ZT8101 Switch

User's Manual

December 2001

Information in this document is provided in connection with Intel® products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

The ZT8101 may contain design defects or errors known as errata that may cause the product to deviate from published specifications. Current characterized errata are available on request.

MPEG is an international standard for video compression/decompression promoted by ISO. Implementations of MPEG CODECs, or MPEG enabled platforms may require licenses from various entities, including Intel Corporation.

This document and the software described in it are furnished under license and may only be used or copied in accordance with the terms of the license. The information in this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Corporation. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document. Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Corporation.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an ordering number and are referenced in this document, or other Intel literature may be obtained by calling
1-800-548-4725 or by visiting Intel's website at http://www.intel.com.

*Other names and brands may be claimed as the property of others.

Copyright © 2001, Intel Corporation. All rights reserved.

Intel Corporation
5200 N.E. Elam Young Parkway
Hillsboro, Oregon 97124-6497

Contents

Revision History

Date	Revision	Description
December 6, 2001	00.2	Made technical corrections.
November 14, 2001	00.1a	Added agency approvals.
November 9, 2001	00.1	First draft.

Introduction 1

The ZT8101 board is a high performance managed switch that supports both Layer 2 and Layer 3 features. For fast connection speeds and flexibility, it has 24 10/100 Mbps Fast Ethernet ports and 2 gigabit Ethernet ports in a 6U CompactPCI* form factor board. The in-chassis switch minimizes external wiring and needs no extra rack height, thus improving density and reliability.

You can manage the switch from a terminal, with Telnet, from a Web browser, or through IPMI via the Chassis Management Module (ZT7101). The ZT8101 routes and switches at full wire speed with its non-blocking architecture, and it has sophisticated multicast protocols to limit unnecessary traffic. It provides an in-chassis switch fabric that you can configure to operate in a redundant configuration.

Highlights

- Full wire speed on all ports
- VLAN ID tagging and priority queues
- Port aggregation
- Port mirroring
- Packet filtering
- Multicast and broadcast storm control
- DHCP/BOOTP packet forwarding
- RIP (v1 and v2), DVMRP, PIM-DM
- Low port latency
- Hot-swappable board with LED indicator

Ethernet Features

Layer 2 Switching Functions

- 10BASE-T, 100BASE-TX, and 1000BASE-T port functions
  - — 22 10/100 Fast Ethernet ports to the mid-plane connectors
  - — 2 10/100 Fast Ethernet ports (RJ45) on the font panel
  - — 2 100/1000 Ethernet ports (RJ45) on the front panel
- Auto-negotiation function for speed (10 MB/100 MB/1000 MB), duplex (full/half), and flow-control
- Back pressure flow control for half-duplex mode
- IEEE 802.3x compliant flow control for full-duplex mode

- Per device packet buffer: 512 KB
- 8.8 Gbps switching fabric capacity
- Store and forward switching forwarding mode
- 8 KB Layer 2 MAC address
- Broadcast and multicast storm control
- Port mirroring
- Port aggregation
- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1Q tagged VLANs
- GVRP (GARP VLAN Registration Protocol) for automatic VLAN configuration
- IEEE 802.1p priority support with 4 priority queues
- IGMP Snooping with broadcast control

Layer 3 Switching Functions

- Wire speed IP forwarding rate per system
- Hardware-based Layer 3 IP switching
- 2 KB Layer 3 IP address entries
- RIP (Routing Information Protocol) v1 and v2
- IP v4
- IGMP (Internet Group Management Protocol) v2
- PIM-DM (Protocol Independent Multicast-Dense Mode)
- DVMRP (Distance Vector Multicast Routing Protocol) v3
- IP multi-netting
- IP fragmentation
- Path MTU discovery
- IEEE 802.1D frame support
- DHCP/BOOTP relay

Additional Features

Front Panel Features

- 2 10/100 RJ45 ports
- 2 100/1000 RJ45 ports
- RS 232 serial console port
- Status LEDs for port link, speed, and activity

