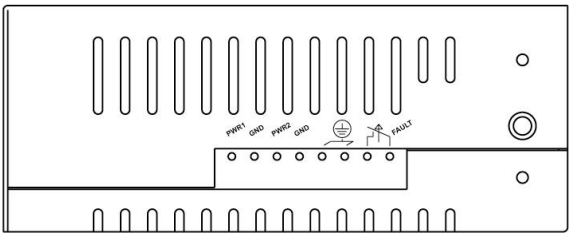
Quick Start Guide

This quick start guide describes how to install and use the hardened managed Ethernet Switch. This is the switch of choice for harsh environments constrained by space.

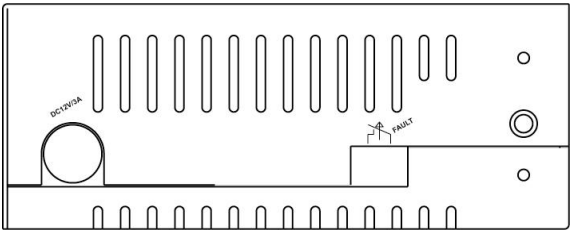
Physical Description

The Terminal Block and Power inputs

The Terminal Block	
PWR1	Power Input 1 (12 to 32VDC)
GND	Power Ground
PWR2	Power Input 2 (12 to 32VDC)
GND	Power Ground
	Earth Ground
FAULT	The relay opens if PWR1 or PWR2 fails (1A)



The DC Power Inputs	
12VDC DC JACK	
FAULT	The relay opens if PWR1 or PWR2 fails (1A)



DC Terminal Block Power Inputs: There are two pairs of power inputs can be used to power up this Switch. Redundant power supplies function is supported. You only need to have one power input connected to run the Switch.

The Connectors

1. The 10/100Base-TX Connections

The following lists the pinouts of 10/100Base-TX ports.

Pin	Regular Ports	Uplink port
1	Input Receive Data +	Output Transmit Data +
2	Input Receive Data -	Output Transmit Data -
3	Output Transmit Data +	Input Receive Data +
4	NC	NC
5	NC	NC
6	Output Transmit Data -	Input Receive Data -
7	NC	NC
8	NC	NC

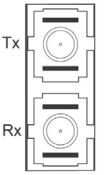
2. The 10/100/1000Base-TX Connections

The following lists the pinouts of 10/100/1000Base-TX ports.

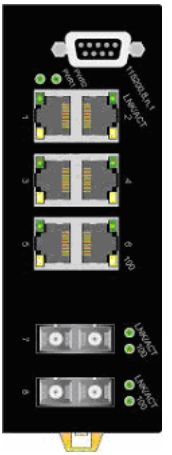
Pin	Ports
1	A+
2	A-
3	B+
4	C+
5	C-
6	B-
7	D+
8	D-

3. The 100Base-FX & 1000Base-SX/LX Connections

The fiber port pinouts: The Tx (transmit) port of device I is connected to the Rx (receive) port of device II, and the Rx (receive) port of device I to the Tx (transmit) port of device II.



The Port Status LEDs



LED	State	Indication
10/100TX or 100FX		
LNK/ACT (Green)	Steady	A valid network connection established. LNK stands for LINK.
	Flashing	Transmitting or receiving data. ACT stands for ACTIVITY.
100 (Yellow)	Steady	Light solid yellow for a port transferring at 100Mbps.
	Off	The port is transferring at 10Mbps If this LED is dark.
10/100/1000TX, 1000SX/LX		
LNK (Green)	Steady	Light solid green for a port transferring at 1000Mbps.
	Off	The port is not transferring at 1000Mbps If this LED is dark.
ACT (Yellow)	Flashing	Transmitting or receiving data. ACT stands for ACTIVITY.
	Off	Neither transmitting nor receiving data.

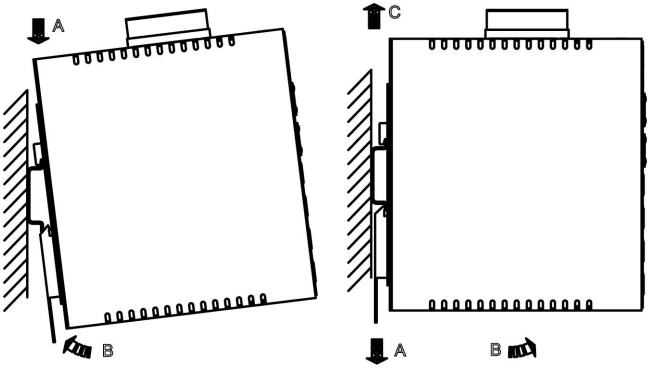
Functional Description

- Meets NEMA TS1/TS2 Environmental requirements such as temperature, shock, and vibration for traffic control equipment.
- Meets IEC61000-6-2 EMC Generic Standard Immunity for industrial environment.
- Manageable via SNMP, Web-based, Telnet, and RS-232 console port.
- Support 802.3/802.3u/802.3ab/802.3z/802.3x. Auto-negotiation: 10/100/1000Mbps, full/half-duplex; Auto MDI/MDIX.
- 100Base-FX: Multi mode SC or ST type; Single mode SC or ST type; WDM Single mode SC type.
- 1000Base-SX/LX: Multi mode SC type, Single mode SC type, or WDM Single mode SC type.
- Support 4096 MAC addresses. Provides 2M bits memory buffer.
- Alarms for power failure by relay output.
- Operating voltage and Max. current consumption: 1.54A @ 12VDC, 0.77A @ 24VDC. Power consumption: 18.48W Max.

- Power Supply: Redundant DC Terminal Block power inputs or 12VDC DC JACK with 100-240VAC external power supply.
- -40℃ to 75℃ (-40℉ to 167℉) operating temperature range. Tested for functional operation @ -40℃ to 85℃ (-40℉ to 185℉).
- Supports DIN-Rail, Panel, or Rack Mounting installation.

Assembly, Startup, and Dismantling

- Assembly: Place the switch on the DIN rail from above using the slot. Push the front of the switch toward the mounting surface until it audibly snaps into place.
- Startup: Connect the supply voltage to start up the switch via the terminal block (or DC JACK).
- Dismantling: Pull out the lower edge and then remove the switch from the DIN rail.



Preface

This manual describes how to install and use the hardened managed Ethernet Switch. This switch integrates full wire speed switching technology with SNMP/RMON web-based management functions. This switch brings the answer to complicated hardened networking environments.

To get the most out of this manual, you should have an understanding of Ethernet networking concepts.

In this manual, you will find:

- Features on the switch
- Illustrative LED functions
- Installation instructions
- Management Configuration
- SNMP…
- Specifications

Table of Contents

QUICK START GUIDE 1

PHYSICAL DESCRIPTION 1
The Terminal Block and Power inputs 1
The Connectors 2
The Port Status LEDs 3
FUNCTIONAL DESCRIPTION 4
ASSEMBLY, STARTUP, AND DISMANTLING 5

PREFACE 6

TABLE OF CONTENTS 7

PRODUCT OVERVIEW 10

HARDENED MANAGED ETHERNET SWITCH 10
PACKAGE CONTENTS 10
PRODUCT HIGHLIGHTS 11
Basic Features 11
Management Support 12
FRONT PANEL DISPLAY 14
PHYSICAL PORTS 15
BASIC FUNCTIONS 16
UNICAST SWITCHING 17
MULTICAST SWITCHING 18
VLAN 19
Broadcast Containment 20
Multicast-Based Multimedia Applications 20
Enhanced Security 20
VLAN Membership 21
VLAN CONFIGURATION 22
Intra-VLAN Communication 22
Inter-VLAN Communication 22
GVRP 23
IGMP SNOOPING AND IP MULTICAST FILTERING 24
SWITCH MANAGEMENT 26

INSTALLATION 27

SELECTING A SITE FOR THE SWITCH 27
DIN RAIL MOUNTING 28
CONNECTING TO POWER 29
12VDC DC Jack 29
Redundant DC Terminal Block Power Inputs 29
Alarms for Power Failure 30
Power-on Self test (POST) 31
CONNECTING TO YOUR NETWORK 32
Cable Type & Length 32

Cabling *33*

SWITCH MANAGEMENT **34**

MANAGEMENT ACCESS OVERVIEW 35
ADMINISTRATION CONSOLE 36
Direct Access *36*
Modem Access *37*
WEB MANAGEMENT 38
Netscape Navigator *38*
Internet Explorer *38*
SNMP-BASED NETWORK MANAGEMENT 39
PROTOCOLS 40
MANAGEMENT ARCHITECTURE 40

MENU-DRIVEN CONSOLE MANAGEMENT **41**

LOGGING ON TO THE SWITCH 41
At the screen prompt *41*
SWITCH MANAGEMENT SCREEN 42
Navigating Through the Console Interface *43*
PERFORMING BASIC MANAGEMENT ACTIVITIES 44
To Perform Basic Management Activities: *44*
PERFORMING ADVANCED MANAGEMENT ACTIVITIES 52
To Perform Advanced Management Activities: *52*
LOGOUT 98
SAVE SETTINGS 98
RESTORE DEFAULT SETTINGS 98
REBOOT 98

WEB-BASED BROWSER MANAGEMENT **99**

LOGGING ON TO THE SWITCH 99
UNDERSTANDING THE BROWSER INTERFACE 100
PERFORMING FILE ACTIVITIES 102
To perform File Activities: *102*
PERFORMING BASIC SETUP ACTIVITIES 105
To perform Basic Setup Activities: *105*
PERFORMING ADVANCED SETUP ACTIVITIES 112
To perform Advanced Setup Activities: *112*

SNMP & RMON MANAGEMENT **151**

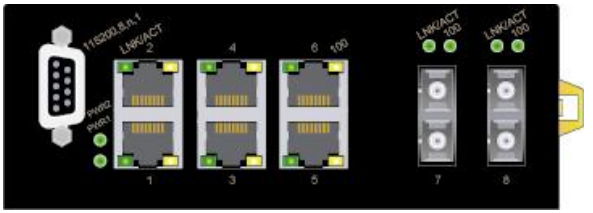
OVERVIEW 151
SNMP AGENT AND MIB-2 (RFC 1213) 152
RMON MIB (RFC 1757) AND BRIDGE MIB (RFC 1493) 153
RMON Groups Supported *153*
Bridge Groups Supported *154*

SPECIFICATIONS **155**

APPENDIX A – CONNECTOR PINOUTS **157**

Product Overview

Hardened Managed Ethernet Switch



Front View

Package Contents

When you unpack the product package, you shall find the items listed below. Please inspect the contents, and report any apparent damage or missing items immediately to your authorized reseller.

- ✓ ***This Management Switch***
- ✓ ***User's Manual***
- ✓ ***External power adapter***

Product Highlights

Basic Features

- Provide:
  - Eight 10/100Base-TX ports
  - Eight 10/100Base-TX ports + one 100Base-FX port
  - Six 10/100Base-TX ports + two 100Base-FX ports
  - Four 10/100Base-TX ports + four 100Base-FX ports
  - Eight 10/100Base-TX ports + one 10/100/1000Base-TX port
  - Eight 10/100Base-TX ports + one 1000Base-SX/LX port
- 100Base-FX Multi-mode fiber using SC or ST connector; single-mode fiber using SC or ST connector; WDM single-mode fiber using SC connector
- 1000Base-SX Multi-mode fiber using SC connector; 1000Base-LX single-mode fiber using SC connector; WDM single-mode fiber using SC connector
- Auto-negotiation for speed and duplexity on all RJ-45 ports
- Auto MDI/MDIX on all RJ-45 ports
- Full wire-speed forwarding rate
- Store-and-forward mechanism
- Back-pressure and IEEE 802.3x compliant flow control
- Support 4096 MAC addresses
- Provide 2M bits memory buffer
- Meet NEMA TS1/2 environmental requirements for traffic control equipment
- Meet IEC61000-6-2 EMC Generic Standard Immunity for industrial environment
- UL1604 Class 1, Division 2 Classified for use in hazardous locations (applicable to versions with terminal block power option)

- Alarms of power failure by relay output
- Operating voltage and Max. current consumption: 1.54A @ 12VDC, 0.77A @ 24VDC
- Power consumption: 18.48W Max
- Power Supply: Redundant DC Terminal Block power inputs or 12VDC DC JACK with 100-240VAC external power supply
- Support DIN-Rail, Panel, or Rack Mounting installation
- Front panel port status LEDs

Management Support

VLAN

- Port-based VLAN
- 802.1Q tagged VLAN

TRUNKING

- Port-based Trunking

PORT-SECURITY

- Limit number of MAC addresses learned per port Load
- Static MAC addresses stay in the filtering table

PORT-MIRRORING

- Port-mirroring provided through dedicated port, Port 1

QOS (Quality of Service)

- Support IEEE802.1p Quality of Service

COS (IEEE802.1P CLASSIFICATION OF SERVICE)

- Packet transmission scheduled using Weighted Round Robin (WRR)
- Classification of packet priority can be based on either a VLAN tag on packet or a user-definable port priority

INTERNETWORKING PROTOCOLS

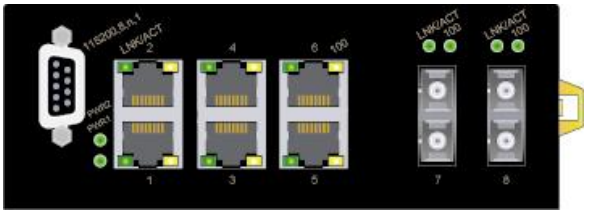
- Bridging: 802.1w Rapid Spanning Tree
  802.1p/Q – GARP/GVRP

- IP Multicast: IGMP Snooping
  VLANs & IP Multicast sessions
- Bandwidth Control
- Rate Control

NETWORK MANAGEMENT METHODS

- Console port access via RS-232 cable
- Telnet remote access
- SNMP agent:
  MIB-2 (RFC1213)
  Bridge MIB (RFC1493)
  RMON MIB (RFC1757) – statistics, history, alarm and events
  VLAN MIB (802.1Q/RFC2674)
  Private MIB
- Java applet-based MIB browser
- Web browser support based on HTTP server and CGI parser
- TFTP software-upgrade capability

Front Panel Display



①Power Status (PWR1, PWR2)

These LEDs come on when the switch is properly connected to power and turned on.

②Port Status LEDs

The LEDs display status for each respective port.

LED	State	Indication
10/100TX or 100FX		
LNK/ACT (Green)	Steady	A valid network connection established. LNK stands for LINK.
	Flashing	Transmitting or receiving data. ACT stands for ACTIVITY.
100 (Yellow)	Steady	Light solid green for a port transferring at 100Mbps.
	Off	The port is transferring at 10Mbps If this LED is dark.
10/100/100TX or 1000SX/LX		
1000 (Green)	Steady	Light solid green for a port transferring at 1000Mbps.
	Off	The port is not transferring at 1000Mbps If this LED is dark.
ACT (Yellow)	Flashing	Transmitting or receiving data. ACT stands for ACTIVITY.
	Off	Neither transmitting nor receiving data.

Physical Ports

This switch provides:

- Eight 10/100Base-TX ports
- Eight 10/100Base-TX ports + one 100Base-FX port
- Six 10/100Base-TX ports + two 100Base-FX ports
- Four 10/100Base-TX ports + four 100Base-FX ports
- Eight 10/100Base-TX ports + one 10/100/1000Base-TX port
- Eight 10/100Base-TX ports + one 1000Base-SX/LX port

CONNECTIVITY

- RJ-45 connectors
- ST or SC connector on 100Base-FX fiber port
- SC connector on 1000Base-SX/LX fiber port

MODE SELECTION

- 10Base-T full-duplex mode
- 10Base-T half-duplex mode
- 100Base-TX full-duplex mode
- 100Base-TX half-duplex mode
- 100Base-FX full-duplex mode
- 1000Base-T/SX/LX full-duplex mode
- Auto-sensing mode

<Note>

i. Half-duplex mode uses back pressure flow control to prevent the receiving buffer from being overrun by data from a source node.

ii. Full-duplex mode uses 802.3x flow control standard to prevent fast data traffic from overrunning slow data traffic.

iii. Auto-sensing mode is in use after auto-negotiating with the other end of the link.

Basic Functions

In general, the switch is responsible for switching both VLAN tagged and untagged frames from a receiving port to one or more transmitting ports. The switch performs multiple steps during the switching process:

VLAN CLASSIFICATION

LEARNING

FILTERING

FORWARDING

AGING

Below is additional information about tasks that the switch performs during unicast and multicast switching.

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 to an associated VLAN.
- If the frame is tagged, the switch uses the tagged VLAN ID to identify the broadcasting domain of the frame.

LEARNING

After VLAN classification, the switch checks the <source MAC address, VLAN> pair in the switching database (SDB) to see whether the <source MAC address, VLAN> pair is known.

- If it is unknown, the switch inserts the <source MAC address, VLAN> into the SDB and learns the <source MAC address, VLAN>.
- If it is known, the switch checks the <source MAC address, VLAN> for a mismatched port ID. If the port ID associated with the <source MAC address, VLAN> pair in the SDB is different than the receiving port, the switch modifies the port ID in the SDB and modifies its management database (MDB) accordingly.

FILTERING

After learning the address, the switch checks:

- Whether the source port or destination port is in the forwarding state.
- Whether the source MAC address or destination MAC address is to be filtered.
- Whether the source port ID is the same as destination port ID.

If any of these conditions are met, the switch drops the receiving packet. Otherwise, it continues with the forwarding process described below.

FORWARDING

During the forwarding process, the switch checks whether the <destination MAC address, VLAN> pair is unknown.

- If it is unknown, the switch floods the receiving frame to all ports in the VLAN, excluding the source port.
- If it is known, the switch forwards the receiving frame to the port associated with the <destination MAC address, VLAN> pair. At the same time, the switch ascertains the individual's port's VLAN tagging/untagging configuration and corresponding VLAN ID to render the appropriate frame tagging when the frame is ready to be transmitted.

MULTICAST SWITCHING

For multicast switching, the switch checks whether the received frame is a BPDU. If a BPDU is received, the switch forwards the frame to the CPU for processing by the spanning tree protocol. Otherwise, the switch performs the following processes:

VLAN CLASSIFICATION
Same as for unicast switching.

LEARNING
Same as for unicast switching.

FILTERING
After learning the address, the switch checks:

- Whether the source port or destination port is not in the forwarding state.
- Whether the source MAC address or destination MAC address is to be filtered.

If any of these conditions are met, the switch drops the receiving packet. Otherwise, it continues with the forwarding process described below.

FORWARDING
The switch floods the received multicast frame to all ports that are in forwarding state within the VLAN, excluding the source port. At the same time, the switch ascertains the individual port's VLAN tagging/untagging configuration and corresponding VLAN ID to render the appropriate frame tagging when the frame is ready to be transmitted.

AGING
The switch performs the aging process for the <MAC addresses, VLAN> pair in the switching database. Once a <MAC address, VLAN> pair is aged out, the SDB is modified.

SPANNING TREE
The switch supports one Spanning Tree per bridged network.

VLAN

A virtual LAN (VLAN) is a network of computers that behave as if they are connected to the same wire, even though they may actually be physically located on different segments of a LAN. VLANs are analogous to a group of end stations, perhaps on multiple physical LAN segments that are not constrained by their physical location and can communicate as if they were on a common LAN.

VLANs are configured through software rather than hardware, which makes them extremely flexible. One of the biggest advantages of VLANs is that when a computer is physically moved to another location, it can stay on the same VLAN without any hardware reconfiguration.

Because VLANs are not limited by the hardware constraints that physically connect traditional LAN segments to a network, they can define a network into various logical configurations. For example, VLANs can define a network by application. In this scenario, a company might create one VLAN for multimedia users and another for email users. VLANs can also define a network by department. For example, a company might have one VLAN for its Engineering Department, another for its Marketing Department, and another for its Account Payable Department.

VLANs can also be set up according to the organization structure within a company. For example, the company president might have his/her own VLAN, the executive staff might have a different VLAN, and the remaining employees might have yet a different VLAN.

As these examples show, VLANs offer unparalleled flexibility. The following sections describe how deploying VLANs can benefit organizations and reduce administration costs.

Broadcast Containment

In traditional networks, traffic broadcasts to all network devices, whether they are the intended recipients or not. However, VLANs can be set up to contain only those devices that need to communicate with each other. As a result, VLANs significantly reduce network congestion. In addition, VLANs prevent broadcast storms from causing network meltdown due to volumes of traffic.

Multicast-Based Multimedia Applications

Multimedia applications, such as interactive training, video conferencing, and news-video transmissions, require large amounts of bandwidth. These applications are also extremely sensitive to variable delays, which are unavoidable on a shared Ethernet network. By defining a VLAN based on the IP multicast address for all subscribing members on the VLAN, sufficient bandwidth will be available for these application, providing true multimedia on Ethernet.

Enhanced Security

Because VLANs are self-contained, only the devices within the same VLAN can communicate with each other. If a device in one VLAN wants to communicate with a device in another VLAN, the traffic must go through a router.

VLAN Membership

VLAN IMPLEMENTATION ALLOWS:

VLANs across multiple switches by using explicit or implicit tagging and the GARP/GVRP protocol defined in IEEE802.1p and 802.1Q.
An end station's network interface card may belong to multiple VLANs.
A switch port may be associated with multiple VLANs.

DEFINITIONS OF VLAN MEMBERSHIP

VLAN implementation allows VLAN membership to be defined based on ports. Port-based VLANs are organized by physical port number. For example, switch ports 1, 2, 4 and 6 can be grouped on VLAN, while server ports 3, 5, 7 and 8 can be on another VLAN. Broadcasts from servers within each group would only go to the members of its own VLAN. This ensures that broadcast storms cannot cause a network meltdown due to traffic volume.

VLAN MEMBERSHIP LEARNING

Port-based VLAN is defined using a static binding between a VLAN and its associated ports. The switch's forwarding decision is based on the destination MAC address and its associated port ID. Therefore, to make valid forwarding and flooding decisions, the switch learns the relationship of the MAC address to its related port – and thus to the VLAN – at runtime.

REMOTE VLAN LEARNING

In addition to providing network management tools that allow network administrators to statically add and delete VLAN member ports, the switch also supports GVRP (GARP VLAN Registration Protocol). GVRP allows for dynamic registration of VLAN port members within switch and across multiple switches.

Other than supporting dynamic updating of registration entries in a switch, GVRP is used to communicate VLAN registration information to other VLAN-aware switches, so that a VLAN member can cover a wide span of switches on a network.

GVRP allows both VLAN-aware workstations and switches to issue and revoke VLAN memberships. VLAN-aware switches register and propagate VLAN membership to all ports that belong to the active topology of the VLAN.

VLAN CONFIGURATION

The switch provides a Local/Remote Management Console Interface for VLAN configuration and management An SNMP-based VLAN MIB is also provided.

Intra-VLAN Communication

The switch supports intra-VLAN communication through hardware, as described in “Basic Functions” section.

Inter-VLAN Communication

The switch supports inter-VLAN communication using CPU-based routing software.

GVRP

In addition to network management tools that allow network administrators to statically add and delete VLAN member ports, the routing switch supports GARP VLAN Registration Protocol (GVRP). GVRP supports dynamic registration of VLAN port members within a switch and across multiple switches.

In addition to dynamically updating registration entries within a switch, GVRP is used to communicate VLAN registration information to other VLAN-aware switches, so that members of a VLAN can cover a wide span of switches on a network.

GVRP allows both VLAN-aware workstations and switches to issue and revoke VLAN memberships. VLAN-aware switches register and propagate VLAN membership to all ports that are part of the active topology of the VLAN.

IGMP Snooping and IP Multicast Filtering

The Internet Group Management Protocol (IGMP) runs between hosts and their immediately neighboring multicast routers. The protocol's mechanisms allow a host to inform its local router that it wants to receive transmissions addressed to a specific multicast group.

Routers periodically query the LAN to determine if known group members are still active. If there is more than one router on the LAN performing IP multicasting, one of the routers is elected "querier" and assumes the responsibility of querying the LAN for group members.

Based on the group membership information learned from the IGMP, a router can determine which (if any) multicast traffic needs to be forwarded to each of its "leaf" sub-networks. Multicast routers use this information, along with a multicast routing protocol, to support IP multicasting across the Internet.

IGMP provides the final step in an IP multicast packet delivery service since it is only concerned with the forwarding of multicast traffic from the local route to group members on directly attached sub-networks.

Routing switches support IP Multicast Filtering by:

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

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts

members and routers instead of flooding to all ports in the subnet (VLAN).

Routing switches with IP multicast filtering/switching capability not only passively monitor IGMP Query and Report messages, DVMRP Probe messages, PIM, and MOSPF Hello messages; they also actively send IGMP Query messages to learn locations of multicast routers and member hosts in multicast groups within each VLAN.

Note, however, IGMP neither alters nor routes any IP multicast packets. Since IGMP is not concerned with the delivery of IP multicast packets across sub-networks, an external IP multicast router is needed if IP multicast packets have to be routed across different sub-networks.

Switch Management

ADMINISTRATION CONSOLE VIA RS-232 SERIAL PORT
The switch provides an onboard serial port, which allows the switch to be configured via a directly connected terminal or a Telnet session.

WEB-BASED BROWSER INTERFACE
The switch also hosts a point-and-click browser-based interface that lets users access full switch configuration and functionality from a Netscape or Internet Explorer browser.

EXTERNAL SNMP-BASED NETWORK MANAGEMENT APPLICATION
The switch can also be configured via SNMP.

For more information on switch management, refer to the "Switch Management" section.

Installation

This chapter gives step-by-step instructions about how to install the switch:

Selecting a Site for the Switch

As with any electric device, you should place the switch where it will not be subjected to extreme temperatures, humidity, or electromagnetic interference. Specifically, the site you select should meet the following requirements:

- The ambient temperature should be between -40 to 75 degrees Celsius.

- The relative humidity should be less than 95 percent, non-condensing.

- Surrounding electrical devices should not exceed the electromagnetic field (RFC) standards.

- Make sure that the switch receives adequate ventilation. Do not block the ventilation holes on each side of the switch or the fan exhaust port on the rear of the switch.

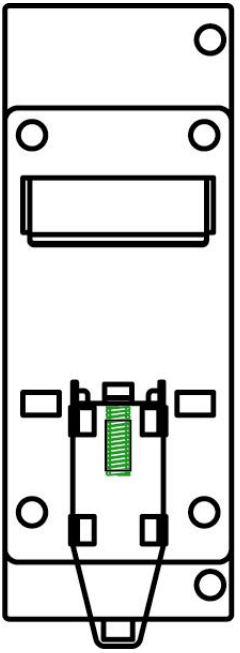
- The power outlet should be within 1.8 meters of the switch.

DIN Rail Mounting

Fix the DIN rail attachment plate to the back panel of the switch.

Installation: Place the switch on the DIN rail from above using the slot. Push the front of the switch toward the mounting surface until it audibly snaps into place.

Removal: Pull out the lower edge and then remove the switch from the DIN rail.



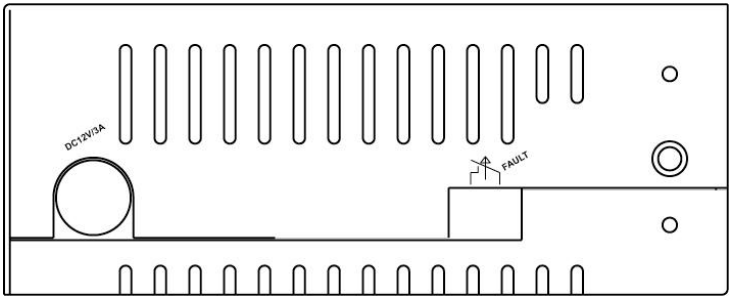
Connecting to Power

Redundant DC Terminal Block Power Inputs or 12VDC DC Jack:

12VDC DC Jack

Step 1: Connect the supplied AC to DC power adapter to the receptacle on the topside of the switch.

Step 2: Connect the power cord to the AC to DC power adapter and attach the plug into a standard AC outlet with the appropriate AC voltage.

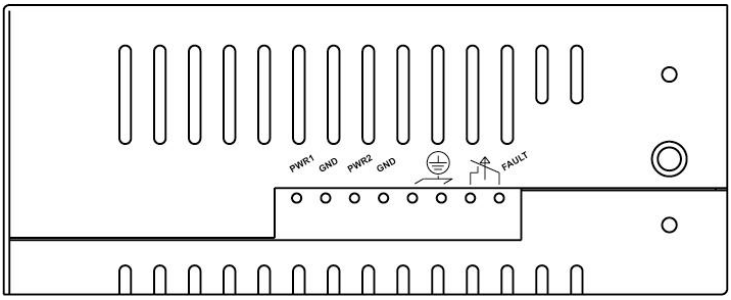


Redundant DC Terminal Block Power Inputs

There are two pairs of power inputs for use with redundant power sources. You only need to have one power input connected to run the switch.

Step 1: Connect the DC power cord to the plug-able terminal block on the switch, and then plug it into a standard DC outlet.

Step 2: Disconnect the power cord if you want to shut down the switch.



Alarms for Power Failure

Step 1: There are two pins on the terminal block used for power failure detection. It provides the normally closed output when the power source is active. Use this as a dry contact application to send a signal for power failure detection.

The Terminal Block	
PWR1	Power Input 1 (12 to 32VDC)
GND	Power Ground
PWR2	Power Input 2 (12 to 32VDC)
GND	Power Ground
⏚	Earth Ground
	The relay opens if PWR1 or PWR2 fails (1A)

Special note:
The relay output is normal open position when there is no power to the switch. Please do not connect any power source to this terminal to prevent shorting your power supply.

Power-on Self test (POST)

The Switch performs its Power-On Self Test (POST) when the power is switched on. During the POST, the switch CPU will:
Perform a series of diagnostic procedures to make sure the basic system is functioning properly.

A command line prompts when you press the Esc key on a terminal connected to the switch serial port during the POST process. Then you can execute the following options:

DOWNLOAD RUNTIME SOFTWARE FROM SERIAL PORT0
This will download the runtime system image to the switch via the serial port. Before selecting this option, make sure:

- A host system is running a terminal emulation program that supports the Kermit file transfer protocol.
- The host system's hard drive has the required binary file that will be downloaded to the switch.

CONFIGURE THE SYSTEM
This option lets you modify any configurable parameter in the switch's flash ROM before the switch system boots.

RUN MANUFACTURING DIAGNOSTICS
This option is to download the manufacturer's diagnostics. Refer to Download Runtime Software for download requirements.

When the file transfer is completed, the target system jumps to the entry point of the diagnostic program and starts executing the diagnostic code. The Main Menu of the diagnostic program appears where you can initiate tests or obtain system information. Note that user intervention is not required when a test runs, unless an error occurs. If an error occurs during testing, you are given the choice of continuing the diagnostics or skip the error.

Connecting to Your Network

Cable Type & Length

It is necessary to follow the cable specifications below when connecting the switch to your network. Use appropriate cables that meet your speed and cabling requirements.

Table 3: Cable Specifications

Speed	Connector	Port Speed Half/Full Duplex	Cable	Max. Distance
10Base-T	RJ-45	10/20 Mbps	2-pair UTP/STP Cat. 3, 4, 5	100 m
100Base-TX	RJ-45	100/200 Mbps	2-pair UTP/STP Cat. 5	100 m
1000Base-T	RJ-45	2000 Mbps	4-pair UTP/STP Cat. 5	100 m
100Base-FX	ST, SC	100/200 Mbps	MMF (50 or 62.5µm)	2 km
100Base-FX	ST, SC	100/200 Mbps	SMF (9 or 10µm)	15, 40, or 75 km
1000Base-SX	SC	2000 Mbps	MMF (50 or 62.5µm)	550 m
1000Base-LX	SC	2000 Mbps	SMF (9 or 10µm)	10, 20, or 60 km

Cabling

Step 1: First, ensure the power of the switch and end devices are turned off.

