the indicated speed and duplex mode.									
Current Type		Indicates the current speed and duplex mode.									
Flow Control	Off	Used to enable or disable flow control. Flow control can eliminate frame loss by blocking traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to a hub. For the Gigabit modules the options for flow control are set out below: <table border="0"> <tr> <td><i>Switch</i></td> <td><i>Link Partner</i></td> <td><i>Flow Control</i></td> </tr> <tr> <td>Rcv/BothWay</td> <td>SendOnly</td> <td>Switch can only receive pause frames, link partner can only send pause frames.</td> </tr> <tr> <td>Rcv/BothWay</td> <td>BothWay</td> <td>Both switch and link partner can send and receive pause frames.</td> </tr> </table>	<i>Switch</i>	<i>Link Partner</i>	<i>Flow Control</i>	Rcv/BothWay	SendOnly	Switch can only receive pause frames, link partner can only send pause frames.	Rcv/BothWay	BothWay	Both switch and link partner can send and receive pause frames.
<i>Switch</i>	<i>Link Partner</i>	<i>Flow Control</i>									
Rcv/BothWay	SendOnly	Switch can only receive pause frames, link partner can only send pause frames.									
Rcv/BothWay	BothWay	Both switch and link partner can send and receive pause frames.									
Jack Type		Shows the jack type for each port. Ports 1-11, 13-23: RJ-45. Ports 12, 24: either RJ-45 or FIBER. Ports 25-26: RJ-45, FIBER									

The gigabit ports (25 and 26) are optional. They are provided as slide-in module. Each port can be empty (unplugged), copper (type 1GBaseT), or fiber (type 1GSX/LX). The user can change the gigabit modules after the switch is off. The Switch will automatically detect the changes and update the information as soon as the power is up again. Note that the speed of the gigabit module is fixed at 1G.

Layer 2 Menu: Port Configuration (Expansion Slots)						
=====						
Port Jack Type	Link Status	Admin Status	Auto Negotiate	Current Type	Flow Control	FC Status
25 FIBER	Off	ENABLED	ENABLED	1GSX/LX-FDX	Off	Off
26 FIBER	Off	ENABLED	ENABLED	1GSX/LX-FDX	Off	Off

<Apply>      <OK>      <Cancel>      <Prev Page> <Next  
 Page>

Administrative status for port 25. |  
 READ/SELECT  
 Use <TAB> or arrow keys to move, <Space> to scroll options.

### 2.5.2.2. Using a Mirror Port for Analysis

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, note that the target port must be included in the same VLAN as the source port. (See “Configuring Virtual LANs” on chapter 2.)

You can use the Port Mirror Configuration screen to mirror one or more ports to the monitor port as shown below.

```

Layer 2 Menu: Mirror Port Configuration
=====

Port Mirroring : DISABLED

Transmission Path
Mirrored Ports

Tx:7 8 9
Rx:8 9 12 23

Monitor Port Tx : 5
Monitor Port Rx : 6

<Apply>          <OK>          <Add>
Enable or disable port mirror function. |
READ/SELECT
Use <TAB> or arrow keys to move, <Space> to scroll options.

```

Parameter	Description
Enable Port Mirror	Enables or disables the mirror function.
Mirrored Ports (Tx/Rx)	The port whose transmitted or received traffic will be mirrored. Select <Add> to specify mirrored ports.
Monitor Port (Tx/Rx)	The port that will duplicate the transmitted or received traffic appearing on the mirrored port.

**Note:**

You can mirror multiple ports to a single port to view traffic such as that crossing a port trunk. However, note that some packets may be dropped for moderate to heavy loading.

### 2.5.2.3. Configuring Port Trunks

Ports can be combined into an aggregate link to increase the bandwidth of a network connection or to ensure fault recovery. You can configure trunks between any two switches. Ports 1-24 on this switch can be grouped into a trunk consisting of two, four or eight ports, creating an aggregate bandwidth up to 400, 800 or 1600 Mbps when operating at full duplex. Ports 25-26 (extender module ports) can be trunked together creating an aggregate bandwidth up to 2 Gps (see chapter 2 “Configuring STA for Ports”). The ports that can be assigned to the same trunk are listed on chapter 2 “Configuring Global Bridge Settings”. Besides balancing the load across each port in the trunk, the additional ports provide redundancy by taking over the load if another port in the trunk fails. However, before making any physical connections between devices, use the Port Trunking Configuration menu to specify the trunk on the devices at both ends.

When using a port trunk, remember that:

- Ports can only be assigned to one trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode, and VLAN assignments.
- All the ports in a trunk have to be treated as a whole when moved from / to, added or deleted from a VLAN.
- The Spanning Tree Algorithm will treat all the ports in a trunk as a whole.
- Enable the trunk prior to connecting any cable between the switches to avoid creating a loop.

You can use the Port Trunking Configuration screen to set up port trunks as shown below:

```

                                Layer 2 Menu: Port Trunking Configuration
                                =====
Index  Port Count  Port Number
Trunk1  2           13  01
Trunk2  4           19  07  20  08

                                <OK>                <Add>
                                Add Link Aggregation.
                                Use <TAB> or arrow keys to move. <Enter> to select.

```

Parameter	Description
Trunk#	The trunk identifier.
Port Count	Trunks can contain 2, 4 or 8 ports.
Port Number	The ports assigned to each trunk.

The port groups permitted include:

- <<13, 1>> <<14, 2>> <<15, 3>> <<16, 4>>
- <<17, 5>> <<18, 6>> <<19, 7>> <<20, 8>>
- <<21, 9>> <<22,10>> <<23,11>> <<24,12>>
- <<13, 1, 14, 2>> <<15, 3, 16, 4>>
- <<17, 5, 18, 6>> <<19, 7, 20, 8>>
- <<21, 9, 22, 10>> <<23, 11, 24, 12>>

<<13, 1, 14, 2, 15, 3, 16, 4>>  
 <<17, 5, 18, 6, 19, 7, 20, 8>>  
 <<21, 9, 22, 10, 23, 11, 24, 12>>  
 <<25, 26>>

**Note:**

For the extender modules (ports 25, 26), the possible port trunking combinations are set out below:

Extender Module

1000BASE-SX/LX, 1000BASE-T Can be trunked together, irrespective of media.

To add a trunk, select <Add>. To delete a trunk, highlight the required entry and select Enter. Before disconnecting a port trunk, take the following steps:

- Before removing a port trunk via the configuration menu, you must disable all the ports in the trunk or remove all the network cables. Otherwise, a loop may be created.
- To disable a single link within a port trunk, you should first remove the network cable, and then disable both ends of the link via the configuration menu. This allows the traffic passing across that link to be automatically distributed to the other links in the trunk, without losing any significant amount of traffic.

### 2.5.2.4. Configuring the Static Unicast Address Table

The Static Unicast Address Table can be used to assign the MAC address for a host device to a specific port on this switch. Static unicast addresses are never aged out, and cannot be learned on another port. If any packets with a source address specified in this table enter another port, they will be dropped. The Static Unicast Address Table is described in the following figure and table.

```

                                Layer 2 Menu: Static Address Table
                                =====
Address          Port          Address          Port
00-80-AD-84-0A-A0  10

Page    1    <Apply>          Total    1    Pages
<OK>    <Next Page>    <Prev Page>    <Add>
                                Return to previous panel.
                                Use <TAB> or arrow keys to move. <Enter> to select.
  
```

Parameter	Description
-----------	-------------

Address	The MAC address of a host device attached to this switch.
Port	The switch port to which the host device is attached.

**Note:**

To assign a MAC address to a specific port, use <Add>. To delete or modify an address, highlight it with the cursor and select Enter.  
 To scroll through the address table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then select <Apply>.

### 2.5.2.5. Configuring the Static Multicast Address Table

The Static Multicast Address Table can be used to assign a destination MAC address (and the corresponding ports) to the VLAN group used for a specific multicast service. Static multicast addresses are never aged out, and traffic with these addresses can be forwarded only to ports specified in this table.

```

Layer 2 Menu: Multicast Address Table
=====
VLAN      Address          Port          1          2
  2  01-80-AD-84-0A-A0 MMMMMMM

```

Page 1 <Apply> Total 1 Pages  
 <OK> <Next Page> <Prev Page> <Add>  
 Return to previous panel.  
 Use <TAB> or arrow keys to move. <Enter> to select.

Parameter	Description
VLAN	The VLAN corresponding to this multicast service.
Address	The destination MAC address for a multicast service.
Port	The ports to which this multicast traffic can be forwarded.

**Note:**

To assign a destination MAC address to one or more ports, use <Add>. To delete or modify an address, highlight it with the cursor and select Enter.  
 To scroll through the address table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then select <Apply>.

## 2.5.3.Using the Bridge Menu

The Bridge menu is used to configure settings for the Spanning Tree Algorithm, as well as the global bridge settings for GMRP (GARP Multicast Registration Protocol) and GVRP (GARP VLAN Registration Protocol), traffic class priority threshold, and address aging time.

The Spanning Tree Algorithm can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down. For a more detailed description of how to use this algorithm, refer to “Spanning Tree Algorithm” on chapter 4.

```

                                Bridge Menu
                                =====

                                Bridge Configuration ...

                                Spanning Tree Port Configuration ...

                                <OK>
                                Change the bridge configuration.
                                Use <TAB> or arrow keys to move. <Enter> to select.
    
```

Menu	Description
Bridge Configuration	Contains global bridge settings for STA (including bridge priority, hello time, forward delay, maximum message age), GMRP, GVRP, traffic class priority threshold, and address aging time.
Spanning Tree Port Configuration	Contains STA settings for individual ports, including port priority, path cost, and fast forwarding

### 2.5.3.1.Configuring Global Bridge Settings

The following figure and table describe bridge configuration for STA, GMRP, GVRP, priority threshold, and address aging time.

```

                                Bridge Menu: Bridge Configuration
                                =====
Spanning Tree                      : ENABLED
GMRP                               : DISABLED
Bridge Priority                     : 32768
GVRP                               : DISABLED
Hello Time (in seconds)            : 2           Priority
Threshold                          : 4
Forward Delay (in seconds)         : 15         Aging Time (in seconds) :
300
Max age (in seconds)               : 20

                                <Apply>           <OK>           <Cancel>
                                The status of the spanning tree.           |
READ/SELECT
                                Use <TAB> or arrow keys to move, <Space> to scroll options.

```

Parameter	Default	Description
Spanning Tree	Enabled	Enable this parameter to participate in a STA compliant network.
Bridge Priority	32,768	Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Enter a value from 0 - 65535. Remember that the lower the numeric value, the higher the priority.
Hello Time	2	Time interval (in seconds) at which the root device transmits a configuration message. The minimum value is 1. The maximum value is the lower of 10 or [(Max. Message Age / 2) - 1].
Forward Delay	15	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The maximum value is 30. The minimum value is the higher of 4 or [(Max. Message Age / 2) + 1].

Max (Message) Age	20	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. The minimum value is the higher of 6 or $[2 \times (\text{Hello Time} + 1)]$ . The maximum value is the lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$ .
GMRP	Disabled	GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. If GMRP is globally enabled for the switch, then you can individually enable or disable GMRP for a specific port. See "VLAN Port Configuration" on chapter 2. IGMP and IGMP Snooping also provide multicast filtering. For multilayer mode, the full IGMP protocol set is automatically enabled / disabled along with DVMRP. (See "IGMP Protocol" on chapter 4, "Configuring DVMRP" on chapter 2 and "Configuring IGMP Snooping" on chapter 2.)
GVRP	Disabled	GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch. If GVRP is globally enabled for the switch, then you can individually enable or disable GVRP for a specific port. See "VLAN Port Configuration" on chapter 2.
Priority Threshold*	4	This switch supports Quality of Service (QoS) by using two priority queues, with Weighted Fair Queuing for each port. Up to 8 separate traffic classes are defined in IEEE 802.1p. Therefore, any packets with a priority equal to or higher than this threshold are placed in the high priority queue.
(Address) Aging Time	300	Timeout period in seconds for aging out dynamically learned forwarding information. Range: 10 - 415 seconds

\* You can use "VLAN Port Configuration" on chapter 2 to configure the default priority for each port.

### 2.5.3.2. Configuring STA for Ports

The following figure and table describe port STA configuration.

```

Spanning Tree Port Configuration (Port 1-12)
=====

Port      Type          Priority   Cost
FastForwarding

-----
1         100TX         128       19   DISABLED
2         100TX         128       19   DISABLED
3         100TX         128       19   DISABLED
4         100TX         128       19   DISABLED
5         100TX         128       19   DISABLED
6         100TX         128       19   DISABLED
7         100TX         128       19   DISABLED
8         100TX         128       19   DISABLED
9         100TX         128       19   DISABLED
10        100TX         128       19   DISABLED
11        100TX         128       19   DISABLED
12        100TX         128       19   DISABLED

<Apply>      <OK>      <Cancel>      <Prev Page>
<Next Page>
              The priority of port 1.
| READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Default	Description
Type		Shows port type as: 100TX : 10BASE-T / 100BASE-TX 100FX : 100BASE-FX 1000SX/LX : 1000BASE-SX/LX (multimode/ single mode) 1000T : 1000BASE-T
Priority	128	Defines the priority for the use of a port in the STA algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the Spanning Tree. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is 0 - 255.
(Path) Cost	100/19/4	This parameter is used by the STA algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) The default and recommended range is: Ethernet: 100 (50~600) Fast Ethernet: 19 (10~60) Gigabit Ethernet: 4 (3~10) The full range is 0 - 65535.
Fast	Disabled	This parameter is used to enable / disabled the Fast Spanning

Forwarding*		Tree mode for the selected port. In this mode, ports skip the Blocked, Listening and Learning states and proceed straight to Forwarding.
-------------	--	--

\* Since end-nodes cannot cause forwarding loops, they can be passed through the Spanning Tree state changes more quickly than allowed by standard convergence time. Fast Forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related timeout problems. (Remember that Fast Forwarding should only be enabled for ports connected to an end-node device.)

## 2.5.4. Configuring Virtual LANs

You can use the VLAN configuration menu to assign any port on the switch to any of up to 256 Virtual LAN groups. In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle traffic such as IPX or NetBEUI. By using IEEE 802.1Q-compliant VLANs, you can organize any group of network nodes into separate broadcast domains, thus confining broadcast traffic to the originating group. This also provides a more secure and cleaner network environment. For more information on how to use VLANs, see “Virtual LANs” on chapter 4. The VLAN configuration screens are described in the following sections.

```

                                VLAN Menu
                                =====

                                VLAN Port Configuration ...
                                VLAN Table Configuration ...

                                <OK>
                                Change the port VLAN configuration.
                                Use <TAB> or arrow keys to move. <Enter> to select.

```

### 2.5.4.1. VLAN Port Configuration

You can use the VLAN Port Configuration screen to configure GARP, the default VLAN identifier, default port priority, VLAN tagging on outgoing frames, GVRP and GMRP status, and filtering of incoming frames for VLAN groups to which this port does not belong.

```

VLAN Menu: VLAN Port Configuration
=====

GARP Configuration

Join Time           20 Centiseconds
Leave Time           60 Centiseconds
Leave All Time      1000 Centiseconds

VLAN and Priority

Port VID            1
Port Default Priority 0
VLAN Tagging       Rx All, Tx All
GVRP               ENABLED
GMRP               ENABLED
Ingress Filtering  DISABLED

Port 1 <Apply> <OK> <Cancel> <Prev Port> <Next
Port>

The join time for the port.
| READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Default	Description
<i>GARP</i> <sup>1</sup>		Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN.
Join Time	20	The interval (centiseconds) between transmitting requests / queries to participate in a group.
Leave Time	60	The interval (centiseconds) a port waits before leaving a group. This time should be set to more than twice the Join Time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can re-join before the port actually leaves the group.
Leave All Time	1000	The interval (centiseconds) between sending out a LeaveAll query message for group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group.
<i>VLAN and Priority</i>		These fields set the default values for VLANs, port priority, GVRP and GMRP.
Port VID	1	The VLAN ID assigned to untagged frames received on this port.

Port Default Priority <sup>2</sup>	0	Set the default ingress priority to any value beneath the priority threshold (chapter 2 “Configuring Global Bridge Setting”) to specify the low priority queue, or to any value equal to or above this threshold to specify the high priority queue.
VLAN Tagging <sup>3</sup>	<p><i>Layer 2 - Rx All, Tx All</i></p> <p><i>Multilayer - Rx All, Tx Untag</i></p>	<p>Indicates whether or not VLAN tags will be included on frames passing through this port. The options include:</p> <p>Rx All: Accepts all frames, tagged or untagged.</p> <p>Rx Untag: Only accepts untagged frames.</p> <p>Tx All: If PVID and frame tag are same, sends tagged frame, otherwise sends untagged.</p> <p>Tx Untag: Sends only untagged frames.</p>

1. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration / deregistration.
2. This switch supports Quality of Service (QoS) by using two priority queues, with Weighted Fair Queuing for each port. Inbound frames that do not have VLAN tags are tagged with the input port’s default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in the low priority queue of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)
3. If you want to create a small port-based VLAN for just one or two switches, you can assign ports to the same untagged VLAN (and use a separate connection where a VLAN crosses the switches). However, to participate in a VLAN group that extends beyond this switch, we recommend using the VLAN ID for that group, (by VLAN tagging for Layer 2 mode, or a common PVID for multilayer mode).  
When operating the switch in Layer 2 mode, ports assigned to a large VLAN group that crosses several switches must use VLAN tagging. But when operating in multilayer mode, this switch does not currently support tagging, so you should set the PVID to the same value at both ends of the link (if the device you are attaching to is VLAN-aware), and configure an IP interface for this VLAN if you need to connect it to other groups. (This limitation will be removed for future firmware versions.)

Parameter	Default	Description
GVRP	Enabled	Enables or disables GVRP for this port. When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. Note that GVRP must be enabled globally for the switch before this setting can take effect. (See “Configuring Global Bridge Settings” on chapter 2.)

GMRP	Enabled	Enables or disables GMRP for this port. When enabled, this port will allow endstations to register with multicast groups using GMRP. Note that GMRP must be enabled for the switch before this setting can take effect (chapter 2 “Configuring Global Bridge Settings”). IGMP and IGMP Snooping also provide multicast filtering. (See “IGMP Protocol” on chapter 4.)
Ingress Filtering <sup>4</sup>	Disabled	If enabled, incoming frames for VLANs which do not include this ingress port in their member set will be discarded at the ingress port.

4. This control does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

### 2.5.4.2.VLAN Table Configuration

Use this screen to create a new VLAN or modify the settings for an existing VLAN.

```

                                VLAN Menu: VLAN Table Configuration
                                =====
                                Port          1          2
                                VLAN         12345678901234567890123456
                                1           SSSSSSSSSSSSSSSSSSSSSSSSSSSSSSS
Normal
Static
Reg. Fixed
Forbidden

                                Page : 1   <Apply>                Total: 1   Pages
                                <OK>     <Prev Page>          <Next Page>          <Add>
                                Enter page number than press 'Apply' to see VLAN group.
READ/WRITE
                                Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
VLAN	The ID for the VLAN currently displayed. Range: 1-4094

Port	Port entries may be marked as: - : ( <i>Normal</i> ) Uses GVRP to determine port membership. S : ( <i>Static</i> ) Adds port as a static entry. GVRP protocol messages are still forwarded through this port. R : ( <i>Registration Fixed</i> ) Adds port as a static entry. GVRP protocol is disabled. X : ( <i>Forbidden</i> ) Disables GVRP for this VLAN on the specified port. If a removed port is no longer assigned to any other group as an untagged port, it will automatically be assigned to VLAN group 1 as untagged.
------	--

**Note:**

Use the <Next Page> and <Prev Page> buttons to scroll through the table. To display a specific page, set the page number in the Page field and select <Apply>. To modify a VLAN group, highlight the entry in the table and select Enter. To add a VLAN group, select <Add>.

## 2.5.5. Configuring IGMP Snooping

Multicasting is used to support real-time applications such as videoconferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts which want to receive the multicast register with their local multicast switch / router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully filtered at every multicast switch / router it passes through to ensure that traffic is only passed on to the hosts which subscribed to this service.

This switch uses IGMP (Internet Group Management Protocol) Snooping to monitor any attached hosts which want to receive a specific multicast service. It looks up the IP Multicast Group used for this service, and adds to it any port that received a similar request .

You can use the IGMP Snooping Configuration screen to configure multicast filtering as shown below.

```

IGMP Snooping Configuration
=====

IGMP Snooping Status           : DISABLED
IGMP Router Timeout (Minutes)  : 5
IGMP Group Timeout (Minutes)   : 5
Act as IGMP Querier           : DISABLED

<Apply>           <OK>           <Cancel>
To enable or disable IGMP snooping on your system. |
READ/SELECT
Use <TAB> or arrow keys to move, <Space> to scroll options.

```

Parameter	Default	Description
IGMP Snooping Status <sup>1</sup>	Disabled	If enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping.
IGMP Router Timeout	5	A switch port that stops receiving multicast protocol packets for this interval will be removed from the IGMP forwarding list. Range: 3 - 5 minutes
IGMP Group Timeout	5	The time between last spotting an IGMP Report message for an IP multicast address on a specific port and the switch removing that entry from its list. Range: 3 - 5 minutes
Act as IGMP Querier <sup>2</sup>	Disabled	If enabled, the switch can serve as the “querier,” which is responsible for asking hosts if they want to receive multicast traffic.

1. This item is only displayed for Layer 2 mode. For multilayer mode, the full IGMP protocol set is automatically enabled / disabled along with DVMRP. (See IGMP on chapter 4. See DVMRP on chapter 2 “*Configuring DVMRP*” and chapter 4 “*DVMRP Routing Protocol*”.)
2. This item is only displayed for Layer 2 mode. When IGMP is enabled for multilayer mode, the switch will always serve as the querier if elected. (“IGMP Snooping Configuration” on chapter 2)

## 2.5.6. Configuring IP Settings

If this switch is set to multilayer mode (chapter 2 “Setting the System Operation Mode”), the IP Menu will be displayed. Use this menu to configure the IP subnets for each VLAN on your switch, the unicast and multicast routing protocols, static ARP entries, static IP

routes, and the default IP route.

```

IP Menu
=====

Subnet Configuration ...

Protocol Configuration ...

Static ARP Configuration ...

Static Route ...

Default Route ...

<OK>
Display and change the subnet configuration.
Use <TAB> or arrow keys to move. <Enter> to select.

```

Parameter	Description
Subnet Configuration	Specifies the IP interface for VLANs configured on this switch, including the subnet address and routing protocols.
Protocol Configuration	Configures ARP timeout, enables Proxy ARP, sets the preferred servers for BOOTP / DHCP Relay, as well as enabling / configuring unicast and multicast protocols globally for this switch.
Static ARP Configuration	Used to map an IP address to a specific physical MAC address.
Static Route	Used to configure static routes to other IP networks, subnetworks, or hosts.
Default Route	Defines the router to which this switch will forward all traffic for unknown networks.

### 2.5.6.1. Subnet Configuration

Use this menu to specify an IP interface for any VLAN configured on this switch that needs to communicate with a device outside of its own group (i.e., another network segment). You also need to define a VLAN for each IP subnet connected directly to this switch. Note that you must first create a VLAN as described under “Configuring Virtual LANs” on chapter 2 before configuring the corresponding subnet. Remember that if you need to manage the switch in-band then you must define the IP subnet address for at least one VLAN.

```

                                IP Subnet Configuration
                                =====
Intf. IP Address      Subnet Mask      VLAN RIP      OSPF      DVMRP
Status
1    192.168.1.254   255.255.255.0      1 DISABLED  DISABLED
DISABLED ON

                                Page 1      <Apply>                                Total 1
Pages
                                <OK>      <Prev Page>      <Next Page>
<Add>
                                The page number.
READ/WRITE
                                Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
IP Address	The IP address associated with the specified VLAN interface. By convention, the last three digits should be set to “254” to readily distinguish this device as a router port.
Subnet Mask	A template that identifies the address bits in the host address used for routing to specific subnets. Each bit that corresponds to a “1” is part of the network / subnet number, and each bit that corresponds to “0” is part of the host number.
VLAN	The VLAN associated with this IP interface.
RIP	Routing Information Protocol for unicast routing.
OSPF	Open Shortest Path First unicast routing protocol.
DVMRP	Distance-Vector Multicast Routing Protocol.

**Note:**  
 Use the <Next Page> and <Prev Page> buttons to scroll through the subnet configuration table. To display a specific page, set the page number in the Page field and then select <Apply>. To modify an IP interface, highlight the entry in the table and select Enter. To add an IP interface, select <Add>.

**Adding an IP Interface**

Select <Add> on the Subnet Configuration menu to add an IP interface. When the Add Subnet screen opens as shown below, assign a VLAN group to this interface, configure the IP address, and then enable the required routing protocols. You can specify a VLAN that has already been configured on this switch or select “Select” to open the Port

Group Configuration screen and create or modify a VLAN group (chapter 2 “*Configuring Port Groups*”). To configure the unicast or multicast routing protocols, select the IP address for a specific interface from the Subnet Configuration menu (chapter 2 “Subnet Configuration”), and then select “Advanced” configuration from the Modify Subnet screen (see chapter 2 “*Modifying an IP Interface*”).

```

                                Add Subnet
                                =====
                                VLAN           : 0                Select
                                IP Address    : 0.0.0.0
                                Subnet Mask  : 255.255.255.0
                                Proxy ARP    : DISABLED
                                RIP          : DISABLED
                                OSPF        : DISABLED
                                DVMRP      : DISABLED

                                <OK>                <Cancel>
                                Please enter VLAN ID.
| READ/WRITE
                                Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
VLAN	The VLAN associated with this IP interface.
Select	Use this option to create or modify a VLAN under the “Port Group Configuration” menu as described below.
IP Address	The IP address associated with the specified VLAN interface. By convention, the last three digits should be set to “254” to readily distinguish this device as a router port.
Subnet Mask	A template that identifies the address bits in the host address used for routing to specific subnets. Each bit that corresponds to a “1” is part of the network / subnet number, and each bit that corresponds to “0” is part of the host number.
Proxy ARP	Enables or disables Proxy ARP for the interface. This feature allows the switch forward an ARP request from a node in the attached subnetwork (that does not have routing or a default gateway configured) to a remote subnetwork. (See “Proxy ARP” on chapter 4.) Note that Proxy ARP must be enabled globally for the switch before this setting can take effect. (See “Protocol Configuration” on chapter 2.)
RIP	Routing Information Protocol for unicast routing.
OSPF	Open Shortest Path First unicast routing protocol.
DVMRP	Distance-Vector Multicast Routing Protocol.

### Configuring Port Groups



```

                                Modify Subnet
                                =====
                                VLAN          : 1                Select
                                IP Address    : 192.168.1.254
                                Subnet Mask   : 255.255.255.0
                                Proxy ARP    : DISABLED
                                RIP           : DISABLED          Advanced ...
                                OSPF         : DISABLED          Advanced ...
                                DVMRP       : DISABLED          Advanced ...

                                <Delete>      <Apply>           <OK>
<Cancel>
                                VLAN ID.
| READ/WRITE
    Use <TAB> or arrow keys to move, other keys to make changes.

```

### **Configuring RIP**

The Routing Information Protocol is used to specify how routers exchange routing table information. (See “RIP and RIP-2 Dynamic Routing Protocols” on chapter 4.) When RIP is enabled on this routing switch, it broadcasts RIP messages to all devices in the network every 30 seconds, and updates its own routing table when RIP messages are received from other routers. RIP messages contain both the IP address and a metric for each destination network it knows about. The metric indicates the number of hops from this device to the destination network.

You can use the following menu to specify authentication, the protocol used for sending or receiving routing messages on this port, the default metric used in calculating the best path, and enable or disable Poison Reverse.

```

Subnet Configuration: Modify RIP Configuration
=====

Authentication Type: No Authentication
Authentication Key :

Send Type           : RIP1 Broadcast
Receive Type        : RIP1

Default Metric      : 0

Poison Reverse      : Enabled

<Apply>             <OK>
<Cancel>
RIP authentication type. |
READ/SELECT
Use <TAB> or arrow keys to move, <Space> to scroll options.

```

Parameter	Description
Authentication Type	Authentication can be used to ensure that routing information comes from a valid source. The options include none or a simple password.
Authentication Key	A simple password must be provided if authentication is enabled. (An authentication string is case sensitive, and can be up to 16 characters.)
Send Type	The protocol used for traffic sent out this port: RIP1 Broadcast    Route information is broadcast to other routers on the network using RIPv1 message. RIP2 Broadcast    Route information is broadcast to other routers on the network using RIPv2 message. RIP2 Multicast    Route information is multicast to other routers on the network using RIPv2 message. Do Not Send        The switch will passively monitor route information transmitted by other routers attached to the network.
Receive Type	The routing protocol messages accepted on this port includes RIP1, RIP2, RIP1 / RIP2, or Disabled (i.e., none received).
Default Metric	A “metric” indicates the number of hops between the switch and the destination network. The “default metric” is used for the default route in RIP updates originated on this interface. A value of zero indicates that no default route should be originated; in this case, a default route via another router may be propagated. Range: 0-15
Poison Reverse*	Propagates routes back to an interface port from which they have been acquired, but sets the distance vector metrics to infinity.

\* This is a method of preventing routing information from looping back to the source. Note that Split Horizon is also enabled on this switch for this purpose. (See “RIP and RIP-2 Dynamic Routing Protocols” on chapter 4.)

## Configuring OSPF

Open Shortest Path First is more suited for large area networks which experience frequent changes in the links. It also allows for subnets. This protocol actively tests the status of each link to its neighbors to generate a shortest path tree, and builds a routing table based on this information. (See “OSPFv2 Dynamic Routing Protocol” on chapter 4.) OSPF then utilizes IP multicast to propagate routing information. A separate routing area scheme is also used to further reduce the amount of routing traffic (chapter 2 “Protocol Configuration”).

You can use the following menu to specify the area identifier, or other key routing parameters as described in the following table.