Management Functions

- RS-232 port for out-of-band management and system diagnostics
- Telnet remote control console
- Web-based management console
- SNMP v1 Agent
- Supported MIBs
  - MIB-II
  - Bridge MIB
  - RMON MIB (Statistics, History, Alarm, Event)
  - RIP MIB
  - CIDR MIB
  - 802.1p MIB
- TFTP
- IP filtering on management interface
- DHCP client
- Password enabled

Warranty

2 years

Product Information and Sales Support

Tel. (805) 541-0488
www.Intel.com
ZiatechInfo@Intel.com

Installation and Initial Setup 2

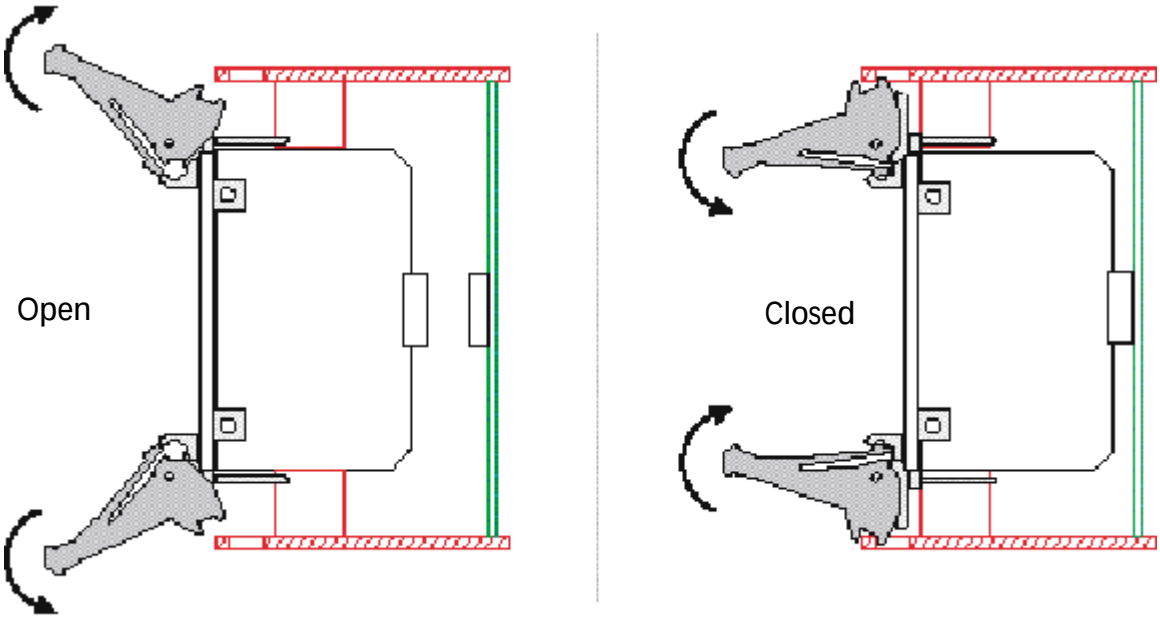
This chapter provides installation and initial setup information for the switch.

Installing the Board

These instructions explain the mechanical aspects of installing a ZT8101board. The board should be installed in a PICMG* 2.16 compliant fabric slot.

1. System power does not need to be off to insert a ZT8101 board.
2. Prepare the board by opening the injector/ejector mechanisms.

Injector/Ejector Operations



3. Carefully align the edges of the board with the left and right card guides in the appropriate slot. It may be helpful to look into the enclosure to verify correct alignment of the rails in the guides.
4. Taking care to keep the board aligned in the guides, slide the board in until the injector/ejector mechanisms engage the retention bars.
5. Simultaneously push in the board and rotate the injector/ejector mechanisms to their closed positions (rotate inward) to seat the backplane connectors. When the board is in place, it will boot if the system power is on.
6. Make the desired connections at the faceplate and configure the board.