<Note> Always ensure that the power is off before any installation.

Step 2: Prepare cable with corresponding connectors for each type of port in use.

<Note> To connect two regular RJ-45 ports between switches or hubs, you need a straight or cross-over cable.

Step 3: Consult Table 3 in previous section for cabling requirements based on connectors and speed.

Step 4: Connect one end of the cable to the switch and the other end to a desired device.

Step 5: Once the connections between two end devices are made successfully, turn on the power and the switch is operational.

Switch Management

This chapter explains the methods that you can use to configure management access to the switch. It describes the types of management applications and the communication and management protocols that deliver data between your management device (workstation or personal computer) and the system. It also contains information about port connection options.

This chapter covers the following topics:

- ***Management Access Overview***
- ***Key Concepts***
- ***Key Guidelines for Implementation***
- ***Administration Console Access***
- ***Web Management Access***
- ***SNMP Access***
- ***Standards, Protocols, and Related Reading***

Management Access Overview

The switch gives you the flexibility to access and manage the switch using any or all of the following methods.

The administration console and web browser interface support are embedded in the switch software and are available for immediate use.

Administration console via RS-232 serial port

Advantages

- No IP address or subnet needed
- Text-based
- Telnet functionality and HyperTerminal built into Windows 95/98/NT/2000 operating systems

Disadvantages

- Must be near switch or use dial-up connection
- Inconvenient for remote users
- Modem connection may prove to be unreliable or slow

Web-based browser interface

Advantages

- Ideal for configuring the switch remotely
- Compatible with all popular browsers
- Can be accessed from any location
- Most visually appealing

Disadvantages

- Security can be compromised (hackers need only know the IP address and subnet mask)
- May encounter lag times on poor connections

External SNMP-based network management application

Advantages

- Communicates with switch functions at the MIB level
- Based on open standards

Disadvantages

- Requires SNMP manager software
- Least visually appealing of all three methods
- Some settings require calculations
- Security can be compromised (hackers need only know the community name)

Administration Console

The administration console is an internal, character-oriented, menu-driven user interface for performing system administration such as displaying statistics or changing option settings.

Using this method, you can view the administration console from a terminal, personal computer, Apple Macintosh, or workstation connected to the switch's console port.

There are two ways to use this management method: direct access or modem access. The following sections describe these methods.

Direct Access

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as HyperTerminal) to the switch console port.

When using the management method, configure the terminal-emulation program to use the following parameters (you can change these settings after login):

[Default parameters]
115,200bps
8 data bits
No parity
1 stop bit

This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use

any terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator such as TIP.

Modem Access

You can access the switch's administration console from a PC or Macintosh using an external modem attached to the console port. The switch management program provides **Console Port** screen, accessible from the **Basic Management** screen, which lets you configure parameters for modem access.

When you have configured the external modem from the administration console, the switch transmits characters that you have entered as output on the modem port. The switch echoes characters that it receives as input on the modem port to the current administration console session. The console appears to be directly connected to the external modem.

Web Management

The switch provides a browser interface that lets you configure and manage the switch remotely.

After you set up your IP address for the switch, you can access the switch's web interface applications directly in your web browser by entering the IP address of the switch. You can then use your web browser to list and manage switch configuration parameters from one central location, just as if you were directly connected to the switch's console port.

Web Management requires either Microsoft Internet Explorer 4.01 or later or Netscape Navigator 4.03 or later.

Netscape Navigator

If you use Netscape Navigator 4.03 or 4.04, install the Netscape JDK 1.1 Patch. Download the patch from:

http://help.hetscape.com/filelib.html#smartupdate

If you encounter problems accessing Help files when you use Netscape, clear the browser memory cache and disk cache, and restart the browser.

Internet Explorer

If you use Internet Explorer, install the latest 4.01 Service Pack 1. This service pack makes Internet Explorer Year 2000 compliant and fixes other product-support issues. Download the 4.01 Service Pack 1 from the following location:

http://www.microsoft.com/msdownload/iebuild/ie4sp1_win32/en/ie4sp1_win32.htm

If the above link is unavailable, download the service pack from the Microsoft home page:
http://www.microsoft.com

SNMP-Based Network Management

You can use an external SNMP-based application to configure and manage the switch. This management method requires the SNMP agent on the switch and the SNMP Network Management Station to use the same community string. This management method, in fact, uses two community strings: the get community string and the set community string. If the SNMP Network management station only knows the set community string, it can read and write to the MIBs. However, if it only knows the get community string, it can only read MIBs. **The default get and set community strings for the switch are public.**

Protocols

The switch supports the following protocols:

VIRTUAL TERMINAL PROTOCOLS, SUCH AS TELNET
A virtual terminal protocol is a software program, such as Telnet, that allows you to establish a management session from a Macintosh, a PC, or a UNIX workstation. Because Telnet runs over TCP/IP, you must have at least one IP address configured on the switch before you can establish access to it with a virtual terminal protocol.

<Note> Terminal emulation is different from a virtual terminal protocol in that you must connect a terminal directly to the console port.

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)
SNMP is the standard management protocol for multivendor IP networks. SNMP supports transaction-based queries that allow the protocol to format messages and to transmit information between reporting devices and data-collection programs. SNMP runs on top of the User Datagram Protocol (UDP), offering a connectionless-mode service.

Management Architecture

All of the management application modules use the same Messaging Application Programming Interface (MAPI). By unifying management methods with a single MAPI, configuration parameters set using one method (e.g. console port) are immediately displayed the other management methods (e.g. SNMP agent of web browser).

The management architecture of the switch adheres to the IEEE open standard. This compliance assures customers that the switch is compatible with, and will interoperate with other solutions that adhere to the same open standard.

Menu-Driven Console Management

The switch provides a menu-driven console interface for configuration purposes. The switch can be configured either locally through its RS-232 port or remotely via a Telnet session.

This chapter describes how to configure the switch using its menu-driven console.

Logging on to the switch

At the screen prompt

Switch Console Login:
Password:

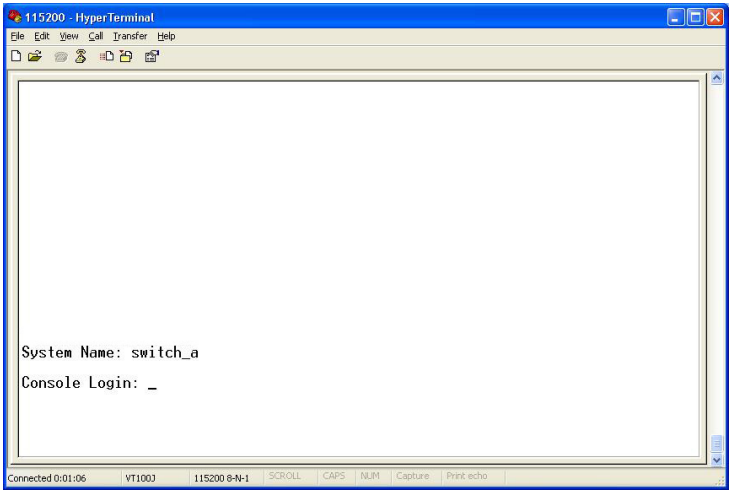
LOGIN NAME
Enter the console interface factory default console name **admin**.

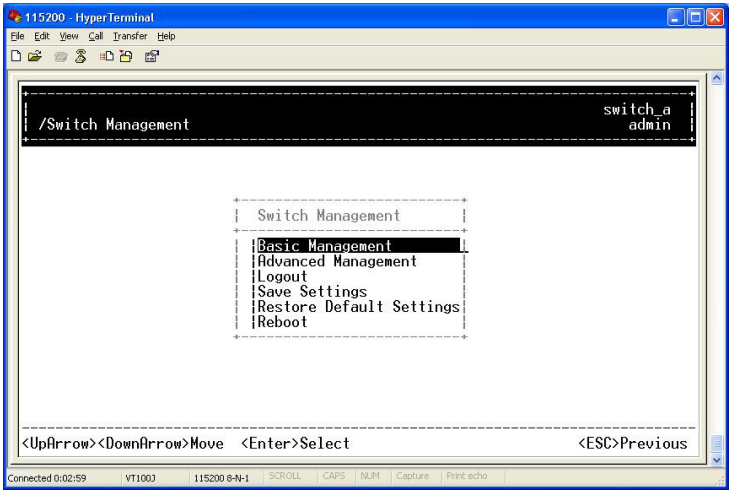
PASSWORD
Enter the factory default password (no password, **press <Enter> directly**). Or enter a user-defined password if you followed the instructions later and changed the factory default password.

Factory Default Password: no password, press **<Enter>** directly.

<Note> Only one console and three telnet users can log on to the switch concurrently. However, it is not recommended that multiple users modify the configuration at the same time.

Switch Management Screen





BASIC MANAGEMENT
Refer to performing basic management activities.

ADVANCED MANAGEMENT
Refer to performing advanced management activities.

LOGOUT
Highlight this option and press Enter to log out.

SAVE SETTINGS
Highlight this option and press Enter to save the current settings and remain in the configuration program.

RESTORE DEFAULT SETTINGS
Highlight this option and press Enter to restore the factory default settings.

REBOOT
Highlight this option and press Enter to reboot.

Navigating Through the Console Interface

The console interface consists of a series of menu boxes. Each menu box has several options, which are listed vertically. Move the highlight to select an option as you wish; press the Enter key to activate that option.

Press this key…	**To**
Up Arrow or K*	Move the highlight one line up in a menu box
Down Arrow or J*	Move the highlight one line down in a menu box
Tab	Move the highlight between screens
Enter	Select the highlighted option
Esc	Move to a previous menu

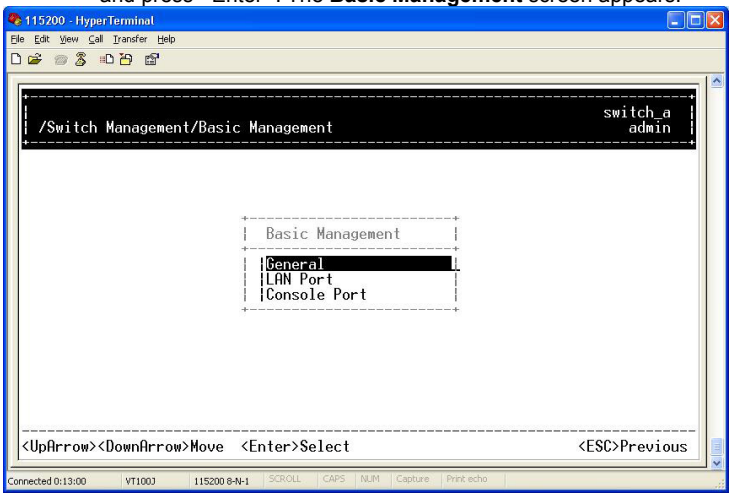
<Note> * Remember to release the <Caps Lock> key if you press <K> or <J> and cannot move the highlight on the screen.

Performing Basic Management Activities

Basic management activities consist of General, LAN Port, and Console Port tasks.

To Perform Basic Management Activities:

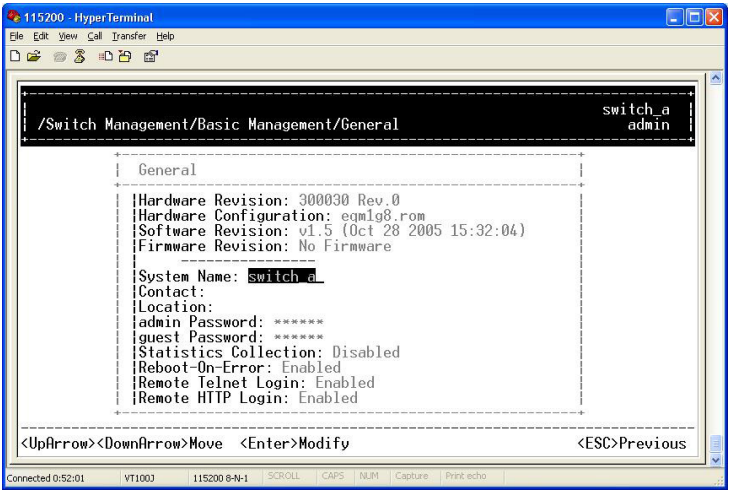
Step 1: Highlight **Basic Management** from **Switch Management** screen and press <Enter>. The **Basic Management** screen appears:



Step 2: Highlight a desired option and press <Enter>. Or press <Esc> to exit.

GENERAL MANAGEMENT CONFIGURATIONS

Step 1: Highlight **General** from **Basic Management** screen and press <Enter>.



System Name

Step 2: **System Name** is highlighted. Press <Enter> if you want to change it.

Contact

Step 3: Move to highlight **Contact** and press <Enter> if you want to change it.

Location

Step 4: Move to highlight **Location** and press <Enter> if you want to change it.

admin Password

Step 5: Move to highlight **admin Password** and press <Enter> if you want to change it.

guest Password

Step 6: Move to highlight **guest Password** and press <Enter> if you want to change it.

Statistics Collection

Step 7: Move to highlight **Statistics Collection** and press <Enter> if you want to change it, Disabled or Enabled.

Reboot-On-Error

Step 8: Move to highlight **Reboot-On-Error** and press <Enter> if you want to change it, Disabled or Enabled.

Remote Telnet Login

Step 9: Move to highlight **Remote Telnet Login** and press <Enter> if you want to change it, Disabled or Enabled.

Remote HTTP Login

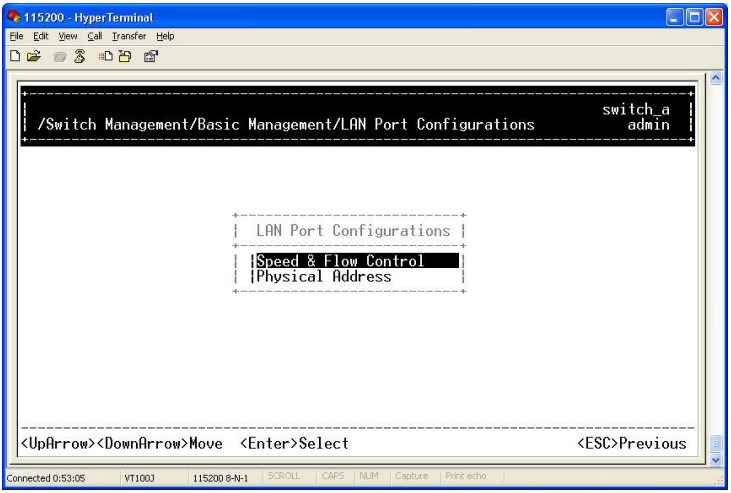
Step 10: Move to highlight **Remote HTTP Login** and press <Enter> if you want to change it, Disabled or Enabled.

Return to Basic Management

Step 11: Press <Esc> to return to **Basic Management** screen when completed.

LAN PORT CONFIGURATIONS

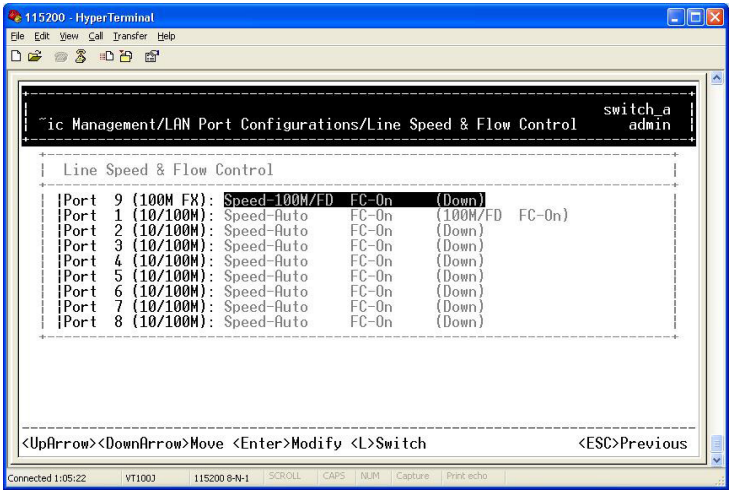
Step 1: Highlight **LAN Port** from **Basic Management** screen and press <Enter>.



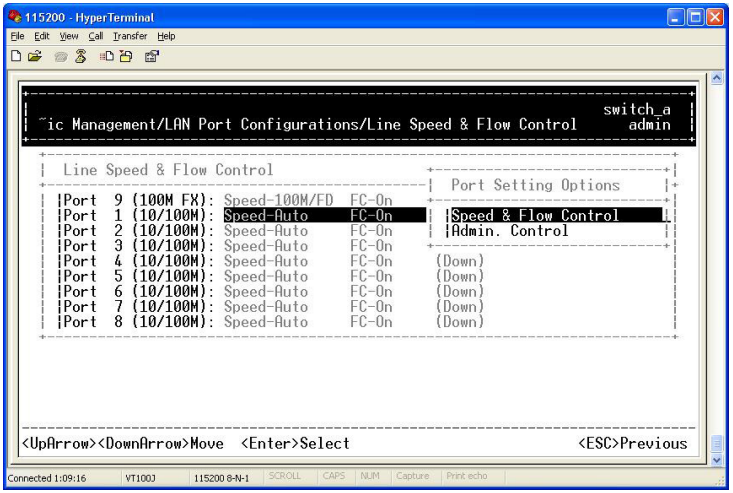
Speed & Flow Control

Step 2: **Speed & Flow Control** is highlighted. Press <Enter> if you want to set speed or flow control on port.

Step 3: Move to highlight each port and press <Enter> to configure individually.

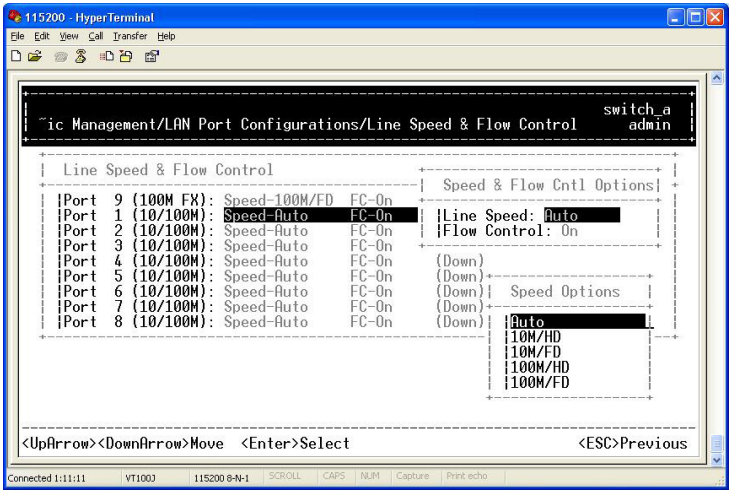


Step 4: **Port Setting Options** screen appears. Highlight **Speed & Flow Control** and press <Enter>.



Line Speed

Step 5: For **Line Speed**, move to highlight a desired setting from **Speed Options** and press <Enter>.

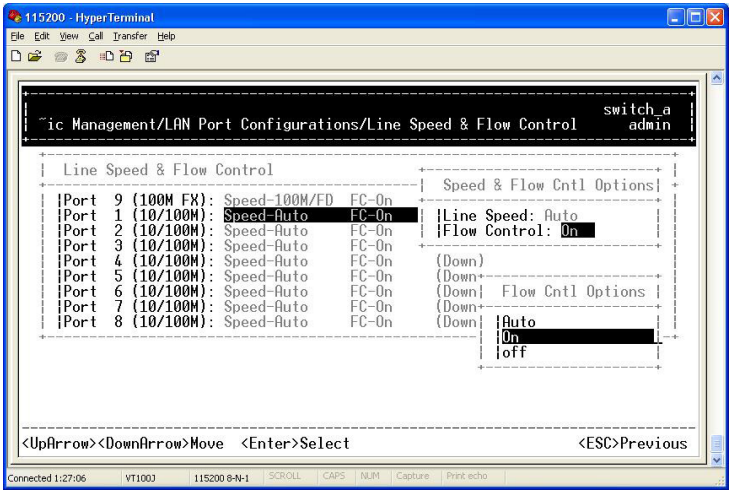


<Note> In the Speed Options, HD denotes half-duplex and FD denotes full-duplex.

Step 6: Press <Esc> to previous screen. Highlight **Flow Control** and press <Enter>.

Flow Control

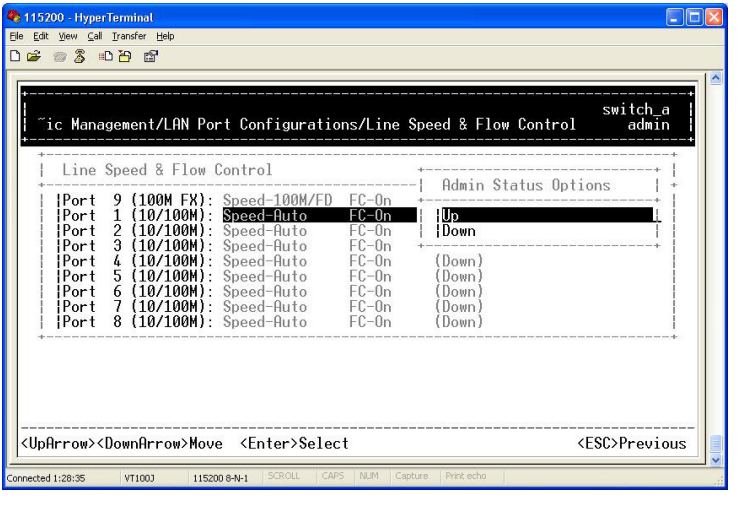
Step 7: For **Flow Control**, move to highlight a desired setting from the **Flow Cntl Options** and press <Enter>.



Step 8: Press <Esc> to a previous screen as shown in Step 3.

Admin. Control

Step 9: For **Admin. Control**, move to highlight Up or Down from **Admin Status Options**.

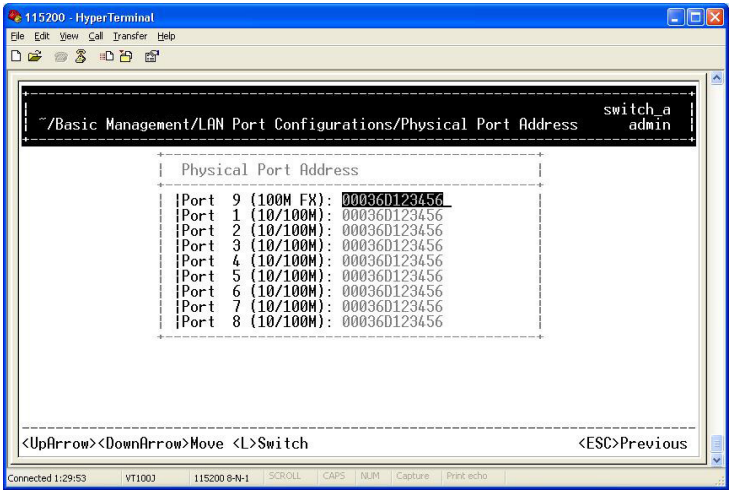


Step 10: The port is set as **Admin Down** to stop TX/RX transmission. To allow TX/RX transmission on the port, move to highlight Up from the options in Step 9.

Physical Port Address

Step 11: Press <Esc> to a previous screen as shown in Step 1.

Step 12: Move to highlight **Physical Address** to view physical port address.

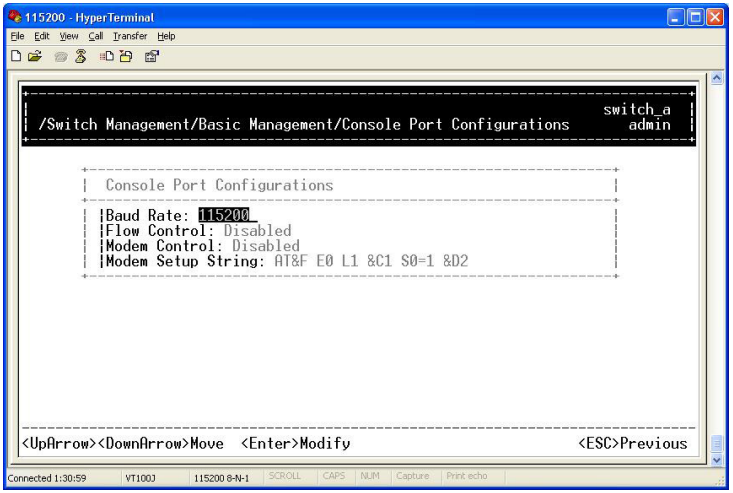


Return to Basic Management

Step 13: Press <Esc> to return to **Basic Management** screen when completed.

CONSOLE PORT CONFIGURATIONS

Step 1: Move to highlight **Console Port** from **Basic Management** screen.



Baud Rate

Step 2: **Baud Rate** is highlighted. Press <Enter> if you want to change the current console baud rate.

Flow Control

Step 3: Move to highlight **Flow Control** and press <Enter> if you want to change the current flow control method.

Modem Control

Step 4: Move to highlight **Modem Control** and press <Enter> to decide a console modem connection, Disabled or Enabled.

Modem Setup String

Step 5: When a modem connection is enabled, move to highlight **Modem Setup String** and press <Enter>. Decide whether you want to use Default or Custom Setup String.

<Note> Default Setup String configures the modem to auto answer. It works for all Hayes compatible modems.

Return to Basic Management

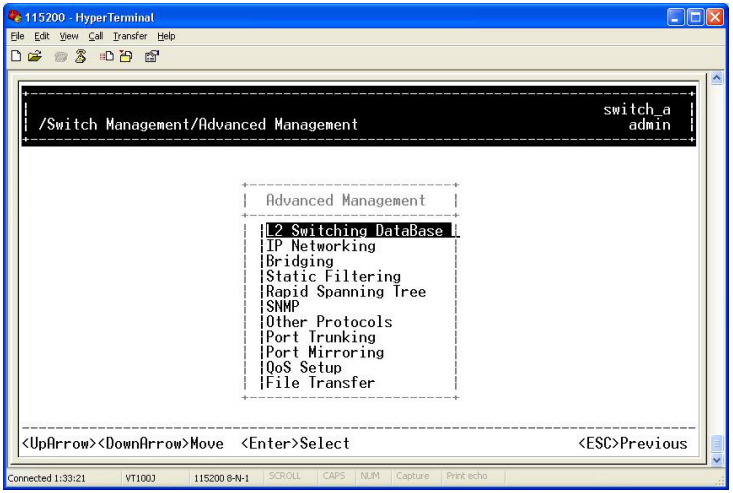
Step 6: Press <Esc> to return to **Basic Management** screen when completed.

Performing Advanced Management Activities

Advanced management activities consist of L2 Switching DataBase / IP Networking / Bridging / Static Filtering / Rapid Spanning Tree / SNMP / Other Protocols / Port Trunking / Port Mirroring / QoS Setup / File Transfer.

To Perform Advanced Management Activities:

Step 1: Highlight **Advanced Management** from **Switch Management** screen and press <Enter>. The **Advanced Management** screen appears:



Step 2: Move to highlight a desired option and press <Enter>.
Or press <Esc> to exit.

L2 SWITCHING DATABASE
View and change VLAN, MAC address, IP multicast group, and port perspectives.

IP NETWORKING
View and change IP settings and ping settings.

BRIDGING
View and change the aging period for a MAC address and the flood limit for all ports.

STATIC FILTERING
View / add / delete / search all source or destination MAC addresses to be filtered.

RAPID SPANNING TREE
View and change spanning tree configurations, ports states, path costs, and port priorities.

SNMP
View and change the SNMP configuration.

OTHER PROTOCOLS
View and change GVRP and IGMP settings.

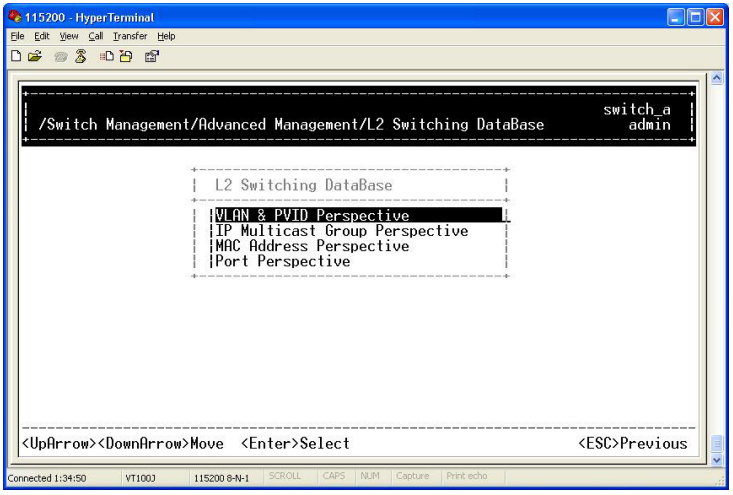
PORT TRUNKING
Assign a range of ports to trunking groups.

PORT MIRRORING
Mirror one port to Port 1.

QOS SETUP
Specify Quality of Service parameter.

FILE TRANSFER
Send files using the TFTP or Kermit protocol.

L2 SWITCHING DATABASE



VLAN & PVID Perspective

There are three types of private VLAN ports: promiscuous, isolated, and community.

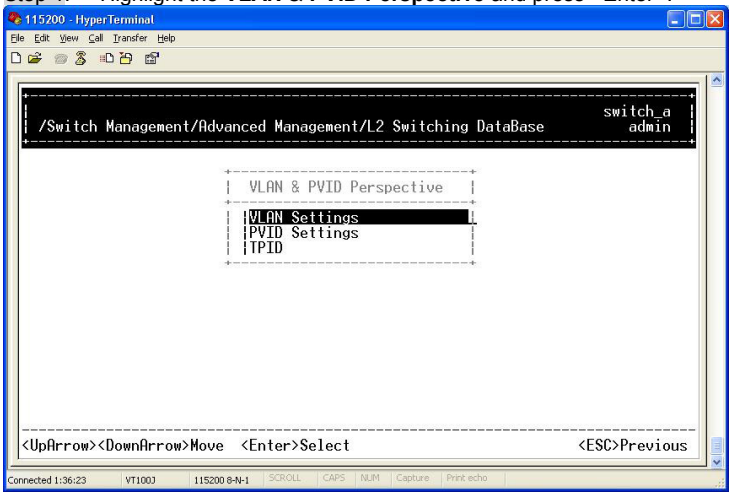
1. A promiscuous port communicates with all other private VLAN ports and is the port you use to communicate with routers, servers, and administrative workstations.
2. An isolated port has complete Layer 2 separation from other ports within the same private VLAN with the exception of the promiscuous port.
3. Community ports communicate among themselves and with their promiscuous ports. These ports are isolated at Layer 2 from all other ports in other communities or isolated ports within their private VLAN.
4. Primary VLAN conveys incoming traffic from the promiscuous port to all other promiscuous, isolated, and community ports.
5. Isolated VLAN used by isolated ports to communicate to the promiscuous ports.
6. Community VLAN used by a group of community ports to communicate among themselves and transmit traffic to outside the group via the designated promiscuous port.

For example:

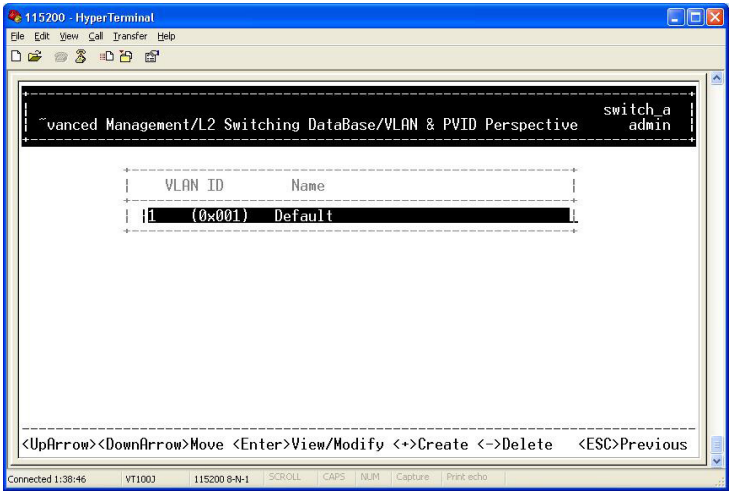
	VLAN ID	Promiscuous port	Isolated port	Community ports
Primary VLAN	2	2	3,4	5,6,7,8
Isolated VLAN	3	2	3	
Isolated VLAN	4	2	4	
Community VLAN	5	2		5,6
Community VLAN	6	2		7,8

1. Create the primary VLAN and bind the promiscuous port, isolated port(s), and community ports to the primary VLAN.
2. Create the isolated VLAN(s) and bind the promiscuous port and isolated port(s) to the isolated VLAN(s).
3. Create the community VLAN(s) and bind the promiscuous port and community ports to the community VLAN(s).
4. Associate the primary VLAN to the promiscuous port.
5. Associate the isolated VLAN(s) to the isolated port(s).
6. Associate the community ports to the community VLAN(s).