```

Subnet Configuration: Modify OSPF Configuration
=====
Area ID                : 0.0.0.0
Router Priority        : 1
Interface Cost        : 100
Transit Delay (in seconds) : 1
Retransmit Interval (in seconds): 5
Hello Interval (in seconds) : 10
Dead Interval (in seconds)  : 40
Poll Interval (in seconds) : 120
Authentication Type : NONE
Authentication Key  : MD5 Key Table

<Apply>                <OK>
<Cancel>
                        Area ID.
| READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Default	Description
Area ID <sup>1</sup>	0.0.0.0	A 32-bit integer uniquely identifying an OSPF protocol broadcast area. This identifier can be in the form of an IP address or integer. Each port on the switch can be configured to represent one OSPF area. You must first specify OSPF areas for global access in the Area ID Configuration menu, before they can be used for a specific IP interface.(see chapter 2 “OSPF Area Configuration”) ID 0.0.0.0 is used for the OSPF backbone.
Router Priority	1	The priority used when selecting the designated router and designated backup router. Range: 0-255; Disable election: 0

Interface Cost	100	This value is used by the router in calculating the shortest path. The default cost is calculated by using the bandwidth of the interface. For this purpose, the bandwidth is taken as that of the highest bandwidth port in the VLAN linked to the interface. The interface cost is inversely proportional to this bandwidth. The shortest path is that with the lowest cost, given by the highest bandwidth
Transit Delay	1 second	The estimated number of seconds it takes to transmit a link state update packet over this interface. Range: 0-3600 seconds
Retransmit Interval	5 seconds	The number of seconds between retransmitting link-state advertisements to router adjacencies on this interface. This value is also used when retransmitting database descriptions and link-state request packets. Range: 0-3600 seconds
Hello Interval <sup>2</sup>	10 seconds	The interval, in seconds, between sending Hello packets out the router interface. This interval determines how fast topology changes will be detected. However, for small intervals, more overhead will be incurred in exchanging routing information. Range: 1-65535 seconds
Dead Interval <sup>2</sup>	40 seconds	The number of seconds that a router's Hello packets have not been seen before its neighbors declare the router down. This should be a multiple of the Hello interval. Range: 1-65535 seconds
Poll Interval	120 seconds	The interval, in seconds, between sending Hello packets to a neighboring router from which Hello packets have not been received for the Dead Interval period of time. The poll interval must be much larger than the Hello Interval.

1. The Area ID is used to specify a group of contiguous networks and hosts. OSPF protocol broadcast messages are restricted by area to limit their impact on network performance.
2. This value must be the same for all routers attached to a common network.

### **Configuring DVMRP**

Distance Vector Multicast Routing Protocol is used to route multicast traffic to nodes which have requested a specific multicast service via IGMP. (See "DVMRP Routing Protocol" on chapter 4.) To configure DVMRP, you must specify the routing metric, probe interval, and neighbor router timeout.

```

Subnet Configuration: Modify DVMRP Configuration
=====
Metrics:                               : 1
Probe Interval (in seconds)           : 10
Neighbor Timeout (in seconds): 35

<Apply>                               <OK>
<Cancel>
Metrics.
| READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Default	Description
Metrics	1 hop	This value is used to select the best reverse path to networks that are connected directly to an interface on this switch. Range: 1-31 hops
Probe Interval	10 seconds	The interval between sending neighbor probe messages to the multicast group address for all DVMRP routers. Range: 5-30 seconds
Neighbor Timeout	35 seconds	The interval to wait without hearing from a DVMRP neighbor before declaring it dead. This is used for timing out routes, and for setting the children and leaf flags. Range: 10-8000 seconds

**Note:**  
IGMP is automatically enabled / disabled along with DVMRP. (See “IGMP Protocol” on chapter 4.)

### 2.5.6.2. Protocol Configuration

Use the Protocol Configuration screen to globally enable or disable unicast or multicast routing protocols for the switch.

```

Protocol Configuration
=====

ARP          :          Advanced ...
Proxy ARP    : ENABLED
RIP          : ENABLED  Advanced ...
OSPF        : DISABLED  Advanced ...
DHCP Relay   : DISABLED  Advanced ...

IGMP Snooping : DISABLED  Advanced ...
DVMRP       : ENABLED

<Apply>          <OK>          <Cancel>
System ARP protocol advanced status.
Use <TAB> or arrow keys to move. <Enter> to select.

```

Parameter	Description
ARP	Sets the aging time for dynamic ARP entries.
Proxy ARP	Enables or disables Proxy ARP globally for the switch. This feature allows the switch to forward an ARP request from a node in the attached subnetwork (that does not have routing or a default gateway configured) to a remote subnetwork. (See “Proxy ARP” on chapter 4.) If Proxy ARP is globally enabled for the switch, then you can enable or disable it for a specific interface. See “Adding an IP Interface” on chapter 2, or “Modifying an IP Interface” on chapter 2.
RIP	Enables or disables the Routing Information Protocol. The Advanced menu sets the interval at which the switch advertises known routes, and also enables / disables advertising for static routes or the default route.
OSPF	Enables or disables the OSPF routing protocol. The Advanced menu organizes an autonomous system into normal, stub, or not so stubby areas; configures a range of subnet addresses for which link state advertisements can be aggregated; and configures virtual links for areas that do not have direct physical access to the OSFP backbone, to add redundancy, or to merge backbone areas.
DHCP Relay	Enables or disables BOOTP / DHCP Relay. The Advanced menu defines the preferred servers or the outbound subnetworks for broadcasting a BOOTP / DHCP request.
IGMP Snooping	Enables or disables IGMP Snooping. The Advanced menu sets the timeout for inactive multicast ports or for specific multicast flows when there are no longer any clients. See chapter 2 “Configuring IGMP Snooping”.
DVMRP	Enables or disables the Distance-Vector Multicast Routing Protocol.

Once RIP, OSPF and DVMRP have been globally enabled, you can enable or disable them for any specific subnet via the Subnet Configuration menu (chapter 2 “Adding an

IP interface”).

### Setting the ARP Timeout

You can use the following configuration screen to modify the aging time for dynamically learned entries in the ARP cache.

```

                                ARP Configuration
                                =====

                                ARP Timeout (Minutes)   : 20

                                <Apply>                <OK>                <Cancel>
                                ARP timeout value (minutes). |
READ/WRITE
                                Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Default	Description
ARP Timeout	20 minutes	The time that dynamically learned entries are retained in the ARP cache. Range: 0-999 minutes, where 0 disables aging

### Setting the RIP Advertisement Policy

You can use the following configuration screen to set the timing interval and policies RIP uses to advertise route information.

```

                                RIP Configuration
                                =====

                                RIP Update Time (Seconds)   : 30
                                Default Route Advertisement : DISABLED
                                Static Route Advertisement   : DISABLED
                                Ignore Host Route            : DISABLED

                                <Apply>                <OK>                <Cancel>
                                RIP timeout value (seconds). |
| READ/WRITE
                                Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Default	Description
-----------	---------	-------------

RIP Update Time	30 seconds	The interval at which RIP advertises known route information. Range: 0-999 seconds, where 0 disables route advertisements
Default Route Advertisement	Disabled	Enables or disables advertising this switch as a default router.
Static Route Advertisement	Disabled	Enables or disables advertisement of static routes.
Ignore Host Route	Disabled	If enabled, the switch will not import a default route from other routers.

### **Configuring Global Settings for OSPF**

To implement OSPF for a large network, you must first organize the network into logical areas to limit the number of OSPF routers that actively exchange Link State Advertisements (LSAs). You can then define an OSPF interface by assigning an IP interface configured on this switch to one of these groups. This OSPF interface will send and receive OSPF traffic to neighboring OSPF routers.

You can further optimize the exchange of OSPF traffic by specifying an area range that covers a large number of subnetwork addresses. This is an important technique for limiting the amount of traffic exchanged between Area Border Routers (ABRs).

And finally, you must specify a virtual link to any OSPF area that is not physically attached to the OSPF backbone. Virtual links can also be used to provide a redundant link between contiguous areas to prevent areas from being partitioned, or to merge backbone areas.

The following menu provides all the global configuration options for OSPF:

```

OSPF Configuration Menu
=====

Router ID Selection : STATIC
Router ID : 192.168.1.254
AS Border Status : Disabled
RFC 1583 compatibility : Disabled

Area ID Configuration ...
OSPF Area Range Configuration ...
OSPF Virtual Link Configuration ...
OSPF Host Route Configuration ...

                                <OK>
                                Use <Enter> to select.

```

Parameter	Description
Router Id	The switch IP that is used as the OSPF Router ID.
Area ID Configuration	Defines an area within which all OSPF routers actively exchange routing information to ensure that they all have an identical link state database.
OSPF Area Range Configuration	Defines a range of subnetwork addresses. An area range is used to summarize route information exchanged between Area Border Routers.
OSPF Virtual Link Configuration	Defines a virtual link that can be used to connect an OSPF area not physically adjacent to the OSPF backbone, or to create a backup link to any area.
OSPF Host Route Configuration	Configures the route to a specific host within the area.

### **OSPF Area Configuration**

OSPF protocol broadcast messages (i.e., Link State Advertisements) are restricted by area to limit their impact on network performance. Before assigning an Area ID to a specific OSPF interface (see chapter 2 “*Configuring OSPF*”), you must first specify the Area ID in this table. Each entry in this table identifies a logical group of OSPF routers that actively exchange Link State Advertisements (LSAs) to ensure that they share an identical view of the network topology. You can configure the area as a normal one which can send and receive external Link State Advertisements (LSAs), a stubby area that cannot send or receive external LSAs, or a not-so-stubby area (NSSA) that can import external route information into its area.

```

                                IP Menu: OSPF Area Configuration
                                =====
Area ID           Type
192.168.2.0      NORMAL
192.168.3.0      NORMAL

                                Page 1      <Apply>      Total 1 Pages
                                <OK>      <Prev Page>      <Next Page>      <Add>
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
Area ID	An OSPF area identifier configured for a group of OSPF routers. (For information on how to assign this identifier to a specific interface, see chapter 2 “ <i>Configuring OSPF</i> ”.)

Type	Indicates area type:
	Normal An area which can send or receive external route information.
	Stub An area which cannot send or receive external route information. It relies on a single default route provided by its Area Border Router (ABR) to access destinations outside of the stub. A stub can be used to reduce the amount of topology data that has to be exchanged over the network.
	NSSA A not so stubby area cannot send but can receive external route information. The ABR imports external routes and floods this information to all routers within the NSSA.

An Autonomous System Boundary Router (ASBR) can import external routes and flood this information to the entire Autonomous System.

**Note:**

To add a new Area ID, use the <Add> button. (The default 0.0.0.0 indicates the OSPF backbone.) To modify or delete an existing Area ID, highlight the table entry with the cursor and select Enter.

***OSPF Area Range Configuration***

After you configure an area identifier, you can specify a subnetwork address range that covers all the individual networks in this area. This technique limits the amount of traffic exchanged between Area Border Routers (ABRs) by allowing them to advertise a single summary range. By summarizing routes, the routing changes within an area do not have to be updated in the backbone ABRs or in other areas.

To optimize the route summary, first configure all the OSPF routers in an area so that they fall within a contiguous address range. The route summary consists of an address and mask, where the mask can be a Variable Length Subnet Mask (VLSM). Using VLSMs allows you to configure each subnetwork within a larger network with its own subnet mask. This provides a longer subnet mask that covers fewer host IP addresses, thereby reducing the size of the routing tables that have to be exchanged. (For more information on VLSMs, see RFCs 1219 and 1878.)



```

                                OSPF Virtual Link Configuration
                                =====
Area ID           Neighbor Router ID   Status
192.168.3.0      192.168.3.254      Down

Page 1   <Apply>                               Total 1 Pages
<OK>     <Prev Page>       <Next Page>       <Add>
                        Add OSPF area entry.
Use <TAB> or arrow keys to move. <Enter> to select.

```

Parameter	Description
Area ID	An identifier for the transit area the virtual link crosses.
Neighbor Router ID	The IP address of the OSPF router on this end of the virtual link.

**Note:**  
 To add a new OSPF Virtual Link, use the <Add> button. To modify or delete a virtual link, highlight the table entry with the cursor and select Enter.

**Modifying a Virtual Link** – You can modify or delete a virtual link by selecting the required entry in the table with your cursor and pressing Enter. The screen will display configuration options as shown in the following example.

```

                                Modify OSPF Virtual Link
                                =====
Area ID           : 192.168.3.0
Neighbor Router ID :
192.168.3.254

Transit Delay      : 1
Retransmit Interval : 5
Hello Interval     : 10
Dead Interval      : 40
Authentication Type : NONE
Authentication Key :
MD5 Key Table

<Delete>         <OK>
<Cancel>
Use <TAB> or arrow keys to move, <Space> to scroll options.

```

Parameter	Default	Description
Area ID		An identifier for the transit area the virtual link crosses.
Neighbor Router ID		The IP address of the OSPF router on this end of the virtual link.
Transit Delay	1 second	The estimated number of seconds it takes to transmit a link state update packet over this virtual link. Range: 0-3600 seconds
Retransmit Interval	5 seconds	The number of seconds between retransmitting link-state advertisements to the router at the other end on the virtual link. This value is also used when retransmitting database descriptions and link-state request packets. Range: 0-3600 seconds
Hello Interval <sup>2</sup>	10 seconds	The interval, in seconds, between sending Hello packets out the router interface. Range: 1-65535 seconds
Dead Interval <sup>2</sup>	40 seconds	The number of seconds that a router's Hello packets have not been seen before the router at the other end of the virtual link is declared down. This should be a multiple of the Hello interval. Range: 1-65535 seconds
Authentication Type	None	Authentication can be used to ensure that routing information comes from a valid source. The options include none or a simple password.
Authentication Key		A simple password must be provided if authentication is enabled. (An authentication string is case sensitive, and can be up to 16 characters.)

### ***OSPF Host Route Configuration***

A host route is a prefix that will be advertised as a stub network in one of the router's link state advertisements. These prefixes may be IP addresses of hosts directly attached to the router, which themselves do not run OSPF. The router advertises these addresses by proxy.

```

                                OSPF Host Route Configuration
                                =====
IP Address          Cost          Area ID

Page 1             <Apply>                Total 0 Pages
<OK>              <Prev Page>          <Next Page>          <Add>
                                The page number.
|READ/WRITE
  Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
IP Address	The IP address of this host.
Cost	The link state cost of this host.
Area ID	The area that the host belongs to.

**Configuring BOOTP / DHCP Relay**

If a DHCP / BOOTP server is not located in the same subnet with a host, you can configure this switch to forward any host configuration queries to a server located on another subnet or on another network. Depending on the configuration setup, the switch either:

- Forwards the packet to a preferred 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.

Specify the address for any DHCP server, or specify the subnet address for an outbound IP interface already configured on this switch (chapter 2 “Subnet Configuration”) as described in the following screens.

```

                                Bootp Relay Database Configuration
                                =====

Index Server Address
  1 10.1.2.3

                                <OK>                                <Add>

                                Return to previous panel.
                                Use <Enter> to select.

```

Parameter	Description
Index Server Address	Used to define any preferred DHCP servers or the outbound subnetwork for relaying a DHCP request broadcast. (Up to five entries are permitted.)

**IGMP Snooping Configuration**  
 If enabled, you can use the IGMP Snooping Configuration screen to configure multicast filtering as shown below. (For further details see "Configuring IGMP Snooping" on chapter 2.)

```

                                IGMP Snooping Configuration
                                =====

                                IGMP Router Timeout (Minutes) : 5
                                IGMP Group Timeout (Minutes)  : 5

                                <Apply>                                <OK>                                <Cancel>
                                IGMP router timeout value (minutes). |
READ/WRITE
                                Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Default	Description
IGMP Router Timeout	5	A switch port that stops receiving multicast protocol packets for this interval will be removed from the IGMP forwarding list. Range: 3 - 5 minutes

IGMP Group Timeout	5	The time between last spotting an IGMP Report message for an IP multicast address on a specific port and the switch removing that entry from its list. Range: 3 - 5 minutes
--------------------	---	--

### 2.5.6.3.Static ARP Configuration

Use the following screen to display or edit entries in the Static ARP Table. Entries added to this table are retained until the associated IP interface is deleted or the switch is reset to the factory defaults.

```

                                Static ARP Table
                                =====
                                IP Address      MAC Address      Interface

Page      1      <Apply>          Total      0          Pages
<OK>     <Prev Page>      <Next Page>      <Add>
                                Return to previous panel.
                                Use <Enter> to select.

```

Parameter	Description
IP Address	IP address statically mapped to a physical MAC address.
MAC Address	MAC address statically mapped to the corresponding IP address.
Interface	The index number of the IP interface that will use this static ARP entry. See chapter 2 "Subnet Configuration" or "Routing Table". (Port "0" refers to the CPU.)

### 2.5.6.4.Static Route Configuration

This switch can be configured to dynamically learn the routes to other IP networks, subnets or hosts using unicast or multicast routing protocols. If the route to a specific destination cannot be learned via these protocols or you wish to restrict the path used for transmitting traffic to a destination, it can be statically configured using the Static Route Table.

Before defining a static route, remember that you must first configure at least one IP interface on this switch (chapter 2 "Subnet Configuration"). Static routes take precedence over dynamically learned routes and remain in the table until you remove

them or the corresponding IP interface from this switch.

```

                                Static Route Table
                                =====
Destination Network   Destination Mask   VLAN   Next Hop
Type

Page      1   <Apply>           Total      0       Pages
<OK>     <Prev Page>       <Next Page>       <Add>
                                Return to previous panel.
                                Use <TAB> or arrow keys to move. <Enter> to select.

```

Parameter	Description
Destination Network	A destination network, subnet or host.
Destination Mask	The subnet mask that specifies the bits to match. A routing entry will be used for a packet if the bits in the address set by the destination mask match the Destination Network.
VLAN	The VLAN within which the gateway or destination address resides.
Next Hop	The IP address of the router at the next hop. Note that the network portion of the next hop must match that used for one of the subnet IP interfaces configured on this switch. (See "Subnet Configuration" on chapter 2.)
Type	The IP route type for the destination network. This switch supports the following types: Direct - A directly connected subnetwork. Indirect - A remote IP subnetwork or host address.

**Note:**

Use the <Next Page> and <Prev Page> buttons to scroll through the static route table. To display a specific page, set the page number in the Page field and then select <Apply>. To modify a static route, highlight the entry in the table and select Enter. To add a static route, select <Add>.

**Adding a Static Route** - The same screen is displayed for modifying or adding a static route. You must provide route information as described in the preceding table, plus the routing metric used to indicate the number of hops to the destination network.

```

Add Routing Entry
=====

Destination Address: 0.0.0.0
Destination Mask    : 255.255.255.0
Next Hop           : 0.0.0.0
Routing Metric     : 0

                                <OK>           <Cancel>
                                |
                                Destination IP address.

READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.

```

### 2.5.6.5. Configuring the Default Route

Defines the router to which this switch will forward all traffic for unknown networks. The default route can be learned from RIP protocol (chapter 2 “*Configuring RIP*”) or manually configured. If the switch does not contain a default route, any packet that does not match an entry in the routing table (chapter 2 “*Routing Table*”) will be dropped. To manually configure a default route, enter the next hop in the following table.

```

Default Route Menu
=====

VLAN                : ----
Next Hop Address    : 0.0.0.0
Metric              : 0

                                <Delete>       <OK>           <Cancel>
                                |
                                Enter Next Hop IP address.

READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
-----------	-------------

VLAN	The VLAN which has the IP interface to the default router. You cannot enter any value in this field. The switch will fill in the corresponding VLAN only after you specify the Next Hop Address and select Enter.
Next Hop Address	The IP address of the default router.
Metric	The number of hops required to reach the default router.

## 2.5.7. Configuring Security Filters

You can use the Security menu to filter MAC and IP addresses.

```

Security Menu
=====
MAC Filtering Configuration ...
Security Mode ...
IP Filtering Configuration ...

<OK>
Config MAC filtering database.
Use <TAB> or arrow keys to move. <Enter> to select.

```

Parameter	Description
MAC Filtering Configuration	Specifies the source or destination MAC address for any traffic to be filtered from the switch.
Security Mode	Configuration the security mode.
IP Filtering Configuration*	Specifies the source or destination IP address for any traffic to be filtered from the switch.

\* This menu item is only displayed if the intelligent switch is set to multilayer mode.

### 2.5.7.1. Configuring MAC Address Filters

Any node that presents a security risk or is functioning improperly can be filtered from this switch. You can drop all the traffic from a host device based on a specified MAC address. Traffic with either a source or destination address listed in the Security Filtering Configuration table will be filtered.

```

MAC Security Filtering Configuration
=====
-----
-
0080AD050000

Page      1      <Apply>          Total      0          Pages
<OK>      <Prev Page>      <Next Page>      <Add>
                                Return to previous panel.
                                Use <TAB> or arrow keys to move. <Enter> to select.

```

**Note:**

To add a MAC address to the security filter, use <Add>. To delete an address, highlight it with the cursor and select Enter.

To scroll through the address table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then select <Apply>.

### 2.5.7.2. Configuring Security Mode

In default type, the switch can auto learning the MAC Address from each port. If you want to let someone to use a specifies port and the other people can not use. You should disable the auto learning function and setup the uplink port (if one packet's DA does not define in any port, it would be forwarding to the uplink port). Then you must to set the static unicast address on the port that you allow someone to use.

```

Security Menu: Security Mode
=====

Learning Function      : DISABLED
Uplink PORT           : 24

<Apply>                <OK>                <Cancel>
Confirm current screen setting.
Use <TAB> or arrow keys to move. <Enter> to select.

```

### 2.5.7.3. Configuring IP Address Filters

If any node presents a security risk, you can filter all traffic for this node by entering its address into the IP Security Filter. Any packet passing through the switch that has a source or destination IP address matching an entry in this table will be filtered.

```
IP Security Filtering Configuration
=====
-----
10.1.1.1

Page      1    <Apply>          Total    0          Pages
<OK>      <Prev Page>    <Next Page>     <Add>
                Return to previous panel.
                Use <TAB> or arrow keys to move. <Enter> to select.
```

**Note:**

To add an IP address to the security filter, use <Add>. To delete an address, highlight it with the cursor and select Enter.

Use the <Next Page> and <Prev Page> buttons to scroll through the table. To display a specific page, set the page number in the Page field and then select <Apply>. To add an entry, select <Add>.

## 2.6. Monitoring the Switch

The Network Monitor Menu provides access to port statistics, address tables, STA information, VLANs registration and forwarding information and multicast groups. Each of the screens provided by these menus is described in the following sections.

```

Network Monitor Menu
=====

Port Statistics ...

Layer 2 Address Table ...

Bridge Menu ...

VLAN Menu ...

IP Multicast Registration Table ...

IP Menu ...

<OK>
Display port statistics.
Use <TAB> or arrow keys to move. <Enter> to select.

```

Menu	Description
Port Statistics	Displays statistics on port traffic, including information from the Interfaces Group, Ethernet-like MIB, and RMON MIB.
Layer 2 Address Table	Contains the unicast address table.
Bridge Menu	Displays Spanning Tree settings for the overall switch and for specific ports.
VLAN Menu	Displays ports dynamically learned through GMRP or GVRP, and ports that are currently forwarding VLAN traffic.
IP Multicast Registration Table <sup>1</sup>	Displays all the multicast groups active on this switch, including the multicast IP address and the corresponding VLANs.
IP Menu <sup>2</sup>	Displays all the IP subnets used on this switch, as well as the corresponding VLANs and ports. Also contains the ARP table, routing table, multicast menu, and OSPF menu.

1. This menu is only displayed when intelligent switch is set to Layer 2 mode or the switch is management model.
2. This menu is only displayed if the intelligent switch is set to multilayer mode.

## 2.6.1. Displaying Port Statistics

Port Statistics display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMOM MIB.

```

                Statistics Menu
                =====

                Port Statistics ...

                RMON Statistics ...

                <OK>
                Display port statistics.
                Use <TAB> or arrow keys to move. <Enter> to select.

```

Parameter	Description
Port Statistics	Displays standard statistics on network traffic passing through the selected port.
RMON Statistics	Displays detailed statistics for the selected port, such as packet type and frame size counters.

### 2.6.1.1. Displaying Ethernet Port Statistics

Port Statistics display key statistics from the Interfaces Group and Ethernet-like MIBs for each port. Error statistics on the traffic passing through each port are displayed. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). The values displayed have been accumulated since the last system reboot.

Select the required port. The statistics displayed are indicated in the following figure and table.

```

                                Port Statistics
                                =====
Interfaces
  In Octets                      : 0          Out
Octets      : 0
  In Unicast Pkts                : 0          Out Unicast
Pkts        : 0
  In Non-Unicast Pkts           : 0          Out Non-Unicast
Pkts      : 0
  In Discards                    : 0          Out
Discards    : 0
  In Errors                      : 0          Out
Errors      : 0
  Alignment Errors               : 0          CRC
Errors      : 0
Ethernet
  Single Collisions              : 0          Multiple
Collisions  : 0
  Defered Transmissions          : 0          Late
Collisions  : 0
  Excess Collisions              : 0          Carrier Sense
Errors      : 0
  Drop Events                    : 0
Fragments   : 0
  Octets                          : 0
Jabbers     : 0

  Port Number: 1    <Apply>          <Reset>
<Reset All>
  <OK>              <Refresh>       <Next Port>
<Prev Port>

                                Return to previous panel.
                                Use <TAB> or arrow keys to move. <Enter> to select.

```

Parameter	Description
<i>Interfaces Group</i>	
In Octets	The total number of octets received on the interface, including framing characters.
In Unicast Pkts.	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
In Non-Unicast Pkts.	The number of non-unicast (i.e., subnetwork- broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.

In Discards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
In Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Alignment Errors	The number of alignment errors (missynchronized data packets).
Out Octets	The total number of octets transmitted out of the interface, including framing characters.
Out Unicast Pkts.	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Out Non-Unicast Pkts.	The total number of packets that higher-level protocols requested be transmitted to a non-unicast (that is, a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent.
Out Discards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Out Errors	The number of outbound packets that could not be transmitted because of errors.
CRC Errors	Number of Ethernet Cyclic Redundancy Check errors detected by this device.
<i>Ethernet-Like</i>	
Single Collisions	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Excessive Collisions	The number of frames for which transmission failed due to excessive collisions.
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Octets	Number of octets passing through this port.
Multiple Collisions	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.

Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
---------	---

**Note:**

Statistics are refreshed every 10 seconds by default (chapter 2 “Configuring the Serial Port”).

### 2.6.1.2. Displaying RMON Statistics

Use the RMON Statistics screen to display key statistics for each port from RMON group 1. (RMON groups 2, 3 and 9 can only be accessed using SNMP management software.) The following screen displays the overall statistics on traffic passing through each port. RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. Values displayed have been accumulated since the last system reboot.

```

                                RMON Statistics
                                =====
Jabbers      Drop Events          : 0
              Bytes              : 0
Collisions   : 0
              Frames             : 0          64 Byte
Frames      : 0
              Broadcast Frames   : 0          65-127 Byte
Frames      : 0
              Multicast Frames   : 0          128-255 Byte
Frames      : 0
              CRC/Alignments Errors : 0          256-511 Byte
Frames      : 0
              Undersize Frames    : 0          512-1023 Byte
Frames      : 0
              Oversize Frames     : 0          1024-1518 Byte
Frames      : 0
              Fragments          : 0          1519-1536 Byte

Port Number:  1      <Apply>          <Reset>
<Reset All>
  <OK>          <Refresh>          <Next Port>
<Prev Port>

                                Return to previous panel.
                                Use <TAB> or arrow keys to move. <Enter> to select.

```

<b>Parameter</b>	<b>Description</b>
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC / Alignment Errors	The number of CRC / alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Byte Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

**Note:**

Statistics are refreshed every 10 seconds by default (chapter “Configuring the Serial Port”).

## 2.6.2.Layer 2 Address Table

This menu includes the unicast address table.

```

Layer 2 Address Table
=====
Unicast Address Table ...