Power on

After the power switch is turned on, the LED indicators should respond as follows:

- All LED indicators will momentarily blink, which represents a reset of the system.
- The board status LED indicator will blink while the switch loads onboard software and performs a self-test. After approximately 20 seconds, the LED will light again to indicate the switch is in a ready state.
- The hot-swap LED indicator will be off.
- The port LED indicators will be off if there is no Ethernet connection and on if there is an Ethernet connection.

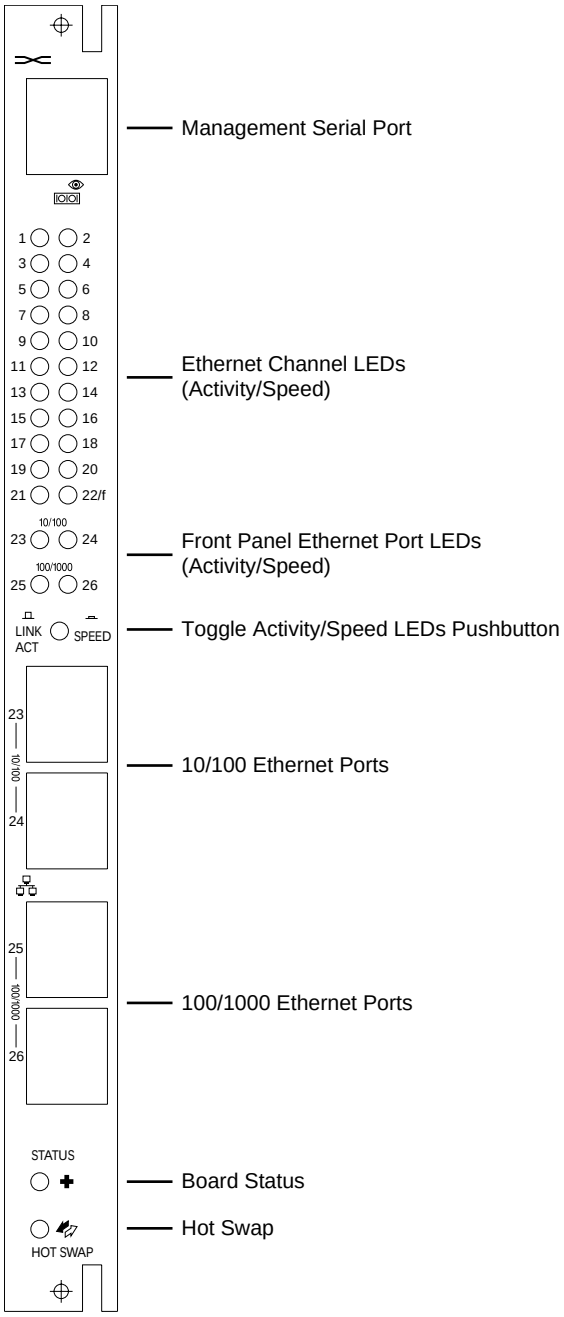
Uninstalling the Board

These instructions explain the mechanical aspects of removing a ZT8101 board from a system.

1. You do not need to turn off the system power to remove a ZT8101 board.
2. Disconnect connections at the faceplate (Ethernet and serial ports).
3. The board should be in a “safe” state to be removed or data may be lost. Signal the system that a board is about to be removed by partially unlatching the ejectors on the board to be removed. Do not fully open the ejectors, as this levers the board out of the enclosure and prematurely breaks its backplane connection.
4. Wait for the blue hot swap LED on the board's faceplate to light; this indicates that board processes have finished and the board is safe to extract. If the hot swap LED fails to light after 30 seconds, re-latch the ejectors and unlatch them again. In this case, the board is safe to extract (though the hot swap LED may not light).
5. Once the hot swap LED lights, open the injector/ejector mechanisms fully, rotating the handles outward until the board disengages from the backplane (refer to “Injector/Ejector Operations” on page 13).
6. Slide the board evenly out of the enclosure.
7. Install a replacement board or cover the empty slot with a filler panel to maintain the enclosure's shielding and cooling performance.