Step 1: Highlight the **VLAN & PVID Perspective** and press <Enter>.



Step 2: Highlight the **VLAN Settings** and press <Enter> to view VLAN info of the default VLAN or if you want to obtain a VLAN perspective instead of the default VLAN.

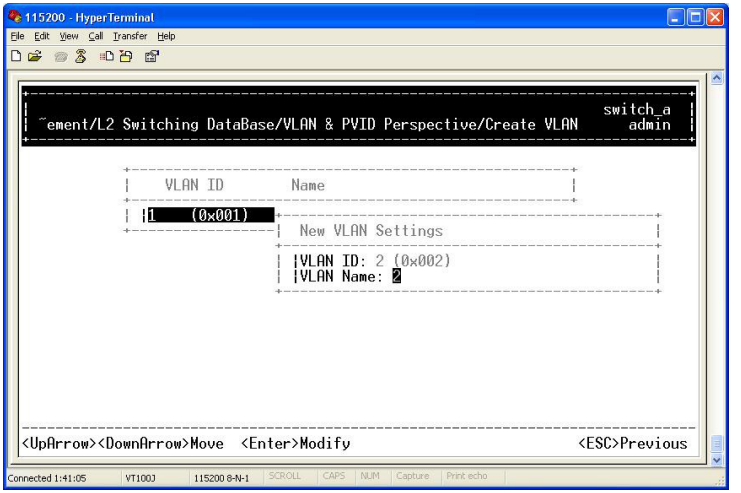


<Note> Default VLAN:

The IEEE802.1Q standard defines VLAN ID #1 as the default VLAN. The default VLAN includes all the ports as the factory default. The default VLAN's egress rule restricts the ports to be all untagged, so it can, by default, be easily used as a simple 802.1D bridging domain. The default VLAN's domain shrinks as untagged ports are defined in other VLANs.

Create VLAN

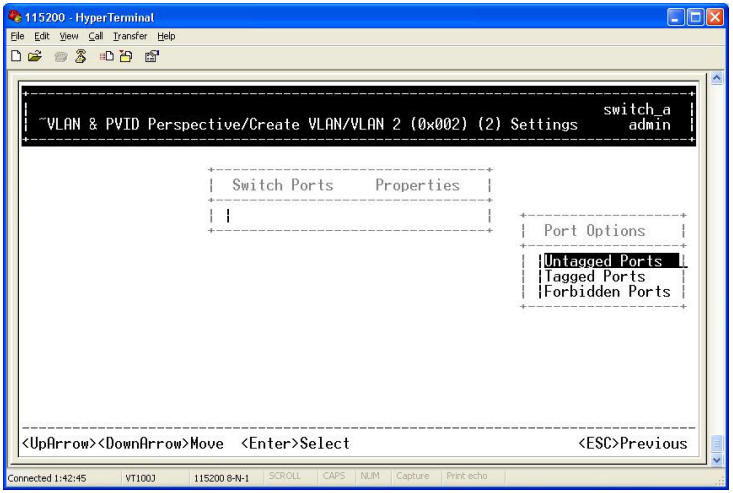
Step 3: Press <Shift> and [+] on keypad to enter **New VLAN Settings**. Enter new VLAN ID and VLAN name.



<Note> "Remote" is appended to the VLAN ID automatically if the VLAN is learned from a remote switch.

Add New Switch Ports

Step 4: Press <Esc> and appears the following screen. Press <Shift> and [+] to add new switch ports to the newly created VLAN.



Step 5: Move to highlight a suitable option from **Port Options** and press <Enter>, e.g. Untagged Ports.

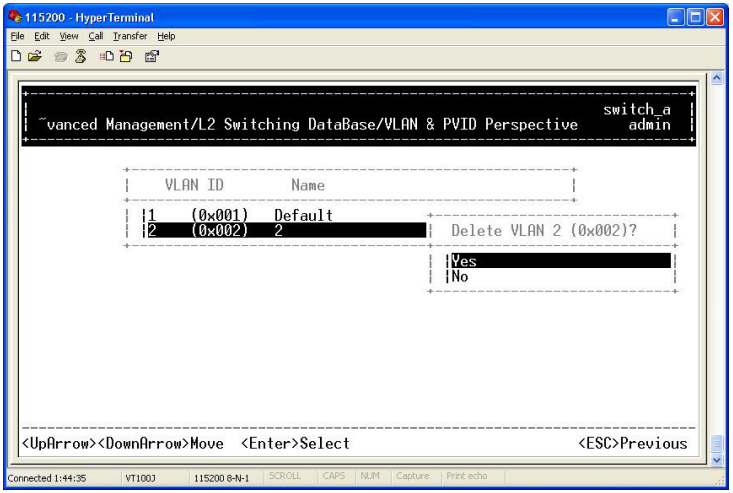
Step 6: From **Select Untagged Ports**, press <Enter> to select All Ports or move to highlight each port individually and press <Enter>. Similar procedure when you select Tagged Ports and Forbidden Ports in Step 4.

<Note> If you added untagged ports and want to now add tagged ports or forbidden ports, or vice versa, repeat Step 4 and Step 5.

Step 7: Press <Esc> to a previous screen as shown in Step 1.

Delete VLAN

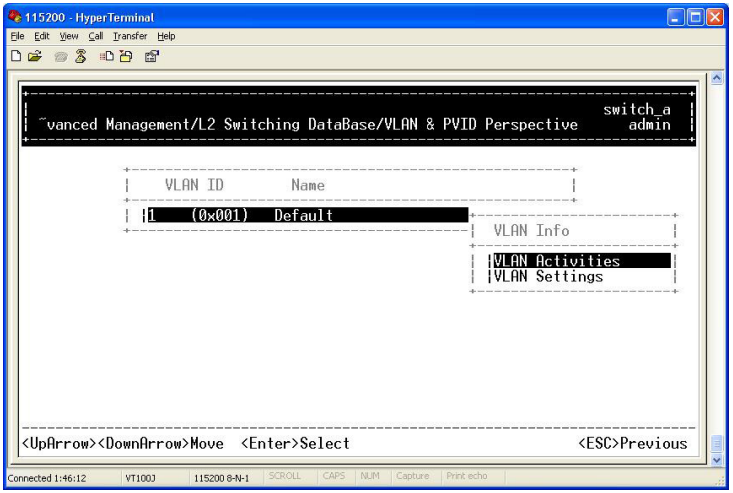
Step 8: Delete VLAN: highlight a VLAN ID and press [-] to delete it. Note that you cannot delete the default VLAN.



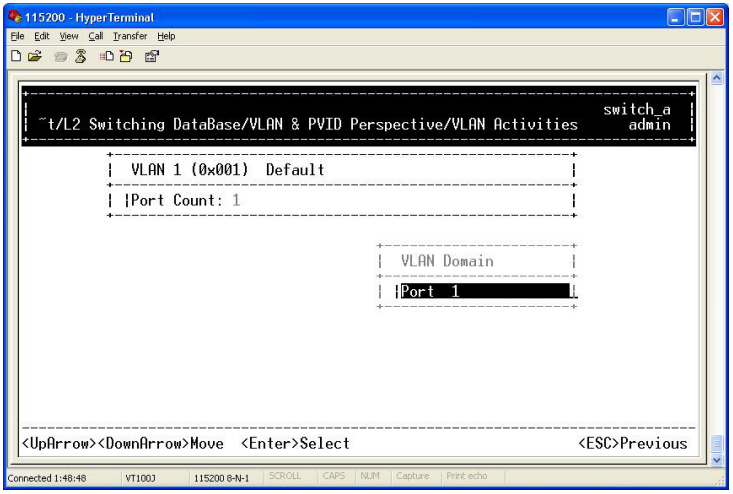
Step 9: Press <Esc> to a previous screen as shown in Step 1 when completed with deleting a VLAN.

VLAN Info

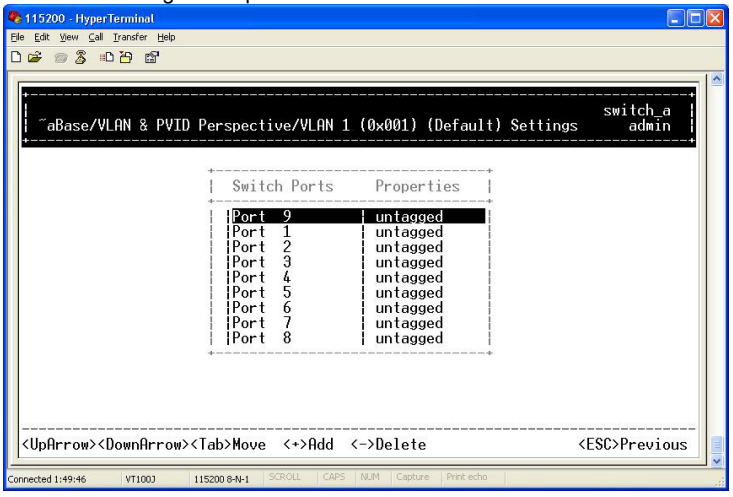
Step 10: Highlight an existing VLAN and press <Enter> to view VLAN information.



Step 11: Move to highlight **VLAN Activities** and press <Enter> to view or search activity information.

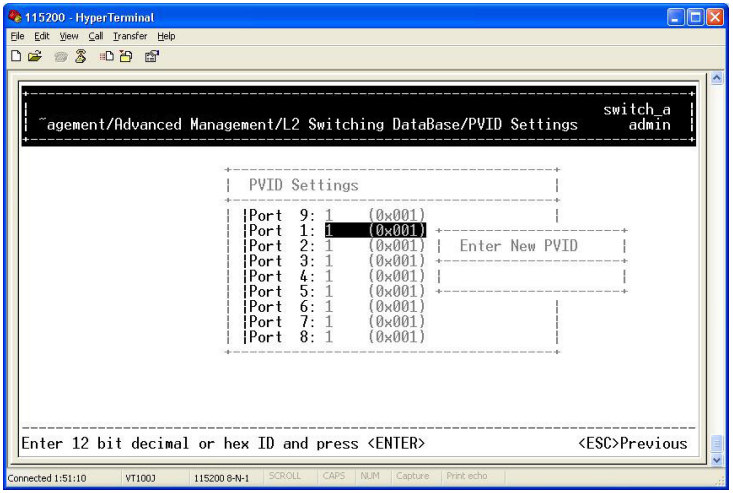


Step 12: Return to Step 9 Move to highlight **VLAN Settings** and press <Enter>. The screen appears as shown in Step 3 for adding or deleting switch ports.



Step 13: Highlight the **VLAN & PVID Perspective** and press <Enter>.

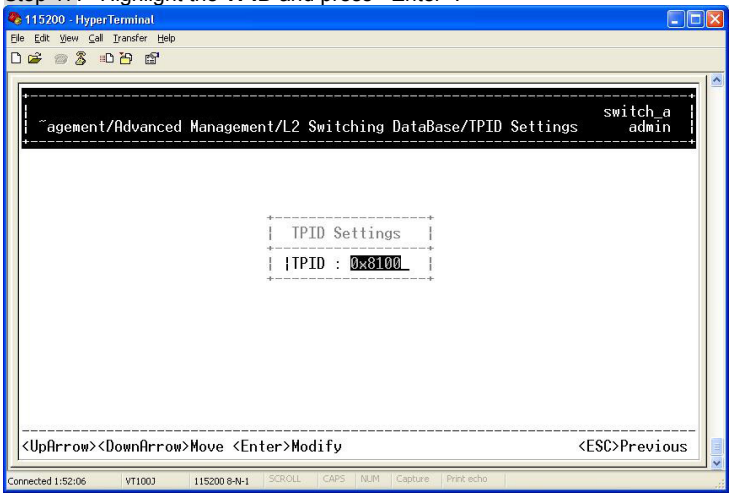
Step 14: Highlight the **PVID Settings** and press <Enter> to apply PVIDs to the ports.



Step 15: Highlight the port and press <Enter> to enter PVID to the port.

Step 16: Highlight the **VLAN & PVID Perspective** and press <Enter>.

Step 17: Highlight the **TPID** and press <Enter>.



Step 18: Press <Enter> to enter TPID value.

IP Multicast Group Perspective

Step 1: Move to highlight **L2 Switching DataBase** from **Advanced Management** screen and press <Enter>.

Step 2: Move to highlight **IP Multicast Group Perspective** from **L2 Switching DataBase** screen and press <Enter>.

Step 3: Move to highlight an address to view information associated with this IP multicast group.

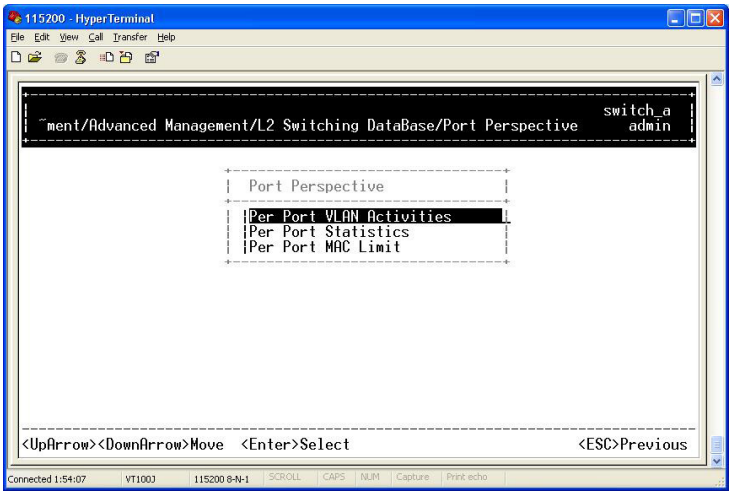
MAC Address Perspective

Step 1: Move to highlight **MAC Address Perspective** from **L2 Switching DataBase** screen, and press <Enter>.

Step 2: Enter a MAC address to view characteristics information, corresponding VLANs, and corresponding ports in the switching database.

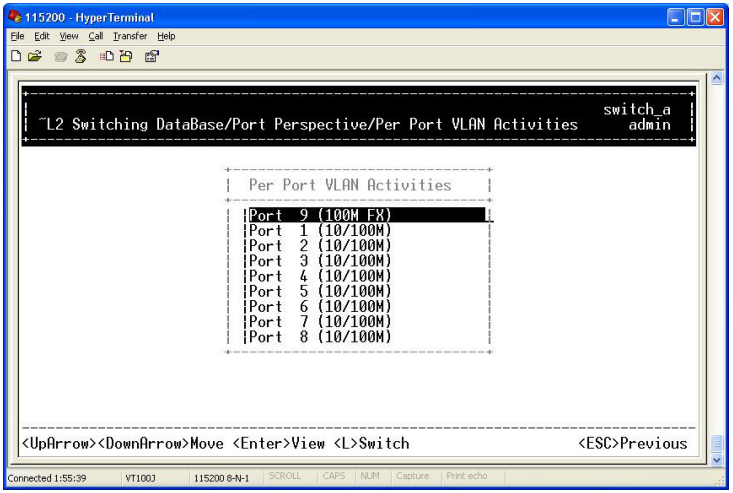
Port Perspective

Step 1: Move to highlight **Port Perspective** from **L2 Switching DataBase** screen, and press <Enter>.
You can view Per Port VLAN activities and Per Port statistics and set Per Port MAC Limit here.

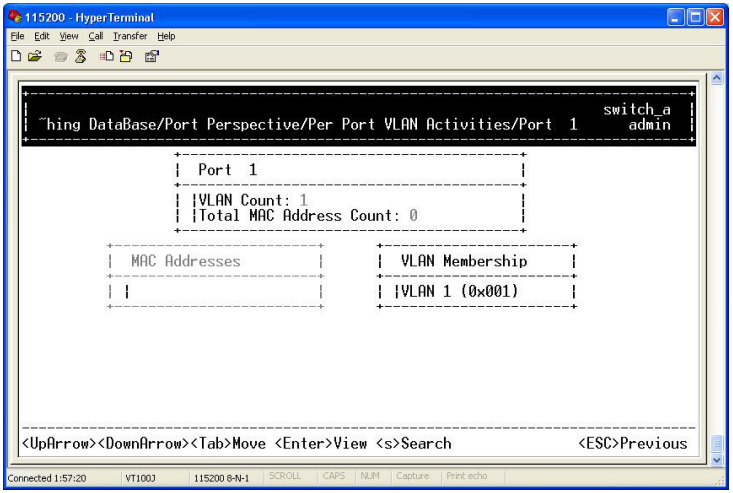


Per Port VLAN Activities

Step 2: **Per Port VLAN Activities** is highlighted. Press <Enter>.



Step 3: Move to highlight a port and press <Enter>.
E.g. select Port 1 to view corresponding VLAN Activities.

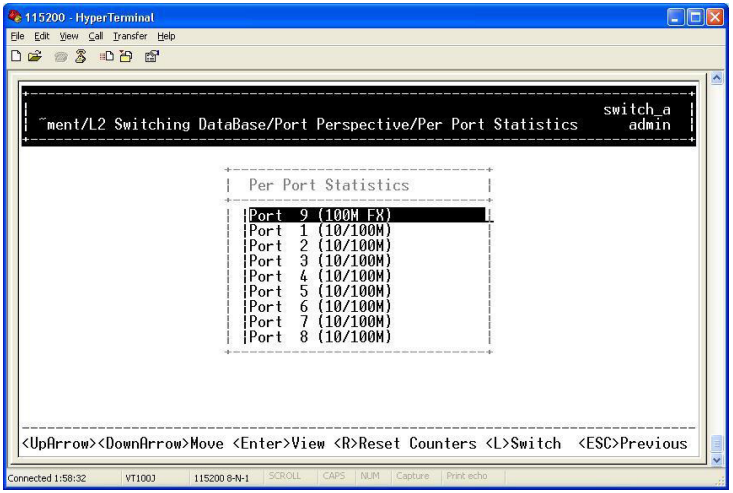


Step 4: View or search by MAC address individually.

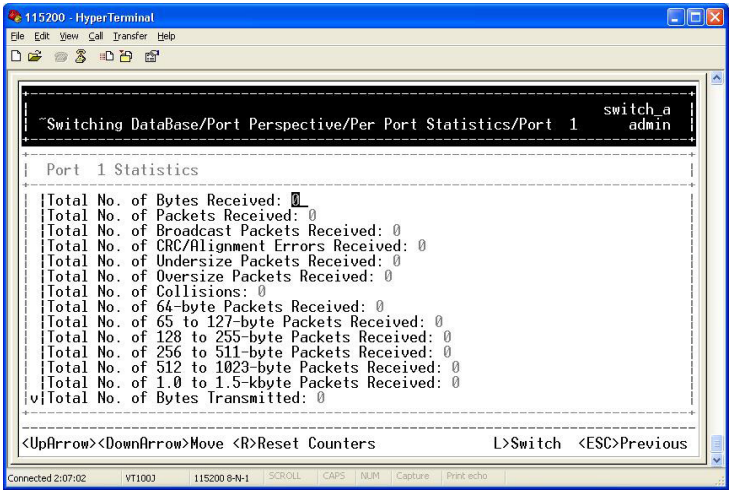
Step 5: Press <Esc> to return to a previous screen as shown in Step 1.

Per Port Statistics

Step 6: Move to highlight **Per Port Statistics** and press <Enter>.



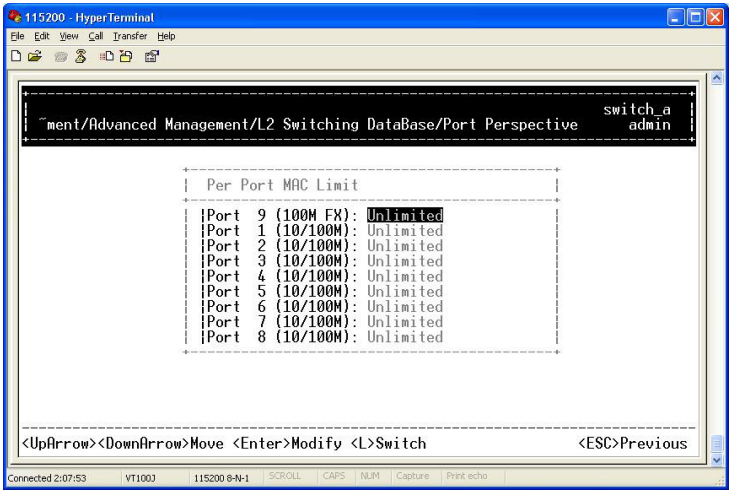
Step 7: Move to highlight a port and press <Enter>.
E.g. select Port 1 to view corresponding VLAN Activities.
Press [R] to reset counter for this port.

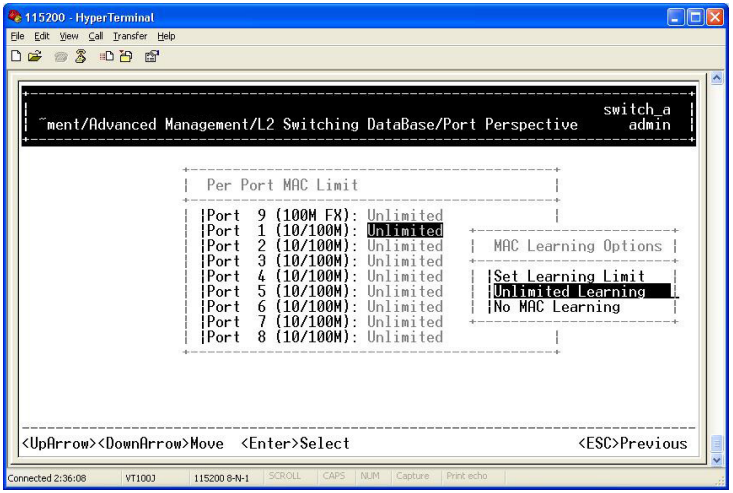


Per Port MAC Limit

Step 8: Move to highlight **Per Port MAC Limit** and press <Enter>.

Step 9: Move to highlight a port and press <Enter>.



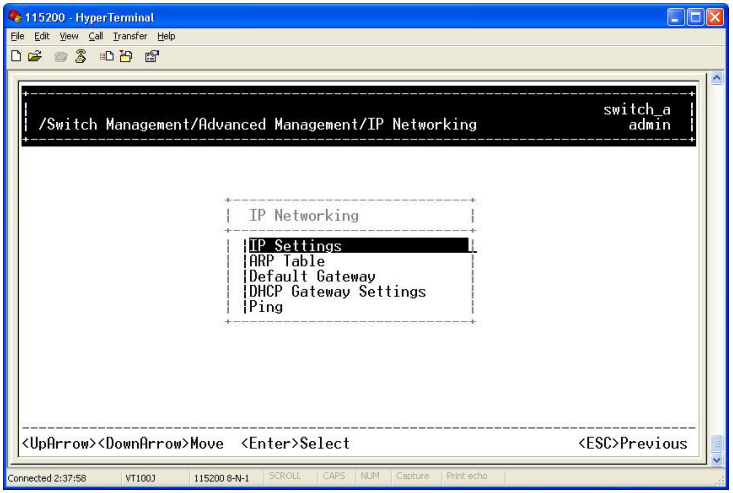


IP NETWORKING

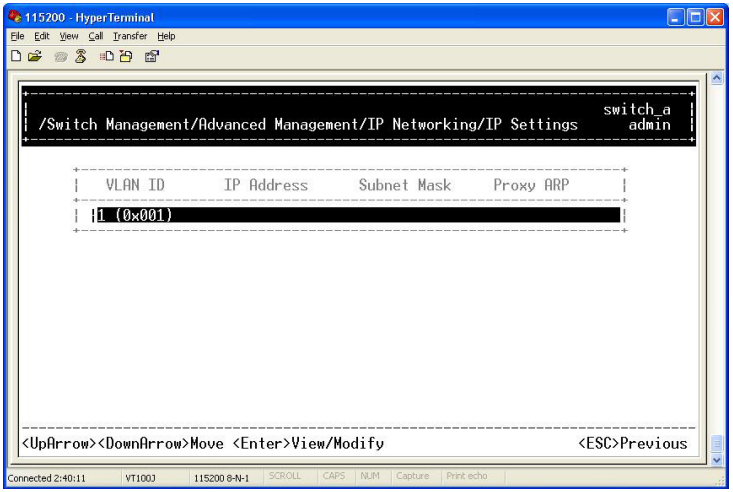
Step 1: Move to highlight **IP Networking** from **Advanced Management** screen and press <Enter>.

IP Settings

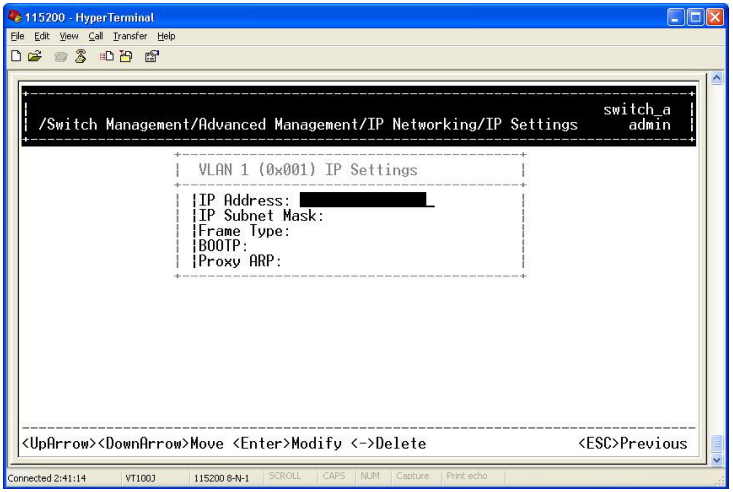
Step 2: Highlight **IP Settings** from **IP Networking** and press <Enter>.



Step 3: The screen shows a list of VLAN IDs, IP addresses, subnet masks, proxy ARPs currently defined.



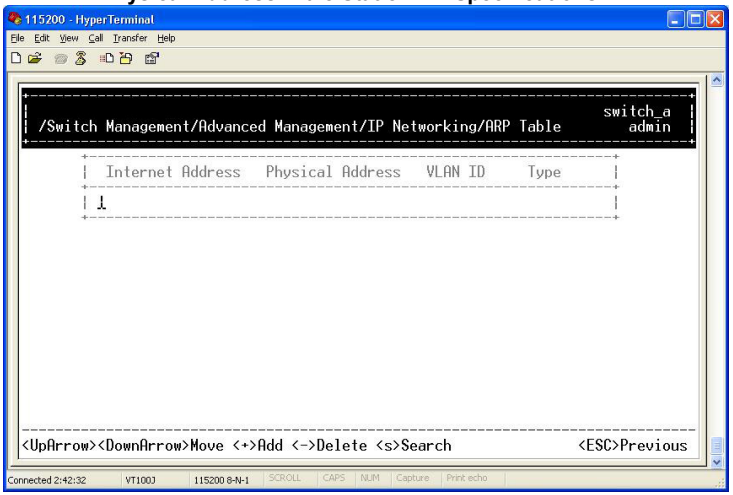
Step 4: Move to highlight the row that contains the parameters you want to change, and then press <Enter>.



ARP Table

Step 5: Highlight **ARP Table** from **IP Networking** and press <Enter>.

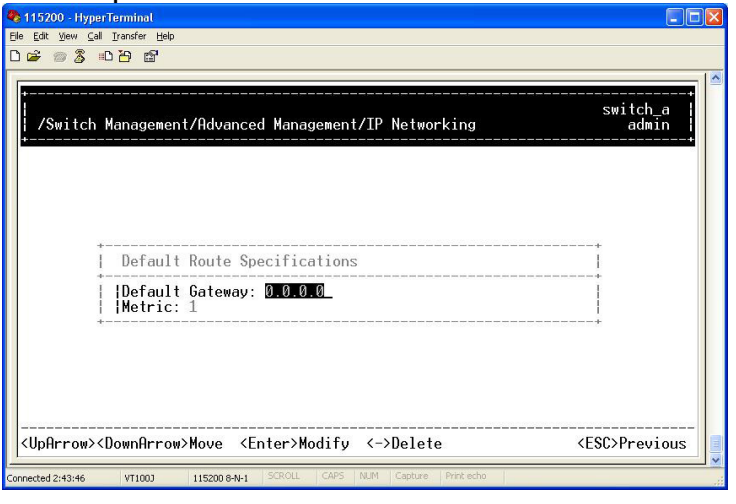
Step 6: Press <Shift> and [+] on keypad to enter **Internet Address** and **Physical Address** in the **Static ARP Specifications**.



Default Gateway

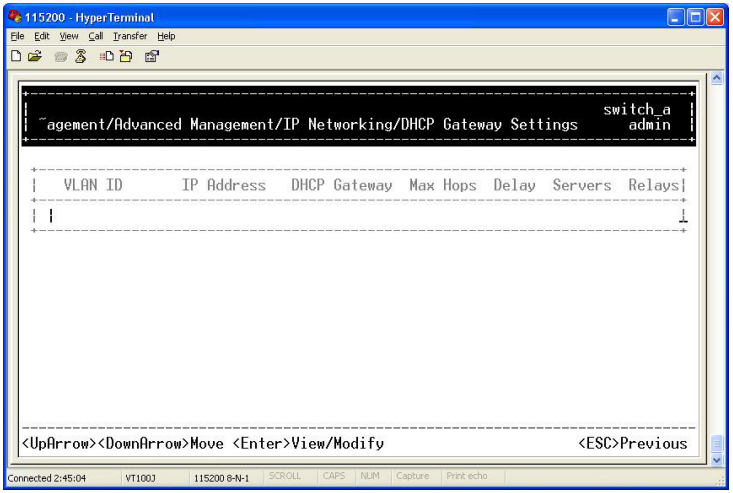
Step 7: Highlight **Default Gateway** from **IP Networking** and press <Enter>.

Step 8: Enter **Default Gateway** and **Metric** in the **Default Route Specifications**.



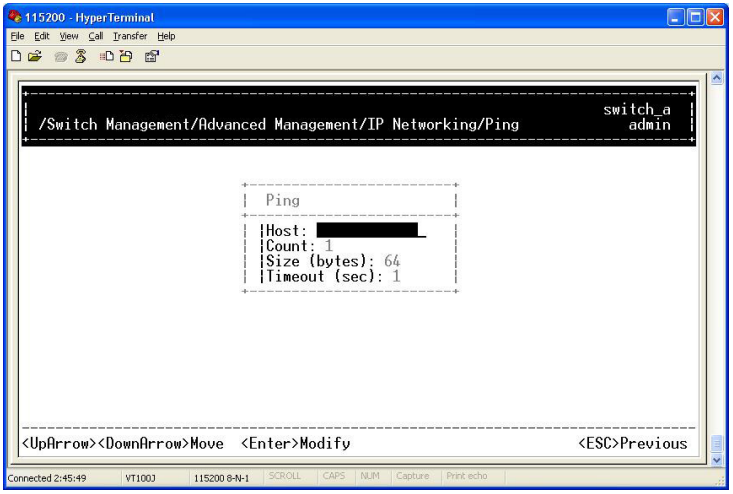
DHCP Gateway Settings

Step 7: Highlight **DHCP Gateway Settings** from **IP Networking** and press <Enter>.