<OK>
Display the unicast address table.
Use <TAB> or arrow keys to move. <Enter> to select.

```

Menu	Description
Unicast Address Table	Provides a full listing for unicast addresses.

### 2.6.2.1. Displaying the Unicast Address Table

The Unicast Address Table contains the MAC addresses associated with each port (that is, the source port associated with the address). The information displayed in the Address Table is indicated in the following figure and table.

```

Layer 2 Menu: Unicast Address Table
=====
Address          Port          Address          Port
00-80-AD-05-00-00  1

Page 1 <Apply>          Total 0          Pages
<OK>          <Next Page>          <Prev

Page>

Return to previous panel.
Use <TAB> or arrow keys to move. <Enter> to select.

```

Parameter	Description
Address	The MAC address of a node seen on this switch.
Port	The port whose address table includes this MAC address.

**Note:** Use the <Next Page> and <Prev Page> buttons to scroll through the table. To display a specific page, set the page number in the Page field and then select <Apply>.

## 2.6.3. Displaying Bridge Information

The Bridge menu is used to display settings for the Spanning Tree Algorithm. For a more detailed description of how to use this algorithm, refer to “Spanning Tree Algorithm” on chapter 4.

```

                                Bridge Menu
                                =====

                                Spanning Tree Bridge Information ...
                                Spanning Tree Port Information ...

                                <OK>
                                Display the spanning tree information.
                                Use <TAB> or arrow keys to move. <Enter> to select.
    
```

Menu	Description
Spanning Tree Bridge Information	Displays a full list of STA values used for the bridge.
Spanning Tree Port Information	Displays a list of STA values used for each port, including status, designated cost, designated bridge, and designated port.

### 2.6.3.1. Viewing the Current Spanning Tree Information

The STA Bridge Information screen displays a summary of STA information for the overall bridge. To make any changes to these parameters, use the Bridge STA Configuration menu as described on chapter 2 “Configuring Global Bridge Settings”. The parameters shown in the following figure and table describe the current Bridge STA settings.

```

                Bridge Menu: Spanning Tree Bridge Information
                =====

Priority          : 32768
Hello Time (in seconds) : 2
Max Age (in seconds)   : 20
Forward Delay (in seconds) : 15
Hold Time (in seconds)  : 1
Designated Root      : 32768.00E800340000
Root Cost            : 0
Root Port           : 0
Configuration Changes : 0
Topology Up Time     : 847850 (0 day 2 hr 21 min 18
sec)

                <OK>
                Return to previous panel.
                Use <Enter> to select.

```

Parameter	Description
Priority	Device priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
Hello Time	The time interval (in seconds) at which the root device transmits a configuration message.
Max Age	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure.
Forward Delay	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding).
Hold Time	The minimum interval between the transmission of consecutive Configuration BPDUs.
Designated Root	The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
Root Cost	The path cost from the root port on this switch to the root device.
Root Port	The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
Configuration Changes	The number of times the Spanning Tree has been reconfigured.
Topology Up Time	The time since the Spanning Tree was last reconfigured.

## 2.6.3.2. Displaying the Current STA for Ports

The parameters shown in the following figure and table are for port STA Information.

```

Bridge Menu: Spanning Tree Port Information (Port
1-12)
=====
Port      Type      Status      Designated      Designated
Designated
Cost      Bridge
-----
-----
   1      100TX      DISABLED      0      32768.00E800340000
128.1
   2      100TX      DISABLED      0      32768.00E800340000
128.2
   3      100TX      DISABLED      0      32768.00E800340000
128.3
   4      100TX      DISABLED      0      32768.00E800340000
128.4
   5      100TX      DISABLED      0      32768.00E800340000
128.5
   6      100TX      DISABLED      0      32768.00E800340000
128.6
   7      100TX      DISABLED      0      32768.00E800340000
128.7
   8      100TX      DISABLED      0      32768.00E800340000
128.8
   9      100TX      DISABLED      0      32768.00E800340000
128.9
  10      100TX      DISABLED      0      32768.00E800340000
128.10
  11      100TX      DISABLED      0      32768.00E800340000
128.11
  12      100TX      DISABLED      0      32768.00E800340000
128.12

                <OK>                <Prev Page>                <Next
Page>

                Return to previous panel.
                Use <TAB> or arrow keys to move. <Enter> to select.

```

Parameter	Description
-----------	-------------

Type	Shows port type as: 100TX : 10BASE-T / 100BASE-TX 100FX : 100BASE-FX 1000SX/LX : 1000BASE-SX/X (multimode/ single mode) 1000T : 1000BASE-T
Status	Displays current state of this port within the Spanning Tree: Disabled No link has been established on this port. Otherwise, the port has been disabled by the user or has failed diagnostics. Blocking Port receives STA configuration messages, but does not forward packets. Listening Port will leave blocking state due to a topology change, start transmitting configuration messages, but does not yet forward packets. Learning Port has transmitted configuration messages. For an interval set by the Forward Delay Parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses. Forwarding The port forwards packets, and continues learning addresses. The rules defining port status are: <ul style="list-style-type: none"> <li>• A port on a network segment with no other STA-compliant bridging device is always forwarding.</li> <li>• If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is blocked.</li> <li>• All ports are blocked when the switch is booted, then some of them change state to listening, to learning, and then to forwarding.</li> </ul>
Designated Cost	The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
Designated Bridge (ID)	The priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
Designated Port (ID)	The priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.

## 2.6.4. Displaying VLAN Information

These menus display information on the ports that have been automatically learned via GVRP, and all the ports that have been configured by dynamic or static means to forward VLAN traffic.

```

                                VLAN Information
                                =====

                                VLAN Dynamic Registration Information ...

                                VLAN Forwarding Information ...

                                <OK>

                                Display VLAN dynamic registration information.
                                Use <TAB> or arrow keys to move. <Enter> to select.

```

Menu	Description
VLAN Dynamic Registration Information	Shows the ports that have been automatically learned via GVRP.
VLAN Forwarding Information	Shows all the ports that have been configured by either dynamic or static means to forward VLAN traffic.

### 2.6.4.1.VLAN Dynamic Registration Information

This table shows the ports that have been automatically learned via GVRP.

```

                                VLAN Dynamic Registration Information
                                =====

                                Port          1          2
                                12345678901234567890123456
                                1
                                Dynamic
                                D:

                                Page : 1   <Apply>                Total: 1   Pages
                                <OK>    <Prev Page>          <Next Page>
                                Enter page number than press 'Apply' to see VLAN group. |
                                READ/WRITE
                                Use <TAB> or arrow keys to move, other keys to make changes.

```

**Note:**

To scroll through the table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then select <Apply>.



```

                                IP Multicast Registration Table
                                =====
                                1          2
VLAN Multicast IP      12345678901234567890123456
Learned by

                                Page 1      <Apply>          Total 0 Pages
                                <OK>      <Prev Page>      <Next Page>
                                The page number.
| READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
VLAN	A VLAN with host members that have asked to receive the indicated multicast service.
Multicast IP	A multicast group address that represents a specific multicast service.
(Multicast Group Port List)	The ports that belong to the indicated VLAN group.
Learned by	Shows if this entry was learned dynamically or via IGMP Snooping. An entry is learned dynamically if a multicast packet was seen crossing the port, or via IGMP Snooping if an IGMP registration packet was seen crossing the port.

**Note:**

To scroll through the table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then select <Apply>.

## 2.6.6.IP Menu

This menu contains IP subnet information, the ARP cache, routing table, as well as multicast groups and multicast routing information.

```

IP Address Table
=====
Subnet Information ...
ARP Table ...
Routing Table ...
Multicast Table ...
OSPF Table ...

<OK>
Display and change the static route table.
Use <TAB> or arrow keys to move. <Enter> to select.

```

Menu	Description
Subnet Information	Displays all the IP subnets configured on this switch, as well as the corresponding VLANs and ports.
ARP Table	Shows the IP-to-MAC addresses discovered by ARP.
Routing Table	Shows the routes through which all recognized Ethernet networks (and the corresponding VLAN) can be reached.
Multicast Table	Displays all the multicast groups active on this switch, including the multicast IP address and the corresponding VLANs. Also includes the IGMP registration table, the multicast forwarding cache, and DVMRP routing information.
OSPF Table	Displays a link state advertisement summary, the neighbor table, and the virtual neighbor table.

### 2.6.6.1. Displaying Subnet Information

You can display a list of all the IP interfaces configured on this switch. This table includes the gateway address, corresponding VLAN, and member ports that use this address.



```

                                ARP Table
                                =====
                                IP Address      MAC Address      VLAN  Port
                                192.168.1.254    00-80-00-00-11-22  1    1

Page 1      <OK>      <First Page>      <Next
Page>

                                Return to previous panel.
                                Use <TAB> or arrow keys to move. <Enter> to select.

```

Parameter	Description
IP Address	IP addresses for which ARP has resolved the physical address through a broadcast message.
MAC Address	MAC address that maps to the corresponding IP address.
VLAN	The VLAN group to which this host has been assigned.
Port	The port to which this host device is attached. (Port "0" refers to an interface defined on this switch.)

**Note:**  
 To scroll through the table, use the <First Page> and <Next Page> buttons.

### 2.6.6.3. Routing Table

The Routing Table lists the routes through which all recognized Ethernet networks (and corresponding VLANs) can be reached. This table includes all routes learned through routing protocols or manual configuration.

```

                                Routing Table
                                =====
Destination Network  Destination Mask  VLAN  Next Hop  Type
Protocol
192.168.1.0          255.255.255.0    1     192.168.2.10  Direct
Local

                                Page      1    <Apply>          Total      0    Pages
                                <OK>    <Prev Page>      <Next Page>      <Flush>
RIP>

                                Return to previous panel.
                                Use <TAB> or arrow keys to move. <Enter> to select.

```

Parameter	Description
Destination Network	A destination network, subnet or host.
Destination Mask	The subnet mask that specifies the bits to match. A routing entry will be used for a packet if the bits in the address set by the destination mask match the Destination Network.
VLAN	The VLAN within which the gateway or destination address resides.
Next Hop	The IP address of the router at the next hop.
Type	The IP route type for the destination network. This switch supports the following types: Direct - A directly connected subnetwork. Indirect - 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. Invalid - An illegal IP address to be filtered.
Protocol	The route was learned in one of the following ways: Local - Manually configured Mgmt. - Set via SNMP ICMP - Obtained via ICMP redirect RIP - Learned via RIP protocol OSPF - Learned via OSPF protocol Other - Learned by some other method

**Note:**  
To scroll through the table, use the <Next Page> and <Prev Page> buttons. To

display a specific page, set the page number in the Page field and then select <Apply>. Select <Flush RIP> to clear any routing entries learned through RIP.

### ***Displaying Detailed Routing Information***

To display detailed routing information, select any entry in the Routing Table with your cursor and select Enter. The following screen will display. All items displayed on this page are the same as those shown in the Routing Table, except for Routing Metric, which represents a relative measure of the path cost from this switch to the destination network. (Note that this metric depends on the specific routing protocol.)

```
Detailed Routing Entry
=====

Destination Address: 192.168.1.0
Destination Mask    : 255.255.255.0
VLAN                : 1

Next Hop            : 192.168.2.10
Type                : Direct
Protocol            : Local

Routing Metric      : 1

                <OK>
                Return to previous panel.
                Use <Enter> to select.
```

### **2.6.6.4. Multicast Table**

You can use this menu to display all the multicast groups currently active on this switch, the IGMP registration table, the multicast forwarding cache, and DVMRP routing information.

```

Multicast Table Menu
=====

IP Multicast Registration Table ...
IGMP Cache ...
Multicast Forwarding Cache Table ...
DVMRP Routing Table ...
DVMRP Neighbor Table ...

<OK>
Display IP Multicast registration table.
Use <TAB> or arrow keys to move. <Enter> to select.

```

Parameter	Description
IP Multicast Registration Table	Displays all active multicast groups, including the multicast IP address and the corresponding VLANs. (See chapter 2 “IP Multicast Registration Table”.)
IGMP Cache	Displays all active multicast groups, including the IP interface each entry appears on, the entry age, and the time left before the entry is aged out.
Multicast Forwarding Cache Table	Displays all active multicast groups, including the multicast source address, the upstream neighbor, the multicast routing protocol, and the entry age.
DVMRP Routing Table	Displays the source address for each known multicast service, the upstream neighbor, the IP interface each entry appears on, the routing metric, and the entry age.
DVMRP Neighbor Table	Displays all the neighbor routers accessible through each IP interface, including the entry age, the time left before the entry is aged out, the protocol version, and the number of routing updates received from each neighboring router.

**Displaying IGMP Cache**

The switch provides a local registry of active multicast groups for each IP interface, including the age and expiration time for each entry.

```

                                IGMP Cache
                                =====
Group Address   Intf Reporter           Up Time   Expire    V1
Timer

Page 1         <Apply>                Total 0   Pages
<OK>          <Prev Page>           <Next Page>
                The page number.

| READ/WRITE
  Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
Group Address	An IP multicast group address with subscribers directly attached or downstream from this switch.
Intf	The IP interface on this switch that has received traffic directed to the IP multicast group address (see chapter 2 “Displaying Subnet Information”).
Reporter	IP address of the source of the last membership report received for this multicast group on this interface. If no membership report has been received, this object has the value 0.0.0.0.
Up Time	The time elapsed since this entry was created.
Expire	The time remaining before this entry will be aged out. (The default is 260 seconds.)
V1 Timer	The time remaining until the switch assumes that there are no longer any IGMP Version 1 members on the IP subnet attached to this interface. (The default is 400 seconds.) If the switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts present which are members of the group for which it heard the report. If there are Version 1 hosts present for a particular group, the switch will ignore any Leave Group messages that it receives for that group.

**Note:** To scroll through the table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then select <Apply>.

### **Displaying the Multicast Forwarding Cache**

The switch maintains a cache of multicast routing entries used to calculate the delivery tree in multicast routing protocols. The Multicast Forwarding Cache includes the subnetwork that contains the multicast source and the nearest upstream neighbor for

each known multicast group address.

```

                                Multicast Forwarding Cache
                                =====
Group Address   Source Address  Mask Upstream Nbr   Protocol Up
Time

Page 1         <Apply>                Total 0  Pages
<OK>          <Prev Page>          <Next Page>
                The page number.
| READ/WRITE
  Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
Group Address	An IP multicast group address with subscribers directly attached or downstream from this switch.
Source Address	The IP subnetwork at the root of the multicast delivery tree. This subnetwork contains a known multicast source.
Mask	Subnet mask that is used for the source address. This mask identifies the host address bits used for routing to specific subnets.
Upstream Nbr	The IP address of the network device immediately upstream for this group.
Protocol	The multicast routing protocol associated with this entry.
Up Time	The time elapsed since this entry was created.

**Note:**

To scroll through the table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then select <Apply>.

**Displaying the DVMRP Routing Table**

The DVMRP Routing Table contains all the IP multicast routes learned by the DVMRP protocol. The routes displayed in this table are used by this switch to forward new IP multicast traffic. They do not reflect active multicast flows.

```

                                DVMRP Routing Table
                                =====
Source Address  Mask Upstream Nbr   Interface      Metric
Up Time

Page 1          <Apply>          Total 0 Pages
<OK>           <Prev Page>     <Next Page>
                The page number.

| READ/WRITE
  Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
Source Address	The IP subnetwork at the root of the multicast delivery tree. This subnetwork contains a known multicast source.
Subnet Mask	Subnet mask that is used for the source address. This mask identifies the host address bits used for routing to specific subnets.
Upstream Nbr	The IP address of the network device immediately upstream for this multicast delivery tree.
Interface	The IP interface on this switch that connects to the upstream neighbor (see chapter 2 “Displaying Subnet Information”).
Metric	The metric for this interface used to calculate distance vectors.
Up Time	The time elapsed since this entry was created.

**Note:**  
 To scroll through the table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then select <Apply>.

**Displaying the DVMRP Neighbor Table**

The DVMRP Neighbor Table contains the switch’s DVMRP neighbors, as discovered by receiving DVMRP protocol messages.

```

                                DVMRP Neighbor Table
                                =====
Interface      Neighbor Address UpTime    ExpireTime Ver
RcvRoute

Page 1        <Apply>                Total 0 Pages
<OK>         <Prev Page>           <Next Page>
                                The page number.
| READ/WRITE
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
Interface	The IP interface on this switch that connects to the upstream neighbor (see chapter 2 “Displaying Subnet Information”).
Neighbor Address	The IP address of the network device immediately upstream for this multicast delivery tree.
UpTime	The time since this device last became a DVMRP neighbor to this switch.
ExpireTime	The time remaining before this entry will be aged out.
Ver	The neighboring router’s DVMRP version number.
RcvRoute	The total number of routes received in valid DVMRP packets from this neighbor. This can be used to diagnose problems such as unicast route injection, as well as giving an indication of the level of DVMRP route exchange activity.

**Note:**  
 To scroll through the table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and then select <Apply>.

### 2.6.6.5.OSPF Table

You can use this menu to display the OSPF router linkages for the autonomous system based on the Interface Table, Link State Table, Neighbor Table, and Virtual Neighbor Table.

```

                OSPF Table Menu
                =====

                Interface Table ...

                Link State Table ...

                Neighbor Table ...

                Virtual Neighbor Table ...

                <OK>
                Display interface database.
                Use <TAB> or arrow keys to move. <Enter> to select.

```

Parameter	Description
Interface Table	
Link State Table	Displays a summary of link state advertisements.
Neighbor Table	Displays current neighbor routers.
Virtual Neighbor Table	Displays current virtual neighbors.

### ***Displaying the Interface Table***

You can use this menu to display parameters of OSPF interfaces.

```

                OSPF Interface Table
                =====

IP Address      Rtr ID  Designated Rtr  Backup DR      Status
Events
192.168.1.254  0       0.0.0.0         0.0.0.0       Down
0

                Page 1      <Apply>          Total 1  Pages
                <OK>      <Prev Page>     <Next Page>
                The page number.

| READ/WRITE
                Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
IP Address	The IP address of this OSPF interface.

Rtr ID	Router ID for this router.
Designated Rtr	The IP of the designated router. The designated router advertises the link state of the OSPF area.
Backup DR	The backup designated router. If the designated router fails, the backup designated router takes its place.
Status	This interface's status in this OSPF area.
Events	The number of events since this designated router was selected.

### **Displaying the Link State Table**

The link state table displays all advertisements in the link state database. This database contains linkage information for all the areas to which this router is attached. Note that all the routers within an area exchange information to ensure that they maintain an identical link state database. This database can therefore be used to troubleshoot network configuration problems.

```

                                OSPF Link State Table
                                =====
Area Identity   Type   Link State Id   Router ID       Sequence No
Age
0.0.0.0         RtrLSA 192.168.1.254   192.168.1.254
0x80000002     1489

Page 1          <Apply>          Total 0 Pages
<OK>           <Prev Page>      <Next Page>
                The page number.

| READ/WRITE
  Use <TAB> or arrow keys to move, other keys to make changes.

```

<b>Parameter</b>	<b>Description</b>
Area Identity	An OSPF area identifier configured for a group of OSPF routers. (For information on how to assign this identifier to a specific interface, see chapter 2 “Configuring OSPF”.)

Type	The link state advertisement type: RtrLSA: Router LSA – All area routers advertise the state of links from the router itself to the its local area. NetLSA: Network LSA – The designated router for each Area advertises the link state for each transit area; i.e., an area with more than one attached router. This LSA includes information about each router attached to the area, including the designated router itself. SumLSA: Summary LSA – Advertise the cost to a specific subnetwork outside the router’s area, or the cost to a specific autonomous system boundary router. ExtLSA: External LSA – Advertises link state information for each known network outside the autonomous system.
Link State ID	The identifier for the router originating this entry, usually in the form of an IP address.
Router ID	The IP address of the originating router.
Sequence No	The link state sequence number, used to remove previous duplicate LSAs.
Age	The number of seconds since this LSA was originated.

**Note:**

To scroll through the table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and select <Apply>.

***Displaying the Neighbor Table***

Each router exchanges link state information with all neighbors physically attached to the same network segment. This table displays a summary of the link state for all adjacent neighbors. (Note that neighboring routers are discovered by this device via Hello messages.).

```

                                OSPF Neighbor Table
                                =====
IP Address      ID      Router ID      Option      Priority State
Events

Page 1          <Apply>          Total 0 Pages
<OK>           <Prev Page>      <Next Page>
                The page number.

| READ/WRITE
  Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
IP Address	IP address of the neighboring router.
ID	The index number of the router interface to which this neighbor is attached. For IP protocol, this value will always be zero.
Router ID	The OSPF identifier for the neighboring router.
Option	The optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its Hello packets. This enables received Hellos to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities. The OSPF optional capabilities currently accepted include external routing capability and TOS capability. You need to map the binary bits to the supported options. For example, "3" indicates both routing capability and TOS capability.
Priority	The neighbor's router priority. This priority is used in electing the designated router for the area in which it exists. This value will be set to zero if this router cannot be elected.

State	<p>The communication state for two adjacent routers:</p> <p><b>Down:</b> This is the initial state of a neighbor conversation. It indicates that there has been no recent information received from the neighbor.</p> <p><b>Attempt:</b> This state is only valid for neighbors attached to non-broadcast networks. It indicates that no recent information has been received from the neighbor, but that the router is attempting to contact the neighbor by sending Hello packets.</p> <p><b>Init:</b> A Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor.</p> <p><b>2-Way:</b> Communication between the two routers has been established. This is the most advanced state short of beginning adjacency establishment. Note that both the Designated Router and Backup Designated Router are selected from the set of neighbors in state 2-Way or greater.</p> <p><b>ExStart:</b> This is the first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial sequence number. Neighbor conversations in this state or greater are called adjacencies.</p> <p><b>Exchange:</b> The router is describing its entire link state database by sending database description packets to the neighbor. (Each database description packet has a sequence number, and is explicitly acknowledged.) All adjacencies in Exchange state or greater are used by the flooding procedure. In fact, these adjacencies are fully capable of transmitting and receiving all types of OSPF routing protocol packets.</p> <p><b>Loading:</b> Link State Request packets are sent to the neighbor asking for more recent advertisements that have been discovered (but not yet received) in the exchange state.</p> <p><b>Full:</b> The neighboring routers are fully adjacent. These adjacencies will now appear in router links and network links advertisements.</p>
Events	The number of events encountered that cause a neighbor state change since boot up.

**Note:**

To scroll through the table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and select <Apply>.

***Displaying the Virtual Neighbor Table***

Virtual links can be used to link an area isolated from the backbone, to create a redundant link between any area and the backbone to help prevent partitioning, or to connect two existing backbone areas into a common backbone. Note that the processes of establishing a active link between virtual neighbors is similar to that used for

physically adjacent neighbors.

```

                                OSPF Virtual Neighbor Table
                                =====
Area ID          Router ID      IP Address      Option   State
Events

Page 1          <Apply>                Total 0  Pages
<OK>           <Prev Page>          <Next Page>
                The page number.
| READ/WRITE
  Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
Area ID	The transit area the virtual link must cross to connect the border routers.
Router ID	The OSPF identifier for the router at the other end of the link.
IP Address	IP address of the border router at the other end of the link.
Option	The optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its Hello packets. This enables received Hellos to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities. The OSPF optional capabilities currently accepted include external routing capability and TOS capability. You need to map the binary bits to the supported options. For example, "3" indicates both routing capability and TOS capability.

State	<p>The communication state for two adjacent routers:</p> <p><b>Down:</b> This is the initial state of a neighbor conversation. It indicates that there has been no recent information received from the neighbor.</p> <p><b>Attempt:</b> This state is only valid for neighbors attached to non-broadcast networks. It indicates that no recent information has been received from the neighbor, but that the router is attempting to contact the neighbor by sending Hello packets.</p> <p><b>Init:</b> A Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor.</p> <p><b>2-Way:</b> Communication between the two routers has been established. This is the most advanced state short of beginning adjacency establishment. Note that both the Designated Router and Backup Designated Router are selected from the set of neighbors in state 2-Way or greater.</p> <p><b>ExStart:</b> This is the first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial sequence number. Neighbor conversations in this state or greater are called adjacencies.</p> <p><b>Exchange:</b> The router is describing its entire link state database by sending database description packets to the neighbor. (Each database description packet has a sequence number, and is explicitly acknowledged.) All adjacencies in Exchange state or greater are used by the flooding procedure. In fact, these adjacencies are fully capable of transmitting and receiving all types of OSPF routing protocol packets.</p> <p><b>Loading:</b> Link State Request packets are sent to the neighbor asking for more recent advertisements that have been discovered (but not yet received) in the exchange state.</p> <p><b>Full:</b> The neighboring routers are fully adjacent. These adjacencies will now appear in router links and network links advertisements.</p>
Events	The number of events encountered that cause a neighbor state change since boot up.

**Note:** To scroll through the table, use the <Next Page> and <Prev Page> buttons. To display a specific page, set the page number in the Page field and select <Apply>.

## 2.7.Resetting the System

Use the Restart command under the Main Menu to reset the management agent. The reset screen is shown below.