Identifying External Components

This chapter describes the front panel and the LED indicators of the ZT-8101switch. The front panel consists of LED indicators, a management serial port, a toggle button, two 10/100 Ethernet ports, and two 100/1000 Ethernet ports.



Status LEDs

The two LEDs at the bottom of the font panel are status LEDs. The top LED indicates the overall status of the board and the bottom LED indicates the hot swap status of the board.

Health Status LED

Status	Meaning
Off	Not powered.
Green	Powered and functioning normally.
Amber	Attention needed due to one of the following conditions: • Over temperature • Backend supplies exceeding voltage limits • IPMB time outs

Hot Swap LED

Status	Meaning
Off	Switch is active or in the process of shutting down; do not remove it.
Blue	Safe to remove the switch.

Port LEDs

The LED array on the front panel displays information about all the Ethernet links on the board. A green/amber two-color LED is used for each of the 26 Ethernet port connections (24 10/100 + 2 Gigabit). A push-button switch just below the array toggles the LED display from Link /Activity mode to Link / Speed mode. The default LED mode is Link /Activity. When you depress the switch button, the LEDs are in Link/Speed mode.

Link / Activity LED Mode

Status	Meaning
Off	No Ethernet connection.
Solid Green	Good connection, link present.
Blinking Green	Port is transmitting or receiving packets (activity is on going).
Solid Amber	Port is not forwarding packets. The port has been disabled by management, an address violation has occurred, or the port is being blocked by STP. **Note:** After a port is reconfigured, the port LED can remain amber for as long as 30 seconds while STP checks the switch for loop paths. When the STP checking is completed, the port then resumes displaying its current connection status.

Link / Speed LED Mode

Port Type	Status	Meaning
10/100	Off	10 Mb/s
	Solid Green	100 Mb/s
100/1000	Solid Green	100 Mb/s
	Solid Amber	1000 Mb/s

Getting Started with Management

The switch contains the following components:

- A CPU
- Memory for data storage
- Flash memory for configuration data, operational programs, and SNMP agent firmware.

These components allow you to manage and monitor the switch from either the board's serial port or the network itself. You can configure and manage the switch from these locations:

- A terminal or a workstation running terminal emulation software and connected to the switch via the RS-232 port.
- A workstation connected to the network and running Telnet.
- A workstation connected to the network and running a Web browser.

To access the switch via Telnet or a Web browser, you must assign the switch an appropriate IP address for your network. To do this, you must access the switch using the RS-232 port via the Local Console.

This section explains how to

- Set up access to the Local Console
- Configure the switch's IP address

Once you complete these tasks, you can access the switch from any of the three locations. Since the Local Console and the Telnet Console use the same interface, chapter 4 explains how to access the switch using Telnet and then explains all the configuration and management options in this interface. Chapter 5 explains the Web Console. Both the Web and the Telnet/Serial interfaces expose the same functionality. Chapter 3 describes some basic concepts that you should be familiar with before configuring the switch.

Accessing the Local Console

The Local Console is a terminal or a workstation running a terminal emulation program that is connected directly to the switch via the RS-232 console port on the front of the switch. Such a connection is referred to as an "Out-of-Band" connection because the console is connected to the switch using a different circuit than the circuit used for normal network communications. The Local Console can be used to set up and manage the switch even when the network is down.

The serial port on the front panel uses Cisco* cable kit (Order Number: ACS-DSBUASYN). This kit includes a DB25 terminal adapter, a DB-9 terminal adapter, and RJ-45 rollover cable.

A terminal (such as a VT-100) or a computer running a terminal emulation program (such as HyperTerminal, which is automatically installed with Windows*) is connected to this cable.