Ping Settings

Step 1: Move to highlight **Ping** from **IP Networking** and press <Enter>.



Host

Step 2: Move to highlight **Host** and press <Enter>.

Step 3: Enter 4 decimal bytes (dot separated) as the IP address to ping.

Count

Step 4: Move to highlight **Count** and press <Enter>.

Step 5: Specify a packet count number from 1 to 999, or type 0 for an infinite packet count. Press <Enter>.

Size (bytes)

Step 6: Move to highlight **Size** and press <Enter>.

Step 7: Specify a packet size from 0-1500. Press <Enter>.

Timeout (sec)

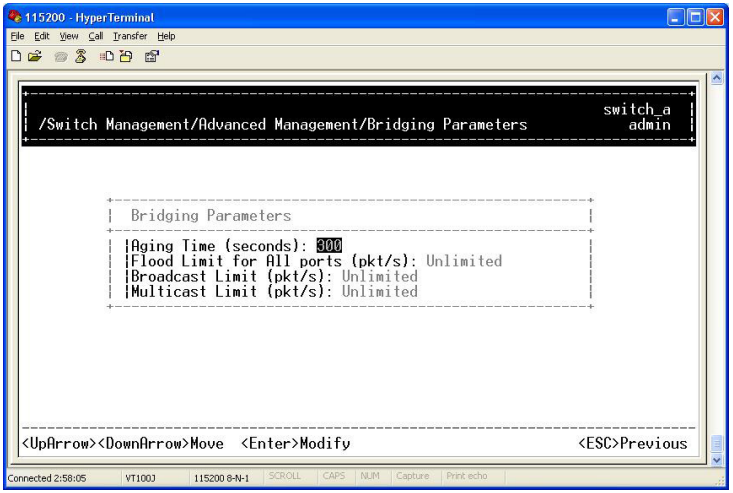
Step 8: Move to highlight **Timeout** and press <Enter>.

Step 9: Specify a timeout value from 1-999. Press <Enter>.

Step 10: Press <Esc> to start to ping when completed with the ping parameters.

BRIDGING

Step 1: Move to highlight **Bridging** from **Advanced Management** screen, and press <Enter>.



Aging Time

Step 2: Move to highlight **Aging Time** and press <Enter>.
Enter a decimal number as bridge aging period in seconds.
Or, enter 0 for no aging.

Flood Limit for All ports

Step 3: Move to highlight **Flood Limit for All ports** and press <Enter>. Choose **Unlimited** or enter a decimal number as flood limit in packets per second. Or, enter 0 for no limit.

Broadcast Limit

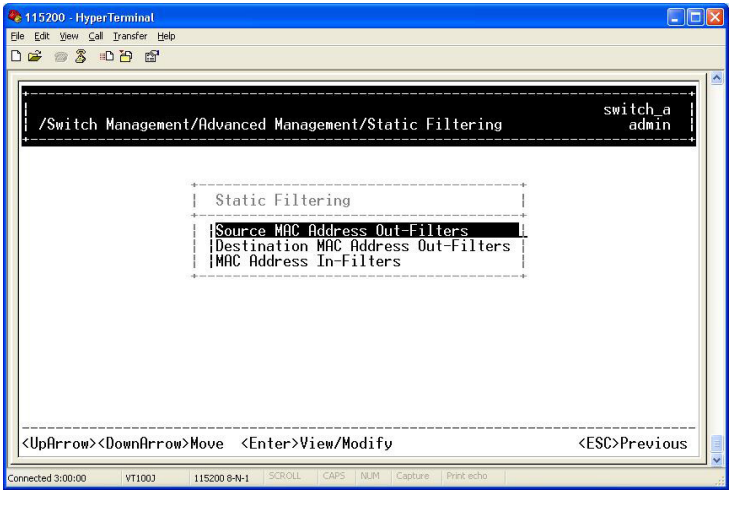
Step 4: Move to highlight **Broadcast Limit** and press <Enter>. Choose **Unlimited** or enter a decimal number as broadcast limit in packets per second. Or, enter 0 for no limit.

Multicast Limit

Step 5: Move to highlight **Multicast Limit** and press <Enter>. Choose **Unlimited** or enter a decimal number as multicast limit in packets per second. Or, enter 0 for no limit.

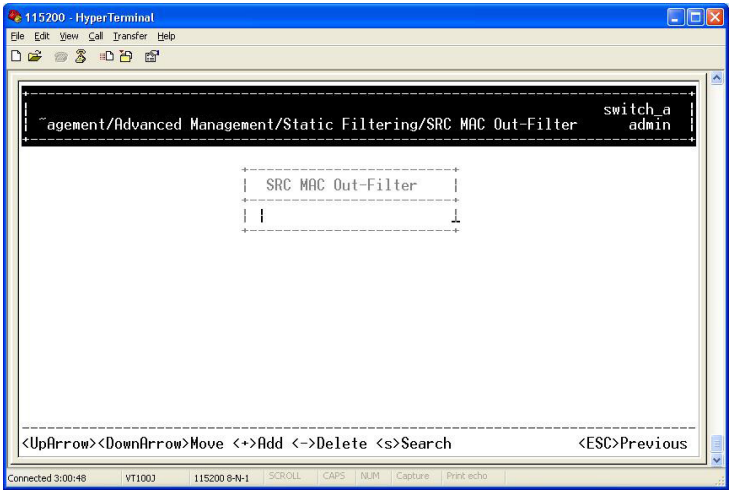
STATIC FILTERING

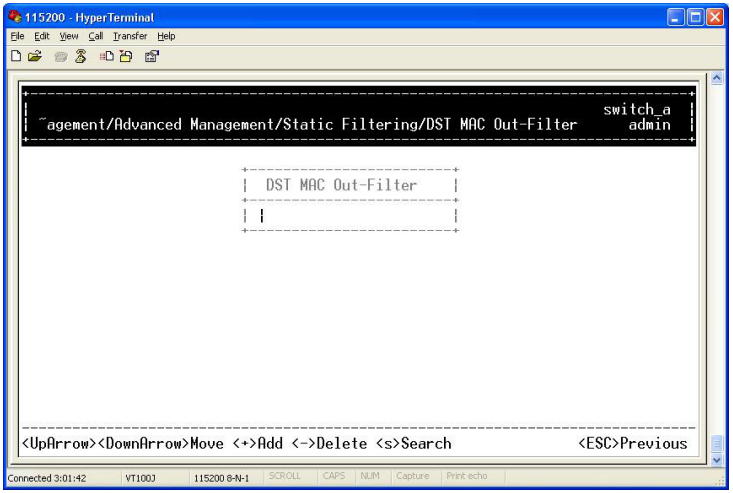
Step 1: Move to highlight **Static Filtering** from **Advanced Management** screen, and press <Enter>.



Source/Destination MAC Address Out-Filters

Step 2: Move to highlight **Source** or **Destination MAC addresses Out-Filters** for static filtering, and press <Enter>.





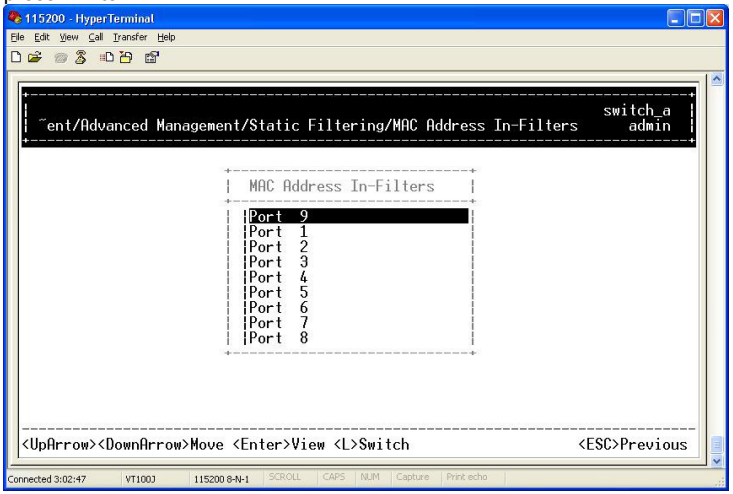
Add/Delete/Search

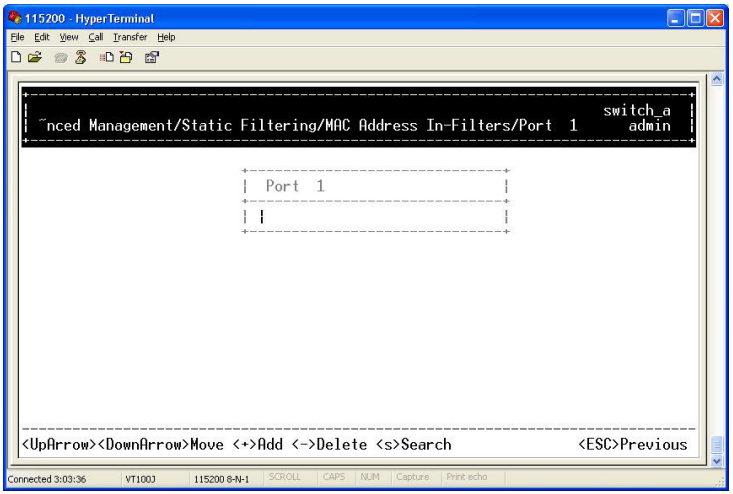
Step 3: Press [+] on keypad to add a specific MAC address to be filtered.
Press [-] to delete a specific MAC address from being filtered.
Press [S] to search through current list of MAC addresses in the static filtering database. The static filtering database maximum capacity is 64.

* No precautionary message appears before you delete a specific MAC address from being filtered.
* Be sure you want to delete it before doing so.

MAC Address In-Filters

Move to highlight **MAC Address In-Filters** from **Static Filtering** screen, and press <Enter>.





Step 1: Move to highlight a port and press <Enter>.

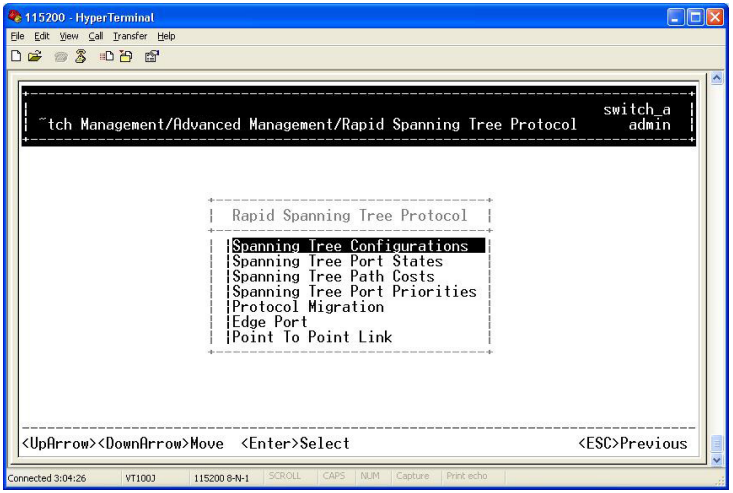
Add/Delete/Search

Step 2: Press <Shift> and [+] on keypad to add a specific MAC address to be filtered.
Press [-] to delete a specific MAC address from being filtered.
Press <S> to search through current list of MAC addresses in the static filtering database.

* No precautionary message appears before you delete a specific MAC address from being filtered.
* Be sure you want to delete it before doing so.

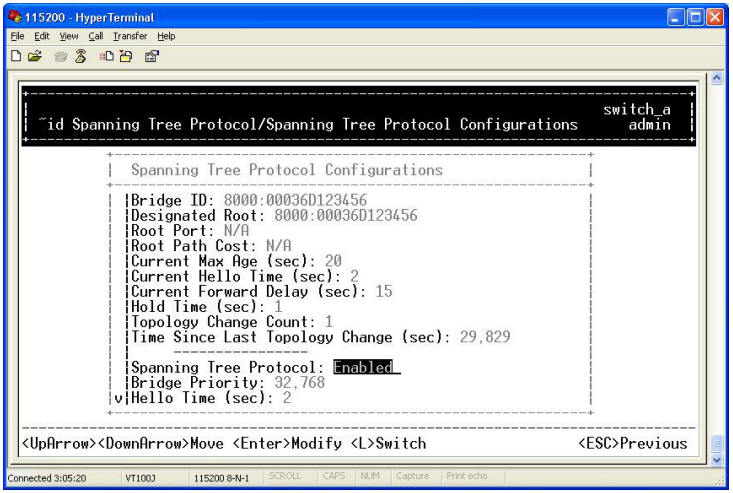
RAPID SPANNING TREE PROTOCOL

Step 1: Move to highlight **Rapid Spanning Tree** from **Advanced Management** screen, and press <Enter>.



Spanning Tree Configurations

Step 2: Move to highlight **Spanning Tree Configurations** if you want to change Spanning Tree Protocol Configurations.



Spanning Tree Protocol

Step 3: Press <Enter> to enter **Spanning Tree Options**.
Decide to have it Disabled or Enabled.

Bridge Priority

Step 4: Move to highlight **Bridge Priority** and press <Enter>.
Type a decimal number for the bridge priority and press <Enter>.

Hello Time (sec)

Step 5: Move to highlight **Hello Time** and press <Enter>.
Type a decimal number for the hello time and press <Enter>.

Max Age (sec)

Step 6: Move to highlight **Max Age** and press <Enter>.
Type a decimal number for the max age.

Forward Delay (sec)

Step 7: Move to highlight **Forward Delay** and press <Enter>.
Type a decimal number for the forward delay.

STP Version

Step 8: Move to highlight **STP Version** and press <Enter>.
Choose **STP Compatible** or **RSTP** and press <Enter>.

Tx Hold Count

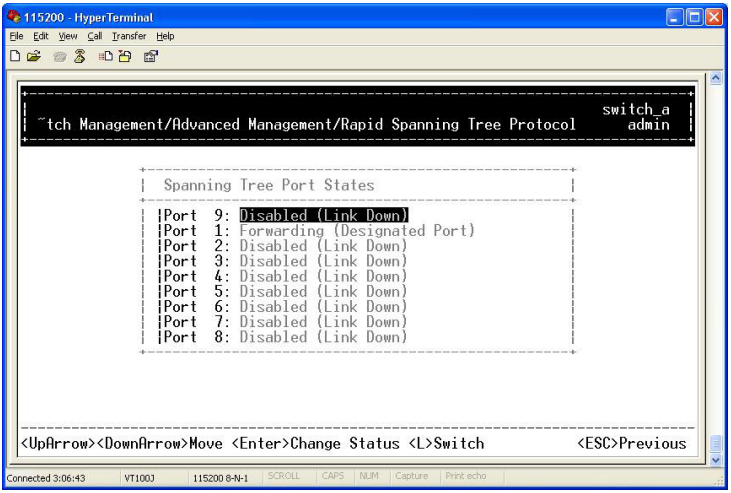
Step 9: Move to highlight **Tx Hold Count** and press <Enter>.
Type a decimal number for the Tx Hold Count.

Path Cost Default

Step 10: Move to highlight **Path Cost Default** and press <Enter>.
Choose **16-bit** or **32-bit** and press <Enter>.

Spanning Tree Port States

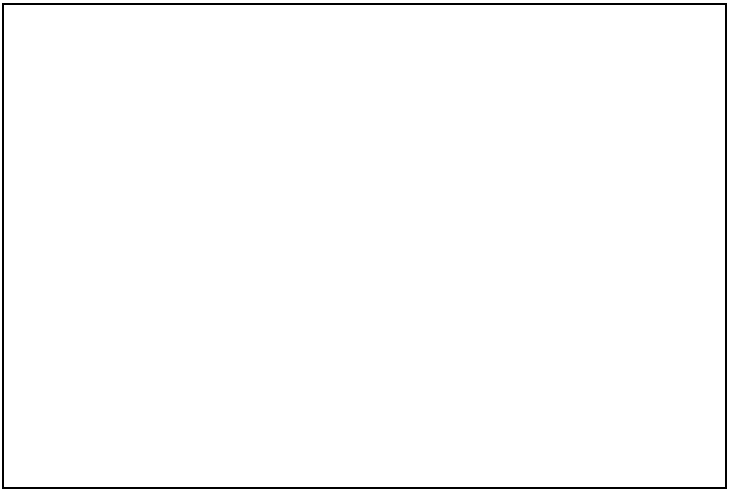
Step 1: Move to highlight **Spanning Tree Port States** if you want to change per port administration status, and press <Enter>.



Step 2: Move to highlight a port if you want to **Enable** or **Disable** its administration status, and press <Enter>.

Spanning Tree Path Costs

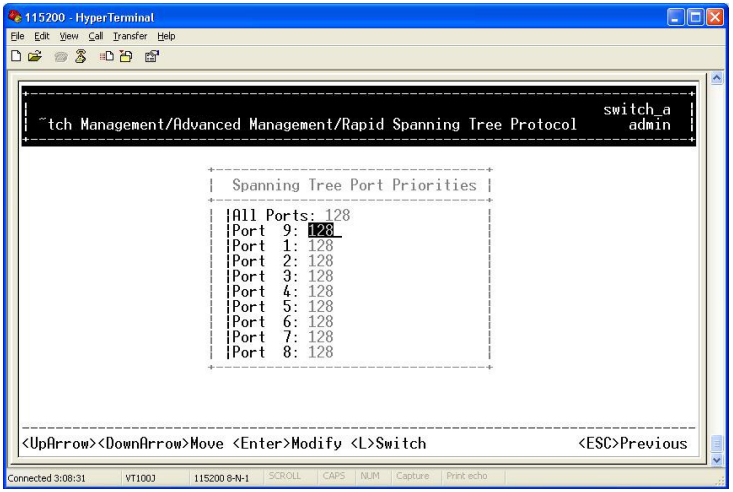
Step 1: Move to highlight **Spanning Tree Path Costs** if you want to change the path cost, and press <Enter>.



Step 2: Move to highlight **All Ports** or each port individually, and press <Enter>. For new path cost, type a decimal number and press <Enter>.

Spanning Tree Port Priorities

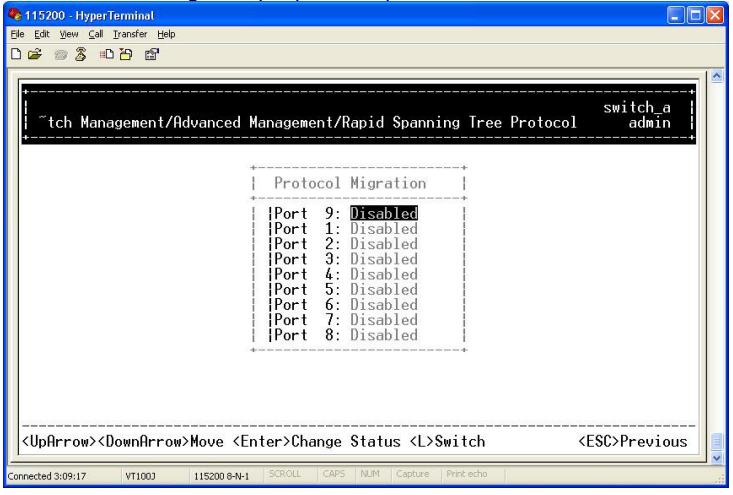
Step 1: Move to highlight **Spanning Tree Port Priorities** if you want to change the priority level per port, and press <Enter>.



Step 2: Move to highlight **All Ports** or each port individually, and press <Enter>. For new priority value, type a decimal number from 0-240, and press <Enter>. A low value gives the port a greater likelihood of becoming a Root port.

Protocol Migration

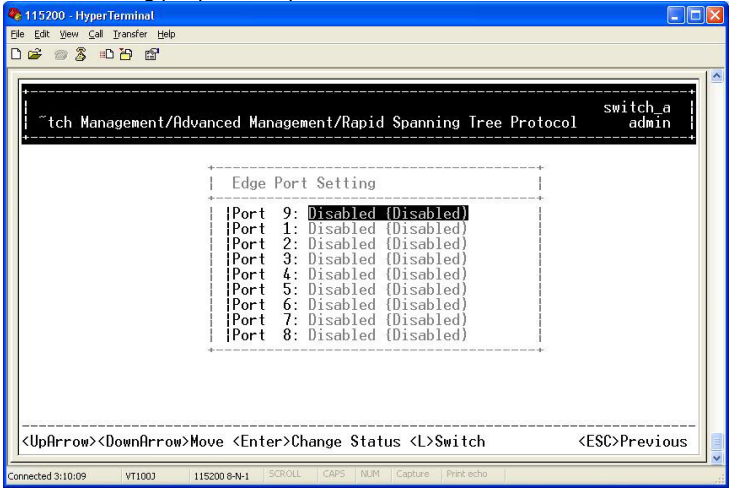
Step 1: Move to highlight **Protocol Migration** if you want to change the Protocol Migration per port, and press <Enter>.



Step 2: Move to highlight each port individually, and press <Enter> to **Enable** or **Disable** Protocol Migration.

Edge Port

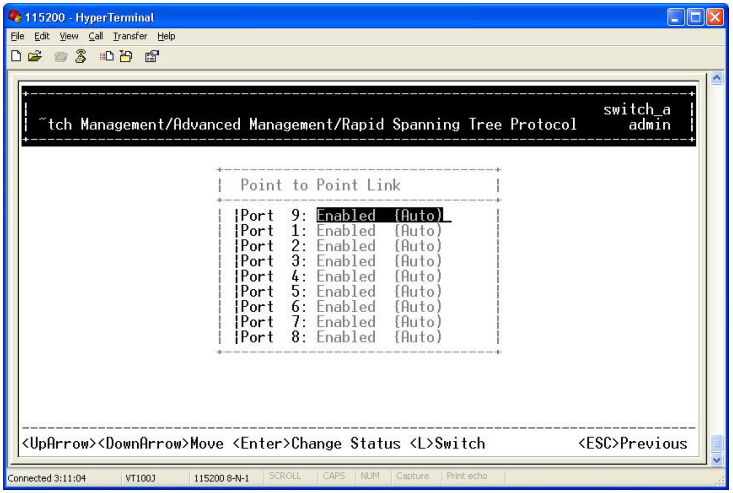
Step 1: Move to highlight **Edge Port** if you want to change the Edge Port Setting per port, and press <Enter>.



Step 2: Move to highlight each port individually, and press <Enter> to **Enable** or **Disable** Edge Port Setting.

Point To Point Link

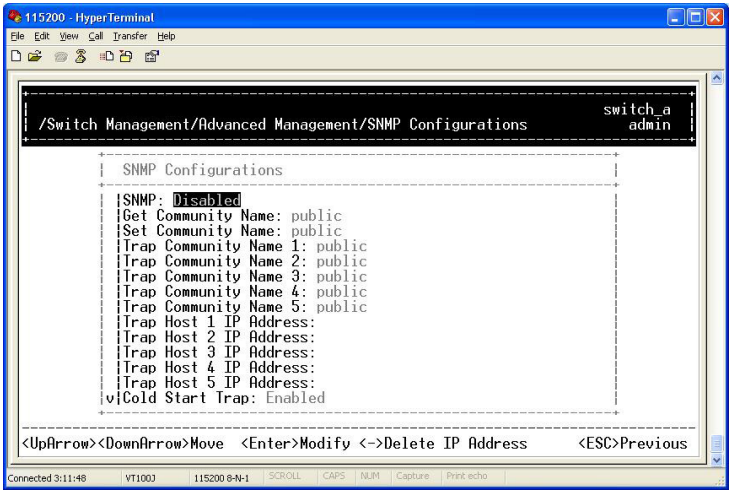
Step 1: Move to highlight **Point To Point Link** if you want to change the Point To Point Link Options per port, and press <Enter>.



Step 2: Move to highlight each port individually, and press <Enter> to choose **Enable, Disable**, or **Auto** Point To Point Link.

SNMP FUNCTIONS

Step 1: Move to highlight **SNMP** from **Advanced Management** screen, and press <Enter>.



SNMP Options
Step 2: Move to highlight **SNMP** and press <Enter>.
Decide to have it **Disabled** or **Enabled**.

Get Community Name
Step 3: Move to highlight **Get Community Name** and press <Enter>.
Enter text and press <Enter>.

Set Community Name
Step 4: Move to highlight **Set Community Name** and press <Enter>.
Enter text and press <Enter>.

Trap Community Name
Step 5: Move to highlight **Trap Community Name 1** and press <Enter>.
Enter text and press <Enter>.
Repeat to specify up to four more trap community names.

Trap Host IP Address
Step 6: Move to highlight **Trap Host 1 IP Address** and press <Enter>.
Type an IP address for trap host 1 and press <Enter>
Repeat to specify up to four more trap host IP addresses

Cold Start Trap
Step 7: Move to highlight **Cold Start Trap** and press <Enter>.
Decide to have it **Disabled** or **Enabled**.

Warm Start Trap
Step 8: Move to highlight **Warm Start Trap** and press <Enter>.
Decide to have it **Disabled** or **Enabled**.

Link Down Trap
Step 9: Move to highlight **Link Down Trap** and press <Enter>.
Decide to have it **Disabled** or **Enabled**.

Link Up Trap
Step 10: Move to highlight **Link Up Trap** and press <Enter>.
Decide to have it **Disabled** or **Enabled**.

Authentication Failure Trap
Step 11: Move to highlight **Authentication Failure Trap** and press <Enter>.
Decide to have it **Disabled** or **Enabled**.

Rising Alarm Trap
Step 12: Move to highlight **Rising Alarm Trap** and press <Enter>.
Decide to have it **Disabled** or **Enabled**.

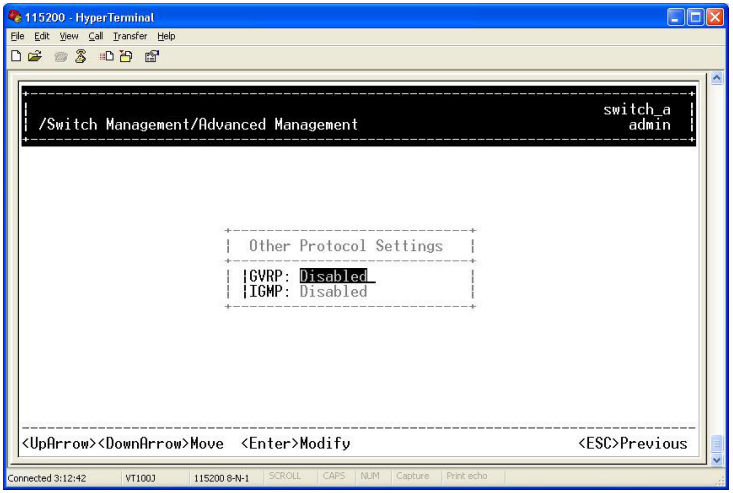
Falling Alarm Trap
Step 13: Move to highlight **Falling Alarm Trap** and press <Enter>.
Decide to have it **Disabled** or **Enabled**.

Topology Change Trap

Step 14: Move to highlight **Topology Change Trap** and press <Enter>. Decide to have it **Disabled** or **Enabled**.

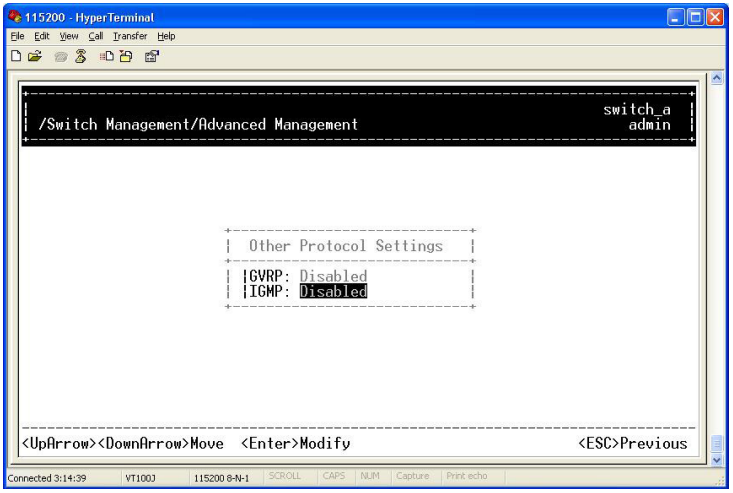
OTHER PROTOCOLS

Step 1: Move to highlight **Other Protocols** from **Advanced Management** screen, and press <Enter>.



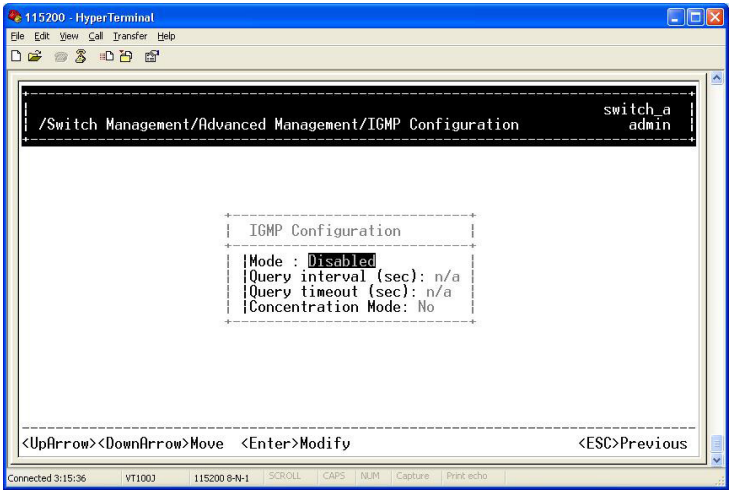
GVRP

Step 2: Move to highlight **GVRP** and press <Enter>. Decide to have it **Disabled** or **Enabled**.



IGMP

Step 3: Move to highlight **Mode** and press <Enter>.
Decide to have it **Disabled** or set in either **Passive** or **Active** mode.

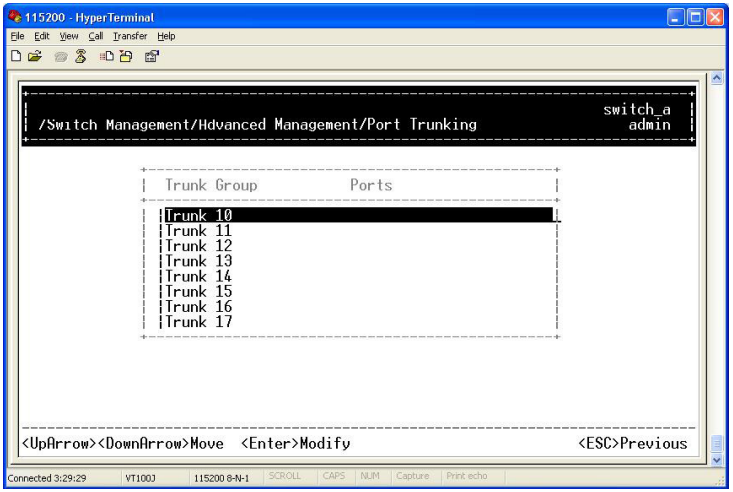


CONCENTRATION MODE

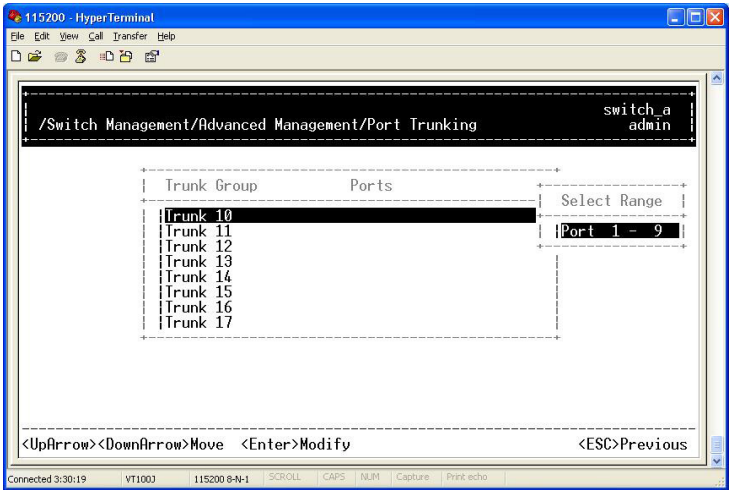
Step 4: Move to highlight **Concentration Mode** and press <Enter>.
Decide to have it **Disabled** or **Enabled**.