```

System Restart Menu
=====

Restart Option  :

Reload Factory Defaults  : NO

                                <Restart>          <Cancel>
Restart system with the factory default settings.
|EAD/SELECT
Use <TAB> or arrow keys to move, <Space> to scroll options.

```

Parameter	Description
Reload Factory Defaults	Reloads the factory defaults
[Restart]	Restarts the switch.

**Note:**

When the system is restarted, it will always run the Power-On Self-Test. It will also retain all system information, unless you elect to reload the factory defaults.

## 2.8. Logging Off the System

Use the Exit command under the Main Menu to exit the configuration program and terminate communication with the switch for the current session.

## 3. Web Interface

### 3.1. Web-Based Configuration and Monitoring

In addition to the menu-driven system configuration program, this switch also provides an embedded HTTP Web agent. Using a Web browser you can configure the switch and view statistics to monitor network activity. The Web agent can be accessed by any computer on the network using a standard Web browser (Internet Explorer 4.0 or above, or Netscape Navigator 4.0 or above).

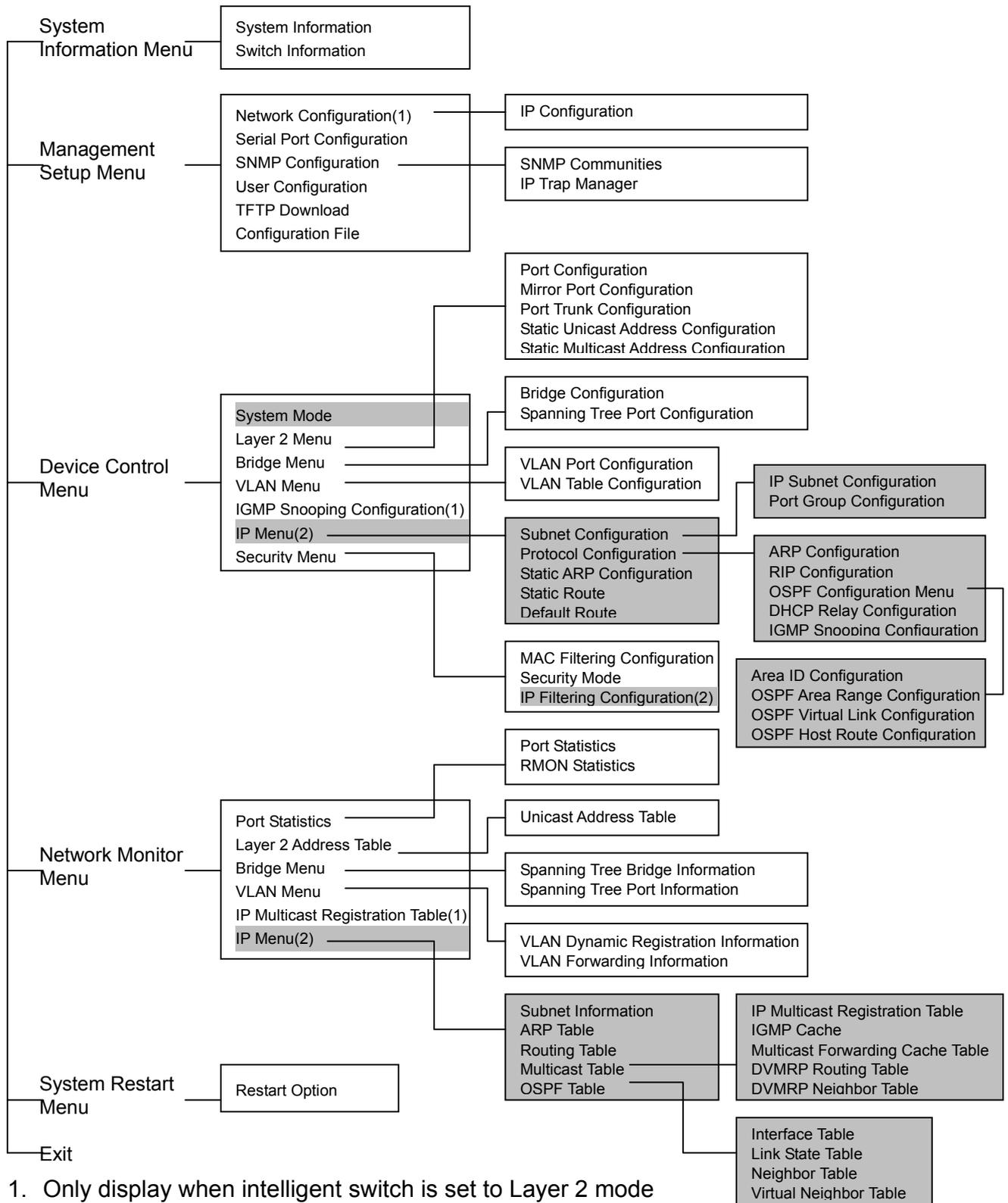
Prior to accessing the switch from a Web browser, be sure you have first performed the following tasks:

1. Configure it with a valid IP address and subnet mask (for Layer 2 mode) using an out-of-band serial connection or BOOTP protocol (Appendix A). Provide a default gateway for Layer 2 operation (chapter 2 "IP Configuration") or a default route for multilayer operation (chapter 2 "Configuring the Default Route").
2. Set a user name and password using an out-of-band serial connection (chapter 2 "User Log-in Configuration"). Access to the Web agent is controlled by the same user name and password as the onboard configuration program.

**Note:**

If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Algorithm, then you can set the switch port attached to your management station to Fast Forwarding (chapter 3 "Configuring the STA for Ports") to improve the switch's response time to management commands issued through the Web interface.

After you enter the user name and password, you will have access to the system configuration program illustrated by the following menu hierarchy:



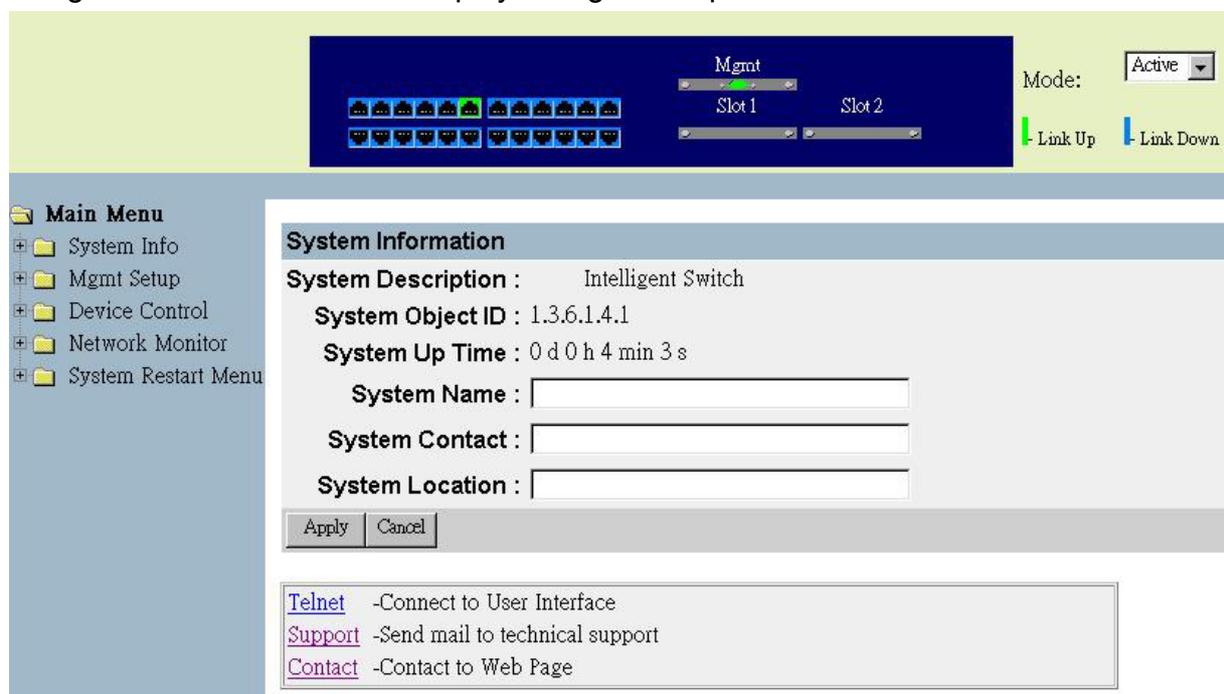
1. Only display when intelligent switch is set to Layer 2 mode or the switch is management model.
2. Only display when intelligent switch is set to multilayer mode.

## 3.2.Navigating the Web Browser Interface

To access the Web-browser interface you must first enter a user name and password. The administrator has Read / Write access to all configuration parameters and statistics. The default user name for the administrator is “admin,” with no password.

### 3.2.1.Home Page

When your Web browser connects with the switch’s Web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and System Information on the right side. The Main Menu links are used to navigate to other menus and display configuration parameters and statistics.



If this is your first time to access the management agent, you should define a new Administrator name and password, record it and put it in a safe place. Select Mgt Setup / User Cfg. from the Main Menu, and then enter a new name and password for the Administrator. Note that user names and passwords can consist of up to 11 alphanumeric characters and are not case sensitive.

#### Note:

You are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

### 3.2.2.Configuration Options

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the “Apply” button at the bottom

of the page to confirm the new setting. The following table summarizes the Web page configuration buttons.

Web Page Configuration Buttons	
Button	Action
Apply	Sets specified values in the SNMP agent.
Cancel	Cancel specified values prior to pressing the “Apply” button.
Refresh	Immediately updates values from the SNMP agent.

**Notes:**

1. To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu “Tools / Internet Options / General / Temporary Internet Files / Settings,” the setting for item “Check for newer versions of stored pages” should be “Every visit to the page.”
2. When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser’s refresh button.

### 3.2.3. Panel Display

The Web agent displays an image of the switch’s ports, showing port links and activity. Clicking on the image of a port displays statistics and configuration information for the port. Clicking on the image of the serial port (labeled “Mgmt”) displays the Console Configuration screen. Clicking on any other part of the front panel displays switch version information as described on chapter 3 “Displaying Switch Version Information”.



### 3.2.4. Port State Display

Click on any port to display a summary or port status as shown below, as well as Etherlike statistics (chapter 3 “Displaying Ethernet Port Statistics”).

Port 1 state summary	
Name	
Type	100BASE-TX
Admin Status	Enabled
Link Status	Down
Speed Status	10M
Duplex Status	Half
Flow Control Status	Off
VLAN ID	1

Parameter	Description
Type	Shows port type as: 100BASE-TX : 10BASE-T / 100BASE-TX 100BASE-FX : 100BASE-FX 1G BASE-SX/LX : 1000BASE-SX/LX (multimode/ single mode) 1G BASE-T : 1000BASE-T
Admin Status	Shows if the port is enabled, or has been disabled due to abnormal behavior or for security reasons. See “Configuring Port Parameters” on chapter 3.
Link Status	Indicates if the port has a valid connection to an external device.
Speed Status	Indicates the current port speed.
Duplex Status	Indicates the port’s current duplex mode.
Flow Control Status	Shows the flow control type in use. Flow control can eliminate frame loss by “blocking” traffic from end stations connected directly to the switch.
VLAN ID	The VLAN ID assigned to untagged frames received on this port. Use the PVID (chapter 3 “VLAN Port Configuration”) to assign ports to the same untagged VLAN.

### 3.2.5. Configuring the Serial Port

If you are having difficulties making an out-of-band console connection to the serial port on the switch, you can display or modify the current settings for the serial port through the Web agent. Click on the serial port icon in the switch image to display or configure these settings, as shown below.

**Serial Port Configuration**

Management Mode : CONSOLE MODE

Baud Rate : 19200

Data Bits : 8

Stop Bits : 1

Parity : None

Timeout : 0 minute(s)

Auto Refresh : 1 second(s)

Apply Cancel

Parameter	Default	Description
Management Mode	Console Mode	Indicates that the port settings are for direct console connection.
Baud Rate	19200	The rate at which data is sent between devices. Options: 9600, 19200 and 38400 baud.
Data Bits	8 bits	Sets the data bits of the RS-232 port. Options: 7, 8
Stop Bits	1 bit	Sets the stop bits of the RS-232 port. Options: 1, 2
Parity	none	Sets the parity of the RS-232 port. Options: none / odd / even
Timeout	0 minutes	If no input is received from the attached device after this interval, the current session is automatically closed. Range: 0 - 100 minutes; where 0 indicates disabled
Auto Refresh	10 seconds	Sets the interval before a console session will auto refresh the console information, such as Spanning Tree Information, Port Configuration, Port Statistics, and RMON Statistics. Range: 0-255 seconds; where 0 indicates disabled

### 3.3.Main Menu

Using the onboard Web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions. The interface screen includes the main menu on the left side, the menu bar beneath the image of the switch, and a list of commands beneath the menu bar. The following table briefly describes the selections available from this program.

Menu	Description
<i>System Information Menu</i>	
System Information	Provides basic system description, including contact information.

Switch Information	Shows hardware / firmware version numbers, power status, and expansion modules used in the switch.
<i>Management Setup Menu</i>	
Network Configuration <sup>1</sup>	Configures the switch's network parameters.
Serial Port Configuration	Sets communication parameters for the serial port, including baud rate, console timeout, and screen data refresh interval.
SNMP Configuration	Activates authentication failure traps, configures community access strings and trap managers.
User Configuration	Sets the user names and passwords for system access.
TFTP Download	Downloads new version of firmware to update your system (in-band).
Configuration File	Saves or restores configuration data based on the specified file.
<i>Device Control Menu</i>	
System Mode <sup>3</sup>	Sets the switch to operate as a Layer 2 switch or as a multilayer routing switch.
Layer 2 Menu	Configures port communication mode, mirror ports, port trunking, and static addresses.
Bridge Menu	Configures GMRP and GVRP for the bridge, as well as Spanning Tree settings for the global bridge or for specific ports.
VLAN Menu	Configures VLAN settings for specific ports, and defines the port membership for VLAN groups.
IGMP Snooping Configuration <sup>1</sup>	Configures IGMP multicast filtering.
IP Menu <sup>2</sup>	Configures the subnets for each VLAN group, global configuration for ARP and ARP proxy, unicast and multicast protocols, BOOTP / DHCP relay, static ARP table entries, static routes and the default route.
Security Menu	Configures MAC and IP <sup>2</sup> address filtering.
<i>Network Monitor Menu</i>	
Port Statistics	Displays statistics on port traffic, including information from the Interfaces Group, Ethernet-like MIB, and RMON MIB.
Layer 2 Address Table	Contains the unicast address table.
Bridge Menu	Displays Spanning Tree information for the overall bridge and for specified ports.
VLAN Menu	Displays dynamic port registration information for VLANs, as well as all VLAN forwarding information for static and dynamic assignment.
IP Multicast Registration Table <sup>1</sup>	Displays all the multicast groups active on this switch, including the multicast IP addresses and corresponding VLANs.
IP Menu <sup>2</sup>	Displays all the IP subnets used on this switch, as well as the corresponding VLANs and ports. Also contains the ARP table, routing table, multicast table, and OSPF table.

<b>System Restart Menu</b>	
Restart Option	Restarts the system with options to restore factory defaults.

1. Only displays if the intelligent switch is set to Layer 2 mode or the switch is management model.
2. Only displays when intelligent switch is set to multilayer mode. (Note that this menu includes IGMP Snooping Configuration.)
3. Only displayed in intelligent switch.

## 3.4. System Information Menu

Use the System Information Menu to display a basic description of the switch, including contact information, and hardware / firmware versions.

Menu	Description
System Information	Provides basic system description, including contact information.
Switch Information	Shows hardware / firmware version numbers, power status, and expansion modules used in the switch.

### 3.4.1. Displaying System Information

Use the System Information screen to display descriptive information about the switch, or for quick system identification as shown in the following figure and table.

The screenshot shows a 'System Information' window with the following content:

- System Description :** Intelligent Switch
- System Object ID :** 1.3.6.1.4.1
- System Up Time :** 0 d 0 h 4 min 3 s
- System Name :**
- System Contact :**
- System Location :**

At the bottom of the window are two buttons: 'Apply' and 'Cancel'.

Parameter	Description
System Description	System hardware description.
Object ID	MIB II object identifier for switch's network management subsystem.
System Up Time	Length of time the current management agent has been running.
System Name*	Name assigned to the switch system.
System Contact*	Contact person for the system.
System Location*	Specifies the area or location where the system resides.

\* Maximum string length is 99, but the screen only displays 45 characters. You can use the arrow keys to browse the whole string.

## 3.4.2. Displaying Switch Version Information

Use the Switch Information screen to display hardware / firmware version numbers for the main board, as well as the power status and modules plugged into the system.

Main Board:	
Hardware Version	R01
Firmware Version	V1.00
Serial Number	00-10-B5-DD-DA-20
Port Number	24
Internal Power Status	Active

Parameter	Description
Hardware Version	Hardware version of the main board.
Firmware Version	System firmware version in ROM.
Serial Number	Serial number of the main board.
Port Number	Number of ports on this switch.
Internal Power Status	Power status for the switch.

Expansion Slot:	
Expansion Slot 1	Empty
Expansion Slot 2	Empty

Parameter	Description
Expansion Slot 1	Shows module type if inserted: 1GBASE-SX/LX : 1000BASE-SX/LX (multimode/ single mode) 1GBASE-T : 1000BASE-T

## 3.5. Management Setup Menu

After initially logging onto the system, you can use this menu to configure access rights. You should set user names and passwords (User Configuration). Remember to record them in a safe place. You should also set the community string which controls access to the onboard SNMP agent via in-band management software (SNMP Configuration). The items provided by the Management Setup Menu are described in the following sections.

Menu	Description
Network Configuration <sup>1</sup>	Configures the switch's IP parameters.
Serial Port Configuration	Sets communication parameters for the serial port, including baud rate, console timeout, and screen data refresh interval. (See "Configuring the Serial Port" on chapter 3.)
SNMP Configuration	Activates authentication failure traps, and configures communities and trap managers.

User Configuration	Sets the user names and passwords for system access.
TFTP Download	Downloads new version of firmware to update your system (in-band).
Configuration File	Saves or restores configuration data based on the specified file.

1. Only display when intelligent switch is set to Layer 2 mode or the switch is management model.

### 3.5.1.Changing the Network Configuration (Layer 2 Mode)

Use the Network Configuration menu to set the bootup option and configure the switch's IP parameters. The screen shown below is described in the following table.

Parameter	Description
IP Address	IP address of the switch you are managing. The system supports SNMP over UDP / IP transport protocol. In this environment, all systems on the Internet such as network interconnection devices and any PC accessing the agent module (or running View) must have an IP address. Valid IP addresses consist of four numbers, of 0 to 255, and separated by periods. Anything outside this format will not be accepted by the configuration program.
Subnet Mask	Subnet mask of the switch. This mask identifies the host address bits used for routing to specific subnets.
Gateway IP	Gateway used to pass trap messages from the system's agent to the management station. Note that the gateway must be defined (when operating at Layer 2) if the management station is located in a different IP segment.

IP State	Specifies whether IP functionality is enabled via manual configuration, or set by Boot Protocol (BOOTP). Options include: User Configuration – IP functionality is enabled based on the default or user specified IP Configuration. (This is the default setting.) BOOTP Get IP – IP is enabled but will not function until a BOOTP reply has been received. BOOTP requests will be broadcast periodically by the switch in an effort to learn its IP address. (BOOTP values can include the IP address, default gateway, and subnet mask.)
Mgt. Access	Allows management access of the switch from all VLANs or only from a specified VLAN. If you select “Mgmt VLAN,” then be sure to specify the required VLAN.

**Note:**

When using multilayer mode, refer to “Subnet Configuration” on chapter 3.

### 3.5.2. Assigning SNMP Parameters

Use the SNMP Configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP). The switch includes an onboard SNMP agent which monitors the status of its hardware as well as the traffic passing through its ports. A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the agent module are controlled by community strings. To communicate with the switch, the NMS must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following figures and table.

#### 3.5.2.1. Configuring Community Names

The following figure and table describe how to configure the community strings authorized for management access. Up to 5 community names may be entered.

SNMP Communities		
Community Name	Access	Status
public	Read Write	Enabled
private	Read Only	Enabled
	Read Only	Disabled
	Read Only	Disabled
	Read Only	Disabled

Save Cancel

Parameter	Description
Community Name	A community entry authorized for management access. (The maximum string length is 20 characters.)
Access	Management access is restricted to Read Only or Read / Write.

Status	Displays the administrative status of entry. An entry can only be to enabled or disabled via the console interface.
--------	---

### 3.5.2.2. Configuring IP Trap Managers

The following figure and table describe how to specify management stations that will receive authentication failure messages or other trap messages from the switch. Up to 5 trap managers may be entered.

IP Trap Manager		
IP Address	Community Name	Status
<input type="text" value="0.0.0.0"/>	<input type="text"/>	Disabled ▾
<input type="text" value="0.0.0.0"/>	<input type="text"/>	Disabled ▾
<input type="text" value="0.0.0.0"/>	<input type="text"/>	Disabled ▾
<input type="text" value="0.0.0.0"/>	<input type="text"/>	Disabled ▾
<input type="text" value="0.0.0.0"/>	<input type="text"/>	Disabled ▾

Save Cancel

Parameter	Description
IP Address	IP address of the trap manager.
Community Name	A community authorized to receive trap messages.
Status	Displays the administrative status of entry. An entry can only be to enabled or disabled via the console interface.

### 3.5.3. User Login Configuration

Use the User Configuration screen to restrict management access based on user names and passwords. The default administrator (admin) has write access for parameters governing the onboard agent. You should therefore assign a password to the administrator as soon as possible, and store it in a safe place.

#### Displaying the Current User Configuration

Use this menu to configure the names and access rights for people authorized to manage the switch.

User Configuration					
User Name	User Password	Access Right	Console	Telnet	HTTP
guest	*****	guest	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
admin	*****	admin	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
		guest	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
		guest	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled
		guest	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled	<input type="checkbox"/> Enabled

Apply Cancel

Parameter	Description
User Name*	Specifies a user authorized management access to the switch via the console, Telnet or HTTP. An entry can only be deleted via the console interface.
User Password*	Password associated with this entry.
Access Right	GUEST: Read Only for all screens. ADMIN: Read / Write for all screens.
Console	Authorizes management via the console.
Telnet	Authorizes management via Telnet.
HTTP	Authorizes management via HTTP.

\*These entries can consist of up to 15 alphanumeric characters and are not case sensitive.

### 3.5.4. Downloading System Software

Use the TFTP Download menu to load software updates to permanent flash ROM in the switch. The download file should be a correct binary file for the switch; otherwise the agent will not accept it. The success of the download operation depends on the accessibility of the TFTP server and the quality of the network connection. After downloading the new software, the agent will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table

TFTP Download Management	
Server IP Address :	<input type="text" value="192.168.1.254"/>
File Name :	<input type="text" value="ram.img"/>
Download Option :	<input type="text" value="Runtime Code"/>
Start TFTP Download Cancel	

Parameter	Description
Server IP Address	IP address of a TFTP server.

File Name	The binary file to download.
Start TFTP Download	Issues request to TFTP server to download the specified file.

### 3.5.5. Saving or Restoring the System Configuration

Use the Configuration File menu to save the switch configuration settings to a file on a TFTP client. The file can be later downloaded to the switch to restore the switch's settings. The success of the operation depends on the accessibility of the TFTP client and the quality of the network connection. Parameters shown on this screen are indicated in the following figure and table.

Parameter	Description
Station IP	IP address of a PC running TFTP client software.
Operation	Download from switch Downloads the current switch configuration to a file on the client PC.
	Upload to switch Uploads a configuration file to the switch from the client PC.

**Note:**

Saving and restoring switch configuration settings can then be initiated by using any TFTP client utility, such as the command line utility included in Windows NT. For example, using Windows NT, from a DOS window command prompt, enter the TFTP command in the form:

TFTP [-i] host [GET : PUT] source [destination]

To transfer a file –

*Switch:* Specify the IP address of the TFTP client, and select “Download from switch” or “Upload from Switch.”

*TFTP Client:* Set the mode to <binary>, specify the IP address of the target switch and the directory path / name of the file to transfer.

*Switch:* Select <START> from the Configuration File menu.

*TFTP Client:* Start transferring the configuration file from the TFTP client or the switch, and wait until the transfer completes.

### 3.6. Device Control Menu

The Device Control menu is used to control a broad range of functions, including port mode, port mirroring, port trunking, Spanning Tree, Virtual LANs, IP subnets, multicast

filtering, and routing protocols. Each of the setup screens provided by these configuration menus is described in the following sections.

Menu	Description
System Mode <sup>3</sup>	Sets the switch to operate as a Layer 2 switch or as a multilayer routing switch.
Layer 2 Menu	Configures port communication mode, mirror ports, port trunking, and static addresses.
Bridge Menu	Configures the Spanning Tree Protocol for the bridge or for specific ports, GMRP and GVRP for automatic registration of multicast and VLAN groups, traffic class priority threshold, and address aging time.
VLAN Menu	Configures VLAN settings for specific ports, and defines the port membership for VLAN groups.
IGMP Snooping Configuration <sup>1</sup>	Configures IGMP multicast filtering.
IP Menu <sup>2</sup>	Configures the subnets for each VLAN group, global configuration for ARP and Proxy ARP, unicast and multicast protocols, static ARP table entries, static routes and the default route.
Security Menu	Configures MAC and IP <sup>2</sup> address filtering.

1. Only displayed if the intelligent switch is set to Layer 2 mode or the switch is management model.
2. Only displayed if the intelligent switch is set to multilayer mode. (Note that this menu includes IGMP Snooping Configuration.)
3. Only displayed in intelligent switch.

### 3.6.1. Setting the System Operation Mode

This switch can be set to operate as a Layer 2 switch, making all filtering and forwarding decisions based strictly on MAC addresses. Or, it can be set to operate as a multilayer routing switch, whereby it switches packets for all non-IP protocols (such as NetBUEI, NetWare or AppleTalk) based on MAC addresses (see “Virtual LANs” on chapter 4), and routes all IP packets based on the specified routing protocol. The System Mode menu is shown below. Note that the switch will be automatically rebooted whenever the system operation mode is changed.

**Please Note: System Mode change will take effect after system reboot. It may also require wiring changes. Please exercise this option with care.**

Parameter	Description
Layer 2	Filtering and forwarding decision will be based on MAC addresses for all protocol traffic.
Multi-Layer	Switching based on MAC addresses will be used for all non-IP protocol traffic, and routing will be used for all IP protocol traffic.

**Note:**

When the switch is set to multilayer mode, the IP menus are enabled, and the “IP Configuration (Layer 2 Mode)” menu on chapter 2 is disabled. When operating in multilayer mode, you should configure an IP interface for each VLAN that needs to communicate with any device outside of the VLAN. (See “Subnet Configuration” on chapter 2.)

### 3.6.2.Layer 2 Menu

The Layer 2 menu contains options for port configuration, port mirroring, and port trunking. These menu options are described in the following sections.

Menu	Description
Port Configuration	Enables any port, enables / disables flow control, and sets communication mode to auto-negotiation, full duplex or half duplex.
Mirror Port Configuration	Sets the source and target ports for mirroring.
Port Trunking Configuration	Specifies ports to group into aggregate trunks.
Static Unicast Address Table	Used to manually configure host MAC addresses in the unicast table.
Static Multicast Address Table	Used to manually configure host MAC addresses in the multicast table.

#### 3.6.2.1.Configuring Port Parameters

Use the Port Configuration menu to display or set communication parameters for any port or module on the switch, including administrative status, auto-negotiation, default communication speed and duplex mode, as well as flow control in use.

Port Configuration							
Port	Link Status	Admin Status	Auto Negotiate	Default Type	Current Control	Flow Control	Jack Type Edit
1	✘	Enabled	Enabled	10M-Half-Duplex	10M-Half-Duplex	Off	RJ45 
2	✘	Enabled	Enabled	10M-Half-Duplex	10M-Half-Duplex	Off	RJ45 
3	✘	Enabled	Enabled	10M-Half-Duplex	10M-Half-Duplex	Off	RJ45 
4	✘	Enabled	Enabled	10M-Half-Duplex	10M-Half-Duplex	Off	RJ45 
5	✘	Enabled	Enabled	10M-Half-Duplex	10M-Half-Duplex	Off	RJ45 
6	✘	Enabled	Enabled	10M-Half-Duplex	10M-Half-Duplex	Off	RJ45 
7	✘	Enabled	Enabled	10M-Half-Duplex	10M-Half-Duplex	Off	RJ45 
8	✘	Enabled	Enabled	10M-Half-Duplex	10M-Half-Duplex	Off	RJ45 

Parameter	Default	Description																				
Link Status		Indicates if the port has a valid connection to an external device.																				
Admin Status	Enabled	Allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then enable it after the problem has been resolved. You may also disable a port for security reasons.																				
Auto Negotiate*	Enabled	<p>Enables or disables auto-negotiation for the following features</p> <table border="1"> <thead> <tr> <th>Port Type</th> <th>Speed</th> <th>Duplex Mode</th> <th>Flow Control</th> </tr> </thead> <tbody> <tr> <td>10/100BASE-T</td> <td>auto</td> <td>auto</td> <td>auto</td> </tr> <tr> <td>100BASE-FX</td> <td>100M</td> <td>full duplex</td> <td>auto</td> </tr> <tr> <td>1000BASE-SX/LX</td> <td>1000M</td> <td>full duplex</td> <td>auto</td> </tr> <tr> <td>1000BASE-T</td> <td>1000M</td> <td>full duplex</td> <td>auto</td> </tr> </tbody> </table> <p>The 10/100BASE-TX ports can autonegotiate the speed to 10/100 Mbps, and the transmission mode to half / full duplex. The 100BASE-FX, 1000BASE-SX/LX, and 1000BASE-T modules are all fixed at the indicated speed and duplex mode. All media types can auto-negotiate flow control.</p>	Port Type	Speed	Duplex Mode	Flow Control	10/100BASE-T	auto	auto	auto	100BASE-FX	100M	full duplex	auto	1000BASE-SX/LX	1000M	full duplex	auto	1000BASE-T	1000M	full duplex	auto
Port Type	Speed	Duplex Mode	Flow Control																			
10/100BASE-T	auto	auto	auto																			
100BASE-FX	100M	full duplex	auto																			
1000BASE-SX/LX	1000M	full duplex	auto																			
1000BASE-T	1000M	full duplex	auto																			
Default Type	10M-Half-Duplex	If auto-negotiation is disabled, the port will be set to the indicated speed and duplex mode.																				
Current Type		Indicates the current speed and duplex mode.																				

Flow Control	Disabled	<p>Used to enable or disable flow control. Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex and IEEE 802.3x for full-duplex. Note that flow control should not be used if a port is connected to a hub. For the Gigabit modules the options for flow control are set out below:</p> <table border="0"> <thead> <tr> <th><i>Switch</i></th> <th><i>Link Partner</i></th> <th><i>Flow Control</i></th> </tr> </thead> <tbody> <tr> <td>Rcv/BothWay</td> <td>SendOnly</td> <td>Switch can only receive pause frames, link partner can only send pause frames.</td> </tr> <tr> <td>Rcv/BothWay</td> <td>BothWay</td> <td>Both switch and link partner can send and receive pause frames.</td> </tr> </tbody> </table>	<i>Switch</i>	<i>Link Partner</i>	<i>Flow Control</i>	Rcv/BothWay	SendOnly	Switch can only receive pause frames, link partner can only send pause frames.	Rcv/BothWay	BothWay	Both switch and link partner can send and receive pause frames.
<i>Switch</i>	<i>Link Partner</i>	<i>Flow Control</i>									
Rcv/BothWay	SendOnly	Switch can only receive pause frames, link partner can only send pause frames.									
Rcv/BothWay	BothWay	Both switch and link partner can send and receive pause frames.									
Jack Type		<p>Shows the jack type for each port.  Ports 1-11,13,23: RJ-45  Ports 12,24: FIBER or RJ-45  Ports 25-26: RJ-45, FIBER</p>									

### 3.6.2.2.Using a Port Mirror for Analysis

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, note that the target port must be included in the same VLAN as the source port. (See “VLAN Table Configuration” on chapter 3.)

You can use the Mirror Configuration screen to mirror one or more ports to the monitor port as shown below.

**Enable Port Mirroring**

**Tx Mirrored Port**

<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/> 7
<input type="checkbox"/> 8	<input type="checkbox"/> 9	<input type="checkbox"/> 10	<input type="checkbox"/> 11	<input type="checkbox"/> 12	<input type="checkbox"/> 13	<input type="checkbox"/> 14
<input type="checkbox"/> 15	<input type="checkbox"/> 16	<input type="checkbox"/> 17	<input type="checkbox"/> 18	<input type="checkbox"/> 19	<input type="checkbox"/> 20	<input type="checkbox"/> 21
<input type="checkbox"/> 22	<input type="checkbox"/> 23	<input type="checkbox"/> 24				

**Rx Mirrored Port**

<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/> 7
<input type="checkbox"/> 8	<input type="checkbox"/> 9	<input type="checkbox"/> 10	<input type="checkbox"/> 11	<input type="checkbox"/> 12	<input type="checkbox"/> 13	<input type="checkbox"/> 14
<input type="checkbox"/> 15	<input type="checkbox"/> 16	<input type="checkbox"/> 17	<input type="checkbox"/> 18	<input type="checkbox"/> 19	<input type="checkbox"/> 20	<input type="checkbox"/> 21
<input type="checkbox"/> 22	<input type="checkbox"/> 23	<input type="checkbox"/> 24				

Cancel Apply

Parameter	Description
Enable Port Mirror	Enables or disables the mirror function.
TX Mirrored Port	The port whose transmitted traffic will be mirrored.
TX Monitored Port	The port that will duplicate the transmitted traffic appearing on the mirrored port.
RX Mirrored Port	The port whose received traffic will be mirrored.
RX Monitored Port	The port that will duplicate the received traffic appearing on the mirrored port.

**Note:**

You can mirror multiple ports to a single port to view traffic such as that crossing a port trunk. However, note that some packets may be dropped for moderate to heavy loading.

### 3.6.2.3. Configuring Port Trunks

Ports can be combined into an aggregate link to increase the bandwidth of a network connection or ensure fault recovery. You can configure trunks between any two switches. Ports 1-24 on this switch can be grouped into a trunk consisting of two, four or eight ports, creating an aggregate bandwidth up to 400, 800 or 1600 Mbps when operating at full duplex. Ports 25-26 (extender module ports) can be trunked together creating an aggregate bandwidth up to 2 Gps. The ports that can be assigned to the same trunk are listed on next page. Beyond balancing the load across each port in the trunk, the additional ports provide redundancy by taking over the load if another port in the trunk should fail. However, before making any physical connections between devices, use the Trunk Configuration menu to specify the trunk on the devices at both ends. When using

a port trunk, remember that:

- Ports can only be assigned to one trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode and VLAN assignments.
- All the ports in a trunk have to be treated as a whole when moved from / to, added to, or deleted from, a VLAN.
- The Spanning Tree Algorithm will treat all the ports in a trunk as a whole.
- Enable the trunk prior to connecting any cable between the switches to avoid creating a loop.

Use the Trunk Configuration screen to set up port trunks as shown below:



Parameter	Description
Trunk List	The port groups currently configured as trunks.
New Setting	The port groups that can still be configured as trunks.

The port groups permitted include:

<<13, 1>> <<14, 2>> <<15, 3>> <<16, 4>>  
 <<17, 5>> <<18, 6>> <<19, 7>> <<20, 8>>  
 <<21, 9>> <<22,10>> <<23,11>> <<24,12>>

<<13, 1, 14, 2>> <<15, 3, 16, 4>>  
 <<17, 5, 18, 6>> <<19, 7, 20, 8>>  
 <<21, 9, 22, 10>> <<23, 11, 24, 12>>

<<13, 1, 14, 2, 15, 3, 16, 4>>  
 <<17, 5, 18, 6, 19, 7, 20, 8>>  
 <<21, 9, 22, 10, 23, 11, 24, 12>>  
 <<25,26>>

To add a trunk, highlight a port group in the New Setting list and press Add. To delete a trunk, highlight a port group in the Trunk List and press Delete. Before disconnecting a port trunk, take the following steps:

- Before removing a port trunk via the configuration menu, you must disable all the ports in the trunk or remove all the network cables. Otherwise, a loop may be created.
- To disable a single link within a port trunk, you should first remove the network cable, and then disable both ends of the link via the configuration menu. This allows the traffic passing across that link to be automatically distributed to the other links in the trunk, without losing any significant amount of traffic.

### 3.6.2.4. Static Unicast Address Table

The Static Unicast Address Table can be used to assign the MAC address for a host device to a specific port on this switch. Static unicast addresses are never aged out, and cannot be learned by another port. If any packets with a source address specified in this table enter another port, they will be dropped. The Static Unicast Address Table is described in the following figure and table.

Static Unicast Address Configuration		
MAC Address	Port	Edit
-	-	-

MAC :  Port :

Parameter	Description
MAC Address	The MAC address of a host device attached to this switch.
Port	The port to which the host device is attached.

**Note:**

To assign an address to a specific port, enter it in the MAC Address field, select the corresponding port, and press Apply. To delete an address, click on the edit icon (✏) for the required entry, and then press Delete.

### 3.6.2.5. Configuring the Static Multicast Address Table

The Static Multicast Address Table can be used to assign a destination MAC address (and the corresponding ports) to the VLAN group used for a specific multicast service. Static multicast addresses are never aged out, and traffic with these addresses can be forwarded only to ports specified in this table.

Multicast Address Configuration			
MAC Address	VLAN	Port	Edit
-	-	-	-

Entry List							
MAC Address:	<input type="text"/>						
VLAN:	<input type="text"/>						
Port:	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/> 7
	<input type="checkbox"/> 8	<input type="checkbox"/> 9	<input type="checkbox"/> 10	<input type="checkbox"/> 11	<input type="checkbox"/> 12	<input type="checkbox"/> 13	<input type="checkbox"/> 14
	<input type="checkbox"/> 15	<input type="checkbox"/> 16	<input type="checkbox"/> 17	<input type="checkbox"/> 18	<input type="checkbox"/> 19	<input type="checkbox"/> 20	<input type="checkbox"/> 21
	<input type="checkbox"/> 22	<input type="checkbox"/> 23	<input type="checkbox"/> 24				
<input type="button" value="Apply"/> <input type="button" value="Delete"/> <input type="button" value="Cancel"/>							

Parameter	Description
MAC Address	The destination MAC address for a multicast service.
VLAN	The VLAN corresponding to this multicast service.
Port	The ports to which this multicast traffic can be forwarded.

**Note:**

To assign a destination MAC address to one or more ports, enter its address and the corresponding VLAN, select the required ports, and then press Apply. To delete an address, click on the edit icon (✎) for the required entry, and then press Delete. To modify an address, press Edit for the required entry to copy the configuration to the edit fields, make any necessary changes, then press Apply.

### 3.6.3.Using the Bridge Menu

The Bridge menu is used to configure settings for the Spanning Tree Algorithm, as well as the global bridge settings for GMRP (GARP Multicast Registration Protocol) and GVRP (GARP VLAN Registration Protocol), traffic classes priority threshold, and address aging time.

The Spanning Tree Algorithm can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links that automatically take over when a primary link goes down. For a more detailed description of how to use this algorithm, refer to “Spanning Tree Algorithm” on chapter 4.

Menu	Description
------	-------------

Bridge Configuration	Contains global bridge settings for STA (including bridge priority, hello time, forward delay, maximum message age), GMRP, GVRP, traffic class priority threshold, and address aging time.
STA Port Configuration	Contains STA settings for individual ports, including port priority, path cost, and fast forwarding

### 3.6.3.1. Configuring Global Bridge Settings

The following figure and table describe bridge configuration for STA, GMRP, GVRP, priority threshold, and address aging time.

Parameter	Default	Description
Spanning Tree	Enabled	Enable this parameter to participate in a STA compliant network.
Bridge Priority	32,768	Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Enter a value from 0 - 65535. Remember that the lower the numeric value, the higher the priority.