PORT TRUNKING

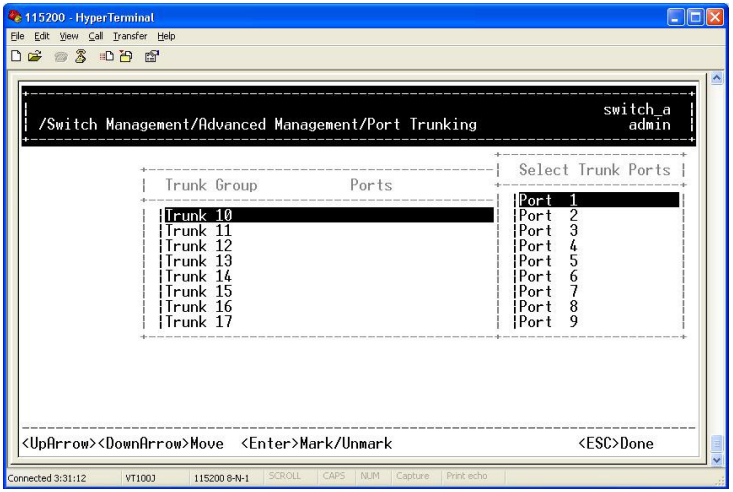
Step 1: Move to highlight **Port Trunking** from **Advanced Management** screen, and press <Enter>.



Step 2: Move to highlight a trunk group to which you want to assign ports, and press <Enter> to enter **Select Range**.



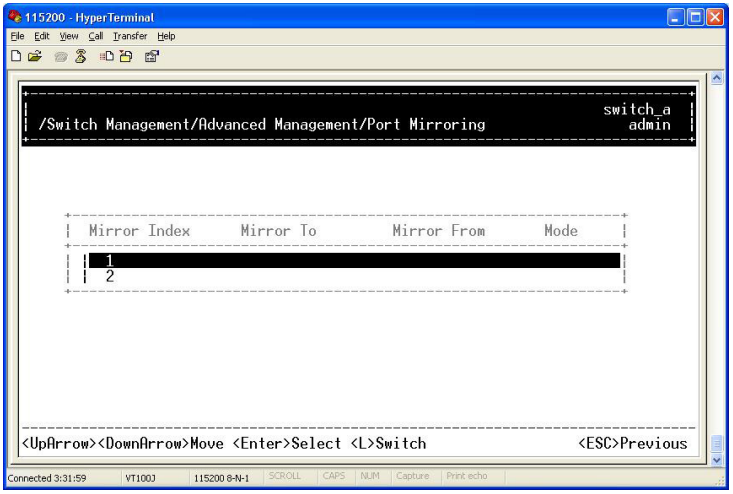
Step 3: Press <Enter> to select each trunk port.



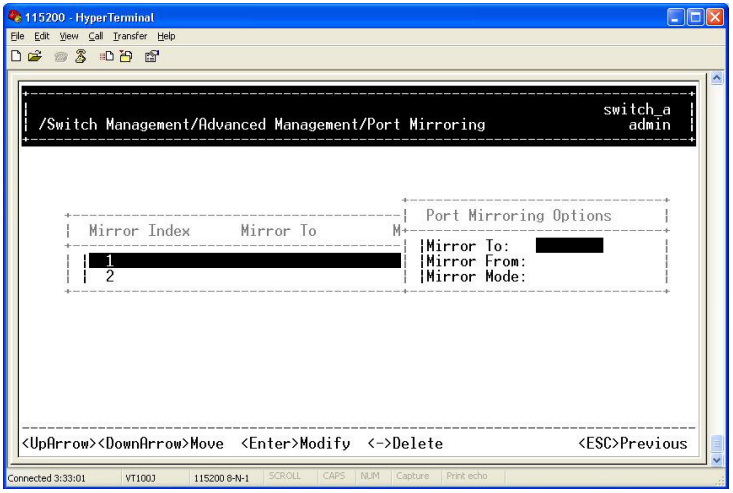
Step 4: Press <Esc> when completed with selecting ports.

PORT MIRRORING

Step 1: Move to highlight **Port Mirroring** from **Advanced Management** screen, and press <Enter>.



Step 2: Press <Enter> to enter **Port Mirroring Options**.



Mirror To

Step 3: Press <Enter> to enter **Mirror To Options**, listing the ports that can be mirrored to.

Step 4: Move to highlight the port you want to mirror to and press <Enter>.

Mirror From

Step 5: Press <Enter> to enter **Mirror From Options**, listing the ports that can be mirrored from.

Step 6: Move to highlight the port you want to mirror from and press <Enter>.

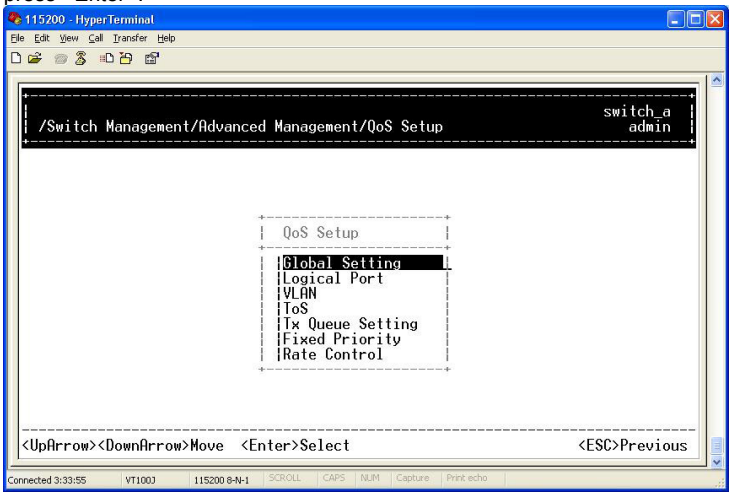
Mirror Mode

Step 7: Move to select **Mirror Mode**. From **Mode Options**, decide whether the port to be mirrored from will be receiving or transmitting.

Step 8: Press <Esc> when completed.

QOS SETUP

Move to highlight **QoS Setup** from **Advanced Management** screen, and press <Enter>.



Global Setting

Step 1: Move to highlight **Global Setting** and press <Enter>.

Step 2: Move to highlight **QoS Status** and press <Enter>. Move to highlight to enable or disable **QoS Status** and press <Enter>.

Step 3: Move to highlight **Diffserv Expedite Forwarding** and press <Enter>. Move to highlight to enable or disable **Diffserv Expedite Forwarding** and press <Enter>.

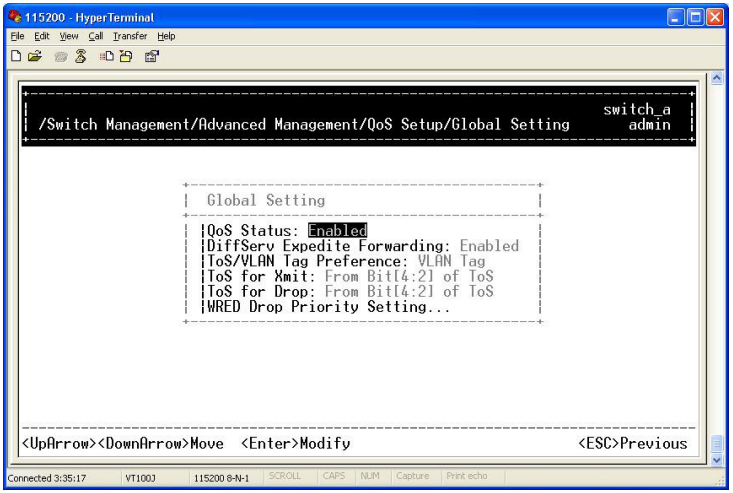
Step 4: Move to highlight **ToS/VLAN Tag Preference** and press <Enter>. Highlight the **VLAN Tag** or **ToS** then press <Enter>.

Step 5: Move to highlight **ToS for Xmit** and press <Enter>. Highlight the desired setting then press <Enter>.

Step 6: Move to highlight **ToS for Drop** and press <Enter>. Highlight the desired setting then press <Enter>.

Step 7: Move to highlight **WRED Drop Priority Setting** and press <Enter>. Move to highlight to **Low Drop Percentage** or **High Drop Percentage** and press <Enter>.

Step 8: Press <Esc> when completed.



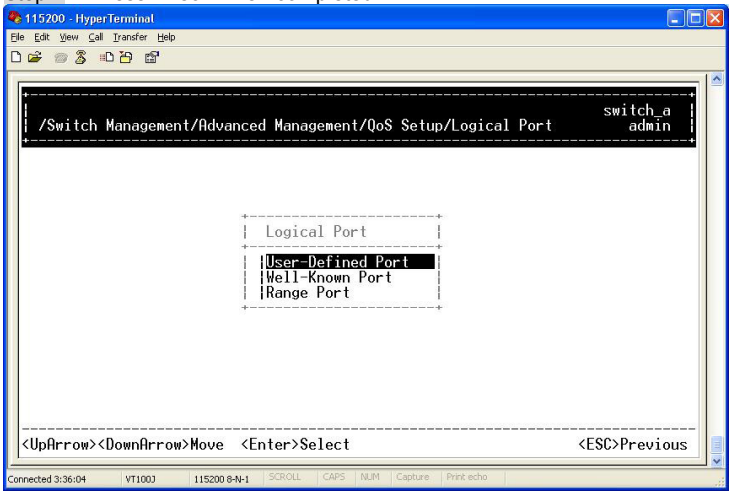
Logical Port

Step 1: Move to highlight **Logical Port** and press <Enter>.

Step 2: Move to highlight **User Define Port**, **Well-Known Port**, or **Range Port** and press <Enter>.

Step 3: Move to highlight the appropriate port and press <Enter>.

Step 4: Press <Esc> when completed.

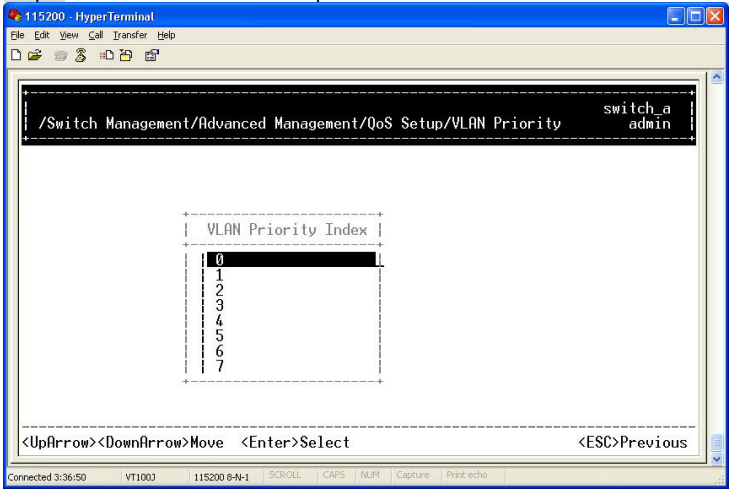


VLAN

Step 1: Move to highlight **VLAN** and press <Enter> to specify the QoS VLAN priority.

Step 2: Move to highlight any **VLAN Priority Index** and press <Enter>. Move to highlight **Drop Priority** or **Transmit Priority** and press <Enter> in the **VLAN Priority Setting** screen.

Step 3: Press <Esc> when completed.

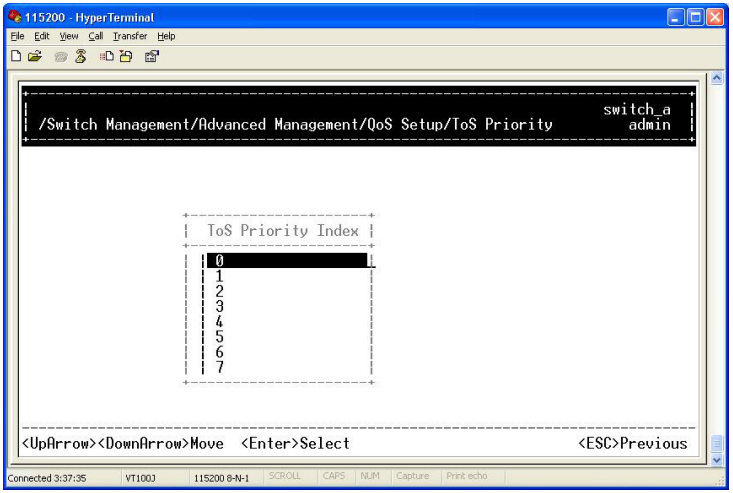


ToS

Step 1: Move to highlight **TOS** and press <Enter> to specify the ToS priority.

Step 2: Move to highlight any **ToS Priority Index** and press <Enter>. Move to highlight **Drop Priority** or **Transmit Priority** and press <Enter> in the **ToS Priority Setting** screen.

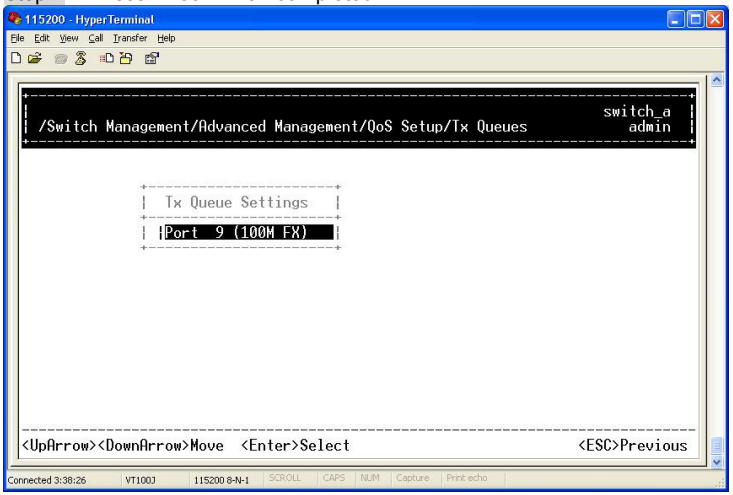
Step 3: Press <Esc> when completed.



Tx Queue Setting

Step 1: Move to highlight **Tx Queue Setting** and press <Enter>.

Step 2: Press <Esc> when completed.

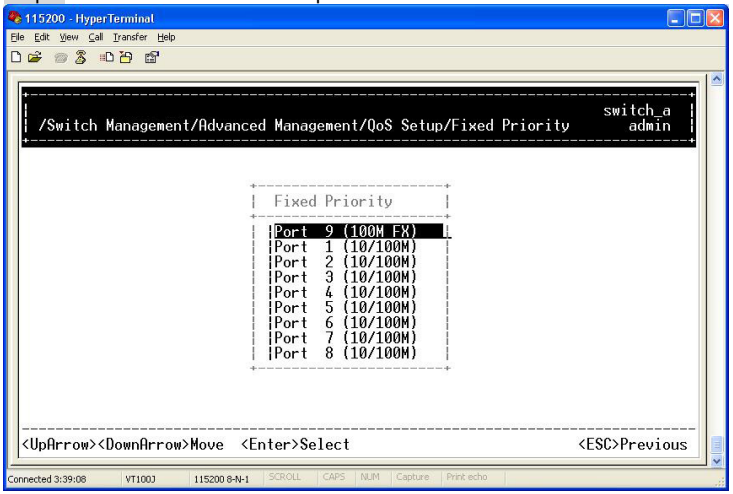


Fixed Priority

Step 1: Move to highlight **Fixed Priority** and press <Enter> to specify the Fixed Priority.

Step 2: Move to highlight any port in the **ToS Priority** screen and press <Enter>. Move to **Fixed Drop Priority, Transmit Priority**, or **Priority**.

Step 3: Press <Esc> when completed.

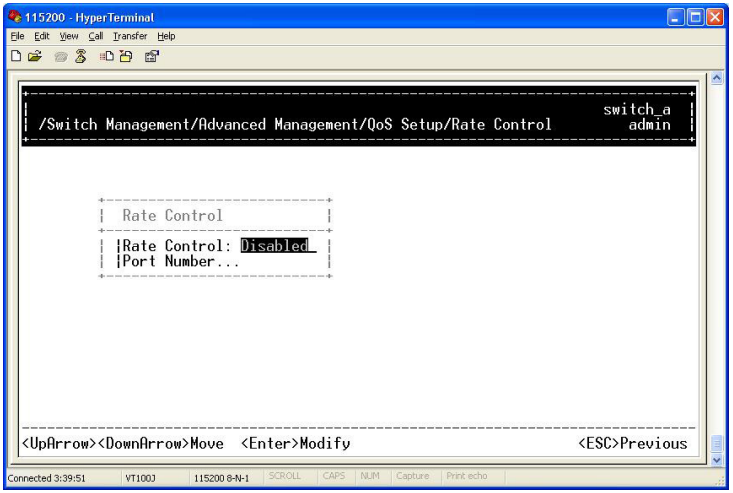


Rate Control

Step 1: Move to highlight **Rate Control** and press <Enter> to specify rate control parameters.

Step 2: Move to highlight **Rate Control**, or **Port Number** and press <Enter>.

Step 3: Press <Esc> when completed.

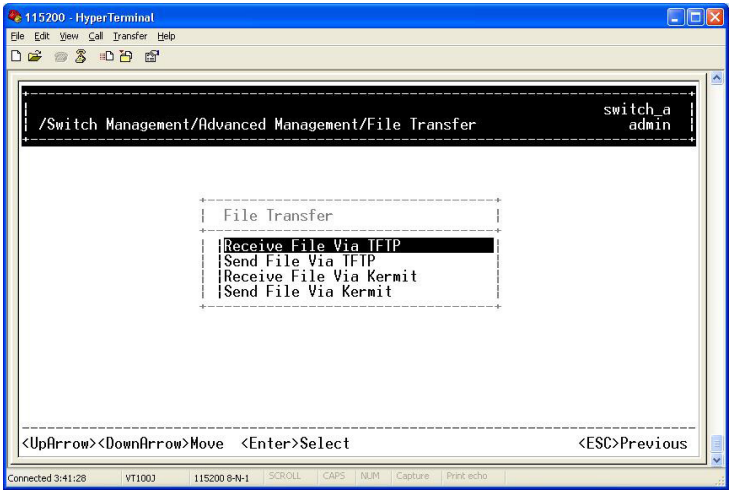


FILE TRANSFER

The TFTP protocol is used to upload software to the switch and download software from the switch.

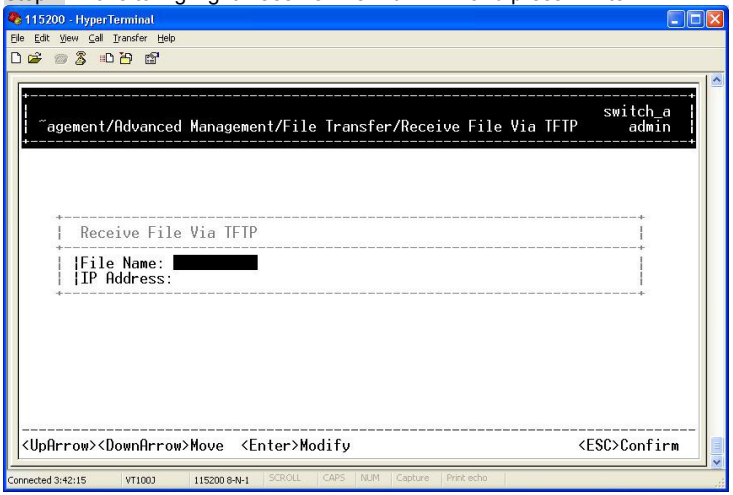
A VLAN with the proper IP address and routing path to the TFTP server must be configured for the switch to access the specified TFTP server.

Step 1: Move to highlight **File Transfer** from **Advanced Management** screen, and press <Enter>.



Receive File Via TFTP

Step 2: Move to highlight **Receive File Via TFTP** and press <Enter>.



Step 3: If the default **File Name** is not the one you intend to receive, press <Enter>. Type the name of the file you intend to receive and press <Enter>.

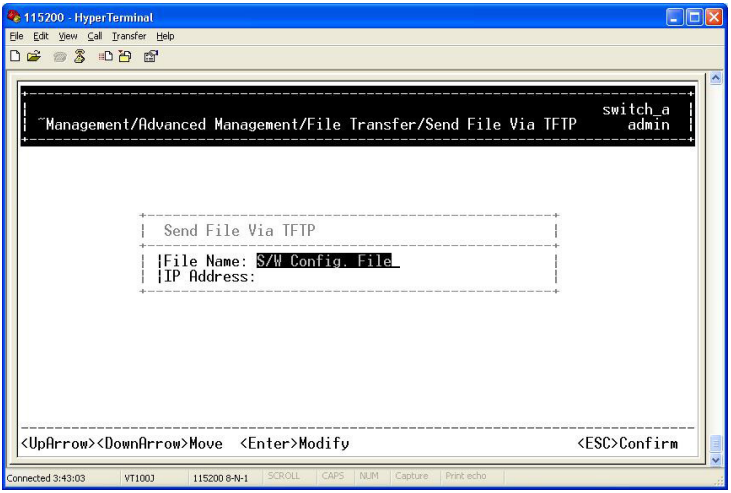
Step 4: Move to highlight **IP Address** and press <Enter>.
Type the IP address from where the file will be obtained.

Step 5: Press <Esc> when completed.

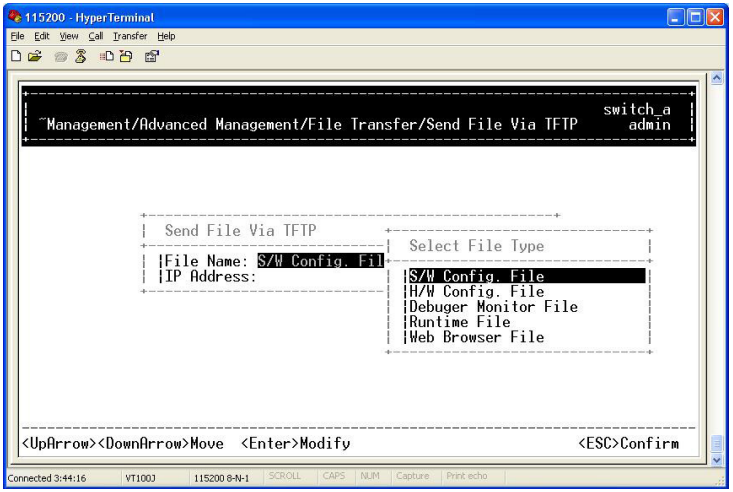
Step 6: A dialog box appears to ask if you want to transfer file now.
Highlight [Yes] and press <Enter> to start file transfer.
Or move to highlight [No] and press <Enter> to deny it.
Or press <Esc> to exit.

Send File Via TFTP

Step 7: Move to highlight **Send File Via TFTP** and press <Enter>.



Step 8: If the default **File Type** is not the one you intend to send, press <Enter>. Select the file type you intend to send and press <Enter>.



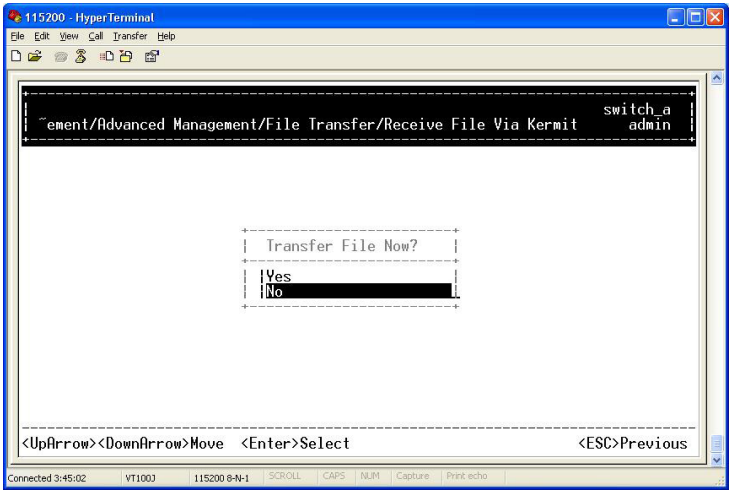
Step 9: Repeat Step 4-6.

Receive File Via Kermit

Step 10: In **File Transfer** screen obtained via console port, move to highlight **Receive File Via Kermit** and press <Enter>.

Step 11: A dialog box appears to ask if you want to transfer file now. Move to highlight [Yes] and press <Enter> to start file transfer. Otherwise, highlight [No] and press <Enter> to deny it.

Step 12: Press <Esc> to a previous screen.

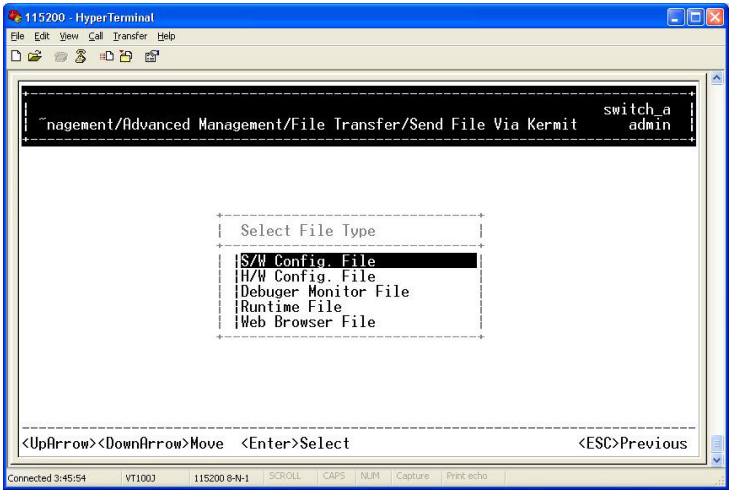


Send File Via Kermit

Step 13: In **File Transfer** screen obtained via console port, move to highlight **Send File Via Kermit** and press <Enter>.

Step 14: Move to highlight a file type you intend to send and press <Enter>.

Step 15: A dialog box appears to ask if you want to transfer file now. Move to highlight [Yes] and press <Enter> to start file transfer. Otherwise, highlight [No] and press <Enter> to deny it.



Step 16: Press <Esc> to a previous screen.

Logout

To log out, highlight [Logout] from [Switch Management] screen and press <Enter>. Please remember to save settings you have changed before you log out.

Save Settings

To save the current settings and remain in the configuration program, highlight [Save Settings] from [Switch Management] and press <Enter>.

Restore Default Settings

To restore the factory default settings, highlight [Restore Default Settings] from [Switch Management] and press <Enter>.

The switch will be rebooted after confirming Yes as to restore the default settings.

Reboot

To reboot the switch, highlight [Reboot] from [Switch Management] and press <Enter>.

Web-Based Browser Management

The switch provides a web-based browser interface for configuring and managing the switch. This interface allows you to access the switch using a preferred web browser.

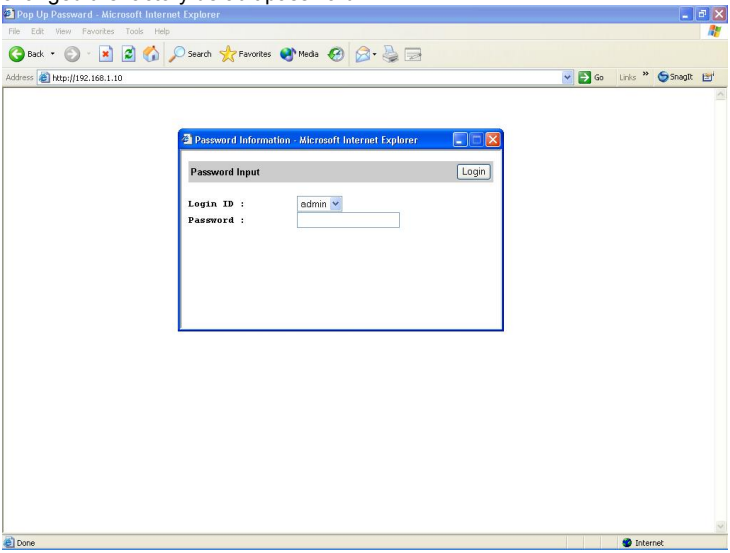
This chapter describes how to configure the switch using its web-based browser interface.

Logging on to the switch

SWITCH IP ADDRESS
In your web browser, specify the IP address of the switch.

LOGIN ID
Enter the factory default login ID: **admin**.

PASSWORD
Enter the factory default password (no password, **press Enter directly**).
Or enter a user-defined password if you followed the instructions later and changed the factory default password.



Understanding the Browser Interface

The web browser interface provides three point-and-click buttons at the upper field of the screen for configuring and managing the switch.

In addition, you can click any port on the switch image to view the switch's current speed, duplex, and activity status.

The **Basic Setup/General** parameters appear at the lower field of the screen. These parameters can also be displayed by clicking **Basic Setup** button and select **General** in sub-menu.

FILE
Save settings configured in the browser interface / upload software via TFTP / download software via TFTP / reboot the switch / logout of the browser interface.

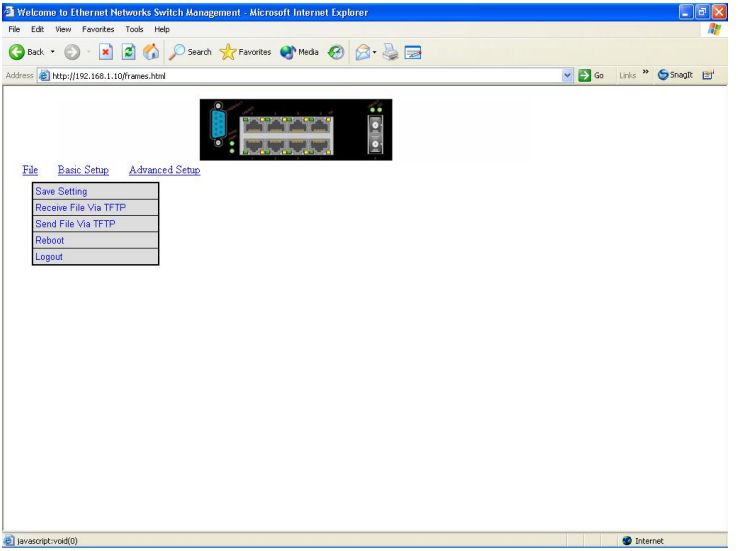
BASIC SETUP
Perform general, LAN port, and console port activities.

ADVANCED SETUP
Perform MAC Address Management / IP Networking / Port Perspective / Bridging / Static MAC Filters / IP Multicast Group / VLAN & PVID Perspective / RSTP / SNMP / Other Protocols / Port Trunking / QoS / Port Mirroring.

Performing File Activities

To perform File Activities:

Click the **File** button at the upper field of the main display, the menu options appear.



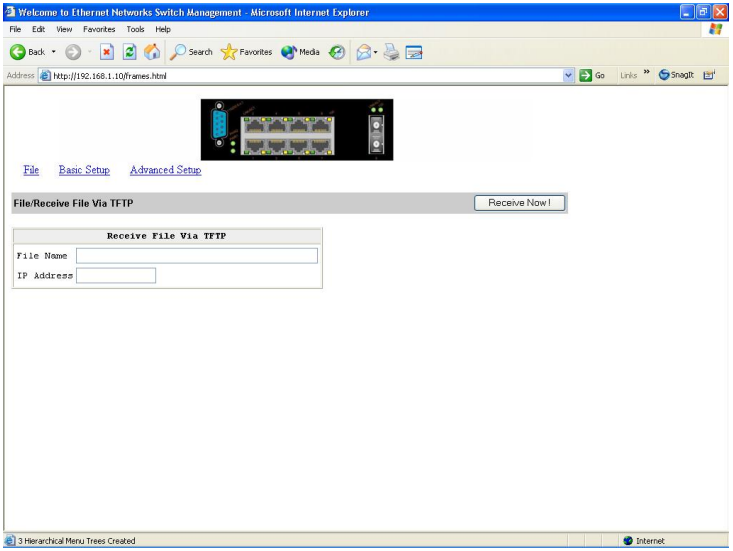
Saving Setting

Step 1: Click **Saving Setting** to save your configuration settings.

Step 2: When you click it, a message asks "**Are you sure you want to save setting?** ", click **OK** to save it or **Cancel** to abort it.

Receive File Via TFTP

Step 1: Click **Receive File Via TFTP** on the **File** display.



<Note> The TFTP protocol is used to upload software to the switch. A VLAN with the proper IP address and routing path to the TFTP server must be configured for the switch to access the specified TFTP server.

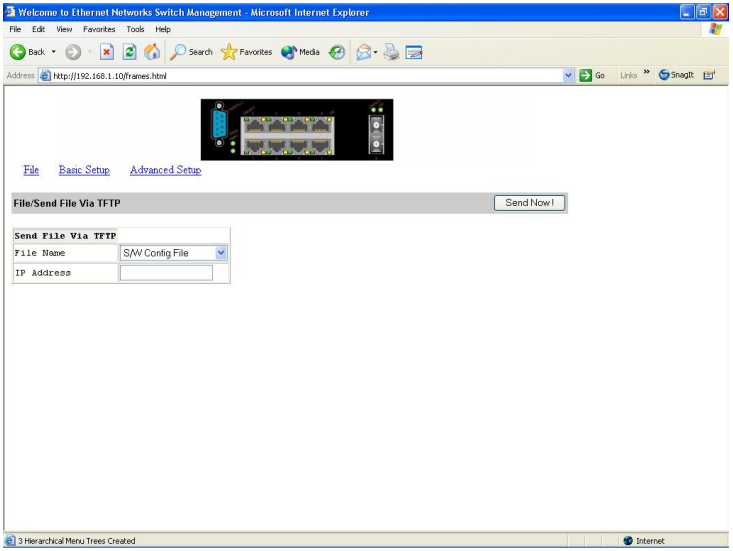
Step 2: For **File Name**, type the name of the file you intend to receive.

Step 3: For **IP Address**, type the IP address from where the file will be obtained.

Step 4: Click **Receive Now!**.

Send File Via TFTP

Step 1: Click **Send File Via TFTP** on the **File** display.



Step 2: For **File Name**, choose the file you intend to send.

Step 3: For **IP Address**, type the IP address you intend to send to.

Step 4: Click **Send Now!**.

Reboot

Step 1: Click **Reboot** on the **File** display.

Step 2: When you click it, a message asks "**Are you sure you want to save setting?** ", click **OK** to save it or **Cancel** to abort it.

Logout

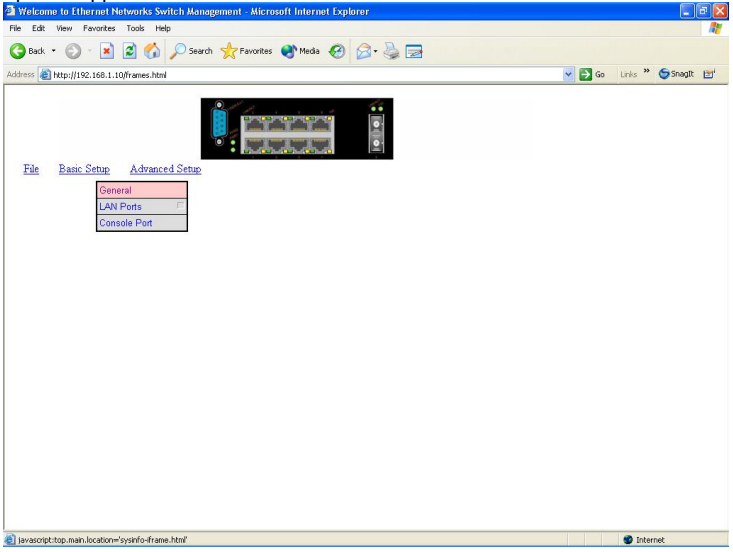
Step 1: Click **Logout** on the **File** display.

Step 2: When you click it, a message asks "**Are you sure you want to save setting?** ", click **OK** to save it or **Cancel** to abort it.

Performing Basic Setup Activities

To perform Basic Setup Activities:

Click the **Basic Setup** button at the upper field of the main display, the menu options appear.



General Management Configuration

Step 1: Click **General** and the screen shows the Basic Setup/General parameters. The screen here is the same when you first access the switch browser interface.

System Name

Step 2: Click in **System Name** text box on the field of **Basic Setup/General**.

Step 3: Type a system name if it is blank, or replace the current system name with a new one.

Location

Step 4: Click in **Location** text box on the field of **Basic Setup/General**.

Step 5: Type a location name if it is blank, or replace the current location name with a new one.

Statistic Collection

Step 6: To enable or disable statistics collection at the switch, click the appropriate option from **Statistic Collection** drop-down menu.

Reboot-On-Error

Step 7: To allow or prevent the switch from rebooting when a fatal error is detected, click the appropriate option from **Reboot-On-Error** drop-down menu.

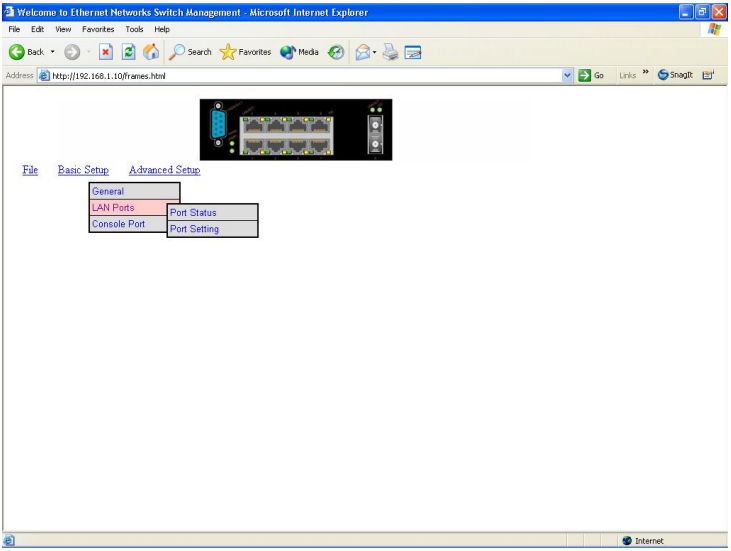
Remote Telnet Login

Step 8: To enable or disable access to the switch management program via Telnet, click the appropriate option from **Remote Telnet Login** drop-down menu.

Step 9: Click **Update Setting**. A confirmation window appears.

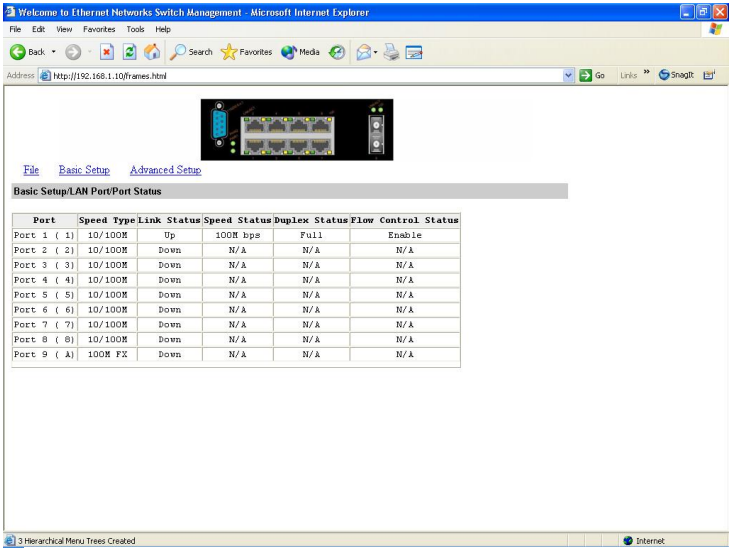
LAN Ports Configuration

Step 1: To access the LAN configuration parameters, click **Basic Setup** button first and then point to **LAN Ports** and click a suitable option.



Port Status

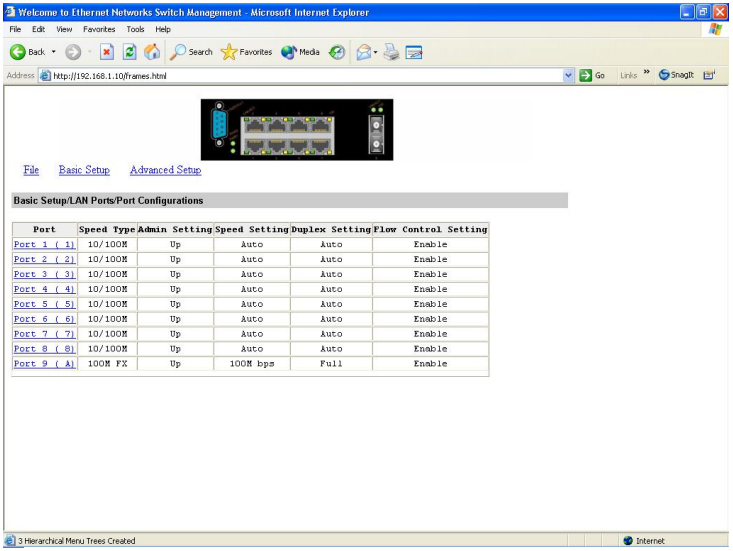
Step 2: Click **Port Status** to view the Speed Type, Link Status, Speed Status, Duplex Status, and Flow Control Status for all ports.



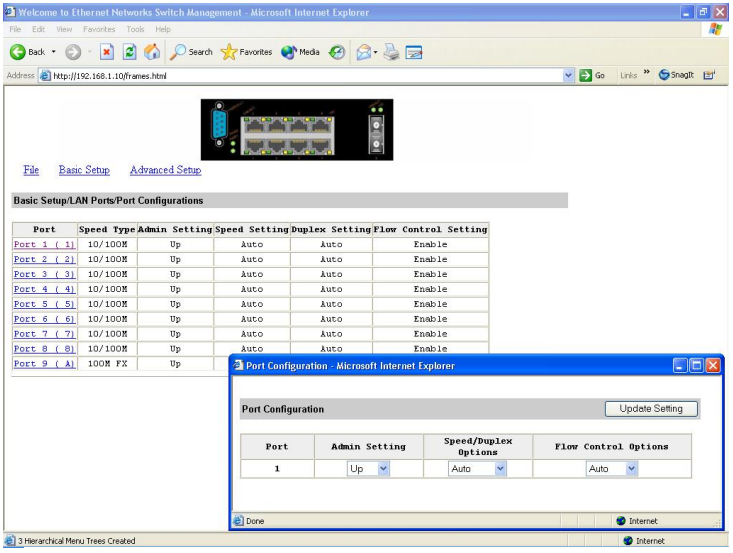
<Note> The information displayed automatically updates every 15 seconds, without requiring you to refresh the window.

Port Setting

Step 3: Click **Port Setting** to access the configuration information for all ports.



Step 4: In the **Port** column, click the port you want to configure. E.g. click Port 1.



Step 5: Click the drop-down menu under **Admin Setting**, decide to disable or enable it.

<Note> Disable: places the port in DOWN state. In this state, packets cannot be switches to and from the port.
Enable: places the port in UP state. In this state, packets can be switched to and from the port.

Step 6: Click the drop-down menu under **Speed/Duplex Options** if you want to change the line speed and duplex settings.

<Note> Auto: allows the switch to automatically ascertain the line speed and duplex mode.
All the other selections force the port to use a specific line speed and duplex mode.
'HD' denotes half-duplex mode; FD denotes full-duplex mode.

Step 7: Click the drop-down menu under **Flow Control Options** if you want to configure the flow control for this port.

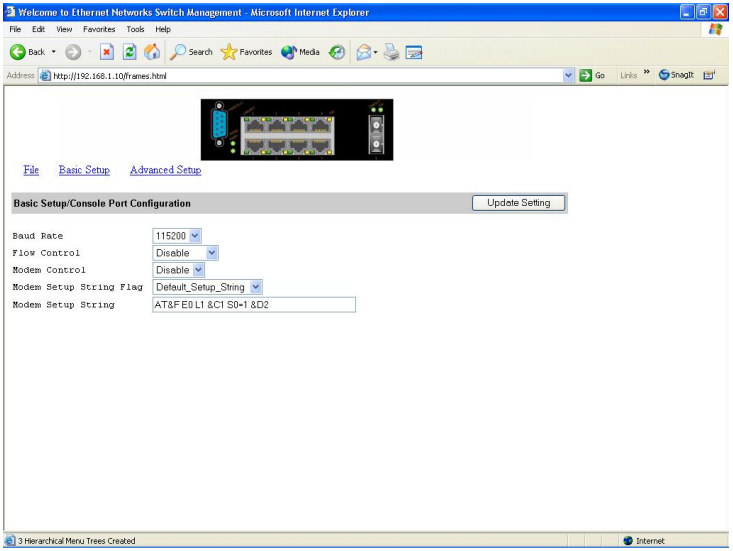
<Note> Auto: allows the switch to automatically ascertain whether or not to use flow control.
Disable: turns off flow control at all times.
Enable: turns on flow control at all times.

Step 8: Click **Update Setting** when completed. A confirmation window appears.

<Note> For your convenience, click the LEDs on the image of the switch and view its current speed, duplex, and link activity.

Console Port Configuration

Step 1: To access the console port configuration parameters, click **Basic Setup** button first and then click **Console Port**.



Baud Rate

Step 2: Click an appropriate speed from **Baud Rate** drop-down menu on the field of **Basic Setup/Console Port Configuration**.

<Note> Auto: allows the switch to autobaud between 9600bps and 115,200bps
All the other selections force a specific console baud rate.

Flow Control

Step 3: Click a flow control method from **Flow Control** drop-down menu.

Modem Control

Step 4: Click an appropriate option from **Modem Control** drop-down menu to disable or enable a modem connection to the console port.

Modem Setup String Flag

Step 5: If you enabled a modem connection to the console port, click in **Modem Setup String Flag** drop-down menu to decide whether you want to use a Default_Setup_String or Custom_Setup_String.

Modem Setup String

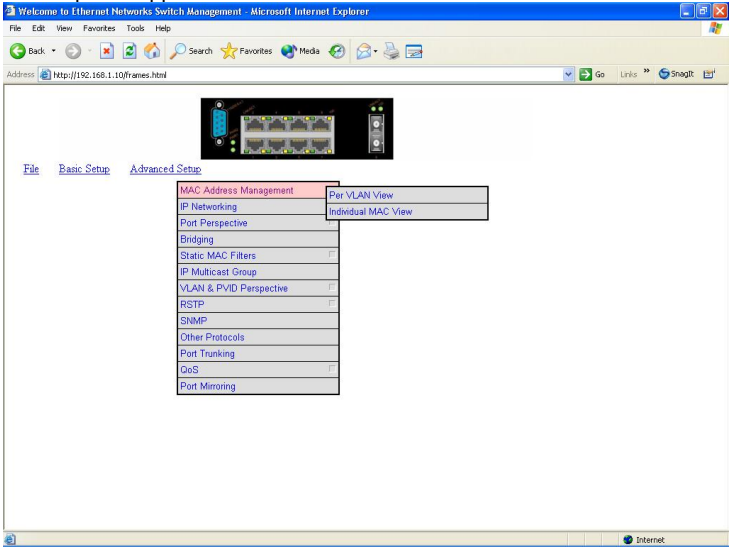
Step 6: If you select Custom_Setup_String, enter the string in the **Modem setup String** text box.

<Note> The default modem setup string configures the modem to auto answer. It works for all Hayes-compatible modems.

Performing Advanced Setup Activities

To perform Advanced Setup Activities:

Click the **Advanced Setup** button at the upper field of the main display, the menu options appear.



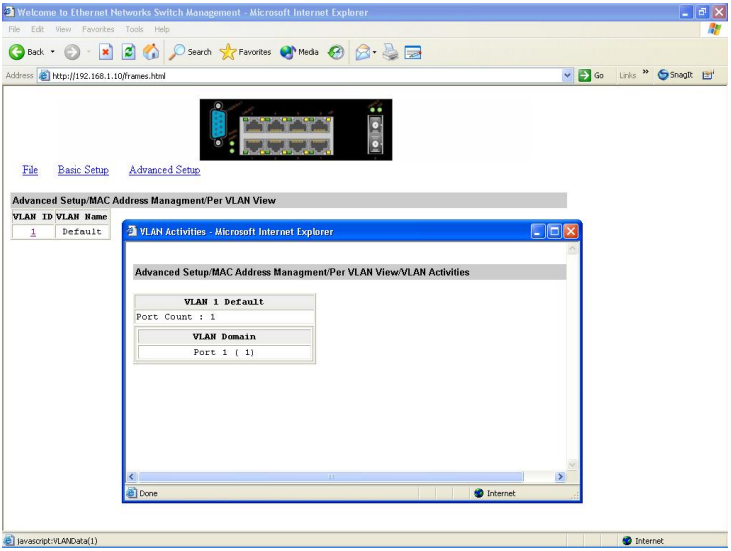
MAC Address Management

Step 1: From the **Advanced Setup** menu, point to **MAC Address Management** to view VLANs and their associated MAC addresses.

Per VLAN View

Step 2: Click **Per VLAN View** first and click on the port that you want to view.

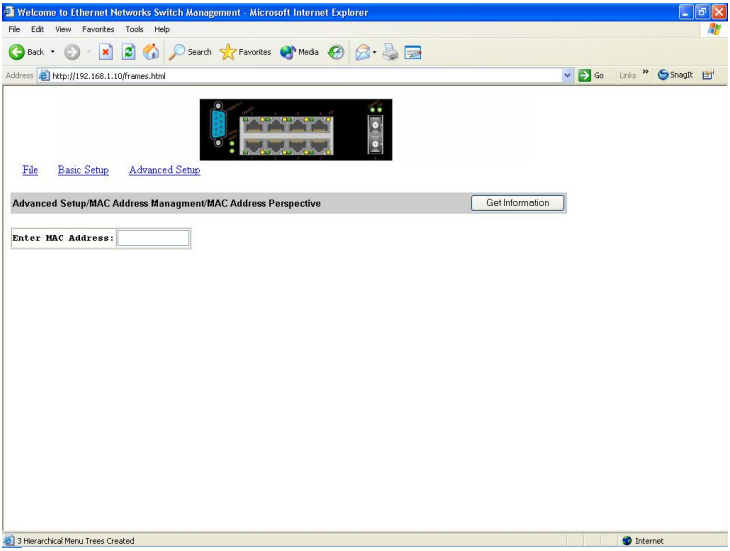
Close the **VLAN Activities** window when finished viewing.



Individual MAC View

Step 3: From the **Advanced Setup** menu as shown in Step 1, point to **MAC Address Management**. Click **Individual MAC View**.

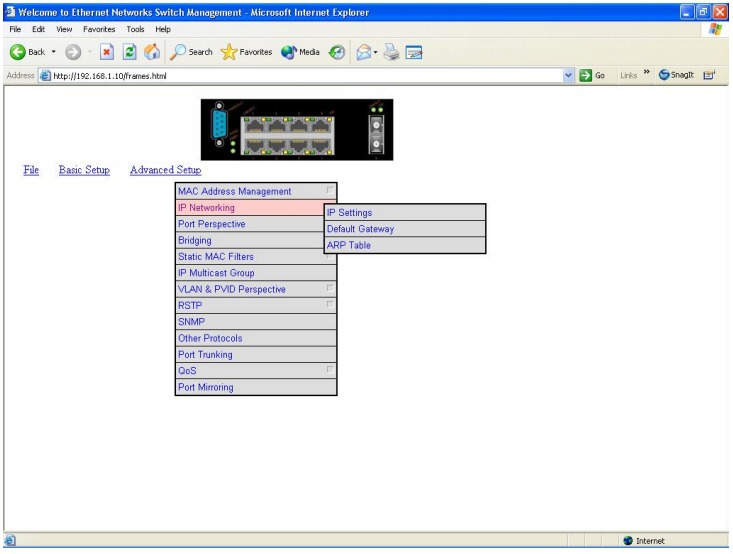
Step 4: Click in the **Enter MAC Address** text box and type the MAC address that you want to view. Then click on the **Get Information** button.



Step 5: Close the **Individual MAC View** window when finished viewing.

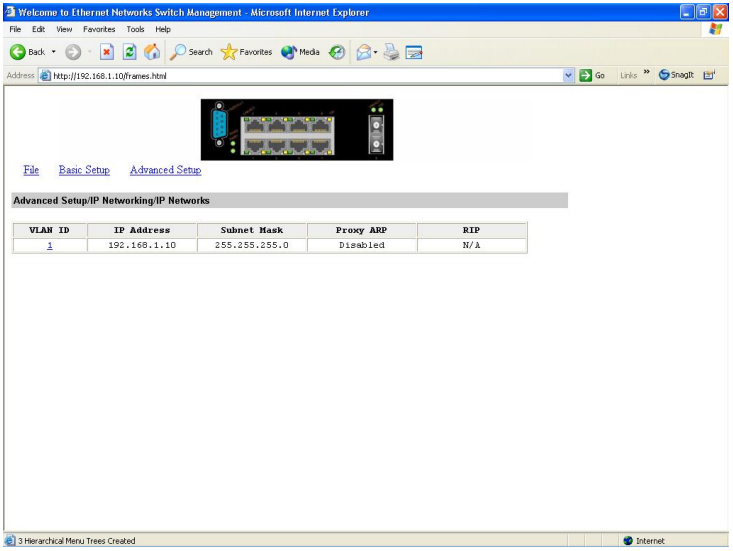
IP Networking

To access the IP networking parameters, click the **Advanced Setup** button, and Point to **IP Networking** from the selection menu.

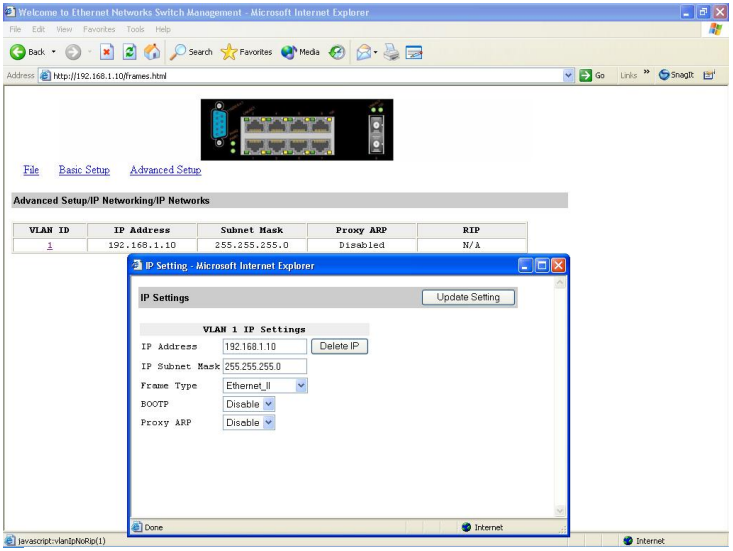


IP Settings

Step 1: Click **IP Settings** to access IP settings. A list of VLAN IDs appears, along with their corresponding IP address and subnet mask.



Step 2: In the **VLAN ID** column, click a VLAN ID whose settings you want to view and/or change.



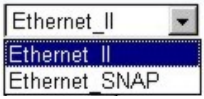
Step 3: To change the **IP Address**, click in the text box and type a new

address. Alternatively, you can use the **Delete IP** button to delete the IP address.

* No precautionary message appears before you delete the IP address.
* Be sure you want to delete it before doing so.
* The IP address is not deleted until you click **Update Setting**.

Step 4: To change the **IP Subnet Mask**, click in the text box and type a new address.

Step 5: To change the **Frame Type**, click a value from the drop-down list.



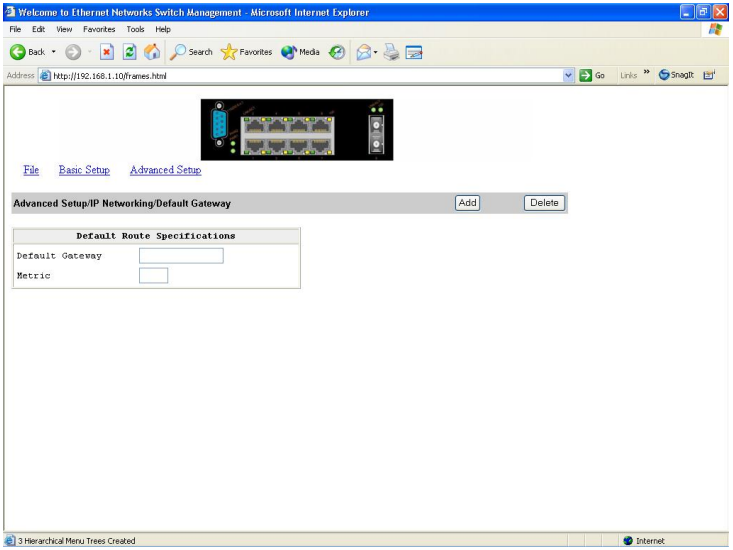
Step 6: To change the **BOOTP** selection, click a value from the drop-down list.

Step 7: To change the **Proxy ARP** selection, click a value from the drop-down list.

Step 8: When you finished with these selections, click Update Setting. A confirmation window appears. Click to close the confirmation window.

Default Gateway

Step 1: Click **Default Gateway** to access Default Gateway settings.



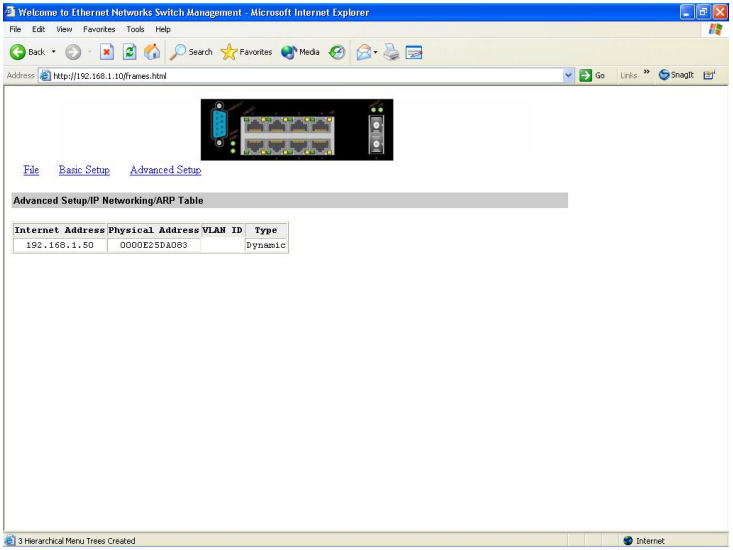
Step 2: To set the **Default Gateway**, click in the text box and type a new Default Gateway.

Step 3: To set the **Metric**, click in the text box and type a new Metric.

Step 4: When you finished with these settings, click **Add** button.
Alternatively, you can use the **Delete** button to delete the settings.

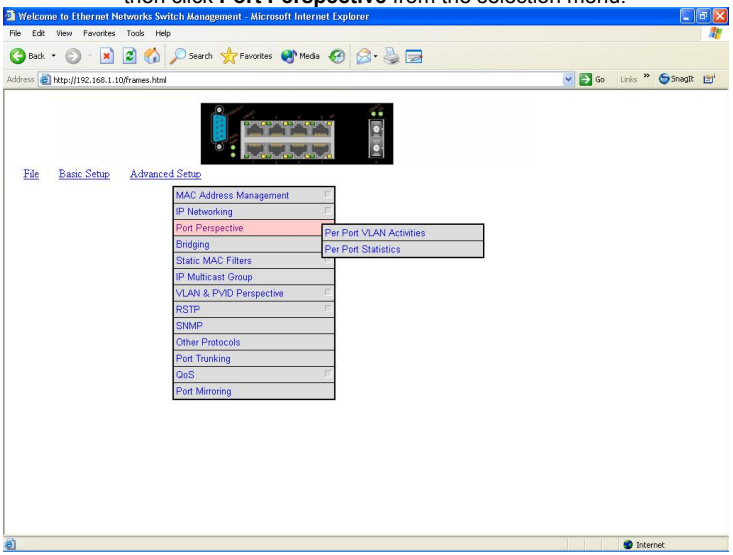
ARP Table

Step 1: Click **ARP Table** to view ARP Table.



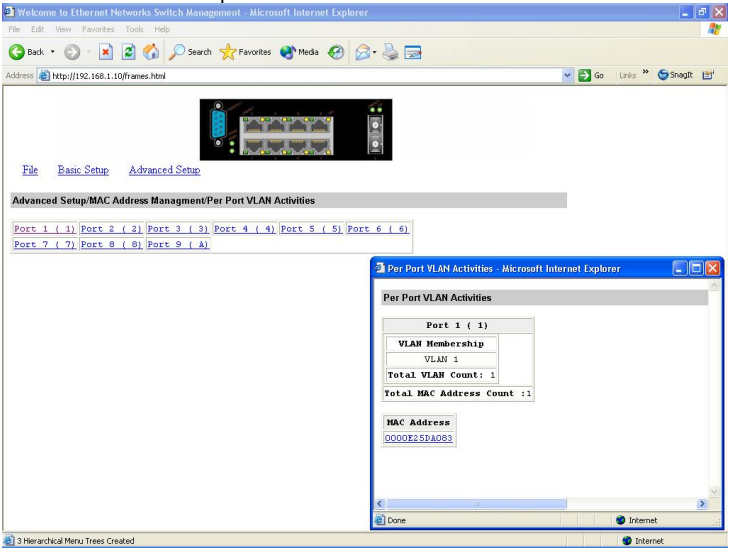
Port Perspective

Step 1: To access Port Perspective, click the **Advanced Setup** button, and then click **Port Perspective** from the selection menu.



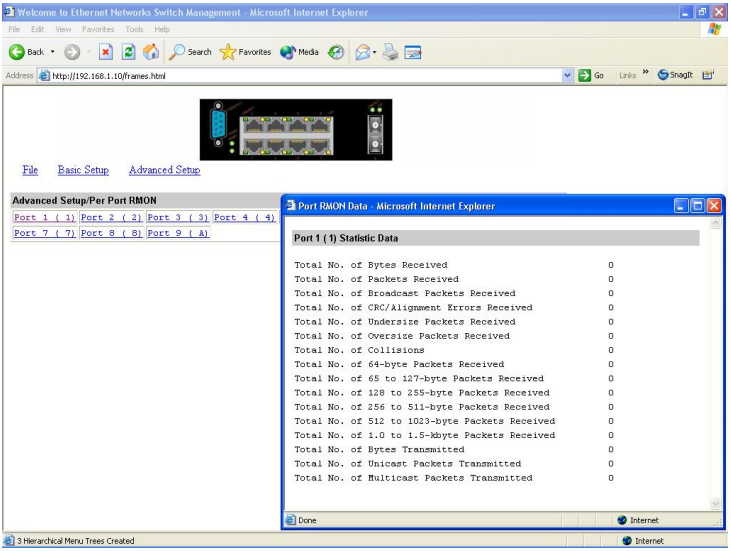
Per Port VLAN Activities

Step 2: To access Port Perspective VLAN Activities, click the **Per Port VLAN Activities** from the selection menu. Click a port to view Port Perspective VLAN Activities.