Hello Time	2	Time interval (in seconds) at which the root device transmits a configuration message. The minimum value is 1. The maximum value is the lower of 10 or [(Max. Message Age / 2) - 1].

Forward Delay	15	The maximum time (in seconds) the root device will wait before changing states (that is, listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The maximum value is 30. The minimum value is the higher of 4 or $[(\text{Max. Message Age} / 2) + 1]$ .
Maximum (Message) Age	20	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. The minimum value is the higher of 6 or $[2 \times (\text{Hello Time} + 1)]$ . The maximum value is the lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$ .
GMRP	Disabled	GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. If GMRP is globally enabled for the switch, then you can individually enable or disable GMRP for a specific port. See "VLAN Port Configuration" on chapter 3. IGMP and IGMP Snooping also provide multicast filtering. For multilayer mode, the full IGMP protocol set is automatically enabled / disabled along with DVMRP. (See "IGMP Protocol" on chapter 4, "Configuring DVMRP" on chapter 3, and "Configuring IGMP Snooping" on chapter 3.)
GVRP	Disabled	GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration and to support VLANs which extend beyond the local switch. If GVRP is globally enabled for the switch, then you can individually enable or disable GVRP for a specific port. See "VLAN Port Configuration" on chapter 3.
Priority Threshold*	4	This switch supports Quality of Service (QoS) by using two priority queues, with Weighted Fair Queuing for each port. Up to 8 separate traffic classes are defined in IEEE 802.1p. Therefore, any packets with a priority equal to or higher than this threshold are placed in the high priority queue.
(Address) Aging Time	300	Timeout period in seconds for aging out dynamically learned forwarding information. Range: 10 - 415 seconds

\* You can use “VLAN Port Configuration” on chapter 3 to configure the default priority for each port.

### 3.6.3.2. Configuring STA for Ports

The following figure and table describe port STA configuration.

STA Port Configuration				
Port	Type	Priority	Cost	FastForwarding
1	100BASE-TX	128	19	<input type="checkbox"/> Enabled
2	100BASE-TX	128	19	<input type="checkbox"/> Enabled
3	100BASE-TX	128	19	<input type="checkbox"/> Enabled
4	100BASE-TX	128	19	<input type="checkbox"/> Enabled
5	100BASE-TX	128	19	<input type="checkbox"/> Enabled
6	100BASE-TX	128	19	<input type="checkbox"/> Enabled
7	100BASE-TX	128	19	<input type="checkbox"/> Enabled

Parameter	Default	Description
Type		Shows port type as: 100BASE-TX : 10BASE-T / 100BASE-TX 100BASE-FX : 100BASE-FX 1G BASE-SX/LX : 1000BASE-SX/LX(multimode/ single mode) 1G BASE-T : 1000BASE-T
Priority	128	Defines the priority for the use of a port in the STA algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is 0 - 255.
(Path) Cost	100/19/4	This parameter is used by the STA algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) The default and recommended range is: Ethernet: 100 (50~600) Fast Ethernet: 19 (10~60) Gigabit Ethernet: 4 (3~10) The full range is 0 - 65535.

Fast Forwarding*	Enabled	This parameter is used to enable / disabled the Fast Spanning Tree mode for the selected port. In this mode, ports skip the Blocked, Listening and Learning states and proceed straight to Forwarding.
------------------	---------	--

\* Since end-nodes cannot cause forwarding loops, they can pass through the Spanning Tree state changes more quickly than allowed by standard convergence time. Fast Forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related timeout problems. (Remember that Fast Forwarding should only be enabled for ports connected to an end-node device.)

### 3.6.4. Configuring Virtual LANs

You can use the VLAN configuration menu to assign any port on the switch to any of up to 256 LAN groups. In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle traffic such as IPX or NetBEUI. By using IEEE 802.1Q compliant VLANs, you can organize any group of network nodes into separate broadcast domains, thus confining broadcast traffic to the originating group. This also provides a more secure and cleaner network environment. For more information on how to use VLANs, see "Virtual LANs" on chapter 4. The VLAN configuration screens are described in the following sections.

#### 3.6.4.1. VLAN Port Configuration

You can use the VLAN Port Configuration screen to configure GARP, the default VLAN identifier, default port priority, VLAN tagging on outgoing frames, GVRP and GMRP status, and filtering for incoming frames for VLAN groups this port does not belong to.

Port Number :

### GARP Configuration

Join Time	<input type="text" value="20"/>	Centiseconds
Leave Time	<input type="text" value="60"/>	Centiseconds
Leave All Time	<input type="text" value="1000"/>	Centiseconds

### VLAN and Priority

Port VID	<input type="text" value="1"/>
Port Default Priority	<input type="text" value="0"/>
VLAN Tagging	<input type="text" value="Rx All, Tx Untag"/>
GVRP	<input type="text" value="Enabled"/>
GMRP	<input type="text" value="Enabled"/>
Ingress Filtering	<input type="text" value="Disabled"/>

Parameter	Default	Description
<i>GARP Configuration<sup>1</sup></i>		Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN.
Join Time	20	The interval (centiseconds) between transmitting requests / queries to participate in a group.
Leave Time	60	The interval (centiseconds) a port waits before leaving a group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group.
Leave All Time	1000	The interval (centiseconds) between sending out a LeaveAll query message for group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group.

1. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing some difficulties with GMRP or GVRP registration / deregistration.

Parameter	Default	Description
<i>VLAN and Priority</i>		These fields set the default values for VLANs, port priority, GVRP and GMRP.

Port VID	1	The VLAN ID assigned to untagged frames received on this port.
Port Default Priority <sup>2</sup>	0	Set the default ingress priority to any value beneath the priority threshold (chapter 3 “Configuring Global Bridge Settings”) to specify the low priority queue, or to any value equal to or above this threshold to specify the high priority queue.
VLAN Tagging <sup>3</sup>	<i>Layer 2 -</i> Rx All, Tx All  <i>Multilayer -</i> Rx All, Tx Untag	Indicates whether or not VLAN tags will be included on frames transmitted out of this port. The options include: Rx All: Accepts all frames, tagged or untagged. Rx Untag: Only accepts untagged frames. Tx All: If PVID and frame tag are same, sends tagged frame, otherwise send untagged. Tx Untag: Sends only untagged frames.
Port GVRP	Enabled	Enables or disables GVRP for this port. When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. Note that GVRP must be enabled globally for the switch before this setting can take effect. (See “Configuring Global Bridge Settings” on chapter 3.)
Port GMRP	Enabled	Enables or disables GMRP for this port. When enabled, this port will allow endstations to register with multicast groups using GMRP. Note that GMRP must be enabled for the switch before this setting can take effect (chapter 3 “Configuring Global Bridge Settings”). IGMP and IGMP Snooping also provide multicast filtering. For multilayer mode, the full IGMP protocol set is automatically enabled / disabled along with DVMRP. (See “IGMP Protocol” on chapter 4, “Configuring DVMRP” on chapter 3, and “Configuring IGMP Snooping” on chapter 3.)
Ingress Filtering <sup>4</sup>	Disabled	If enabled, incoming frames for VLANs which do not include this ingress port in their member set will be discarded at the ingress port.

2. This switch supports Quality of Service (QoS) by using two priority queues, with Weighted Fair Queuing for each port. Inbound frames that do not have VLAN tags are tagged with the input port’s default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in the low priority queue of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)
3. If you want to create a small port-based VLAN for just one or two switches, you can assign ports to the same untagged VLAN (and use a separate connection where a

VLAN crosses the switches). However, to participate in a VLAN group that extends beyond this switch, we recommend using the VLAN ID for that group (using VLAN tagging for Layer 2 mode, or a common PVID for multilayer mode).

When operating the switch in Layer 2 mode, ports assigned to a large VLAN group that crosses several switches must use VLAN tagging. But when operating in multilayer mode, this switch does not currently support tagging, so you should set the PVID to the same value at both ends of the link (if the device you are attaching to is VLAN-aware), and configure an IP interface for this VLAN if you need to connect it to other groups. (This limitation will be removed for future firmware versions.)

4. This control does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.

### 3.6.4.2.VLAN Table Configuration

Use this screen to create a new VLAN or modify the settings for an existing VLAN.

**VLAN Table Configuration** N:Normal X:Forbidden S:Static R:Reg. Fixed

VLAN	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
1	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	

VID :

N	X	R	S	1	N	X	R	S	2	N	X	R	S	3	N	X	R	S	4	N	X	R	S	5	N	X	R	S	6
<input type="radio"/>																													
<input type="radio"/>																													
<input type="radio"/>																													
<input type="radio"/>																													
<input type="radio"/>																													

Add / Save    Delete    Cancel

Parameter	Description
VLAN	The ID for the VLAN currently displayed. Range: 1-4094
(Port)	Port entries may be marked as: N: ( <i>Normal</i> ) Uses GVRP to determine port membership. S: ( <i>Static</i> ) Adds port as a static entry. GVRP protocol messages are still forwarded through this port. R: ( <i>Registration Fixed</i> ) Adds port as a static entry. GVRP protocol is disabled. X: ( <i>Forbidden</i> ) Disables GVRP for this VLAN on the specified port. If a removed port is no longer assigned to any other group as an untagged port, it will automatically be assigned to VLAN group 1 as untagged.

**Note:**

To add a new VLAN, enter a new VLAN number in the VID field, select the port members, and press Add. To modify a VLAN, click on the edit icon (✎) for the required entry, modify the port settings, and press Save. To delete a VLAN, click on the edit icon (✎) for the required entry, and then press Delete.

### 3.6.5. Configuring IGMP Snooping

Multicasting is used to support real-time applications such as video conferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts which want to receive the multicast register with their local multicast switch / router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully filtered at every multicast switch / router it passes through to ensure that traffic is passed on only to the hosts which subscribed to this service.

This switch uses IGMP (Internet Group Management Protocol) Snooping to monitor for any attached hosts who want to receive a specific multicast service. It looks up the IP Multicast Group used for this service, and adds any port which received a similar request to that group.

You can use the IGMP Snooping Configuration screen to configure multicast filtering as shown below.

Parameter	Default	Description
IGMP Snooping Status <sup>1</sup>	Disabled	If enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping.
IGMP Router Timeout	5	A switch port that stops receiving multicast protocol packets for this interval will be removed from the IGMP forwarding list. Range: 3 - 5 minutes
IGMP Group Timeout	5	The time between spotting an IGMP Report message for an IP multicast address on a specific port before the switch removes that entry from its list. Range: 3 - 5 minutes

Act as IGMP Querier <sup>2</sup>	Disabled	If enabled, the switch can serve as the “querier,” which is responsible for asking hosts if they want to receive multicast traffic.
----------------------------------	----------	---

1. This item is only displayed for Layer 2 mode. For multilayer mode, the full IGMP protocol set is automatically enabled / disabled along with DVMRP. (See IGMP on chapter 4. See DVMRP on chapter 3 “*Configuring DVMRP*” and chapter 4 “*DVMRP Routing Protocol*”.)
2. This item is only displayed for Layer 2 mode. When IGMP is enabled for multilayer mode, the switch will always serve as the querier if elected.

### 3.6.6. Configuring IP Settings

If this switch is set to multilayer mode (chapter 2 “Setting the System Operation Mode”), the IP Menu will be displayed. Use this menu to configure the IP subnets for each VLAN on your switch, the unicast and multicast routing protocols, static ARP entries, static IP routes, and the default IP route.

Parameter	Description
Subnet Configuration	IP Subnet Configuration Specifies the IP interface for VLANs configured on this switch, including the subnet address and routing protocols. Port Group Configuration See “VLAN Table Configuration” on chapter 3.
Protocol Configuration	Configures ARP timeout, enables Proxy ARP, sets the preferred servers for BOOTP / DHCP Relay, as well as enabling / configuring unicast and multicast protocols globally for this switch.
Static ARP Configuration	Used to map an IP address to a specific physical MAC address.
Static Route	Used to configure static routes to other IP networks, subnetworks, or hosts.
Default Route	Defines the router to which this switch will forward all traffic for unknown networks.

#### 3.6.6.1. Subnet Configuration

Use this menu to specify an IP interface for any VLAN configured on this switch that needs to communicate with a device outside of its own group (that is, another network segment). You also need to define a VLAN for each IP subnet connected directly to this switch. Note that you must first create a VLAN as described under “Configuring Virtual LANs” on chapter 3 before configuring the corresponding subnet.

Subnet Configuration							
Destination Network	Subnet Mask	VLAN	Proxy Arp	RIP	OSPF	DVMRP	EDIT
192.72.53.110	255.255.255.0	1	✘	✘	✘	✘	
192.72.52.1	255.255.255.0	1	✘	✘	✘	✘	

IP Address:	<input type="text"/>	Proxy Arp:	<input type="text" value="Disabled"/>	
Subnet Mask:	<input type="text"/>	RIP:	<input type="text" value="Disabled"/>	<input type="button" value="Advanced &gt;&gt;"/>
VLAN:	<input type="text"/>	OSPF:	<input type="text" value="Disabled"/>	<input type="button" value="Advanced &gt;&gt;"/>
		DVMRP:	<input type="text" value="Disabled"/>	<input type="button" value="Advanced &gt;&gt;"/>

Parameter	Description
IP Address	The IP address associated with the specified VLAN interface. By convention, the last three digits should be set to “254” to readily distinguish this device as a router port.
Subnet Mask	A template that identifies the address bits in the host address used for routing to specific subnets. Each bit that corresponds to a “1” is part of the network / subnet number and each bit that corresponds to “0” is part of the host number.
VLAN	The VLAN associated with this IP interface.
Proxy ARP	Enables or disables Proxy ARP for the interface. This feature allows the switch forward an ARP request from a node in the attached subnetwork (that does not have routing or a default gateway configured) to a remote subnetwork. (See “Proxy ARP” on chapter 4.) Note that Proxy ARP must be enabled globally for the switch before this setting can take effect. (See “Protocol Configuration” on chapter 3.)
RIP	Routing Information Protocol for unicast routing.
OSPF	Open Shortest Path First unicast routing protocol.
DVMRP	Distance-Vector Multicast Routing Protocol.

**Note:**

To add an IP interface, specify the interface settings in the dialog box at the bottom of the screen, and press Add. To modify an interface, click on the edit icon () for the required entry, update the interface settings in the dialog box at the bottom of the screen, and press Save. To delete an interface, click on the edit icon () for the required entry, and then press Delete.

**Adding an IP Interface**

To add an IP interface, specify the interface settings in the dialog box at the bottom of the screen. Configure the IP address, assign an existing VLAN group to this interface, enable the required routing protocols, and then press Add. To configure the unicast and

multicast routing protocols, you must edit an existing entry (as described in the following section) and press the Advanced button for RIP or DVMRP.

### **Modifying an IP Interface**

To modify an IP interface, click on the edit icon (✎) for the required entry, update the interface settings in the dialog box at the bottom of the screen, use the Advanced button to configure the unicast and multicast routing protocols (as described in the following sections), and then press Save.

### **Configuring RIP**

The Routing Information Protocol is used to specify how routers exchange routing table information. (See “RIP and RIP-2 Dynamic Routing Protocols” on chapter 4.) When RIP is enabled on this routing switch, it broadcasts RIP messages to all devices in the network every 30 seconds, and updates its own routing table when RIP messages are received from other routers. RIP messages contain both the IP address and a metric for each destination network it knows about, and the metric indicates the number of hops from this device to the destination network.

You can use the following menu to specify authentication, the protocol used for sending or receiving routing messages on this port, the default metric used in calculating the best path, and enable or disable Poison Reverse.

**Modify RIP Configuration**

Authentication Type :

Authentication Key :

Send Type :

Receive Type :

Default Metric :

Poison Reverse :

Parameter	Description
Authentication Type	Authentication can be used to ensure that routing information comes from a valid source.
Authentication Key	A simple password must be provided if authentication is enabled. (An authentication string is case sensitive, and can be up to 16 characters.)

Send Type	The protocol used for traffic sent out this port: RIP1 Broadcast: Route information is broadcast to other routers on the network using RIPv1. RIP2 Broadcast: Route information is broadcast to other routers on the network using RIPv2. RIP2 Multicast: Route information is multicast to other routers on the network using RIPv2. Do Not Send: The switch will passively monitor route information advertised by other routers attached to the network.
Receive Type	The routing protocol messages accepted on this port includes RIP1, RIP2, RIP1 / RIP2, or Do Not Receive.
Default Metric	A “metric” indicates the number of hops between the switch and the destination network. The “default metric” is used for the default route in RIP updates originated on this interface. A value of zero indicates that no default route should be originated; in this case, a default route via another router may be propagated. Range: 0-15
Poison Reverse*	Directs routes back to an interface port from which they have been acquired, but sets the distance vector metrics to infinity.

\* This is a method of preventing routing information from looping back to the source. Note that Split Horizon is also enabled on this switch for this purpose. (See “RIP and RIP-2 Dynamic Routing Protocols” on chapter 4.)

### **Configuring OSPF**

Open Shortest Path First is more suited for large area networks which experience frequent changes in the links. It also allows for subnets. This protocol actively tests the status of each link to its neighbors to generate a shortest-path tree, and builds a routing table based on this information. (See “OSPFv2 Dynamic Routing Protocol” on chapter 4.) OSPF then utilizes IP multicast to propagate routing information. A separate routing area scheme is also used to further reduce the amount of routing traffic (chapter 3 “Router ID”).

You can use the following menu to specify the area identifier or other key routing parameters as shown in the following table.

### Modify OSPF Configuration

Area ID :

Router Priority :

Transit Delay (in seconds) :

Retransmit Interval (in seconds) :

Hello Interval (in seconds) :

Dead Interval (in seconds) :

Polling Interval (in seconds) :

Authentication Type :

Authentication Key :  [MD5 Table](#)

Parameter	Default	Description
Area ID <sup>1</sup>		A 32-bit integer uniquely identifying an OSPF protocol broadcast area. This identifier can be in the form of an IP address or integer. Each port on the switch can be configured to represent one OSPF area. ID 0.0.0.0 is used for the OSPF backbone.
Router Priority	1	The priority used when selecting the designated router and designated backup router. Range: 0-255; Disable election: 0
Transit Delay	1 second	The estimated number of seconds it takes to transmit a link state update packet over this interface. Range: 0-3600 seconds
Retransmit Interval	5 seconds	The number of seconds between retransmitting link-state advertisements to router adjacencies on this interface. This value is also used when retransmitting database descriptions and link-state request packets. Range: 0-3600 seconds
Hello Interval <sup>2</sup>	10 seconds	The interval, in seconds, between sending Hello packets out the router interface. Range: 1-65535 seconds
Dead Interval <sup>2</sup>	40 seconds	The number of seconds that a router's Hello packets have not been seen before its neighbors declare the router down. This should be a multiple of the Hello interval. Range: 1-65535 seconds

1. The Area ID is used to specify a group of contiguous networks and hosts. OSPF protocol broadcast messages are restricted by area to limit their impact on network performance.
2. This value must be the same for all routers attached to a common network.

### Configuring DVMRP

Distance Vector Multicast Routing Protocol is used to route multicast traffic to nodes which have requested a specific multicast service via IGMP. (See “DVMRP Routing Protocol” on chapter 4.) To configure DVMRP, you must specify the routing metric, probe interval, and neighbor router timeout.

**Modify DVMRP Configuration**  
**Metrics :**   
**Probe Interval :**   
**Neighbor Timeout :**

Parameter	Default	Description
Metrics	1 hop	This value is used to select the best reverse path to networks that are connected directly to an interface on this switch. Range: 1-31 hops
Probe Interval	10 seconds	The interval between sending neighbor probe messages to the multicast group address for all DVMRP routers. Range: 5-30 seconds
Neighbor Timeout	35 seconds	The interval to wait without hearing from a DVMRP neighbor before declaring it dead. This is used for timing out routes, and for setting the children and leaf flags. Range: 10-8000 seconds

#### Note:

IGMP is automatically enabled / disabled along with DVMRP. (See “IGMP Protocol” on chapter 4.)

### 3.6.6.2. Protocol Configuration

Use the Protocol Configuration screen to globally enable or disable unicast or multicast routing protocols for the switch.

Parameter	Description
ARP	Sets the aging time for dynamic ARP entries.
RIP	Sets the interval at which the switch advertises known routes, enables or disables advertising the switch as the default router, and enables or disables advertising static routes.
OSPF	Organizes an autonomous system into normal, stub, or not so stubby areas; configures a range of subnet addresses for which link state advertisements can be aggregated; and configure virtual links for areas that do not have direct physical access to the OSPF backbone, to add redundancy, or to merge backbone areas.
Boot Relay	Defines the preferred servers or the outbound subnetworks for

	broadcasting a BOOTP / DHCP request.
IGMP Snooping	Enables or disables IGMP Snooping. The Advanced menu sets the timeout for inactive multicast ports or for specific multicast flows when there are no longer any clients. See chapter 3 “Configuring IGMP Snooping”.

**Note:**

Once RIP and DVMRP have been enabled globally (chapter 2 “Protocol Configuration”), you can enable or disable them for any specific subnet via the Subnet Configuration menu (chapter 3 “Subnet Configuration”).

**Setting the ARP Timeout**

You can use the following configuration screen to modify the aging time for dynamically learned entries in the ARP cache.

**ARP Configuration**

ARP Timeout (Minutes) :

Parameter	Default	Description
ARP Timeout	20 minutes	The time that dynamically learned entries are retained in the ARP cache. Range: 0-999 minutes, where 0 disables aging

**Setting the RIP Advertisement Policy**

You can use the following configuration screen to set the timing interval and policies RIP uses to advertise route information.

**RIP Configuration**

RIP Update Time (Sec.)	<input type="text" value="30"/>
Default Route Advertisement	<input type="button" value="Disabled"/> ▾
Static Route Advertisement	<input type="button" value="Disabled"/> ▾
Ignore Host Route	<input type="button" value="Disabled"/> ▾

Parameter	Default	Description
RIP Update Time	30 seconds	The interval at which RIP advertises known route information. Range: 0-999 seconds, where 0 disables route advertisements
Default Route Advertisement	Disabled	Enables or disables advertising this switch as a default router.

Static Route Advertisement	Disabled	Enables or disables advertisement of static routes.
----------------------------	----------	---

### **Configuring Global Settings for OSPF**

To implement OSPF for a large network, you must first organize the network into logical areas to limit the number of OSPF routers that actively exchange Link State Advertisements (LSAs). You can then define an OSPF interface by assigning an IP interface configured on this switch to one of these groups. This OSPF interface will send and receive OSPF traffic to neighboring OSPF routers.

You can further optimize the exchange of OSPF traffic by specifying an area range that covers a large number of subnetwork addresses. This is an important technique for limiting the amount of traffic exchanged between Area Border Routers (ABRs).

And finally, you must specify a virtual link to any OSPF area that is not physically attached to the OSPF backbone. Virtual links can also be used to provide a redundant link between contiguous areas to prevent areas from being partitioned, or to merge backbone areas.

The following menu items provide all the global configuration options for OSPF:

<b>Parameter</b>	<b>Description</b>
Area ID Configuration	Defines a area within which all OSPF routers actively exchange routing information to ensure that they all have an identical link state database.
OSPF Area Range Configuration	Defines a range of subnetwork addresses. An area range is used to summarize route information exchanged between Area Border Routers.
OSPF Virtual Link Configuration	Defines a virtual link that can be used to connect an OSPF area not physically adjacent to the OSPF backbone, or to create a backup link to any area.
OSPF Host Route Configuration	Configures the route to a specific host within the area.

### **OSPF Area Configuration**

OSPF protocol broadcast messages (i.e., Link State Advertisements) are restricted by area to limit their impact on network performance. Before assigning an Area ID to a specific OSPF interface (see chapter 3 “*Configuring OSPF*”), you must first specify the Area ID in this table. Each entry in this table identifies a logical group of OSPF routers that actively exchange Link State Advertisements (LSAs) to ensure that they share an identical view of the network topology. You can configure the area as a normal one which can send and receive external Link State Advertisements (LSAs), a stubby area that cannot send or receive external LSAs, or a not-so-stubby area (NSSA) that can import external route information into its area.

OSPF Area Configuration		
Area ID	Type	Delete
192.168.1.0	NORMAL	
<a href="#">Add New Entry</a>		

Parameter	Description
Area ID	An OSPF area identifier configured for a group of OSPF routers. (For information on how to assign this identifier to a specific interface, see chapter 3 “ <i>Configuring OSPF</i> ”.)
Type	Indicates area type: Normal An area which can send or receive external route information. Stub An area which cannot send or receive external route information. It relies on a single default route provided by its Area Border Router (ABR) to access destinations outside of the stub. A stub can be used to reduce the amount of topology data that has to be exchanged over the network. NSSA A not so stubby area cannot send but can receive external route information. The ABR imports external routes and floods this information to all routers within the NSSA.

An Autonomous System Boundary Router (ASBR) can import external routes and flood this information to the entire Autonomous System.

**Note:**

To add an Area ID, click the string ([Add New Entry](#)). The screen can be show as below. Specify the identifier and type in the dialog boxes at the bottom of the screen, and press Save. To delete an Area ID, click on the Delete icon () for the required entry.

**Add OSPF Area**

Area ID:   
Type : NORMAL ▼  

Save
Reset
Cancel

**OSPF Area Range Configuration**

After you configure an area identifier, you can specify a subnetwork address range that covers all the individual networks in this area. This technique limits the amount of traffic exchanged between Area Border Routers (ABRs) by allowing them to advertise a single summary range. By summarizing routes, the routing changes within an area do not have to be updated in the backbone ABRs or in other areas.

To optimize the route summary, first configure all the OSPF routers in an area so that they fall within a contiguous address range. The route summary consists of an address and mask, where the mask can be a Variable Length Subnet Mask (VLSM). Using

VLSMs allows you to configure each subnetwork within a larger network with its own subnet mask. This provides a longer subnet mask that covers fewer host IP addresses, thereby reducing the size of the routing tables that have to be exchanged. (For more information on VSLMs, see RFCs 1219 and 1878.)

OSPF Area Range Configuration				
Area Identity	IP Address	Address Mask	Advertisement	Delete
192.168.1.0	192.168.1.0	255.255.255.0	Advertise	
<a href="#">Add New Entry</a>				

Parameter	Description
Area Identity	An OSPF area that includes all the OSPF routers within the assigned address range.
IP Address	The IP address used to calculate the area range.
Address Mask	The subnet mask used to calculate the area range.
Advertisement	Enables or disables advertising for this range.

**Note:**

To add an Area Range, click the string ([Add New Entry](#)). The screen can be show as below. Specify the required parameters in the dialog boxes at the bottom of the screen, and press Save. To delete an Area Range, click on the Delete icon () for the required entry.

**Add OSPF Area Range**

Area ID:

IP Address:

Address Mask:

Advertisement :  

**OSPF Virtual Link Configuration**

All OSPF areas must connect to the backbone. If an area does not have a direct physical connection to the backbone, you can configure a virtual link that provides a logical path to the backbone. To connect an isolated area to the backbone, the logical path can cross a single nonbackbone area to reach the backbone. To define the path, you must specify one endpoint on the ABR that connects the isolated area to the common nonbackbone area, and the other endpoint on the ABR that connects this common nonbackbone area and the backbone itself. (However, note that you cannot configure a virtual link that runs through a stub or NSSA area.)

Virtual links can also be used to create a redundant link between any area and the backbone to help prevent partitioning, or to connect two existing backbone areas into a

common backbone.

To configure a virtual link, specify the transit area through which the endpoint routers connect, and the address of the router on this side of the link.

OSPF Virtual Link Configuration			
Area ID	Neighbor Router ID	Status	Edit
192.168.1.0	192.168.1.254	Down	
<a href="#">Add New Entry</a>			

Parameter	Description
Area ID	An identifier for the transit area the virtual link crosses.
Neighbor Router ID	The IP address of the OSPF router on this end of the virtual link.

**Note:**

To add a Virtual Link, click the string ([Add New Entry](#)). The screen can be show as below. Specify the required parameters in the dialog boxes at the bottom of the screen, and press Add. To delete or modify a Virtual Link, click on the edit icon () for the required entry, and then press Delete or Save.

**Add OSPF Virtual Link**

Area ID :

Neighbor Router ID :

Add Reset Cancel

**OSPF Host route Configuration**

A host route is a prefix that will be advertised as a stub network in one of the router's link state advertisements. These prefixes may be IP addresses of hosts directly attached to the router, which themselves do not run OSPF. The router advertises these addresses by proxy.

OSPF Host Route Configuration			
IP Address	Cost	Area ID	Delete
192.168.1.0	19	192.168.1.0	
<a href="#">Add New Entry</a>			

Parameter	Description
IP Address	The IP address of this host.
Cost	The link state cost of this host. The range is 0 - 65535.
Area ID	The area that the host belongs to.

**Note:**

To add a Host Route, click the string ([Add New Entry](#)). The screen can be show as below. Specify the required parameters in the dialog boxes at the bottom of the screen, and press Save. To delete a Virtual Link, click on the Delete icon () for the required entry.

**Add OSPF Host Route**

IP Address :

Cost :

Area ID :

### Configuring BOOTP / DHCP Relay

If a DHCP / BOOTP server is not located in the same subnet with a host, you can configure this switch to forward any host configuration queries to a server located on another subnet or on another network. Depending on the configuration setup, the switch either:

- Forwards the packet to a preferred 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.

Specify the address for any DHCP server, or specify the subnet address for an outbound IP interface already configured on this switch (chapter 3 “Subnet Configuration”) as described in the following screens.

**DHCP Relay Database Configuration**

Index Server Address	Edit
-	-

Index Server Address:

Parameter	Description
Index Server Address	Used to define any preferred DHCP servers or the outbound subnetwork for relaying a DHCP request broadcast. (Up to five entries are permitted.)

#### Note:

To add a Relay Server, specify the IP address in the dialog box at the bottom of the screen, and press Add. To delete a Relay Server, click on the edit icon (✎) for the required entry, and then press Delete.

### IGMP Snooping Configuration

If enabled, you can use the IGMP Snooping Configuration screen to configure multicast filtering as shown below. (For further details see “Configuring IGMP Snooping” on

chapter 3.)

**IGMP Snooping Configuration**

IGMP Router Timeout (Minutes) :

IGMP Group Timeout (Minutes) :

Parameter	Default	Description
IGMP Router Timeout	5	A switch port that stops receiving multicast protocol packets for this interval will be removed from the IGMP forwarding list. Range: 3 - 5 minutes
IGMP Group Timeout	5	The time between last spotting an IGMP Report message for an IP multicast address on a specific port and the switch removing that entry from its list. Range: 3 - 5 minutes

### 3.6.6.3.Static ARP Configuration

Use the following screen to display or edit entries in the Static ARP Table. Entries added to this table are retained until the associated IP interface is deleted or the switch is reset to the factory defaults.

**Static ARP Table**

IP Address	MAC Address	Interface	Edit
-	-	-	-

IP Address :  MAC Address :  Interface :

Parameter	Description
IP Address	IP address statically mapped to a physical MAC address.
MAC Address	MAC address statically mapped to the corresponding IP address.
Interface	The index number of the IP interface that will use this static ARP entry. See chapter 3 "Subnet Configuration" or chapter 3 "Displaying Subnet Information".

**Note:**

To add a static address, specify it in the dialog box at the bottom of the screen, and press Add. To delete a static address, click on the edit icon (✎) for the required entry, and then press Delete.

### 3.6.6.4. Static Route Configuration

This switch can be configured to dynamically learn the routes to other IP networks, subnets or hosts using unicast or multicast routing protocols. If the route to a specific destination cannot be learned via these protocols, or you wish to restrict the path used for transmitting traffic to a destination, it can be statically configured using the Static Route Table.

Before defining a static route, remember that you must first configure at least one IP interface on this switch (chapter 3 “Subnet Configuration”). Static routes take precedence over dynamically learned routes and remain in the table until you remove them or the corresponding IP interface from this switch.

Static Route Table						
Destination Network	Destination mask	Vlan	Next hop	Type	Metrics	Edit
-	-	-	-	-	-	-
Destination Network : <input type="text"/> Destination Mask : <input type="text"/> Next Hop : <input type="text"/> Routing Metric : <input type="text"/>						
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Cancel"/>						

Parameter	Description
Destination Network	A destination network, subnet or host.
Destination Mask	The subnet mask that specifies the bits to match. A routing entry will be used for a packet if the bits in the address set by the destination mask match the Destination Network.
VLAN	The VLAN within which the gateway or destination address resides.
Next Hop	The IP address of the router at the next hop. Note that the network portion of the next hop must match that used for one of the subnet IP interfaces configured on this switch. (See “Subnet Configuration” on chapter 3.)
Type	The IP route type for the destination network. This switch supports the following types: Direct: A directly connected subnetwork. Indirect: A remote IP subnetwork or host address.