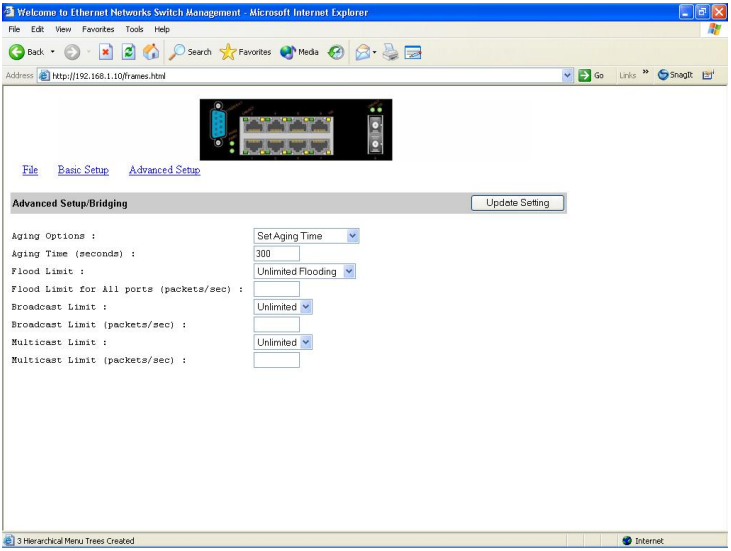
Per Port Statistics

Step 3: To access Per Port Statistics, click the **Per Port Statistics** from the selection menu. Click a port to view statistic data.



Bridging

Step 1: To access bridging parameters, click the **Advanced Setup** button, and then click **Bridging** from the selection menu.



Aging Options

Step 2: Click the drop-down list for **Disabled (No Aging)** or **Set Aging Time**.

Aging Time

Step 3: Click the text box and type a decimal number as bridge aging period in seconds.

Flood Limit

Step 4: Click the drop-down list for **No Flooding, Controlled Flooding, Unlimited Flooding**.

Flood Limit for All Ports (packets/sec)

Step 5: Click the text box and type a decimal number as flood limit in packets per second.

Broadcast Limit

Step 4: Click the drop-down list for **Set Limit** or **Unlimited**.

Broadcast Limit (packets/sec)

Step 5: Click the text box and type a decimal number as broadcast limit in packets per second.

Multicast Limit

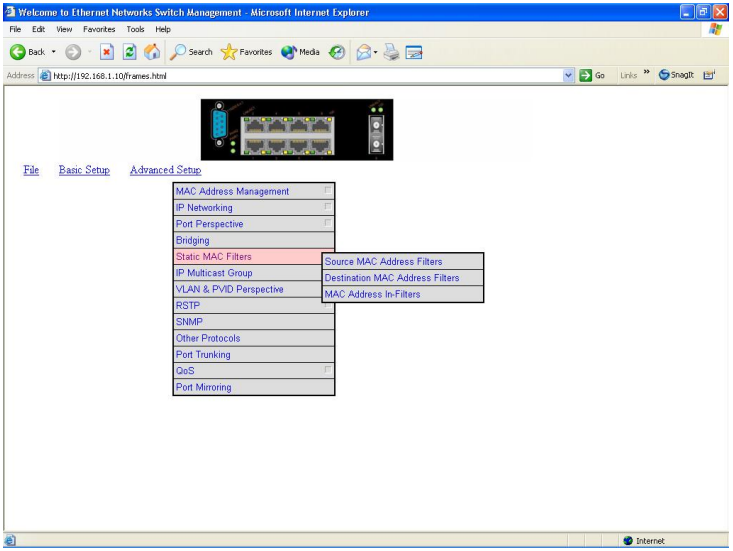
Step 4: Click the drop-down list for **Set Limit** or **Unlimited**.

Multicast Limit (packets/sec)

Step 5: Click the text box and type a decimal number as multicast limit in packets per second.

Static MAC Filters

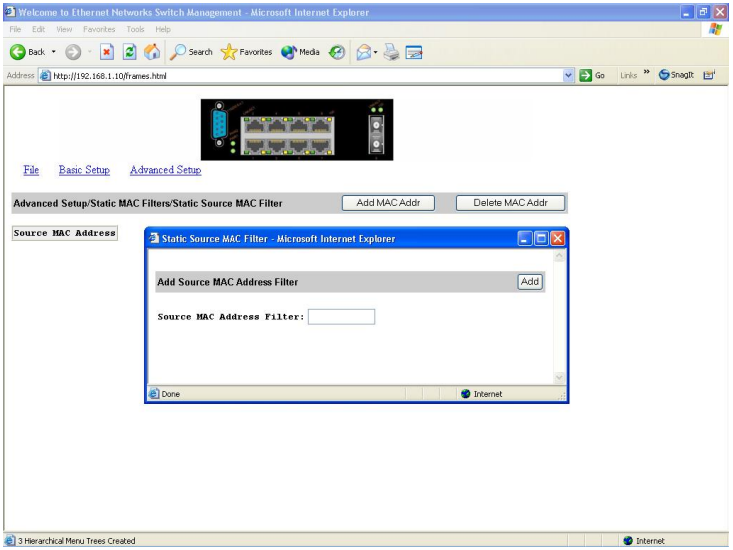
To access the Static MAC Filters parameters, click the **Advanced Setup** button, and point to **Static MAC Filters** in the selection menu.



Source MAC Address Filters

Step 1: Click **Source MAC Address Filters**.

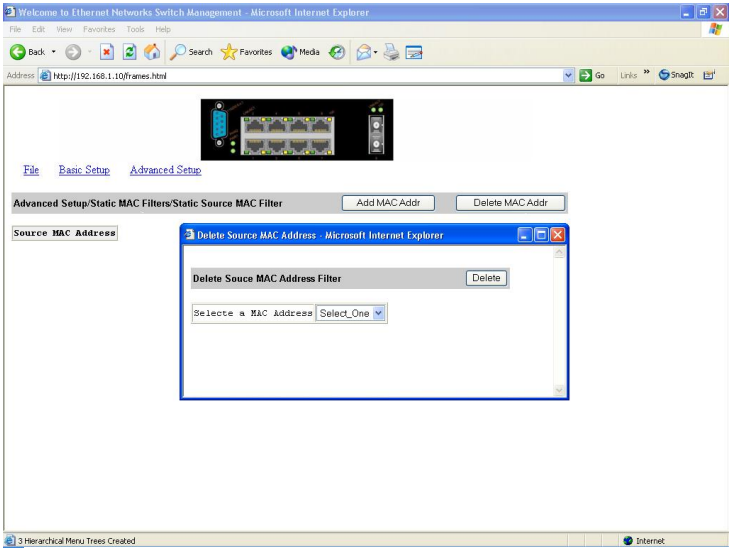
Step 2: Click **Add MAC Addr** button to add a source MAC address for static filtering.



Step 3: The **Static Source MAC Filter** window appears. Click in the **Source MAC Address Filter** text box and type a unique MAC source address you want to add. Then click the **Add** button.

Step 4: A confirmation window appears. Close the confirmation window.

Step 5: If you no longer need a source MAC address, click **Delete MAC Addr** button to delete it in Step 2.



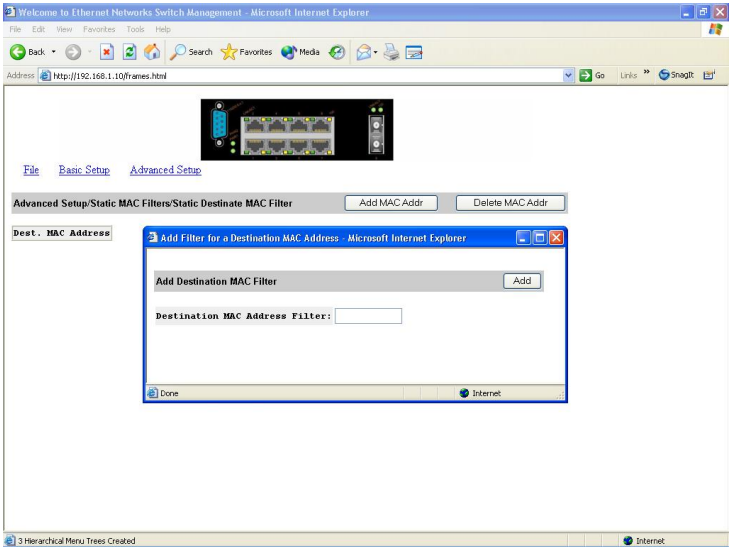
Step 6: The **Delete Source MAC Address** window appears. Click the **Select a MAC Address** drop-down list and select the source MAC address you want to delete. Then click the **Delete** button.

Step 7: A confirmation window appears. Close the confirmation window.

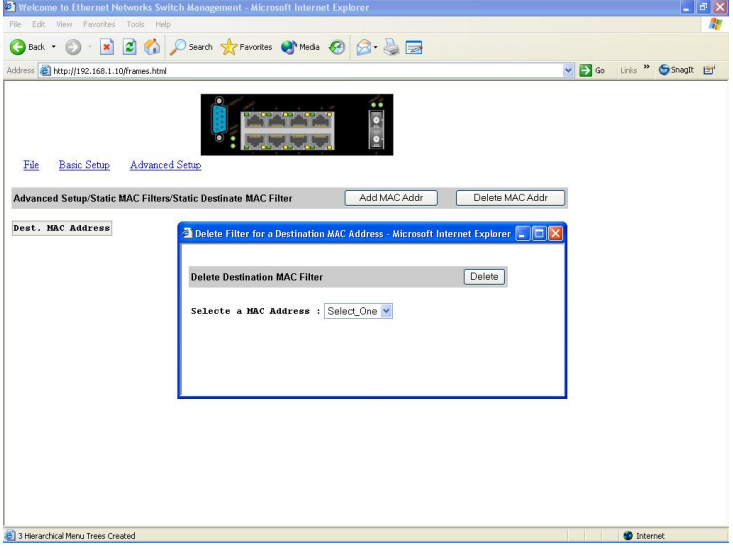
Destination MAC Address Filters

Step 1: Click the **Advanced Setup** button, and point to **Static MAC Filters** in the selection menu. Click **Destination MAC Address Filters**.

Step 2: Click **Add MAC Addr** button to add a destination MAC address for static filtering. Refer to Step 2~4 in **Source MAC Address Filters** section for similar procedure.

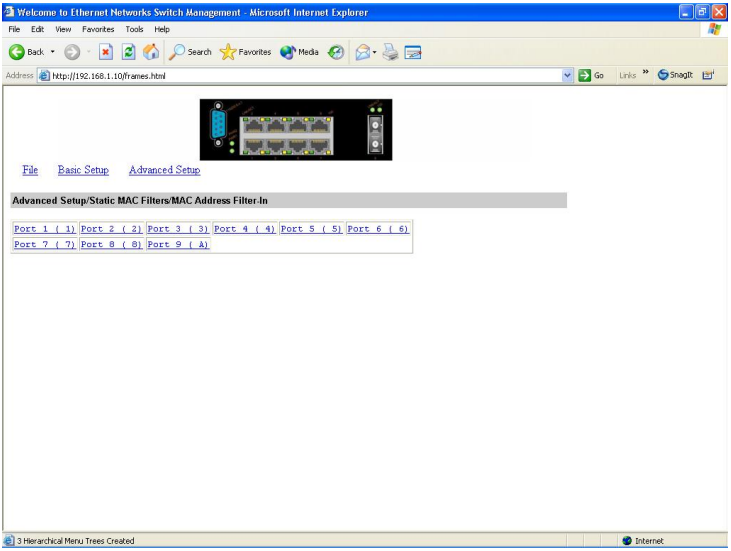


Step 3: Click **Delete MAC Addr** button to delete a destination MAC address for static filtering. Refer to Step 5~7 in **Source MAC Address Filters** section for similar procedure.

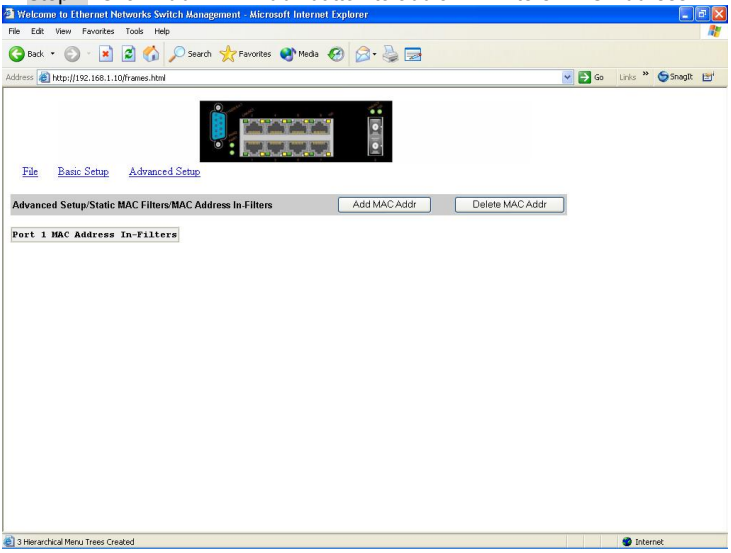


MAC Address In-Filters

Step 1: Click **MAC Address In-Filters**. Click a port to add or delete In-Filters MAC Address.



Step 2: Click **Add MAC Addr** button to add an In-Filters MAC Address.



Step 3: The **Add New MAC Address In-Filter** window appears. Click in the **MAC Address In-Filter** text box and type a unique MAC source address you want to add. Then click the **Add** button.

Step 4: A confirmation window appears. Close the confirmation window.

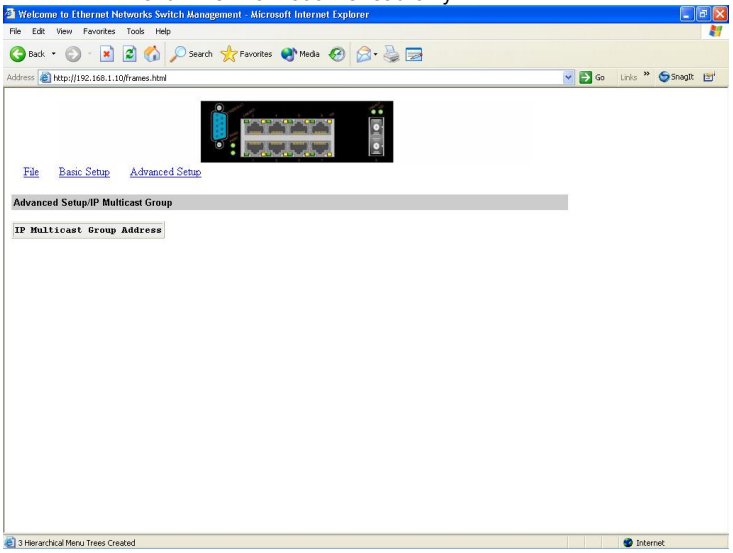
Step 5: If you no longer need an In-Filters MAC Address, click **Delete MAC Addr** button to delete it in Step 2.

Step 6: The **Delete MAC Address In-Filter** window appears. Click the **Select a MAC Address** drop-down list and select the In-Filters MAC Address you want to delete. Then click the **Delete** button.

Step 7: A confirmation window appears. Close the confirmation window.

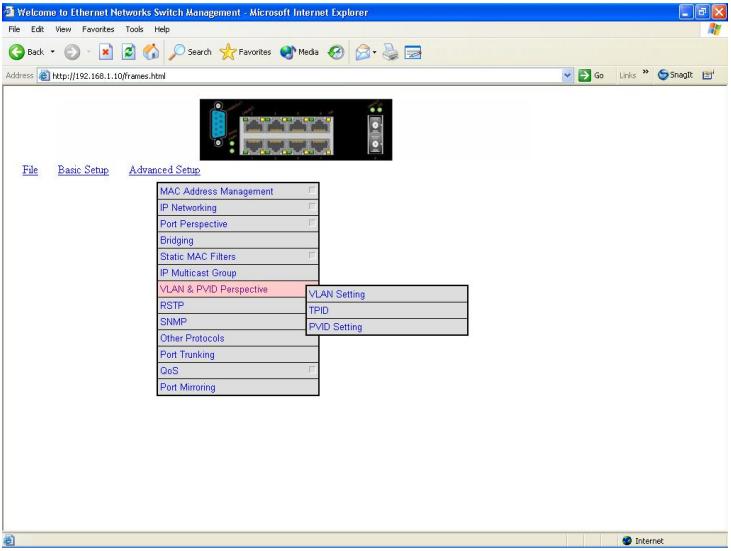
IP Multicast Group

To view the IP multicast group addresses, click the **Advanced Setup** button, and click **IP Multicast Group** in the selection menu. The information is read-only.



VLAN & PVID Perspective

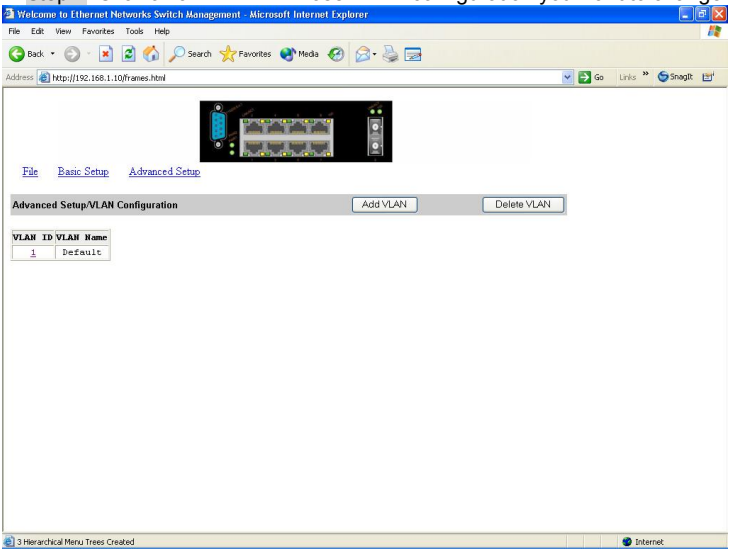
To view the VLAN configuration information, click the **Advanced Setup** button, and point to **VLAN & PVID Perspective** in the selection menu.



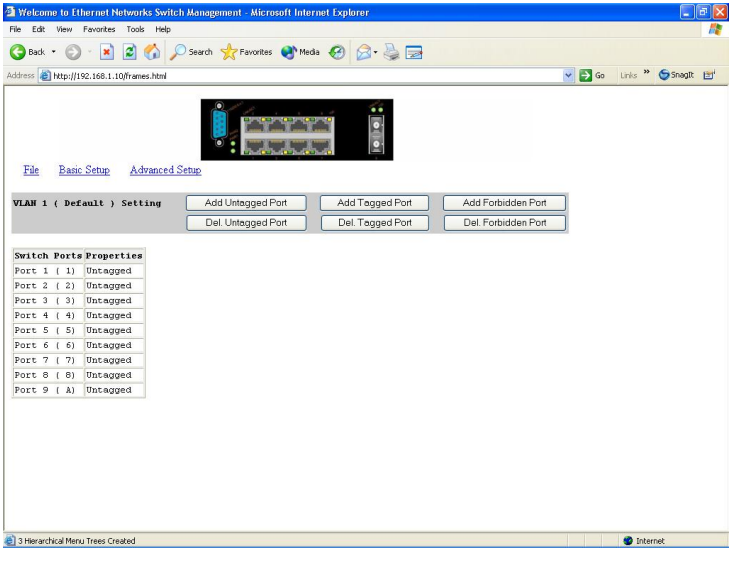
VLAN Setting

Step 1: Click **VLAN Setting**.

Step 2: Click on a VLAN ID whose VLAN configuration you want to change.



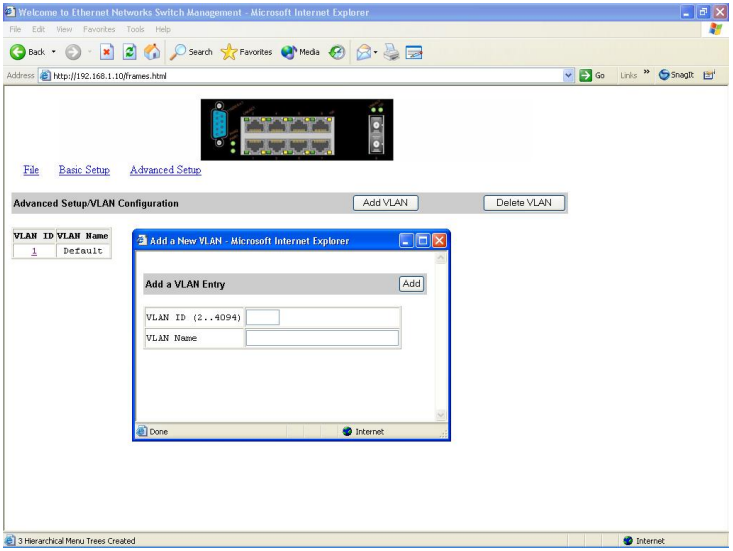
Step 3: The **VLAN Setting** window appears.
Add or delete switch ports for VLAN ID 1.
For each switch, the port options include **Tagged Ports**, **Untagged Ports**, or **Forbidden Ports**.



Add a VLAN Entry

Step 4: Click on the **Add VLAN** button to create a new VLAN.

Step 5: The **Add a New VLAN** window appears.



Step 6: Click in the **VLAN ID** textbox and specify a new VLAN ID number from 2~4094.

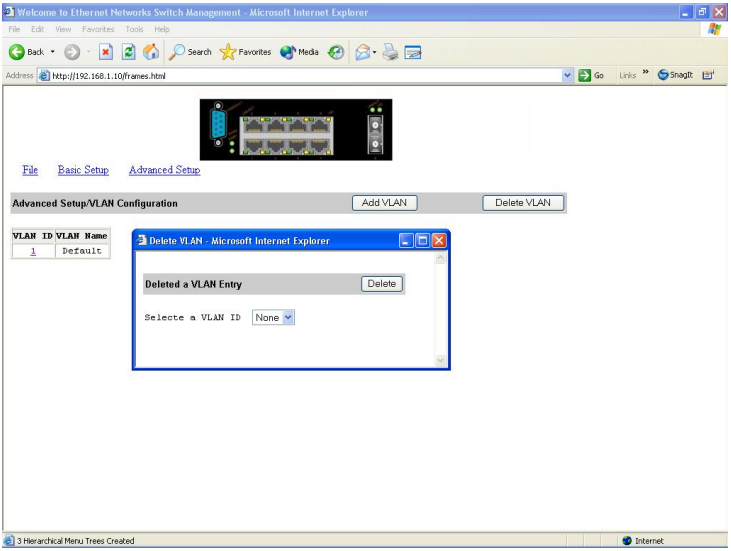
Step 7: Click in the **VLAN Name** textbox and type a name for this newly created VLAN.

Step 8: Assign switch ports to this VLAN.
For each switch, the port options include **Tagged Ports**, **Untagged Ports**, or **Forbidden Ports**.

Step 9: Click **Add Now!** button.

Delete a VLAN Entry

Step 10: Click on the **Delete VLAN** button to delete a VLAN.
VLAN ID 1 is the default VLAN and cannot be deleted.



Step 11: The **Delete VLAN** window appears.

Step 12: Click the drop-down menu to select a VLAN ID, which you want to delete.

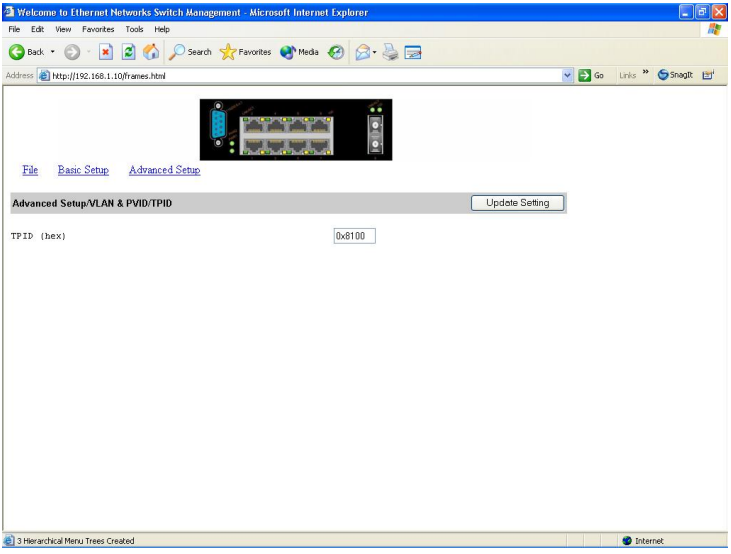
Step 13: Click the **Delete** button.

* No precautionary message appears before you delete a VLAN.
* Be sure you want to delete it before doing so.

TPID Setting

Step 1: Click **TPID Setting**.

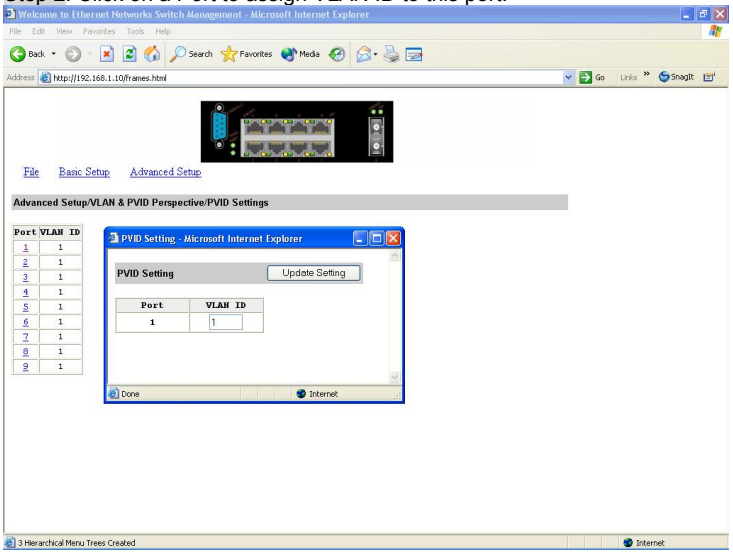
Step 2: Click in the **TPID** textbox and type an address for TPID.



PVID Setting

Step 1: Click **PVID Setting**.

Step 2: Click on a Port to assign VLAN ID to this port.

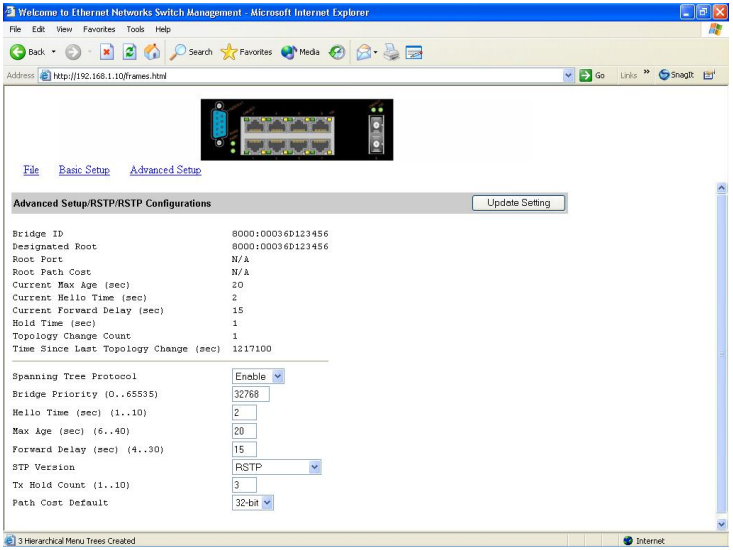


RSTP (Rapid Spanning Tree Protocol)

To view the rapid spanning tree protocol parameters, click the **Advanced Setup** button, and point to **RSTP** in the selection menu.

Configurations

Step 1: To view and/or change the RSTP configurations, click **Configurations** from the above screen.



Step 2: For **Spanning Tree Protocol**, specify whether you want to have it Disabled or Enabled by clicking the drop-down list.

Step 3: For **Bridge Priority**, click in the text box and type a decimal number between 0 and 65535.

Step 4: For **Hello Time**, click in the text box and type a decimal number between 1 and 10.

Step 5: For **Max Age**, click in the text box and type a decimal number between 6 and 40.

Step 6: For **Forward Delay**, click in the text box and type a decimal number between 4 and 30.

Step 7: For **STP Version**, specify whether you want to choose STP Compatible or RSTP by clicking the drop-down list.

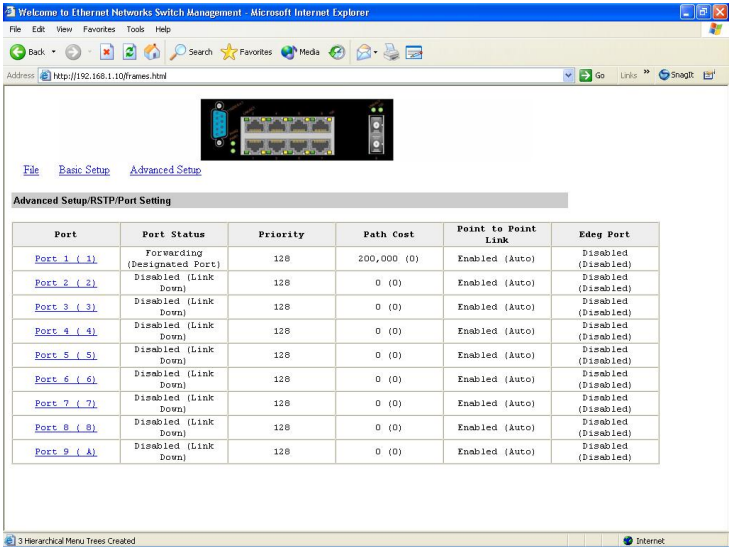
Step 8: For **Tx Hold Count**, click in the text box and type a decimal number between 1 and 10.

Step 9: For **Path Cost Default**, specify whether you want to choose 16-bit or 32-bit by clicking the drop-down list.

Step 10: Click **Update Setting**. A confirmation window appears. Close the confirmation window.

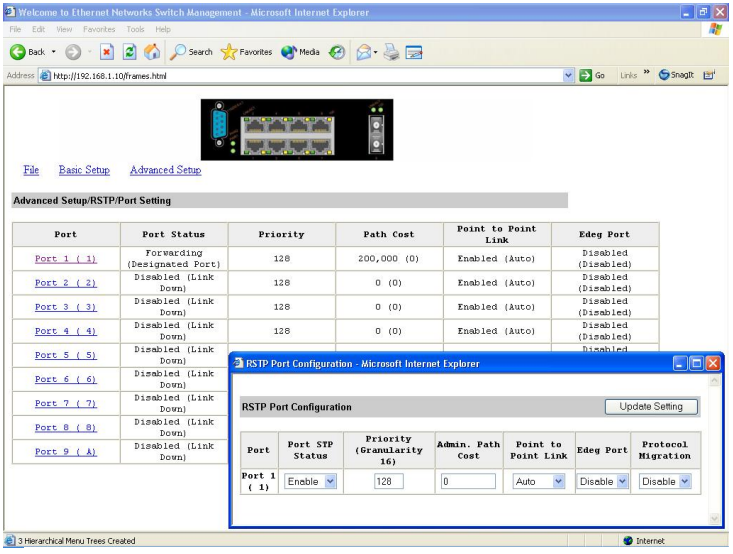
Port Setting

Step 1: To view and/or change the RSTP Port Configuration by port, click the **Advanced Setup** button, point to **RSTP** in the selection menu, and click **Port Setting**.



Port	Port Status	Priority	Path Cost	Point to Point Link	Edeg Port
Port 1 (1)	Forwarding (Designated Port)	128	200,000 (0)	Enabled (Auto)	Disabled (Disabled)
Port 2 (2)	Disabled (Link Down)	128	0 (0)	Enabled (Auto)	Disabled (Disabled)
Port 3 (3)	Disabled (Link Down)	128	0 (0)	Enabled (Auto)	Disabled (Disabled)
Port 4 (4)	Disabled (Link Down)	128	0 (0)	Enabled (Auto)	Disabled (Disabled)
Port 5 (5)	Disabled (Link Down)	128	0 (0)	Enabled (Auto)	Disabled (Disabled)
Port 6 (6)	Disabled (Link Down)	128	0 (0)	Enabled (Auto)	Disabled (Disabled)
Port 7 (7)	Disabled (Link Down)	128	0 (0)	Enabled (Auto)	Disabled (Disabled)
Port 8 (8)	Disabled (Link Down)	128	0 (0)	Enabled (Auto)	Disabled (Disabled)
Port 9 (A)	Disabled (Link Down)	128	0 (0)	Enabled (Auto)	Disabled (Disabled)

Step 2: In the **Port** column, click the port whose RSTP Port Configuration you want to change.