Routing Metric*	A relative measure of the path cost from this switch to the destination network.

\*This value depends on the specific routing protocol.

**Note:**

To add a static route, specify it in the dialog boxes at the bottom of the screen,

and press Add. To delete a static route, click on the edit icon (✎) for the required entry, and then press Delete.

### 3.6.6.5. Configuring the Default Route

Defines the router to which this switch will forward all traffic for unknown networks. The default route can be learned from RIP protocol (chapter 3 “Configuring RIP”) or manually configured. If the switch does not contain a default route, any packet that does not match an entry in the routing table (chapter 3 “Routing Table”) will be dropped. To manually configure a default route, enter the next hop in the following table.

Default Route	
VLAN:	0
Next Hop Address:	<input type="text"/>
Metric:	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Delete"/> <input type="button" value="Cancel"/>	

Parameter	Description
VLAN	The VLAN which has the IP interface to the default router.
Next Hop Address	The IP address of the default router.
Metric	The number of hops required to reach the default router.

### 3.6.7. Configuring Security Filters

You can use the Security menu to filter MAC and IP addresses.

Parameter	Description
MAC Filtering Configuration	Specifies the source or destination MAC address for any traffic to be filtered from the switch.
IP Filtering Configuration*	Specifies the source or destination IP address for any traffic to be filtered from the switch.
Security Mode	Configuration the security mode.

\* This menu item is only displayed when intelligent switch is set to multilayer mode.

#### 3.6.7.1. Configuring MAC Address Filters

Any node that presents a security risk or is functioning improperly can be filtered from this switch. You can drop all the traffic from a host device based on a specified MAC address. Traffic with either a source or destination address listed in the Security Filtering Configuration table will be filtered.

MAC Filtering Configuration	
MAC Address	Edit
-	-

MAC Address:

**Note:**

To add a MAC address to the security filter, press Add. To delete an address, click on the edit icon (✎) for the required entry, and then press Delete.

### 3.6.7.2. Configuring IP Address Filters

If any node presents a security risk, you can filter all traffic for this node by entering its address into the IP Security Filter. Any packet passing through the switch that has a source or destination IP address matching an entry in this table will be filtered.

IP Filtering Configuration	
IP Filter Entry List	Edit
-	-

IP Address :

**Note:**

To add an IP address to the security filter, press Add. To delete an address, click on the edit icon (✎) for the required entry, and then press Delete.

### 3.6.7.3. Configuring Security Mode

In default type, the switch can auto learning the MAC Address from each port. If you want to let someone to use a specifies port and the other people can not use. You should disable the auto learning function and setup the uplink port (if one packet's DA does not define in any port, it would be forwarding to the uplink port). Then you must to set the static unicast address on the port that you allow someone to use.

Security Mode	
Learning Function :	Enabled ▾
Uplink Port :	24 ▾
Apply	Cancel

## 3.7. Monitoring the Switch

The Network Monitor Menu provides access to port statistics, address tables, STA information, VLANs registration and forwarding information, multicast groups, and subnet addresses. Each of the screens provided by these menus is described in the following sections.

Menu	Description
Port Statistics	Displays statistics on port traffic, including information from the Interfaces Group, Ethernet-like MIB, and RMON MIB.
Layer 2 Address Table	Contains the unicast address table.
Bridge Menu	Displays Spanning Tree settings for the overall switch and for specific ports.
VLAN Menu	Displays ports dynamically learned through GMRP or GVRP, and ports that are currently forwarding VLAN traffic.
IP Multicast Registration Table <sup>1</sup>	Displays all the multicast groups active on this switch, including the multicast IP address and the corresponding VLANs.
IP Menu <sup>2</sup>	Displays all the IP subnets used on this switch, as well as the corresponding VLANs and ports. Also contains the ARP table, routing table, multicast menu, and OSPF menu.

1. This menu is displayed only if intelligent switch is set to Layer 2 mode or the switch is management model.
2. This menu is displayed if the intelligent switch is set to multilayer mode.

### 3.7.1. Displaying Port Statistics

Port Statistics display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMON MIB.

Parameter	Description
Port Statistics	Displays standard statistics on network traffic passing through the selected port.
RMON Statistics	Displays detailed statistics for the selected port, such as packet type and frame size counters.

### 3.7.1.1. Displaying Ethernet Port Statistics

Port Statistics display key statistics from the Interfaces Group and Ethernet-like MIBs for each port. Error statistics on the traffic passing through each port are displayed. This information can be used to identify potential problems with the switch, such as a faulty port or unusually heavy loading. The values displayed have accumulated since the last system reboot.

Select the required port. The statistics displayed are indicated in the following figure and table.

Port Number :

Interfaces			
In Octets	0	Out Octets	0
In Unicast Pkts.	0	Out Unicast Pkts.	0
In Non-Unicast Pkts.	0	Out Non-Unicast Pkts.	0
In Discards	0	Out Discards	0
In Errors	0	Out Errors	0
Alignment Errors	0	CRC Errors	0
Ethernet			
Single Collisions	0	Multiples Collisions	0
Deferred Transmissions	0	Late Collisions	0
Excess Collisions	0	Carrier Sense Errors	0
Drop Events	0	Fragments	0
Octets	0	Jabbers	0

Parameter	Description
<i>Interfaces Group</i>	
In Octets	The total number of octets received on the interface, including framing characters.
In Unicast Pkts.	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
In Non-Unicast Pkts.	The number of non-unicast (that is, subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.
In Discards	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
In Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Alignment Errors	The number of alignment errors (missynchronized data packets).

Out Octets	The total number of octets transmitted out of the interface, including framing characters.
Out Unicast Pkts.	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Out Non-Unicast Pkts.	The total number of packets that higher-level protocols requested be transmitted to a non- unicast (that is, a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent.
Out Discards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Out Errors	The number of outbound packets that could not be transmitted because of errors.
CRC Errors	Number of Ethernet Cyclic Redundancy Check errors detected by this device.
<i>Ethernet-Like</i>	
Single Collisions	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Excessive Collisions	The number of frames for which transmission failed due to excessive collisions.
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Octets	Number of octets passing through this port.
Multiple Collisions	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and contained either an FCS or alignment error.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and contained either an FCS or alignment error.

**Note:**

Statistics are refreshed every 10 seconds by default (chapter 3 “Configuring the Serial Port”).

### 3.7.1.2. Displaying RMON Statistics

Use the RMON Statistics screen to display key statistics for each port from RMON group 1. (RMON groups 2, 3 and 9 can only be accessed using SNMP management software.) The following screen displays the overall statistics on traffic passing through each port. RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. Values displayed have been accumulated since the last system reboot.

Port Number :

Drop Events	0	Jabbers	0
Received Bytes	0	Collisions	0
Received Frames	0	64 Byte Frames	0
Broadcast Frames	0	65-127 Byte Frames	0
Multicast Frames	0	128-255 Byte Frames	0
CRC/Alignments Errors	0	256-511 Byte Frames	0
Undersize Frames	0	512-1023 Byte Frames	0
Oversize Frames	0	1024-1518 Byte Frames	0
Fragments	0	1519-1536 Byte Frames	0

refresh    Reset Port Statistics    Reset All Statistics

Parameter	Description
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC / Alignment Errors	The number of CRC / alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.

Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and contained either an FCS or alignment error.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and contained either an FCS or alignment error.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
64 Byte Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

**Note:**

Statistics are refreshed every 10 seconds by default (chapter 3 “Configuring the Serial Port”).

### 3.7.2.Layer 2 Address Table

This menu includes the unicast address table.

Menu	Description
Unicast Address Table	Provides a full listing for unicast addresses.

#### 3.7.2.1.Displaying the Unicast Address Table

The Unicast Address Table contains the MAC addresses associated with each port that is, the source port associated with the address). The information displayed in the Address Table is indicated in the following figure and table.

Unicast Address Table	
Address	Port
0080AD-05E7D7	12

Parameter	Description
Address	The MAC address of a node seen on this switch.
Port	The port whose address table includes this MAC address.

### 3.7.3. Displaying Bridge Information

The Bridge menu is used to display settings for the Spanning Tree Algorithm. For a more detailed description of how to use this algorithm, refer to “Spanning Tree Algorithm” on chapter 4.

Menu	Description
Spanning Tree Bridge Information	Displays a full list of STA values used for the bridge.
Spanning Tree Port Information	Displays a list of STA values used for each port, including status, designated cost, designated bridge, and designated port.

#### 3.7.3.1. Viewing the Current Spanning Tree Information

The STA Bridge Information screen displays a summary of STA information for the overall bridge. To make any changes to these parameters, use the Bridge STA Configuration menu as described on chapter 3 “Configuring Global Bridge Settings”.

The parameters shown in the following figure and table describe the current Bridge STA settings.

STA Bridge Information
Priority : 32768
Hello Time : 2 seconds
Max Age : 20 seconds
Forward Delay : 15 seconds
Hold Time : 1 seconds
Designated Root : 32768.00C00C400000
Root Cost : 19
Root Port : 6
Configuration Changes : 0
Topology Up Time : 166372

Parameter	Description
Priority	Device priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
Hello Time	The time interval (in seconds) at which the root device transmits a configuration message.
Max Age	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure.

Forward Delay	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding).
Hold Time	The minimum interval between the transmission of consecutive Configuration BPDUs.
Designated Root	The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
Root Cost	The path cost from the root port on this switch to the root device.
Root Port	The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
Configuration Changes	The number of times the Spanning Tree has been reconfigured.
Topology Up Time	The time since the Spanning Tree was last reconfigured.

### 3.7.3.2. Displaying the Current STA for Ports

The parameters shown in the following figure and table are for port STA Information.

STA Port Information					
Port	Type	Status	Designated Cost	Designated Bridge	Designated Port
1	100BASE-TX	Disabled	0	32768.0010B5DDDA20	128.1
2	100BASE-TX	Disabled	0	32768.0010B5DDDA20	128.2
3	100BASE-TX	Disabled	0	32768.0010B5DDDA20	128.3
4	100BASE-TX	Disabled	0	32768.0010B5DDDA20	128.4
5	100BASE-TX	Disabled	0	32768.0010B5DDDA20	128.5
6	100BASE-TX	Disabled	0	32768.0010B5DDDA20	128.6

Parameter	Description
Type	Shows port type as: 100BASE-TX: 10BASE-T / 100BASE-TX 100BASE-FX: 100BASE-FX 1G BASE-SX/LX: 1000BASE-SX/LX (multimode/ single mode) 1G BASE-T: 1000BASE-T

Status	<p>Displays current state of this port within the Spanning Tree:</p> <p><b>Disabled</b> No link has been established on this port. Otherwise, the port has been disabled by the user or has failed diagnostics.</p> <p><b>Blocking</b> Port receives STA configuration messages, but does not forward packets.</p> <p><b>Listening</b> Port will leave blocking state due to a topology change, start transmitting configuration messages, but does not yet forward packets.</p> <p><b>Learning</b> Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.</p> <p><b>Forwarding</b> The port forwards packets, and continues learning addresses.</p> <p>The rules defining port status are:</p> <ul style="list-style-type: none"> <li>• A port on a network segment with no other STA-compliant bridging device is always forwarding.</li> <li>• If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is blocked.</li> <li>• All ports are blocked when the switch is booted, then some of them change state to listening, to learning, and then to forwarding.</li> </ul>
Designated Cost	The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
Designated Bridge (ID)	The priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
Designated Port (ID)	The priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.

### 3.7.4. Displaying VLAN Information

These menus display information on the ports that have been automatically learned via GVRP and all those ports that have been configured by dynamic or static means to forward VLAN traffic.

Menu	Description
VLAN Dynamic Registration Information	Shows the ports that have been automatically learned via GVRP.
VLAN Forwarding Information	Shows all those ports that have been configured by either dynamic or static means to forward VLAN traffic.

#### 3.7.4.1. VLAN Dynamic Registration Information

This table shows the ports that have been automatically learned via GVRP.

VLAN Dynamic Registration Information	
VLAN	Port Members
1	-

### 3.7.4.2.VLAN Forwarding Information

Shows all those ports that have been configured by either dynamic or static means to forward VLAN traffic.

VLAN Forwarding Information		
VLAN	Type	Port Members
1	Static	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

### 3.7.5.IP Multicast Registration Table

This table displays all the multicast groups active on the switch, including the multicast IP address and the corresponding VLANs.

IP Multicast Registration Table			
VLAN	Multicast IP	Multicast Group Ports	Learn By
-	-	-	-

Parameter	Description
VLAN	A VLAN with host members that have asked to receive the indicated multicast service.
Multicast IP	A source IP address that represents a specific multicast service.
Multicast Group Ports	The ports that belong to the indicated VLAN group.
Learned By	Shows if this entry was learned dynamically or via IGMP Snooping. An entry is learned dynamically if a multicast packet was seen crossing the port, or via IGMP Snooping if an IGMP registration packet was seen crossing the port.

### 3.7.6.IP Menu

This menu contains IP subnets information, the ARP cache, routing table, as well as multicast groups and multicast routing information.

Menu	Description
Subnet Information	Displays all the IP subnets configured on this switch, as well as the corresponding VLANs and ports.
ARP Table	Shows the IP-to-MAC addresses discovered by ARP.
Routing Table	Shows the routes through which all recognized Ethernet networks (and the corresponding VLAN) can be reached.
Multicast Table	Displays all the multicast groups active on this switch, including the multicast IP address and the corresponding VLANs. Also includes the IGMP registration table, the multicast forwarding cache, and DVMRP routing information.
OSPF Table	Displays a link state advertisement summary, the neighbor table, and the virtual neighbor table.

### 3.7.6.1. Displaying Subnet Information

You can display a list of all the IP interfaces configured on this switch. This table includes the gateway address, corresponding VLAN, and member ports that use this address.

Subnet Information																										
IP Address	Subnet Mask	VLAN	Port Members																							
192.72.53.109	255.255.255.0	1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

Parameter	Description
IP Address	The address for an IP interface on this switch.
Subnet Mask	A template that identifies the address bits in the host address used for routing to specific subnets. Each bit that corresponds to a “1” is part of the network / subnet number; each bit that corresponds to “0” is part of the host number.
VLAN	The VLAN group associated with this IP interface.
Port Members	The ports that can be reached through this IP interface.

### 3.7.6.2. ARP Table

Address Resolution Protocol (ARP) defines a method for extracting a host’s Ethernet address from its Internet address. This table shows the IP-to-MAC address cache discovered via ARP.

ARP Table			
IP Address	Mac Address	VLAN	Port
192.72.53.76	0080AD-05E7D7	1	12
192.72.53.109	0010B5-DDDA20	1	0

Parameter	Description
IP Address	IP addresses for which ARP has resolved the physical address through a broadcast message.

MAC Address	MAC address that maps to the corresponding IP address.
VLAN	The VLAN group to which this host has been assigned.
Port	The port this to which host device is attached. (Port "0" refers to an interface defined on this switch.)

### 3.7.6.3. Routing Table

The Routing Table lists the routes through which all recognized Ethernet networks (and corresponding VLANs) can be reached. This table includes all routes learned through routing protocols or manual configuration.

Routing Table								
Destination Network	Destination Mask	VLAN	Next Hop	Type	Protocol	Route Tag	Route Aging	Routing Metric
192.72.53.0	255.255.255.0	1	192.72.53.109	Direct	Local	-	-	1

Parameter	Description
Destination Network	A destination network, subnet or host.
Destination Mask	The subnet mask that specifies the bits to match. A routing entry will be used for a packet if the bits in the address set by the destination mask match the Destination Network.
VLAN	The VLAN within which the gateway or destination address resides.
Next Hop	The IP address of the router at the next hop.
Type	The IP route type for the destination network. This switch supports the following types: Direct: A directly connected subnetwork. Indirect: 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. Invalid: A illegal IP address to be filtered.
Protocol	The route was learned in one of the following ways: Local: Manually configured Mgmt. : Set via SNMP ICMP: Obtained via ICMP redirect. RIP: Learned via RIP protocol. OSPF: Learned via OSPF protocol. Other: Learned by some other method.
Route Tag	The route tag represents the device that originated this routing entry.
Route Aging	The number of seconds elapsed since this route was last updated or otherwise determined to be correct. (This entry only applies to RIP.)
Routing Metric	A relative measure of the path cost from this switch to the destination network. (This value depends on the specific routing protocol.)

### 3.7.6.4.Multicast Table

You can use this menu to display all the multicast groups currently active on this switch, the IGMP cache, the multicast forwarding cache, and DVMRP routing information.

Parameter	Description
IP Multicast Registration Table	Displays all active multicast groups, including the multicast IP address and the corresponding VLANs. (See chapter 3 “IP Multicast Registration Table”.)
IGMP Cache	Displays all active multicast groups, including the IP interface each entry appears on, the entry age, and the time left before the entry is aged out.
Multicast Forwarding Table	Displays all active multicast groups, including the multicast source address, the upstream neighbor, the multicast routing protocol, and the entry age.
DVMRP Routing Table	Displays the source address for each known multicast service, the upstream neighbor, the IP interface each entry appears on, the routing metric, and the entry age.
DVMRP Neighbor Table	Displays all the neighbor routers accessible through each IP interface, including the entry age, the time left before the entry is aged out, the protocol version, and the number of routing updates received from each neighboring router.

#### **Displaying IGMP Cache**

The switch provides a local registry of active multicast groups for each IP interface, including the age and expiration time for each entry.

IGMP Registration Table					
Group Address	Interface	Reporter	Up Time	Expire Time	V1 Timer
-	-	-	-	-	-

Parameter	Description
Group Address	An IP multicast group address with subscribers directly attached or downstream from this switch.
Interface	The IP interface on this switch that has received traffic directed to the IP multicast group address. (See chapter 3 “Displaying Subnet Information”.)
Reporter	The IP address of the source of the last membership report received for this IP Multicast group address on this interface. If no membership report has been received, this object has the value 0.0.0.0.
Up Time	The time elapsed since this entry was created.
Expire Time	The time remaining before this entry will be aged out. (The default is 260 seconds.)

V1 Timer	<p>The time remaining until the switch assumes that there are no longer any IGMP Version 1 members on the IP subnet attached to this interface. (The default is 400 seconds.)</p> <p>If the switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts present which are members of the group for which it heard the report.</p> <p>If there are Version 1 hosts present for a particular group, the switch will ignore any Leave Group messages that it receives for that group.</p>
----------	--

### ***Displaying the Multicast Forwarding Cache***

The switch maintains a cache of multicast routing entries used to calculate the delivery tree in multicast routing protocols. The Multicast Forwarding Cache includes the subnetwork that contains the multicast source and the nearest upstream neighbor for each known multicast group address.

Multicast Forwarding Cache					
Group Address	Source Address	Mask	Upstream Neighbor	Protocol	Up Time
-	-	-	-	-	-

Parameter	Description
Group Address	An IP multicast group address with subscribers directly attached or downstream from this switch.
Source Address	The IP subnetwork at the root of the multicast delivery tree. This subnetwork contains a known multicast source.
Mask	Subnet mask that is used for the source address. This mask identifies the host address bits used for routing to specific subnets.
Upstream Neighbor	The IP address of the network device immediately upstream for this group.
Protocol	The multicast routing protocol associated with this entry.
Up Time	The time elapsed since this entry was created.

### ***Displaying the DVMRP Routing Table***

The DVMRP Routing Table contains all the IP multicast routes learned by the DVMRP protocol. The routes displayed in this table are used by this switch to forward new IP multicast traffic. They do not reflect active multicast flows.

Dvmrp Routing Table					
Source Address	Subnet Mask	Upseam Neighbor	Interface	Metric	Up Time
-	-	-	-	-	-

Parameter	Description
Source Address	The IP subnetwork at the root of the multicast delivery tree. This subnetwork contains a known multicast source.

Subnet Mask	Subnet mask that is used for the source address. This mask identifies the host address bits used for routing to specific subnets.
Upstream Neighbor	The IP address of the network device immediately upstream for this multicast delivery tree.
Interface	The IP interface on this switch that connects to the upstream neighbor. (See chapter 3 “Displaying Subnet Information”.)
Metric	The metric for this interface used to calculate distance vectors.
Up Time	The time elapsed since this entry was created.

### **Displaying the DVMRP Neighbor Table**

The DVMRP Neighbor Table contains the switch’s DVMRP neighbors, as discovered by receiving DVMRP protocol messages.

DVMRP Neighbor Table					
Interface	Neighbor Address	Up Time	Expire Time	Version	Rcv Route
-	-	-	-	-	-

Parameter	Description
Interface	The IP interface on this switch that connects to the upstream neighbor. (See chapter 3 “Displaying Subnet Information”.)
Neighbor Address	The IP address of the network device immediately upstream for this multicast delivery tree.
UpTime	The time since this device last became a DVMRP neighbor to this switch.
ExpireTime	The time remaining before this entry will be aged out.
Version	The neighboring router’s DVMRP version number.
Rcv Route	The total number of routes received in valid DVMRP packets from this neighbor. This can be used to diagnose problems such as unicast route injection, as well as giving an indication of the level of DVMRP route exchange activity.

### 3.7.6.5.OSPF Table

You can use this menu to display the OSPF router linkages for the autonomous system based on the Link State Table, Neighbor Table, and Virtual Neighbor Table.

Parameter	Description
Interface Table	
Link State Table	Displays a summary link state advertisements.
Neighbor Table	Displays current neighbor routers.
Virtual Neighbor Table	Displays current virtual neighbors.

### **Displaying the Interface Table**

The OSPF Interface Table contains the parameters of OSPF interfaces configured on this router.

OSPF Interface Table					
IP Address	Router ID	Designated Router	Backup DR	Status	Events
192.72.53.110	0.0.0.0	0.0.0.0	0.0.0.0	Down	0

Parameter	Description
IP Address	The IP address of this OSPF interface.
Router ID	Router ID for this router.
Designated Router	The IP of the designated router. The designated router advertises the link state of the OSPF Area.
Backup DR	The backup designated router. If the designated router fails, the backup designated router takes its place.
Status	This interface's status in this OSPF area.
Events	The number of events since the designated router was selected.

### Displaying the Link State Table

The link state table displays all advertisements in the link state database. This database contains linkage information for all the areas to which this router is attached. Note that all the routers within an area exchange information to ensure that they maintain an identical link state database. This database can therefore be used to troubleshoot network configuration problems.

OSPF Link State Table					
Area ID	Type	Link State ID	Router ID	SN	Age
-	-	-	-	-	-

Parameter	Description
Area ID	An OSPF area identifier configured for a group of OSPF routers. (For information on how to assign this identifier to a specific interface, see chapter 3 "Configuring OSPF".)
Type	The link state advertisement type: RtrLSA: Router LSA – All area routers advertise the state of links from the router itself to the its local area. NetLSA: Network LSA – The designated router for each area advertises the link state for each transit area; i.e., an area with more than one attached router. This LSA includes information about each router attached to the area, including the designated router itself. SumLSA: Summary LSA – Advertise the cost to a specific subnetwork outside the router's area, or the cost to a specific autonomous system boundary router. ExtLSA: External LSA – Advertises link state information for each known network outside the autonomous system.
Link State ID	The identifier for the router originating this entry, usually in the form of an IP address.
Router ID	The IP address of the originating router.

SN	The link state sequence number, used to remove previous duplicate LSAs.
Age	The number of seconds since this LSA was originated.

### ***Displaying the Neighbor Table***

Each router exchanges link state information with all neighbors physically attached to the same network segment. This table displays a summary of the link state for all adjacent neighbors. (Note that neighboring routers are discovered by this device via Hello messages.)

OSPF Neighbor Table						
IP Address	ID	Router ID	Option	Priority	State	Events
-	-	-	-	-	-	-

Parameter	Description
IP Address	IP address of the neighboring router.
ID	The index number of the router interface to which this neighbor is attached. For IP protocol, this value will always be zero.
Router ID	The OSPF identifier for the neighboring router.
Option	The optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its Hello packets. This enables received Hellos to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities. The OSPF optional capabilities currently accepted include external routing capability and TOS capability. You need to map the binary bits to the supported options. For example, "3" indicates both routing capability and TOS capability.
Priority	The neighbor's router priority. This priority is used in electing the designated router for the area in which it exists. This value will be set to zero if this router cannot be elected.

State	<p>The communication state for two adjacent routers:</p> <p><b>Down:</b> This is the initial state of a neighbor conversation. It indicates that there has been no recent information received from the neighbor.</p> <p><b>Attempt:</b> This state is only valid for neighbors attached to non-broadcast networks. It indicates that no recent information has been received from the neighbor, but that the router is attempting to contact the neighbor by sending Hello packets.</p> <p><b>Init:</b> A Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor.</p> <p><b>2-Way:</b> Communication between the two routers has been established. This is the most advanced state short of beginning adjacency establishment. Note that both the Designated Router and Backup Designated Router are selected from the set of neighbors in state 2-Way or greater.</p> <p><b>ExStart:</b> This is the first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial sequence number. Neighbor conversations in this state or greater are called adjacencies.</p> <p><b>Exchange:</b> The router is describing its entire link state database by sending database description packets to the neighbor. (Each database description packet has a sequence number, and is explicitly acknowledged.) All adjacencies in Exchange state or greater are used by the flooding procedure. In fact, these adjacencies are fully capable of transmitting and receiving all types of OSPF routing protocol packets.</p> <p><b>Loading:</b> Link State Request packets are sent to the neighbor asking for more recent advertisements that have been discovered (but not yet received) in the Exchange state.</p> <p><b>Full:</b> The neighboring routers are fully adjacent. These adjacencies will now appear in router links and network links advertisements.</p>
Events	The number of events encountered that cause a neighbor state change since boot up.

***Displaying the Virtual Neighbor Table***

Virtual links can be used to link an area isolated from the backbone, to create a redundant link between any area and the backbone to help prevent partitioning, or to connect two existing backbone areas into a common backbone. Note that the processes of establishing a active link between virtual neighbors is similar to that used for physically adjacent neighbors.

OSPF Virtual Neighbor Table					
Area ID	Router ID	IP Address	Option	State	Events
-	-	-	-	-	-

Parameter	Description
Area ID	The transit area the virtual link must cross to connect the border routers.
Router ID	The OSPF identifier for the router at the other end of the link.
IP Address	IP address of the border router at the other end of the link.
Option	<p>The optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its Hello packets. This enables received Hellos to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities. The OSPF optional capabilities currently accepted include external routing capability and TOS capability.</p> <p>You need to map the binary bits to the supported options. For example, "3" indicates both routing capability and TOS capability.</p>

State	<p>The communication state for two adjacent routers:</p> <p><b>Down:</b> This is the initial state of a neighbor conversation. It indicates that there has been no recent information received from the neighbor.</p> <p><b>Attempt:</b> This state is only valid for neighbors attached to non-broadcast networks. It indicates that no recent information has been received from the neighbor, but that the router is attempting to contact the neighbor by sending Hello packets.</p> <p><b>Init:</b> A Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor.</p> <p><b>2-Way:</b> Communication between the two routers has been established. This is the most advanced state short of beginning adjacency establishment. Note that both the Designated Router and Backup Designated Router are selected from the set of neighbors in state 2-Way or greater.</p> <p><b>ExStart:</b> This is the first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial sequence number. Neighbor conversations in this state or greater are called adjacencies.</p> <p><b>Exchange:</b> The router is describing its entire link state database by sending database description packets to the neighbor. (Each database description packet has a sequence number, and is explicitly acknowledged.) All adjacencies in Exchange state or greater are used by the flooding procedure. In fact, these adjacencies are fully capable of transmitting and receiving all types of OSPF routing protocol packets.</p> <p><b>Loading:</b> Link State Request packets are sent to the neighbor asking for more recent advertisements that have been discovered (but not yet received) in the Exchange state.</p> <p><b>Full:</b> The neighboring routers are fully adjacent. These adjacencies will now appear in router links and network links advertisements.</p>
Events	The number of events encountered that cause a neighbor state change since boot up.

### 3.8.Resetting the System

Use the Restart command under the Main Menu to reset the management agent. The reset screen is shown below.

**Restart Option**

Reload Factory Default :

Parameter	Description
Reload Factory Defaults	Reloads the factory defaults
Apply	Restarts the switch.

**Note:**

When restarting the system, it will always run the Power-On Self-Test. It will also retain all system information, unless you elect to reload the factory defaults.

## 4. Chapter 4: Advanced Topics

This switch supports both Layer 2, which is based on physical device addresses, and Layer 3 switching, which is based on IP network addresses. These functions, along with other advanced features are described in this chapter.

### 4.1.Layer 2 Switching

When a frame enters a port, its destination MAC address is checked in the address database to see which port leads to this destination. If the destination address belongs to the incoming port, the frame is dropped or “filtered.” If the destination port is found on another port, the frame is forwarded to that port and queued for output. But, if the destination address is not found in the address database, the frame is sent to one or more output ports based on the rules for handling tagged or untagged VLAN frames. If the source MAC address of the frame was not found in the address database, it is recorded along with the incoming port number where it entered the switch. This information is then used to make later decisions for frame forwarding.

During switching, the switch performs multiple steps, including:

- VLAN Classification
- Learning
- Filtering
- Forwarding
- Aging

The following sections provide additional information about the tasks the switch performs during unicast and multicast switching.

#### 4.1.1.Unicast Switching

This section describes VLAN classification, learning, filtering, and forwarding for unicast switching.

- VLAN Classification—When the switch receives a frame, it classifies the frame in one of two ways:
  - If the frame is untagged, the switch classifies the frame into the default VLAN for the incoming port.
  - If the frame is tagged, the switch uses the tagged VLAN ID to identify the broadcast domain of the frame.
- Learning—After VLAN classification, the switch checks the <source MAC address, VLAN> pair in the address table to see whether this pair is known.
  - If unknown, the switch adds this pair to the address table.
  - If known, the switch checks the pair for an incorrect Port ID. If the PID

associated with the pair in the address table is different from the receiving port, the switch modifies the PID in the address table.

- Filtering—After learning the address, the switch checks:
  - If the source or destination port is not in the forwarding state. (For example, if it is in blocking state or has been disabled.)
  - If the source or destination MAC address is to be filtered.
  - If the source PID is the same as the destination PID.

If any of these conditions are met, the switch drops the received frame.

Otherwise, it continues with the forwarding process as described below.

- Forwarding—During the forwarding process, the switch checks whether the <destination MAC address, VLAN> pair is unknown.
  - If unknown, the switch floods the received frame to all ports in the VLAN, excluding the source port.
  - If known, the switch forwards the received frame to the port associated with the pair. At the same time, the switch decides whether a VLAN tag needs to be added to or stripped from the frame, depending on the VLAN tagged / untagged configuration and VLAN ID for the output port.
- Aging—the switch performs the aging process for the <MAC addresses, VLAN> pair in the MAC address table. Once a pair is aged out, the address table is modified.

## 4.1.2. Multicast Switching

For multicast switching, the switch checks whether the received frame is a Bridge Protocol Data Unit (BPDU). If a BPDU is received, the switch forwards the frame for processing by the Spanning Tree Protocol. Otherwise, the switch performs the following processes:

- VLAN classification—same as for unicast switching (chapter 4 “Unicast Switching”).
- Learning—same as for unicast switching (chapter 4 “Unicast Switching”).
- Filtering—after learning, the switch checks the same filtering criteria used for unicast switching (chapter 4 “Unicast Switching”), except there is no destination MAC address to check.
- Forwarding—the switch floods the received multicast frame to all ports within the VLAN, excluding the source port. At the same time, the switch decides whether a VLAN tag needs to be added to or stripped from the frame, depending on the VLAN tagged / untagged configuration and VLAN ID for the output port.
- Aging—same as for unicast switching (chapter 4 “Unicast Switching”).

## 4.1.3. Spanning Tree Algorithm

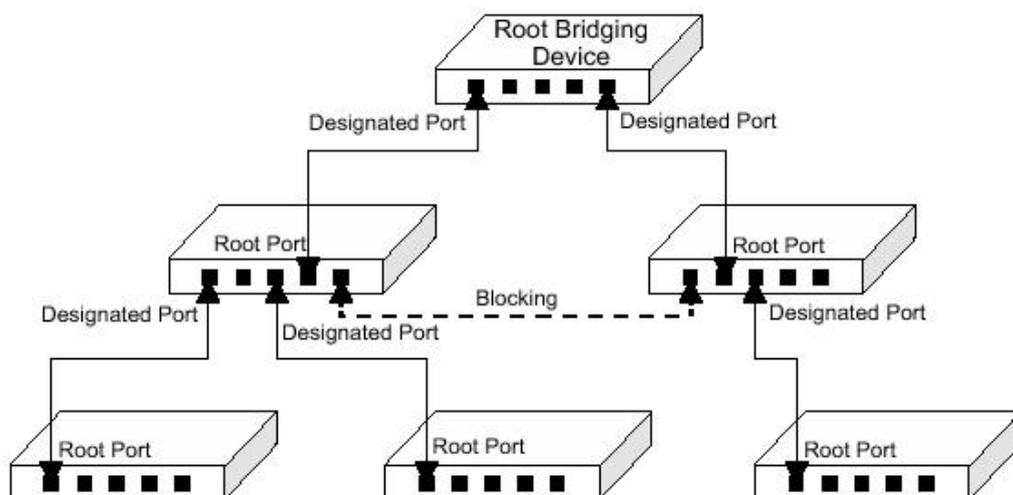
The Spanning Tree Algorithm (that is, the STA-configuration algorithm as outlined in

IEEE 802.1D) can be used to detect and disable network loops, and to provide link backup. This allows the switch to interact with other bridging devices (including STA-compliant switches, bridges or routers) in your network to ensure that only one route exists between any two stations on the network. If redundant paths or loops are detected, one or more ports are put into a blocking state (stopped from forwarding packets) to eliminate the extra paths. Moreover, if one or more of the paths in a stable spanning tree topology fail, this algorithm will automatically change ports from blocking state to forwarding state to reestablish contact with all network stations.

STA uses a distributed algorithm to select a bridging device (STA-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

The following figure gives an illustration of how the Spanning Tree Algorithm assigns bridging device ports.



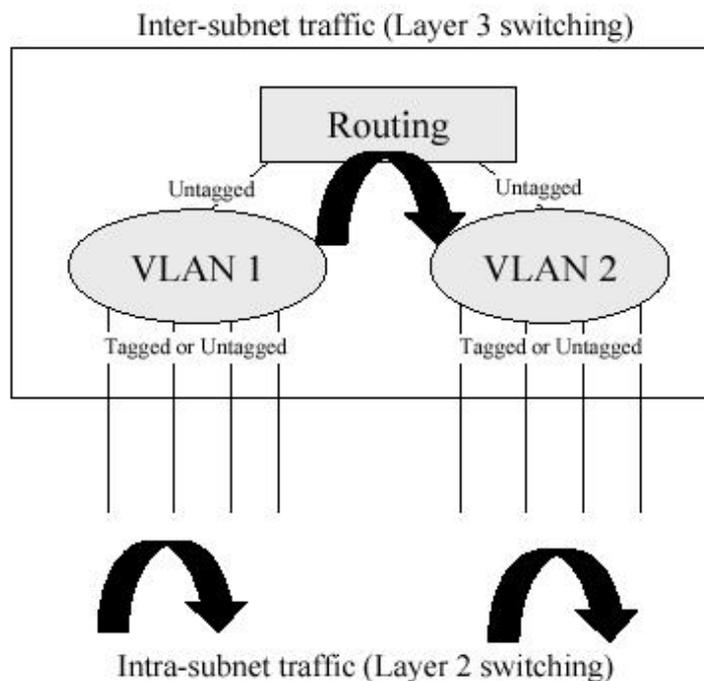
## 4.2.Layer 3 Switching

The two major functions provided by a Layer 3 switch include IP Switching and Routing Path Management. When the switch is set to multilayer mode (chapter 2 "Setting the System Operation Mode"), it acts as a routing switch, with support for standard IP routing and the ability to pass traffic between VLANs as required. However, when the switch is first set to multilayer mode, no default routing is defined. As with all traditional routers, the routing function must first be configured to work. (RIP: chapter 2 , 3 "Configuring RIP"; OSPF: chapter 2 ,3 "Configuring OSPF").

### 4.2.1.Initial Configuration

In the default configuration, all ports belong to the same virtual LAN and the switch provides only Layer 2 functionality. Therefore, you should first group all the ports that belong to the same subnet into virtual LANs (chapter 2 , 3 "VLAN Table Configuration"). By separating the switch into different VLANs, the network is partitioned into subnetworks that are disconnected at Layer 2. Network traffic within the same subnet is still switched using Layer 2 switching. And the VLANs can now be interconnected (only as required) with Layer 3 switching.

Each VLAN represents a virtual interface to Layer 3. You just need to provide the network addresses for each virtual interface (chapter 2 , 3 "Subnet Configuration"), and the traffic between different subnetworks will be routed by Layer 3 switching.



**Note:**

When operating the switch in multilayer mode, this switch does not currently

support tagging, so you should set the PVID to the same value at both ends of the link (if the device you are attaching to is VLAN-aware), and configure an IP interface for this VLAN if you need to connect it to other groups. (See “VLAN Tagging” on chapter 2 and chapter 3.) This limitation will be removed for future firmware versions.

## 4.2.2.IP Switching

IP Switching (or packet forwarding) encompasses tasks required to forward packets for both Layer 2 and Layer 3, as well as traditional routing. These functions include:

- Layer 2 forwarding (switching) based on the Layer 2 destination MAC address
- Layer 3 forwarding (routing):
  - Based on the Layer 3 destination address
  - Replacing destination / source MAC addresses for each hop
  - Incrementing the hop count
  - Decrementing the time-to-live
  - Verifying and recalculating the Layer 3 checksum

If the destination node is on the same subnetwork as the source network, then the packet can be transmitted directly without the help of a router. However, if the MAC address is not yet known to the switch, an Address Resolution Protocol (ARP) packet with the destination IP address is broadcast to get the destination MAC address from the destination node. The IP packet can then be sent directly with the destination MAC address.

If the destination belongs to a different subnet on this switch, the packet can be routed directly to the destination node. However, if the packet belongs to a subnet not included on this switch, then the packet should be sent to a router (with the MAC address of the router itself used as the destination MAC address, and the destination IP address of the destination node). The router will then forward the packet to the destination node via the correct path. The router can also use the ARP protocol to find out the MAC address of the destination node of the next router as necessary.

### **Note:**

In order to perform IP switching, the switch should be recognized by other network nodes as an IP router, either by setting it as the default gateway or by redirection from another router via the ICMP process.

When the switch receives an IP packet addressed to its own MAC address, the packet follows the Layer 3 routing process. The destination IP address is checked against the Layer 3 address table. If the address is not already there, the switch broadcasts an ARP packet to all the ports on the destination VLAN to find out the destination MAC address.

After the MAC address is discovered, the packet is reformatted and sent out to the destination. The reformat process includes decreasing the Time-To-Live (TTL) field of the IP header, recalculating the IP header checksum, and replacing the destination MAC address with either the MAC address of the destination node or that of the next hop router.

When another packet destined to the same node arrives, the destination MAC can be retrieved directly from the Layer 3 address table; the packet is then reformatted and sent out the destination port. IP switching can be done at wire-speed when the destination address entry is already in the Layer 3 address table.

If the switch determines that a frame must be routed, the route is calculated only during setup. Once the route has been determined, all packets in the current flow are simply switched or forwarded across the chosen path. This takes advantage of the high throughput and low latency of switching by enabling the traffic to bypass the routing engine once path calculation has been performed.

### **4.2.3. Routing Path Management**

Routing Path Management involves the determination and updating of all the routing information required for packet forwarding, including:

- Handling routing protocols
- Updating the routing table
- Updating the Layer 3 switching database

### **4.2.4. ICMP Router Discovery**

Before a host can send IP datagrams beyond its directly attached subnet, it must find the address of at least one operational router on that subnet. Typically, this can be accomplished by reading a list of one or more router addresses from a configuration file at startup time. On multicast links, some hosts also discover router addresses by listening to routing protocol traffic.

The ICMP Router Discovery message is an alternative router discovery method that uses a pair of ICMP messages on multicast links. It eliminates the need to manually configure router addresses and is independent of any specific routing protocol.

ICMP Router Discovery messages are called “Router Advertisements” and “Router Solicitations.” Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address(es) of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the subsequent, periodic ones to

arrive.

Router Discovery messages do not constitute a routing protocol; they merely enable hosts to discover the existence of neighboring routers, but not which router provides a route to a particular destination. If a host chooses a poor first-hop router for a particular destination, it should receive an ICMP Redirect from that router, identifying a better one.

### **4.2.5.Proxy ARP**

When a node in the attached subnetwork does not have routing or a default gateway configured, ARP Proxy can be used to forward an ARP request to a remote subnetwork. When the switch receives an ARP request for a remote network and ARP Proxy is enabled, it determines if it has the best route to the remote network, and then answers the ARP request by sending its own MAC address to the requesting node. That node then sends traffic to the switch, which in turn uses its own routing table to forward the traffic to the remote destination.

End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet mask than that used by the switch or other relevant network devices. Note that extensive use of Proxy ARP can adversely affect the performance of the switch because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

### **4.2.6.Routing Protocols**

The switch supports both static and dynamic routing.

- Static routing requires routing information to be stored in the switch either manually or when a connection is set up by an application outside the switch.
- Dynamic routing uses a routing protocol to exchange routing information, calculate routing tables, and respond to changes in the status or loading of the network.

Dynamic routing involves the determination and updating of all the routing information required for packet forwarding, as listed on chapter 4 “Routing Path Management”.

- Handling routing protocols
- Updating the routing table
- Updating the Layer 3 switching database

The switch supports RIP, RIP-2 and OSPFv2 dynamic routing protocols.

#### **4.2.6.1.RIP and RIP-2 Dynamic Routing Protocols**

The RIP protocol is the most widely used routing protocol. The RIP protocol uses a distance-vector-based approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together

with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets.

Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless retransmission of data traffic. RIP utilizes the following three methods to prevent loops from occurring:

- Split horizon—never propagate routes back to an interface port from which they have been acquired.
- Poison reverse—propagate routes back to an interface port from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)
- Triggered updates—whenever a route gets changed, broadcast an update message after waiting for a short random delay, but without waiting for the periodic cycle.

RIP-2 is a compatible upgrade to RIP. RIP-2 adds useful capabilities for plain text authentication, multiple independent RIP domains, variable length subnet masks, and multicast transmissions for route advertising (RFC 1723).

There are several serious problems with RIP that you should consider. First of all, RIP (version 1) has no knowledge of subnets, both RIP versions can take a long time to converge on a new route after the failure of a link or router during which time routing loops may occur, and its small hop count limitation of 15 restricts its use to smaller networks. Moreover, RIP (version 1) wastes valuable network bandwidth by propagating routing information via broadcasts; it also considers too few network variables to make the best routing decision.

#### 4.2.6.2.OSPFv2 Dynamic Routing Protocol

OSPF overcomes all the problems of RIP. It uses a link state routing protocol to generate a shortest-path tree, then builds up its routing table based on this tree. OSPF produces a more stable network because the participating routers act on network changes predictably and simultaneously, converging on the best route more quickly than RIP. Moreover, when several equal-cost routes to a destination exist, traffic can be distributed equally among them.

OSPF looks at more than just the simple hop count. When adding the shortest path to any node into the tree, the optimal path is chosen on the basis of delay, throughput and connectivity. OSPF utilizes IP multicast to reduce the amount of routing traffic required when sending or receiving routing path updates. The separate routing area scheme used by OSPF further reduces the amount of routing traffic, and thus inherently provides another level of routing protection. In addition, all routing protocol exchanges can be authenticated. Finally, the OSPF algorithms have been tailored for efficient operation in TCP / IP Internets.

OSPFv2 is a compatible upgrade to OSPF. It involves enhancements to protocol message authentication, and the addition of a point-to-multipoint interface which allows OSPF to run over non-broadcast networks, as well as support for overlapping area ranges.

*Area Configuration* – OSPF routers exchange information with other routers in their area to determine the shortest path to every destination. Each router in a common area should therefore have an identical map of their local network topology. At the top level, the largest area is known as an Autonomous System, and contains all the routers in your network. However, for large networks you should organize your OSPF routers into smaller contiguous areas to reduce the amount of routing information that has to be exchanged and to simplify network management.

When designing an OSPF network architecture, first create a backbone area to which all other areas are adjacent. Note that when you enable OSPF for any IP interface on the switch, it is assigned to the backbone by default (Area 0.0.0.0). As a general rule, no area should contain more than 50 routers. To create a new area, designate an Area ID that will be used by all of the other routers in this area, specify the area type as Normal, Stub, or NSSA (chapter 2,3 “Configuring Global Settings for OSPF”), and then assign the ID to an interface (chapter 2,3 “Configuring OSPF”). A Stub does not accept or send external routing information. Instead, it uses a single default route for destinations outside the area. Stubs further minimize the amount of routing data that has to be stored or exchanged with other areas. An NSSA (Not-So-Stubby Area) is similar to a Stub, except that it can import external route information into its area. Note that if there are not external routes into your network, then there are no advantages to configuring a Stub or NSSA.

*Neighbors* – Neighboring OSPF routers within a common area are found using Hello messages. These messages also list the other routers from which the originator has received hello messages. When a router finds its address in the hello messages received from another router, both routers initiate communications as neighbors. Only after these routers successfully exchange and synchronize their routing tables, will they be considered fully adjacent (chapter 2 “Displaying the Interface Table” or chapter 3 “Displaying the DVMRP Neighbor Table”). Routing information is only exchanged between adjacent neighbors.

*Designated Router* – A Designated Router (DR) and Backup Designated Router (BDR) are selected by the OSPF protocol for each area. The Designated Router exchanges routing information with all other routers in its area, and then floods Link State Advertisements (LSAs) to each router, allowing them to update their database. This eliminates the need for each router to exchange information with every other router in its area. The OSPF protocol selects the DR and BDR based on the router with the highest

priority, or highest Router ID in case of a tie (chapter 2,3 “*Configuring OSPF*”).

*Area Border Router* – An Area Border Router (ABR) must be configured between each area and the backbone. An ABR should be configured with an IP interface that connects directly to both the backbone and the area on which it borders (chapter 2,3 “*Adding an IP Interface*”). However, if an area is not physically connected to the backbone, you can configure a virtual link that crosses a neighboring area to reach the backbone. Just define an ABR (i.e., virtual neighbor) on the boundary between the isolated area and transit area, as well as an ABR on the boundary between the transit area and the backbone. An ABR can be situated between one or more areas, but we advise limiting the maximum number of areas supported by a single ABR to three. You can also define a virtual link as a backup path between an ABR and the backbone.

*Area Range* – An ABR maintains a separate routing table for each area to which it is attached, and sends routing summaries for each attached area to the backbone, which in turn distributes this information to other areas in the autonomous system. This reduces the size of the routing tables that have to be maintained throughout the system, and prevents frequent updates from flooding the system whenever a link change occurs. To configure a routing summary, you must define the OSPF Area Range for all the networks within an ABR’s area. This range is specified with an IP address and network mask (chapter 2 “*OSPF Area Configuration*” or chapter 3 “*OSPF Area Range Configuration*”). Moreover, since OSPF supports Variable Length Subnet Masks (VLSMs), you can specify a mask on a bit boundary, which can further reduce the number of advertised addresses.

*Autonomous System Boundary Router* – An Autonomous System (AS) contains all the routers in your network, each of which shares information with other routers to determine a shortest-path route to every destination in the AS. However, when an AS is connected to an outside network, it must import external routing information through an Autonomous System Boundary Router (ASBR). An ASBR can import routing information through other routing protocols such as RIP.

An ASBR will generate external link advertisements on selected interfaces if OSPF is enabled globally (chapter 2 “*Protocol Configuration*”), and any of the following conditions exist on an interface:

- RIP is enabled (chapter 2 “*Adding an IP Interface*” or chapter 3 “*Adding an IP Interface*”), or
- RIP and OSPF are both disabled (chapter 2 “*Adding an IP Interface*” or chapter 3 “*Adding an IP Interface*”).

*Link State Advertisements* – Each router maintains a link state database that contains information received from all the other routers within the same area (chapter 2 “*Displaying the Interface Table*” or chapter 3 “*Displaying the Interface Table*”). There are

four types of Link State Advertisements (LSA). Router LSAs advertise area links known by the originator, and are issued by all routers. Network LSAs advertise transit areas through which traffic can be passed to reach other areas in the system. Network LSAs contain information about all the routers that provide a link across the transit area, and are issued by Designated Routers. Summary LSAs are issued by Area Border Routers (ABR), and advertise routing information for a single subnetwork outside the ABR's area or for an Autonomous System Boundary Router (ASBR). External LSAs are issued by the ASBR, and contain information about external networks outside the AS.

*Virtual Links* – All areas within an Autonomous System must connect to the backbone. In cases where an area cannot be physically connected to the backbone, you can create a virtual link which crosses a transit area to reach the backbone. (Virtual links can only span one intermediate area to reach the backbone.) Virtual links can be used as a redundant link, preventing partitioning from the backbone. They can also be used to merge two separate backbone areas.

To create a virtual link, you must specify an Area Border Router (ABR) and a common transit area at both ends of the link (chapter 2 “*OSPF Virtual Link Configuration*” or chapter 3 “*OSPF Virtual Link Configuration*”). One ABR will border on the target area and the transit area, while the other borders on the transit area and the backbone. The configuration on each router must include the transit area identifier and the ABR at the other end of the link.

## 4.2.7. Non-IP Protocol Routing

The switch supports IP routing only. Non-IP protocols such as IPX and Appletalk cannot be routed by this switch, and will be confined within their local VLAN group unless bridged by an external router.

To coexist with a network built on multilayer switches, the subnetworks for non-IP protocols must follow the same logical boundary as that of the IP subnetworks. A separate multi-protocol router can then be used to link the subnetworks by connecting to one port from each available VLAN on the network.

## 4.3. Virtual LANs

Switches do not inherently support broadcast domains, which can lead to broadcast storms in large networks that handle a lot of traffic, such as NetBUEI or IPX. In conventional networks with routers, broadcast traffic is split up into separate domains to confine this traffic to the originating group and provide a much cleaner network environment. Instead of using physically separate subnets which are linked by traditionally slow routers, this switch creates segregated broadcast domains based on easily configurable VLANs, and then links these VLANs as required with wire-speed

routing.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This switch supports the following VLAN features:

- Up to 256 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

### **4.3.1. Assigning Ports to VLANs**

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate (chapter 2 “VLAN Table Configuration”). By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port (that is, a port attached to a VLAN-aware device) if you want it to carry traffic for one or more VLANs and if the device at the other end of the link also supports VLANs (chapter 2 “Configuring Virtual LANs” and chapter 3 “Configuring Virtual LANs”). Then assign the port at the other end of the link to the same VLAN(s). However, if you want a port on this switch to participate in one or more VLANs, but the device at the other end of the link does not support VLANs, then you must add this port as an untagged port (that is, a port attached to a VLAN-unaware device).

#### **4.3.1.1. VLAN Classification**

When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the PVID of the receiving port (chapter 2 “VLAN Port Configuration” and chapter 3 “VLAN Port Configuration”). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

### 4.3.1.2.Port Overlapping

Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by setting this switch to multilayer mode, and assigning an IP interface address to the different VLANs. (See “Connecting VLAN Groups” on chapter 4.)

### 4.3.1.3.Port-based VLANs

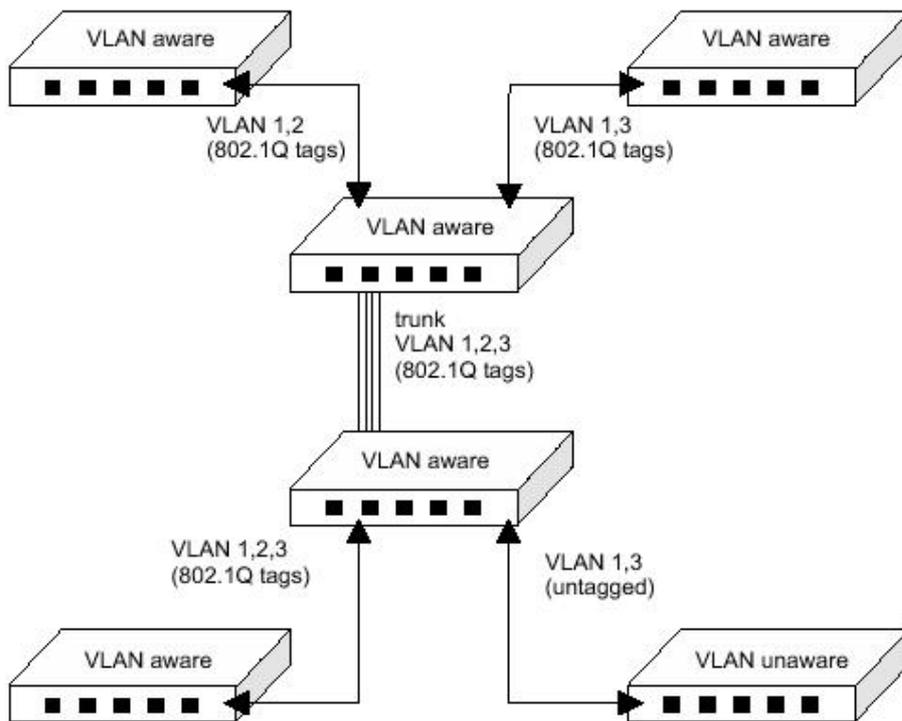
Port-based (or static) VLANs are manually tied to specific ports. The switch’s forwarding decision is based on the destination MAC address and its associated port. Therefore, to make valid forwarding or flooding decisions, the switch must learn the relationship of the MAC address to its related port—and thus to the VLAN—at run-time. However, when GVRP is enabled, this process can be fully automatic.

### 4.3.1.4.Automatic VLAN Registration (GVRP)

GVRP defines a system whereby the switch can automatically learn the VLANs to which each endstation should be assigned. If an endstation (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on endstation requests.

## 4.3.2.Forwarding Tagged / Untagged Frames

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. To forward a frame from a VLAN-aware device to a VLAN-unaware device, the switch first decides where to forward the frame, and then strips off the VLAN tag. However, to forward a frame from a VLAN-unaware device to a VLAN-aware device, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting this port’s default VID. The default PVID is VLAN 1 for all ports, but this can be changed (see chapter 2 “VLAN Port Configuration” or chapter 3 “VLAN Port Configuration”).



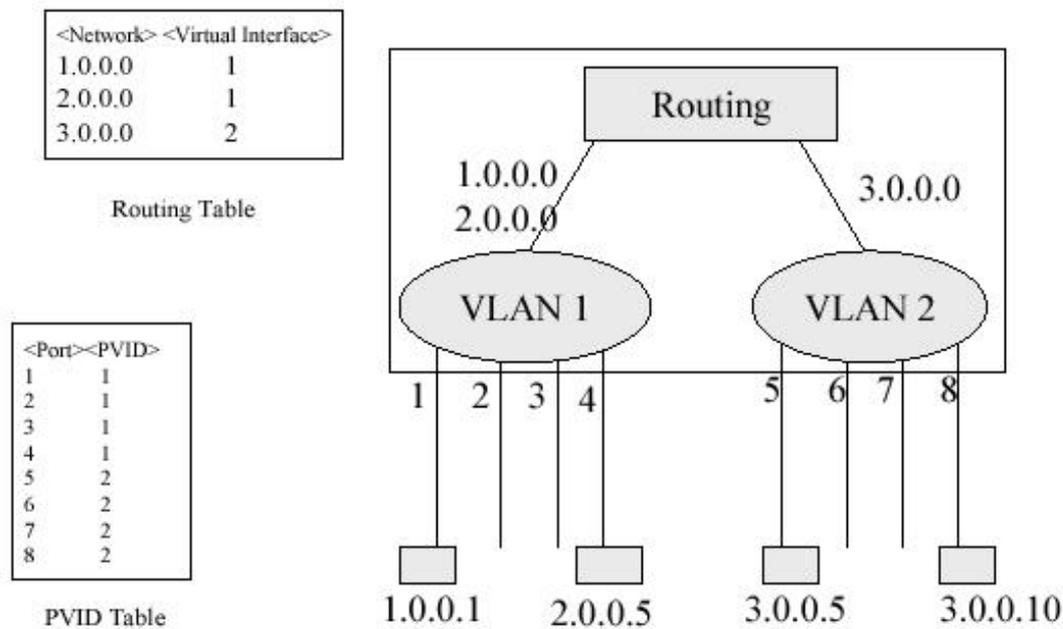
### 4.3.3. Connecting VLAN Groups

The switch supports communication within a common VLAN using store-and-forward switching. However, if you have devices in separate VLANs that need to communicate, and it is not practical to include these devices in a common VLAN, then the VLANs can be connected via the Layer 3 routing provided by this switch.

Traditional routers use only physical port numbers in their routing tables, which provides no support for VLANs. By contrast, this device supports Layer 3 routing by using both logical and physical port numbers to support VLANs and Layer 3 switching simultaneously.

By using the abstraction of a logical port number to represent a collection of physical switch ports in the same VLAN, Layer 3 switching can occur from one VLAN to another transparently, without changing the routing protocol and IP routing software, while Layer 2 switching is still used for intra-VLAN traffic.

The switch uses standard routing tables that are constructed via static configuration or dynamic routing protocols such as RIP and OSPF. Each routing entry consists of a network address (that is, an IP address with a subnet mask), and a virtual interface number. Each virtual interface corresponds to a virtual LAN, identified by the VLAN ID. Also note that multiple routing entries can be provided for the same virtual interface by adding the required routing table entries for the same VLAN (chapter 2 “Subnet Configuration” and chapter 3 “Subnet Configuration”). A typical VLAN configuration that supports routing is shown below.



## 4.4. Multicast Filtering

Multicasting sends data to a group of nodes instead of a single destination. The simplest way to implement multicasting is to broadcast data to all nodes on the network.

However, such an approach wastes a great deal of bandwidth if the target group is small compared to the overall broadcast domain.

Because applications such as videoconferencing and data sharing are now widely used, efficient multicasting has become vital. A common approach is to use a group registration protocol that allows nodes to join or leave multicast groups. A switch or router can then easily determine which ports contain group members and send data out to those ports only. This procedure is called multicast filtering.

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 or multicast routers / switches, instead of flooding traffic to all ports in the subnet (VLAN).

The routing switch supports IP multicast filtering not only by passively monitoring IGMP Query and Report messages and DVMRP Probe messages to register end-stations as multicast group members (Layer 2), but also by actively sending GMRP Query messages to learn the location of multicast routers / switches and member hosts in multicast groups within each VLAN (Layer 3). This switch also supports the DVMRP multicast routing protocol required to forward multicast traffic to other subnets.

### 4.4.1. IGMP Snooping

A Layer 2 switch can passively snoop on IGMP Query and Report packets transferred

between IP multicast routers / switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures multicast filters accordingly. IGMP Snooping generates no additional network traffic, and allows you to significantly reduce the multicast traffic passing through your switch.

## 4.4.2.IGMP Protocol

The Internet Group Management Protocol (IGMP) runs between hosts and their immediately adjacent multicast router / switch. IGMP is a multicast host registration protocol that allows any host to inform its local router that it wants to receive transmissions addressed to a specific multicast group.

A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router / switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the role of querying the LAN for group members. It then propagates the service requests on to any adjacent multicast switch / router to ensure that it will continue to receive the multicast service.

Based on the group membership information learned from IGMP, a router / switch can determine which (if any) multicast traffic needs to be forwarded to each of its ports. At Layer 3, multicast routers use this information, along with a multicast routing protocol such as DVMRP, to support IP multicasting across the Internet.

Note that IGMP neither alters nor routes IP multicast packets. A multicast routing protocol must be used to deliver IP multicast packets across different subnetworks. Therefore, when DVMRP routing is enabled for a subnet on this switch, the switch will automatically enable IGMP (chapter 2 “*Configuring DVMRP*” and chapter 3 “*Configuring DVMRP*”).

## 4.4.3.GMRP Protocol

GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. GMRP requires that any participating network devices or endstations comply with the IEEE 802.1p standard. Compliant endstations can request to receive traffic from a multicast group simply by issuing a *join* packet that includes a known multicast address. When the join packet reaches a port on the switch, it configures this port to receive multicast traffic for the requested group, and then issues a similar join packet to all other ports on the switch, informing them that incoming multicast traffic for the stated group is to be forwarded to the requesting port.

#### **4.4.4.DVMRP Routing Protocol**

The Distance-Vector Multicast Routing Protocol (DVMRP) behaves somewhat similarly to RIP. A router supporting DVMRP periodically floods its attached networks to pass information about supported multicast services along to new routers and hosts. Routers that receive a DVMRP packet send a copy out to all paths (except the path back to the origin). These routers then send a prune message back to the source to stop a data stream if the router is attached to a LAN which does not want to receive traffic from a particular multicast group. However, if a host attached to this routing switch issues an IGMP message indicating that it wants to subscribe to the concerned multicast service, this switch will use DVMRP to build up a source-rooted multicast delivery tree that allows it to prevent looping and determine the shortest path to the source of this multicast traffic.

When this switch receives the multicast message, it checks its unicast routing table to locate the port that provides the shortest path back to the source. If that path passes through the same port on which the multicast message was received, then this switch records path information for the concerned multicast group in its routing table and forwards the multicast message on to adjacent routers, except for the port through which the message arrived. This process eliminates any potential loops from the tree and ensures that the shortest path (in terms of hop count) is always used.

#### **4.5.Class-of-Service (CoS) Support**

The switch provides two transmit queues on each port, with a weighted fair queuing scheme. This function can be used to provide independent priorities for various types of data, such as real-time video or voice, and best-effort data.

Priority assignment to a packet in the switch can be accomplished in any of the following ways:

- Priority can be explicitly assigned by endstations which have applications that require a higher priority than best-effort. This switch utilizes the IEEE 802.1p and 802.1Q tag structure to decide priority assignments for the received packets.
- A port may be manually configured as high priority. In this case, when any other port receives traffic from a high-priority port, that traffic is automatically placed in the high-priority output queue.

#### **4.6.BOOTP / DHCP Relay**

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 a broadcast mechanism, a DHCP server and its client must physically reside on the same subnet. However, it is 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 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's 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.

## **4.7.Security Features**

The switch provides security features which allow you to control management access and network access as described in the following sections.

### **4.7.1.SNMP Community Strings**

Access to the switch using network management tools is controlled by SNMP community strings. This switch supports up to five community strings. A character string indicating the access rights of the management community must be provided whenever you send an SNMP message to the switch. Each community has either read-only or read / write access rights. A community that has read-only access can use only use GET and GETNEXT commands to view the current configuration settings and status of the switch. But a community with read / write access can use GET and GETNEXT commands, as well as the SET command to configure the switch.

## **4.7.2. User Name and Passwords**

This switch can also be accessed via a direct connection to the console port or through a network connection using Telnet or a Web browser. When managing the switch by any of these means, a user name and password is required to enter the system. The factory defaults include two sets of user names and passwords. One set has administrator rights, which allows you to view or modify system parameters. The other set has read-only access, which allows you to view the status of the system, but not to modify it.

## **4.7.3. MAC Address Filters**

If you discover that some nodes are sending abnormal or destructive data that could adversely affect the network or cause security problems, you can set their MAC addresses to be filtered by the switch. Any packets with a source or destination address listed in the MAC address filter will then be dropped by the switch upon entry.

## **4.7.4. IP Address Filters**

IP addresses can also be set to be filtered by the switch. IP packets with a source or destination address listed in the IP address filter will be dropped by the switch upon entry.

## **4.8. SNMP Management Software**

SNMP (Simple Network Management Protocol) is a communication protocol designed specifically for managing devices or other elements on a network. Network equipment commonly managed with SNMP includes hubs, switches, bridges, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance and detect potential problems.

## **4.9. Remote Monitoring (RMON)**

Remote Monitoring provides a cost-effective way to monitor large networks by placing embedded or external probes on distributed network equipment (hubs, switches or routers). RMON has already become a valuable tool for network managers faced with a quickly changing network landscape that contains dozens to hundreds of separate segments. RMON is the only way to retain control of the network and analyze applications running at multi-megabit speeds. It provides the tools you need to implement either reactive or proactive policies that can keep your network running based on real-time access to key statistical information.

This switch provides support for mini-RMON which contains the four key groups

required for basic remote monitoring. These groups include:

**Statistics:** Includes all the tools needed to monitor your network for common errors and overall traffic rates. Information is provided on bandwidth utilization, peak utilization, packet types, errors and collisions, as well as the distribution of packet sizes.

**History:** Can be used to create a record of network utilization, packet types, errors and collisions. You need a historical record of activity to be able to track down intermittent or recurring problems. Historical data can also be used to establish normal baseline activity, which may reveal problems associated with high traffic levels, broadcast storms, or other unusual events. Historical information can also be used to predict network growth and to plan for expansion before your network becomes overloaded.

**Alarms:** Can be set to test data over any specified time interval, and can monitor absolute or changing values (such as a statistical counter reaching a specific value, or a statistic changing by a certain amount over the set interval). Alarms can be set to respond to either rising or falling thresholds.

**Events:** Defines the action to take when an alarm is triggered. The response to an alarm can include recording the alarm in the Log Table or sending a message to a trap manager. Note that the Alarm and Event Groups are used together to record important events or respond immediately to critical network problems.

## 5. Appendix A: Troubleshooting

### 5.1. Troubleshooting Chart

Troubleshooting Chart	
Symptom	Action
Cannot connect using Telnet, Web browser, or SNMP software	<ul style="list-style-type: none"><li>• Be sure you have configured the agent with a valid IP address, subnet mask and default gateway (Layer 2).</li><li>• Check that you have a valid network connection to the switch and that the port you are using has not been disabled.</li><li>• Check network cabling between the management station and the switch.</li><li>• If you cannot connect using Telnet, there may already be four active sessions. Try connecting again at a later time.</li></ul>
Cannot access the onboard configuration program via a serial port connection	<ul style="list-style-type: none"><li>• Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and 19200 bps.</li><li>• Check that the null-modem serial cable conforms to the pin-out connections provided in Appendix B.</li></ul>
Forgot or lost the password	<ul style="list-style-type: none"><li>• Reinstall the switch firmware as described on the next page.</li></ul>

### 5.2. Upgrading Firmware via the Serial Port

You can upgrade system firmware by connecting your computer to the serial port on the switch and using a console interface package that supports the Xmodem protocol. (See “Required Connections” on chapter 1.)

1. Restart the system by using the Restart System command, or by pulling out the power cord to reset the power, waiting five seconds, and plugging it back in.
2. When the system initialization screen appears as shown below, press “D” to download system firmware, and then indicate the code type (<r> Runtime image or <d> Diagnostic image).