Step 3: For **Port STP Status**, specify whether the Port STP Status is Enable or Disable by clicking the drop-down list.

Step 4: For **Priority**, click in the text box and type a decimal number as a new priority value.

Step 5: For **Admin. Path Cost**, click in the text box and type a decimal number as a new admin. path cost value.

Step 6: For **Point to Point Link**, specify whether the Point to Point Link is Enable, Disable, or Auto by clicking the drop-down list.

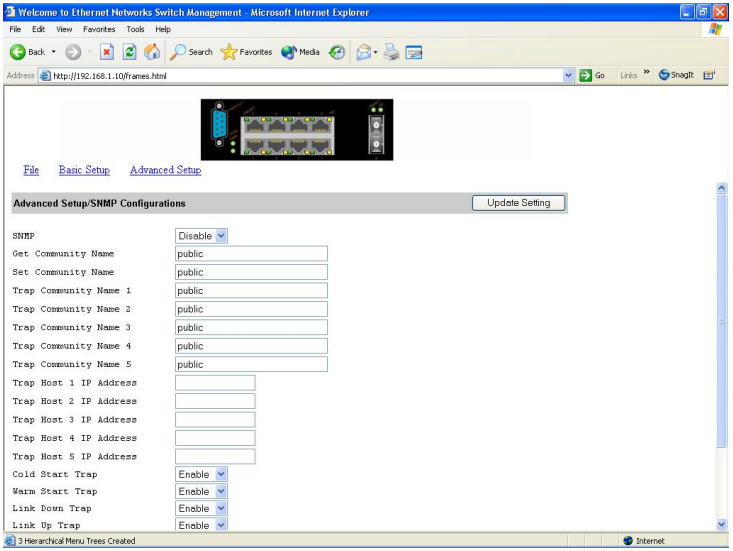
Step 7: For **Edge Port**, specify whether the Edge Port is Enable or Disable by clicking the drop-down list.

Step 8: For **Protocol Migration**, specify whether the Protocol Migration is Enable or Disable by clicking the drop-down list.

Step 9: Click **Update Setting**. A confirmation window appears. Close the confirmation window.

SNMP

To view and/or change all SNMP-related information, click the **Advanced Setup** button, and click **SNMP** in the selection menu. The **SNMP Configurations** window appears. As shown below, the factory-default **Community Name** value is **public**.



SNMP

Step 1: For **SNMP**, specify whether it is Disabled or Enabled by clicking the drop-down list.

Get Community Name

Step 2: For **Get Community Name**, click in the text box and type a get community name.

Set Community Name

Step 3: For **Set Community Name**, click in the text box and type a set community name.

Trap Community Name

Step 4: For each **Trap Community Name**, click in the text box and type a trap community name.

Trap Host IP Address

Step 5: For each **Trap Host IP Address**, click in the text box and type a IP address for trap host 1~5.

Cold Start Trap

Step 6: For **Cold Start Trap**, specify whether it is Disabled or Enabled by clicking the drop-down list.

Warm Start Trap

Step 7: For **Warm Start Trap**, specify whether it is Disabled or Enabled by clicking the drop-down list.

Link Down Trap

Step 8: For **Link Down Trap**, specify whether it is Disabled or Enabled by clicking the drop-down list.

Link Up Trap

Step 9: For **Link Up Trap**, specify whether it is Disabled or Enabled by clicking the drop-down list.

Authentication Failure Trap

Step 10: For **Authentication Failure Trap**, specify whether it is Disabled or Enabled by clicking the drop-down list.

Rising Alarm Trap

Step 11: For **Rising Alarm Trap**, specify whether it is Disabled or Enabled by clicking the drop-down list.

Failure Alarm Trap

Step 12: For **Failure Alarm Trap**, specify whether it is Disabled or Enabled by clicking the drop-down list.

Topology Change Trap

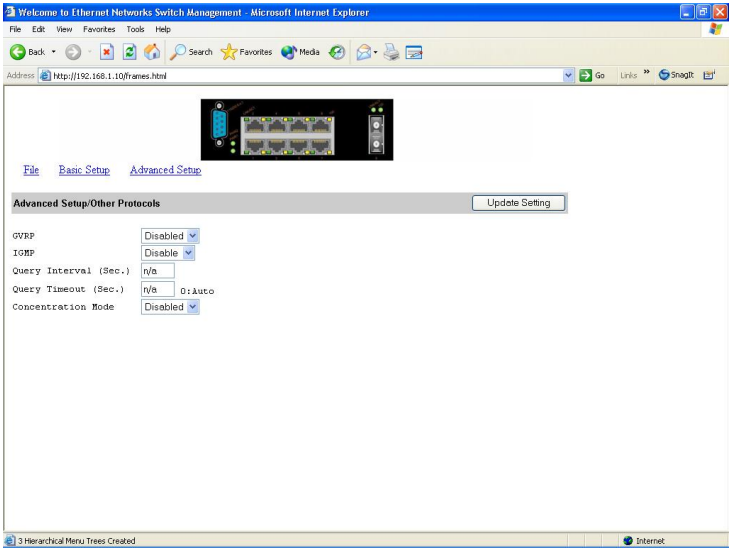
Step 13: For **Topology Change Trap**, specify whether it is Disabled or Enabled by clicking the drop-down list.

Update Setting

Step 14: Click **Update Setting** when completed. A confirmation window appears. Close the confirmation window.

Other Protocols

To enable or disable the GVRP and/or IGMP protocols, click the **Advanced Setup** button, and click **Other Protocols** in the selection menu.



GVRP

Step 1: For **GVRP**, specify whether it is Disabled or Enabled by clicking the drop-down list.

IGMP

Step 2: For **IGMP**, specify whether it is Disabled or Passive or Active by clicking the drop-down list.

CONCENTRATION MODE

Step 3: For **Concentration Mode**, specify whether it is Disabled or Enabled by clicking the drop-down list.

Update Setting

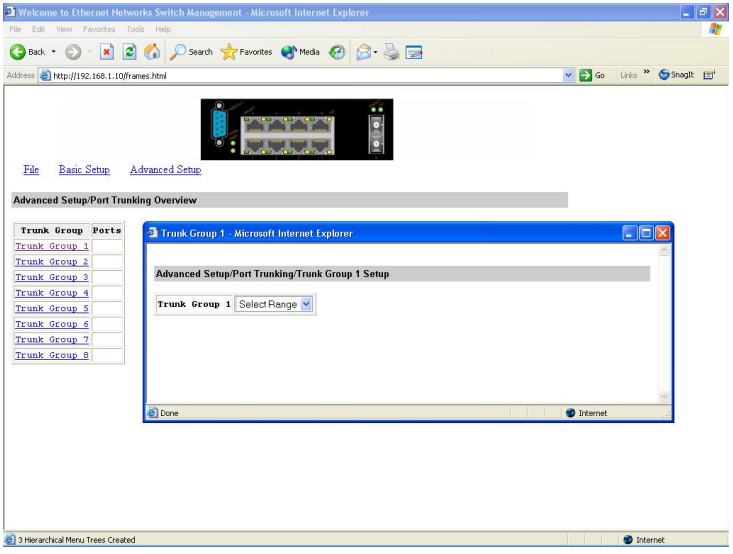
Step 4: Click **Update Setting** when completed. A confirmation window appears. Close the confirmation window.

Port Trunking

To use the switch's trunking capability to gain more bandwidth, click the **Advanced Setup** button, and click **Port Trunking** in the selection menu.

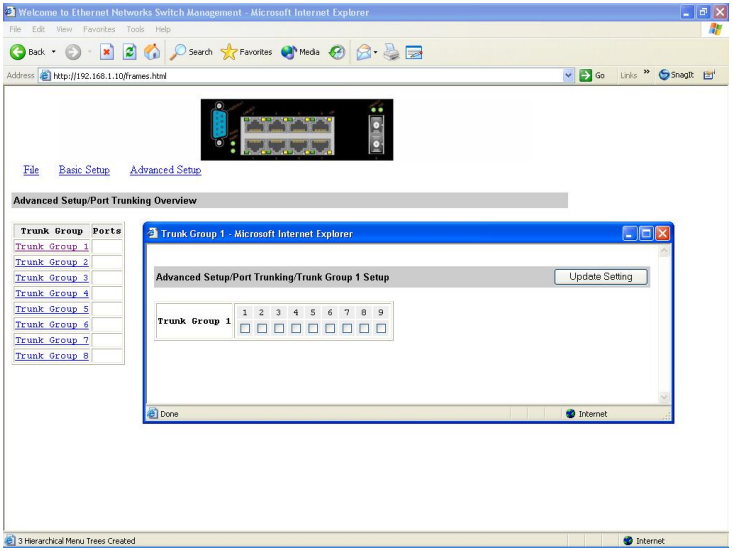
Step 1: The **Port Trunking Overview** window appears.

E.g. Click **Trunk Group 1** in the **Trunk Group** column.



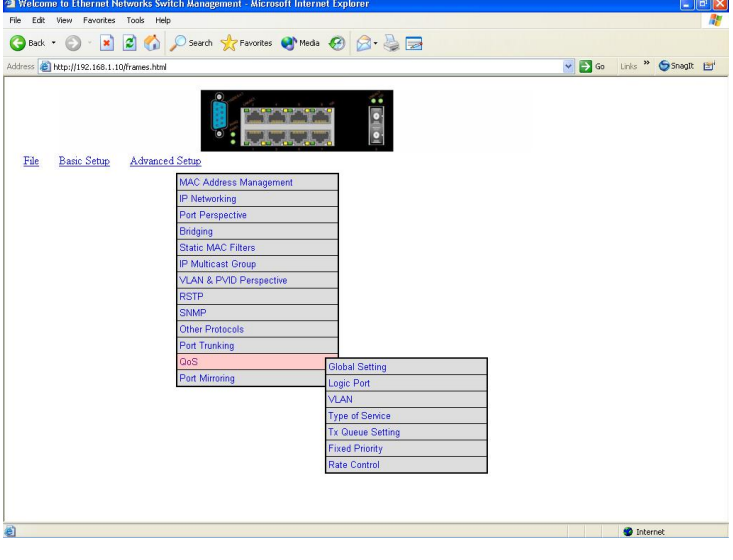
Step 2: The **Trunk Group 1** window appears.
Click the drop-down menu to select a desired range.

Step 3: Click to assign ports to the trunk group.



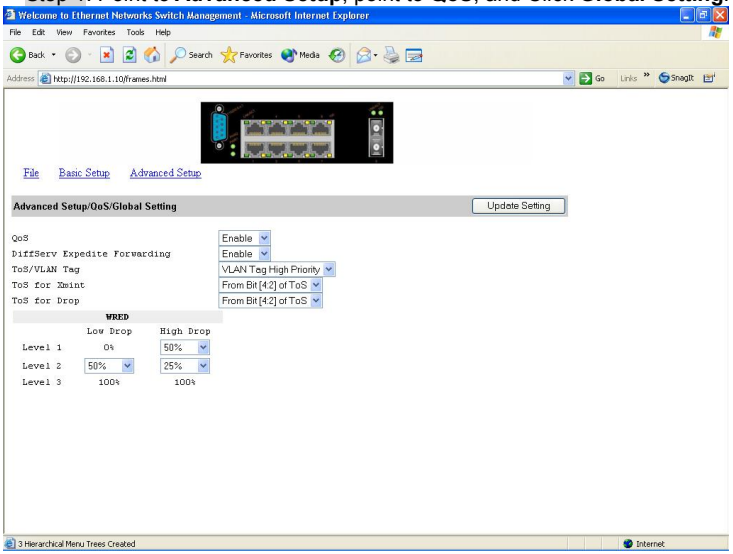
QoS

To use the switch's QoS capability, point to the **Advanced Setup** button, and point to **QoS** in the selection menu.



Global Setting

Step 1: Point to **Advanced Setup**, point to **QoS**, and Click **Global Setting**.



Step 2: Use the **QoS** drop-down list to enable or disable QoS.

Step 3: Use the **DiffServ Expedite Forwarding** drop-down list to specify whether you want to enable or disable DiffServ Expedite Forwarding.

Step 4: Use the **ToS/VLAN Tag** drop-down list to select the priority you want to use.

Step 5: Use the **ToS for Xmint** drop-down list to select the Bits of ToS you want to use.

Step 6: Use the **ToS for Drop** drop-down list to select the Bits of ToS you want to use.

Step 7: Under **WRED**, use the drop-down list boxes to select the:

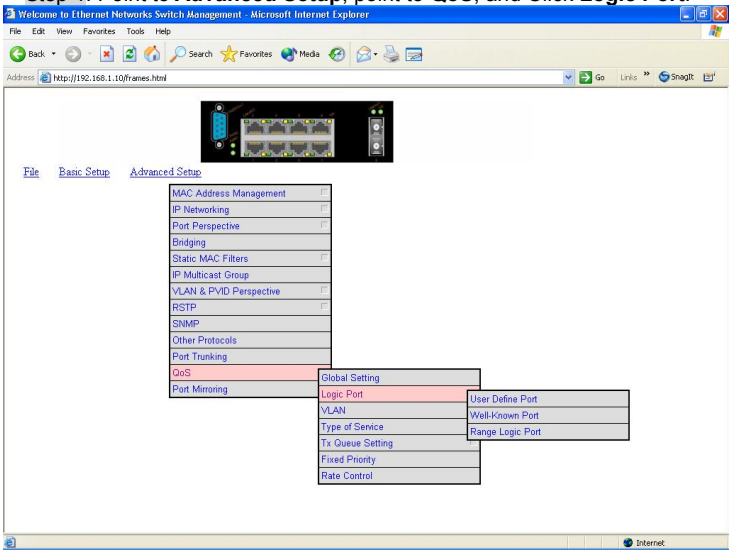
- High drop percentage for level 1.
- Low drop and high drop percentages for level 2.

The low drop percentage for level 1 remains fixed at 0%, while the low drop and high drop percentages for level 3 remain fixed at 100%.

Step 8: Click **Update Setting** when completed. A confirmation window appears. Click to close the confirmation window.

Logic Port

Step 1: Point to **Advanced Setup**, point to **QoS**, and Click **Logic Port**.

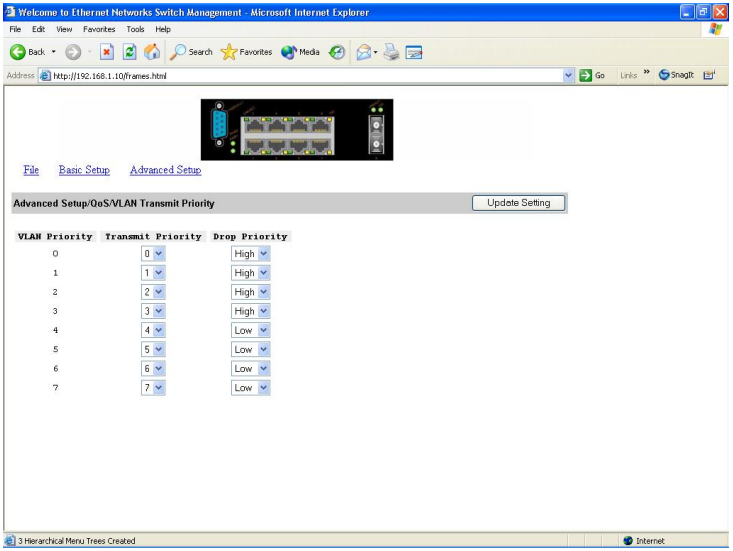


Step 2: Point to **Advanced Setup**, point to **QoS**, point to **Logic Port**, and click **User Define Port**, **Well-Known Port**, or **Range Logic Port**.

Step 3: Click **Update Setting** when completed. A confirmation window appears. Click to close the confirmation window.

VLAN

Step 1: Point to **Advanced Setup**, point to **QoS**, and Click **VLAN**.

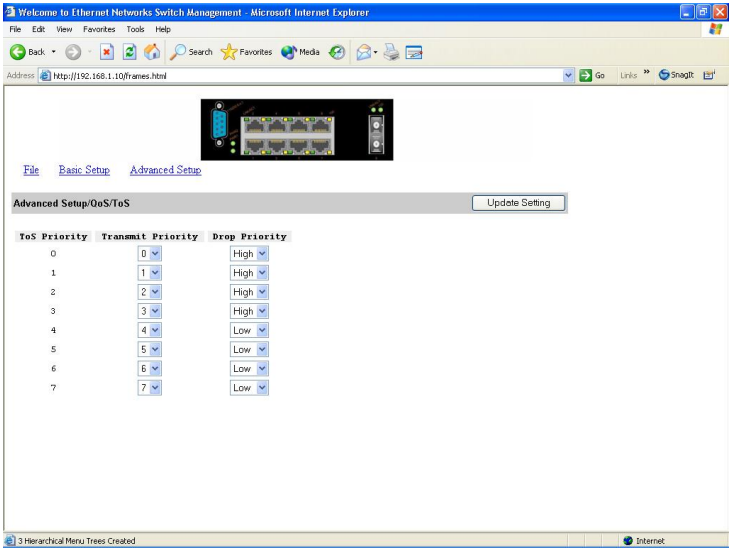


Step 2: For each VLAN priority, use the right drop-down list to select a **Transmit Priority** for that VLAN and use the right drop-down list to select a High or Low **Drop Priority** for that VLAN.

Step 3: Click **Update Setting** when completed. A confirmation window appears. Click to close the confirmation window.

Type of Service

Step 1: Point to **Advanced Setup**, point to **QoS**, and Click **Type of Service**.

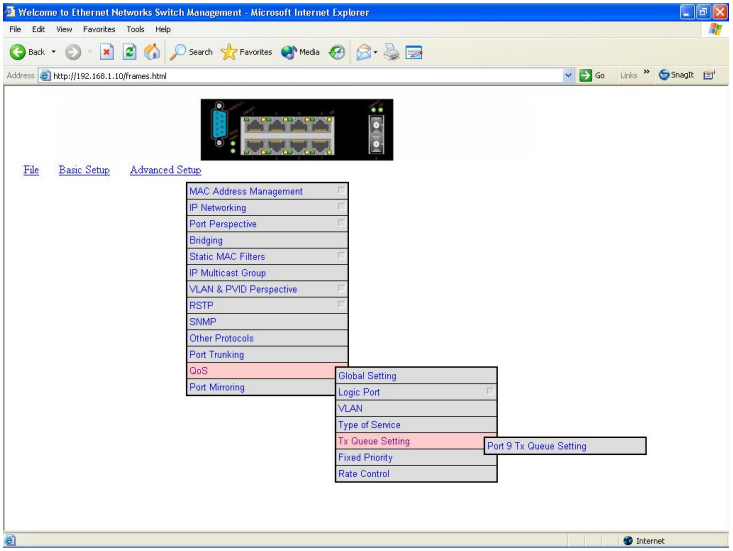


Step 2: For each Type of Service priority, use the right drop-down list to select a **Transmit Priority** for that Type of Service and use the right drop-down list to select a High or Low **Drop Priority** for that Type of Service.

Step 3: Click **Update Setting** when completed. A confirmation window appears. Click to close the confirmation window.

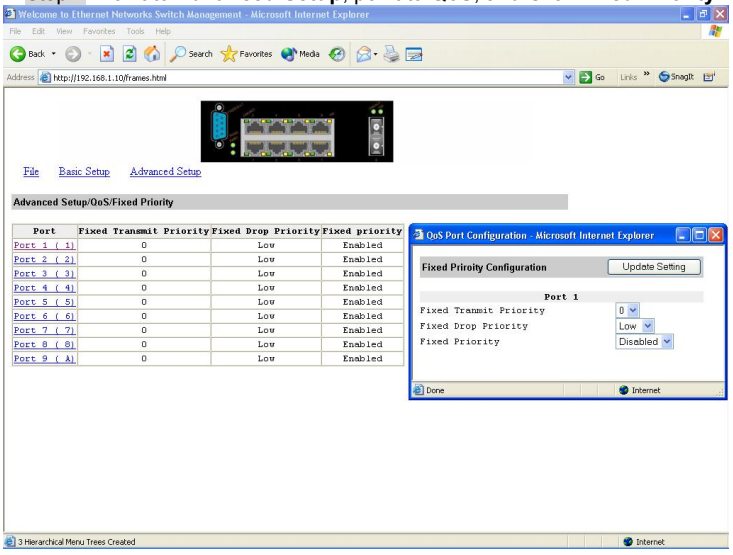
Tx Queue Setting

Step 1: Point to **Advanced Setup**, point to **QoS**, point to **Tx Queue Setting**, and Click **Port 9 Tx Queue Setting**.



Fixed Priority

Step 1: Point to **Advanced Setup**, point to **QoS**, and Click **Fixed Priority**.



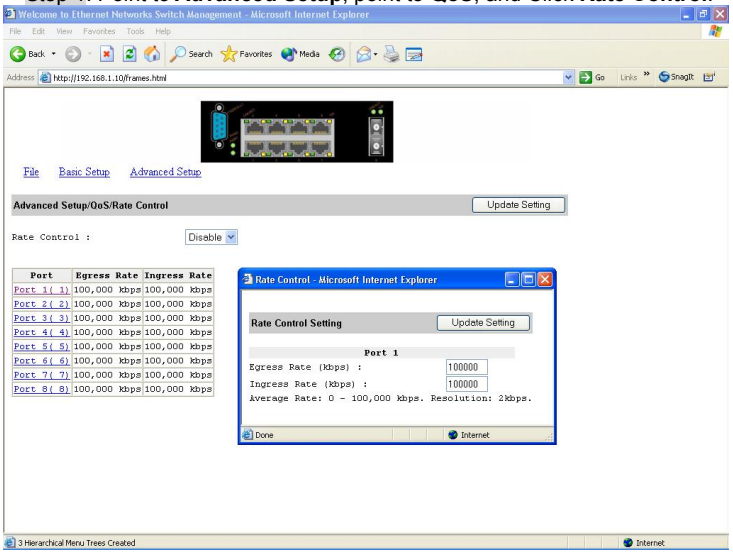
Step 2: Click a port number under **Port**. Use the **Fixed Transmit Priority**,

Drop Priority, and **Priority** drop-down list to select a different priority for the port.

Step 3: Click **Update Setting** when completed. A confirmation window appears. Click to close the confirmation window.

Rate Control

Step 1: Point to **Advanced Setup**, point to **QoS**, and Click **Rate Control**.



Step 2: Use the **Rate Control** drop-down list to enable or disable rate control.

Step 3: Click a port number under **Port**. Set the Egress Rate and Ingress Rate for the port.

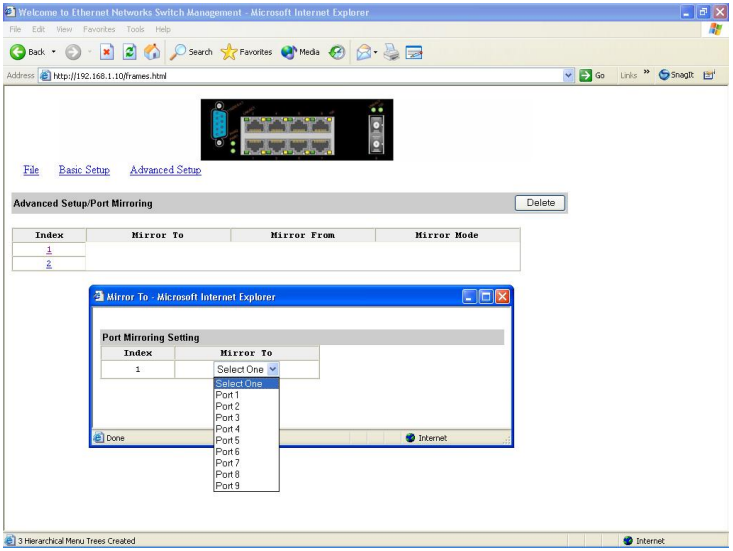
Step 4: Click **Update Setting** when completed. A confirmation window appears. Click to close the confirmation window.

Port Mirroring

To use the switch's mirroring capability to mirror one port to another port, click the **Advanced Setup** button, and click **Port Mirroring** in the selection menu.

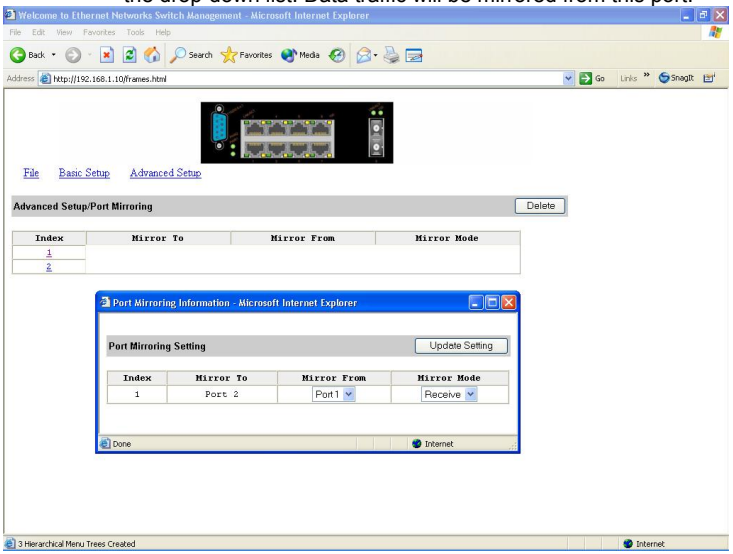
Mirror To

Step 1: Click **1** or **2** in the Index column. In the **Mirror To** column, select a "mirror to" port by clicking the drop-down list. Data traffic will be mirrored to this port.



Mirror From

Step 2: In the **Mirror From** column, select a "mirror from" port by clicking the drop-down list. Data traffic will be mirrored from this port.



Mirror Mode

Step 2: In the **Mirror Mode** column, specify whether the "mirrored from" port will be receiving or transmitting data by clicking the drop-down list.

Step 3: Click **Update Setting** when completed. A confirmation window appears. Close the confirmation window.

SNMP & RMON Management

This chapter describes the switch's Simple Network Management Protocol (SNMP) and Remote Monitoring (RMON) capabilities.

Overview

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

RMONs typically consist of two components: an RMON probe and a management workstation:

- The RMON probe is an intelligent device or software agent that continually collects statistics about a LAN segment or VLAN. The RMON probe transfers the collected data to a management workstation on request or when a pre-defined threshold is reached.

- The management workstation collects the statistics that the RMON probe gathers. The workstation can reside on the same network as the probe, or it can have an in-band or out-of-band connection to the probe.

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

SNMP Agent and MIB-2 (RFC 1213)

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

- Retrieving MIB counters from various layers of software modules according to the SNMP GET/GET NEXT frame messages.

- Setting MIB variables according to the SNMP SET frame message.

- Generating an SNMP TRAP frame message to the Network Management Station if the threshold of a certain MIB counter is reached or if other trap conditions (such as the following) are met:

WARM START
COLD START
LINK UP
LINK DOWN
AUTHENTICATION FAILURE
RISING ALARM
FALLING ALARM
TOPOLOGY ALARM

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

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

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

RMON Groups Supported

The switch supports the following RMON MIB groups defined in RFC 1757:

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

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

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

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

Bridge Groups Supported

The switch supports the following four groups of Bridge MIB (RFC 1493):

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

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

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

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

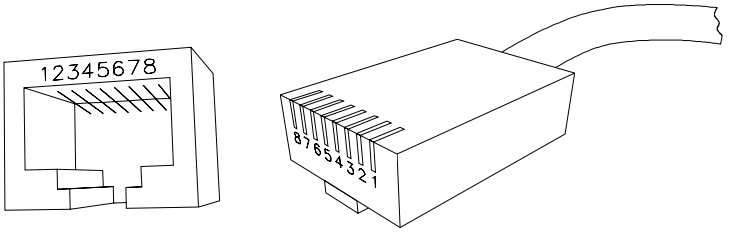
Specifications

Hardened Managed Ethernet Switch	10/100Base-TX auto-negotiating ports with RJ-45 connectors, 100Base-FX fiber ports, 10/100/1000Base-TX auto-negotiating ports with RJ-45 connectors, and 1000Base-SX/LX fiber ports combination
Applicable Standards	IEEE 802.3 10Base-T IEEE 802.3u 100Base-TX/FX IEEE 802.3ab 1000Base-T IEEE 802.3z 1000Base-SX/LX
Switching Method	Store-and-Forward
Forwarding Rate 10Base-T: 100Base-TX/FX: 1000Base-T/SX/LX:	 10 / 20Mbps half / full-duplex 100 / 200Mbps half / full-duplex 2000Mbps full-duplex
Performance	14,880pps for 10Mbps 148,810pps for 100Mbps 1,488,100pps for 1000Mbps
Cable 10Base-T: 100Base-TX: 1000Base-T: 100Base-FX: 1000Base-SX/LX:	 2-pair UTP/STP Cat. 3, 4, 5 2-pair UTP/STP Cat. 5 4-pair UTP/STP Cat. 5 Up to 100m (328ft) MMF (50 or 62.5µm), SMF (9 or 10µm) MMF (50 or 62.5µm), SMF (9 or 10µm)
LED Indicators	Per unit – Power status (PWR1, PWR2) Per port – 10/100TX, 100FX – LNK (Link) / ACT (Activity) (Green) 100 (Yellow) 10/100/1000TX, 1000SX/LX – 1000 (Green) ACT (Activity) (Yellow)
Dimensions	50mm (W) × 125mm (D) × 135mm (H) (1.97" (W) × 4.92" (D) × 5.31" (H))
Net Weight	0.8Kg (1.76lbs.)
Power	DC Jack: 12VDC, External AC/DC required Terminal Block: 12-32VDC
Operating Voltage & Max. Current Consumption	1.54A @ 12VDC, 0.77A @ 24VDC
Power Consumption	18.48W Max.

Operating Temperature	-40°C to 75℃ (-40℉ to 167℉) Tested for functional operation @ -40℃ to 85℃ (-40℉ to 185℉)
Storage Temperature	-40°C to 85°C (-40℉ to 185℉)
Humidity	5%-95% non-condensing
Safety	Hazardous locations: Class 1, Division 2 group A, B, C & D UL60950-1, EN60950-1, IEC60950-1
EMI	FCC Part 15, Class A EN61000-6-3: EN55022, EN61000-3-2, EN61000-3-3
EMS	EN61000-6-2: EN61000-4-2 (ESD Standard) EN61000-4-3 (Radiated RFI Standards) EN61000-4-4 (Burst Standards) EN61000-4-5 (Surge Standards) EN61000-4-6 (Induced RFI Standards) EN61000-4-8 (Magnetic Field Standards) EN61000-4-11 (Voltage Dips Standards)
Environmental Test Compliance	IEC60068-2-6 Fc (Vibration Resistance) IEC60068-2-27 Ea (Shock) IEC60068-2-32 Ed (Free Fall)
NEMA TS1/2 Environmental requirements for traffic control equipment	

Appendix A – Connector Pinouts

Pin arrangement of RJ-45 connectors:



RJ-45 Connector and Cable Pins

The following table lists the pinout of 10/100Base-TX ports.

Pin	Regular Ports	Uplink port
1	Input Receive Data +	Output Transmit Data +
2	Input Receive Data -	Output Transmit Data -
3	Output Transmit Data +	Input Receive Data +
4	NC	NC
5	NC	NC
6	Output Transmit Data -	Input Receive Data -
7	NC	NC
8	NC	NC

The following table lists the pinout of 10/100/1000Base-TX ports.

Pin	Ports
1	A+
2	A-
3	B+
4	C+
5	C-
6	B-
7	D+
8	D-