```

POST Version      V2.57      9/11/2001
----- Power-On Self Test (POST)-----
Int. Loopback Testing SCC2 UART Channel ... PASS
Testing the System SDRAM ..... PASS
Int. Loopback Testing _____ UART Channel ... PASS
Int. Loopback Testing _____ UART Channel ... PASS
CPU Self Test ..... PASS
Test Accessing Agent's Config EEPROM ..... PASS
FlashROM CheckSum Test ..... PASS
!!! If you want to download image file, Please press < D > to download :
!!!          < r > Download Runtime image
!!!          < d > Download Diagnostic image
!!!          < c > Clear the system parameter
!!!          < q > QUIT r
Please input the Baud Rate as following :
Press 1: Baud Rate = 9600
Press 2: Baud Rate = 19200
Press 3: Baud Rate = 38400
Press 4: Baud Rate = 57600
Press 5: Baud Rate = 115200
Select a number and then press <ENTER> !!! 5
Please change local console BaudRate to exact rate and press
<ENTER>!!!

```

3. Change your baud rate to the selected value and press Enter to enable download. From the terminal emulation program, select the file you want to download, set the protocol to XModem, and then initialize downloading.

**Notes:**

1. If you use Windows HyperTerminal, disconnect , set the baud rate, and reconnect.
2. The download file should be a correct binary file for the switch; otherwise the agent will not accept it.
3. After the file has been downloaded, the console screen will display information similar to that shown below. Press Enter to download to permanent memory, change the baud rate back to 19200, press Enter to start decompressing the new firmware, then press Enter to open the Log-on screen.

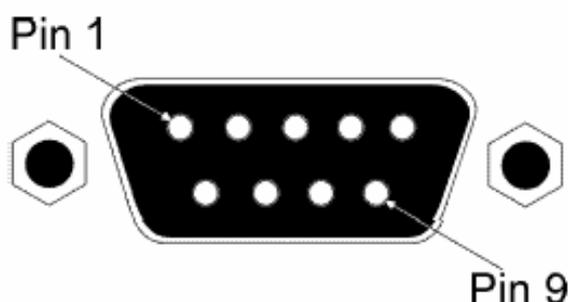
```
XModem Download to 0x00400020: ... SUCCESS !
(P)ermanent or (T)emporary Download: [P]
Update RunTime Image at 0x03040000 ... .. SUCCESS !
Change to original Baud Rate and Press <ENTER> to Run Application !!!
Decompress now..... !!!
run-time code starting now. !!! Starting System...
MAINBOARD OCTOPUS0 RAMBIST TEST..... PASS!
MAINBOARD OCTOPUS1 RAMBIST TEST..... PASS!
MAINBOARD OCTOPUS2 RAMBIST TEST..... PASS!
MAINBOARD OCTOPUS3 RAMBIST TEST..... PASS!
MAINBOARD DOLPHIN RAMBIST TEST..... PASS!
MAINBOARD STARFISH RAMBIST TEST..... PASS!
Press <Enter> to start UI
```

For details on managing the switch, refer to Chapter 2 for information on the out-of-band console interface, or Chapter 3 for information on the Web interface.

## 6. Appendix B: Pin Assignments

### 6.1. Console Port Pin Assignments

The DB-9 serial port on the switch's rear panel is used to connect to the switch for out-of-band console configuration. The onboard menu-driven configuration program can be accessed from a terminal, a PC running a terminal emulation program, or from a remote location via a modem connection. The pin assignments used to connect to the serial port are provided in the following tables.



**Figure B-1. DB-9 Console Port Pin Numbers**

#### 6.1.1. DB-9 Port Pin Assignments

EIA Circuit	CCITT Signal	Description	Switch's DB9 DTE Pin #	PC DB9 DTE Pin #	Modem DB25 DCE Pin #	Signal Direction DTE-DCE
CF	109	<b>DCD</b> (Data Carrier Detected)	1	1	8	<-----
BB	104	<b>RxD</b> (Received Data)	2	2	3	<-----
BA	103	<b>TxD</b> (Transmitted Data)	3	3	2	----->
CD	108.2	<b>DTR</b> (Data Terminal Ready)	4	4	20	----->
AB	102	<b>SG</b> (Signal Ground)	5	5	7	-----
CC	107	<b>DSR</b> (Data Set Ready)	6	6	6	<-----
CA	105	<b>RTS</b> (Request-to-Send)	7	7	4	----->
CB	106	<b>CTS</b> (Clear-to-Send)	8	8	5	<-----
CE	125	<b>RI</b> (Ring Indicator)	9	9	22	<-----

## 6.1.2. Console Port to 9-Pin COM Port on PC

Switch's 9-Pin Serial Port	CCITT Signal	PC's 9-Pin COM Port
1 DCD	----- DCD -----	1
2 RXD	<----- TXD -----	3
3 TXD	----- RXD ----->	2
4 DTR	----- DSR ----->	6
5 SGND	----- SGND -----	5
6 DSR	----- DTR -----	4
7 RTS	----- CTS ----->	8
8 CTS	<----- RTS -----	7
9 RI	----- RI -----	9

## 6.1.3. Console Port to 25-Pin DCE Port on Modem

Switch's 9-Pin Serial Port	CCITT Signal	Modem's 25-Pin DCE Port
1	<----- DCD -----	8
2	<----- RXD -----	3
3	----- TXD ----->	2
4	----- DTR ----->	20
5	----- SGND -----	7
6	<----- DSR -----	6
7	----- RTS ----->	4
8	<----- CTS -----	5
9	<----- RI -----	22

## 6.1.4. Console Port to 25-Pin DTE Port on PC

Switch's 9-Pin Serial Port	Null Modem	PC's 25-Pin DTE Port
1 DCD	1 _____ 1	8 DCD
2 RXD	2 _____ 3	3 TXD
3 TXD	3 _____ 2	2 RXD
4 DTR	4 _____ 8	20 DTR
5 SGND	5 _____ 20	7 SGND
6 DSR	6 _____ 7	6 DSR
7 RTS	7 _____ 4	4 RTS
8 CTS	9 _____ 5	5 CTS
9 RI	20 _____ 6	22 RI

## **7. Glossary**

### **7.1.1. Bandwidth Utilization**

The historical percentage of packets received as compared to total bandwidth.

### **7.1.2. BOOTP**

Boot protocol used to load the operating system or configuration settings for devices connected to the network.

### **7.1.3. Distance Vector Multicast Routing Protocol**

(DVMRP)

A distance-vector-style routing protocol used for routing multicast datagrams through the Internet. DVMRP combines many of the features of RIP with Reverse Path Broadcasting (RPB).

### **7.1.4. GARP VLAN Registration Protocol (GVRP)**

Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

### **7.1.5. Generic Attribute Registration Protocol (GARP)**

GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

### **7.1.6. Group Attribute Registration Protocol**

*See Generic Attribute Registration Protocol.*

### **7.1.7. Generic Multicast Registration Protocol (GMRP)**

GMRP allows network devices to register endstations with multicast groups. GMRP requires that any participating network devices or endstations comply with the IEEE 802.1p standard.

### **7.1.8. ICMP Router Discovery**

ICMP Router Discovery message is an alternative router discovery method that uses a

pair of ICMP messages on multicast links. It eliminates the need to configure router addresses manually, and is independent of any specific routing protocol.

### **7.1.9. Internet Control Message Protocol (ICMP)**

Commonly used to send echo messages (i.e., Ping) for monitoring purposes.

### **7.1.10. IEEE 802.1D**

Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

### **7.1.11. IEEE 802.1Q**

VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

### **7.1.12. IEEE 802.3ac**

Defines frame extensions for VLAN tagging.

### **7.1.13. Internet Group Management Protocol (IGMP)**

A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast router on a given subnetwork, one of the routers is made the “querier” and assumes responsibility for keeping track of group membership.

### **7.1.14. IGMP Snooping**

Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

### **7.1.15. In-Band Management**

Management of the network from a station attached directly to the network.

### **7.1.16. IP Multicast Filtering**

A process whereby this switch can pass multicast traffic along to participating hosts.

### **7.1.17. Layer 2**

Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

## **7.1.18.Layer 3**

Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

## **7.1.19.Link Aggregation**

See Port Trunk.

## **7.1.20.Management Information Base (MIB)**

An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

## **7.1.21.Multicast Switching**

A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

## **7.1.22.Open Shortest Path First (OSPF)**

OSPF is a link-state routing protocol that functions better over a larger network such as the Internet, as opposed to distance-vector routing protocols such as RIP. It includes features such as unlimited hop count, authentication of routing updates, and Variable Length Subnet Masks (VLSM).

## **7.1.23.Out-of-Band Management**

Management of the network from a station not attached to the network.

## **7.1.24.Port Mirroring**

A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

## **7.1.25.Port Trunk**

Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

## **7.1.26.Remote Monitoring (RMON)**

RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions,

including specific error types.

### **7.1.27. Routing Information Protocol (RIP)**

The RIP protocol seeks to find the shortest route to another device by minimizing the distance-vector, or hop count, which serves as a rough estimate of transmission cost. RIP-2 is a compatible upgrade to RIP. It adds useful capabilities for subnet routing, authentication, and multicast transmissions.

### **7.1.28. Simple Network Management Protocol (SNMP)**

The application protocol in the Internet suite of protocols which offers network management services.

### **7.1.29. Spanning Tree Protocol (STP)**

A technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

### **7.1.30. Telnet**

Defines a remote communication facility for interfacing to a terminal device over TCP / IP.

### **7.1.31. Trivial File Transfer Protocol (TFTP)**

A TCP / IP protocol commonly used for software downloads.

### **7.1.32. Virtual LAN (VLAN)**

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

### **7.1.33. XModem**

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.