The serial port is set at the factory for the following configuration:

- Baud rate: 9600
- Data width: 8 bits
- Parity: None
- Stop bits: 1
- Flow Control: None

Make sure the terminal or computer you are using to make this connection is configured to match these settings.

If you are having problems making this connection on a computer, make sure the emulation is set to VT-100. If you still don't see anything, press **CTRL+R** to refresh the screen.

To log in to the switch the first time

The usernames and passwords used to access the switch are case sensitive; therefore, "S" is not the same as "s."

When you first connect to the switch, you will be presented with a login screen.

1. Use the Arrow keys or the Tab key to move to the Username field. Leave the field blank and press **Enter**. There is no initial username.
2. Move to the Password field. Leave the field blank and press **Enter**. There is no initial password. The Main Menu appears.

The first created user automatically gets administrator privileges. One of your first configuration tasks should be to create at least one Admin-level user for the switch to protect it from unauthorized users.

Press **CTRL+R** to refresh the screen. This command can be used at any time to force the console program in the switch to refresh the console screen.

Setting the IP Address

You use the Basic Network Setup menu to set the boot-up operation for obtaining an IP address or to manually assign the IP address for the switch. The switch needs a valid IP address for your network to access the switch via Telnet or the Web.

To configure the IP address

1. From the Main Menu, select **Basic Network Setup** and press **Enter**.

2. To configure the IP address, use the Arrow keys or the Tab key to modify the settings in the New Switch IP Settings column.

Parameter	Default	Description
Get IP From	Manual	Specifies the method for assigning the switch an IP address. Use the spacebar to toggle to Manual, DHCP, or BOOTP.
IP Address	10.90.90.90	Specifies the IP address assigned to the switch.
Subnet Mask	255.0.0.0	Specifies the subnet mask assigned to the switch and to the other devices on this segment of the network.
Default Gateway	0.0.0.0	Specifies the IP address of the device that routes to different networks. A gateway must be defined if the workstation you are going to use for switch management is located on a different IP segment than the switch.
VLAN Name	default	Specifies the name of the VLAN that contains the workstations that you will use to manage the switch. This VLAN must already exist.

3. To configure a name and contact information for the switch, enter information in the following fields.

Parameter	Description
Name	Specifies the name assigned to the switch. If you are installing multiple switches, you should give each a unique name.
Location	Specifies the physical location of the switch.
Contact	Specifies the name of the person responsible for the switch.

4. Highlight **APPLY** and press **Enter**.
5. Press **Escape** to return to the Main Menu.
6. To save your changes to NV-RAM, highlight **Save Changes** and press **Enter**.

To continue configuring the switch, see chapter 4 for information on this interface. See chapter 5 for information about using the Web Console.

Upgrading Firmware through Zmodem

Generally, TFTP is the first choice to use to upgrade firmware. The Telnet Console and the Web Console both have options for upgrading the firmware using a TFTP server (see chapters 4 and 5). However, you can also use Zmodem to upgrade the firmware from the serial port.

Note: If FLASH becomes corrupted because you lose power when upgrading the firmware, you must use Zmodem to fix the problem.

To upgrade the firmware using Zmodem

1. Obtain the runtime firmware.
2. Using Windows HyperTerminal*, log in to the switch through the serial port.
3. From the Main Menu, select **Reboot** and press **Enter**.

4. When the power on self test message appears, press the **#** key and wait for the following message:

   Please change your baud rate to 115200 for the Zmodem upgrade, or
   press CTRL+C to go to the BOOT Menu.

   If you press CTRL+C, you can configure the baud rate to a different value.

5. Change HyperTerminal's baud rate to match the target's setting.
6. Use the Send File function of HyperTerminal to upgrade the firmware.

   When the download is completed, Zmodem will display a message indicating that it is done and then a message about loading the Runtime image.

7. Change the baud rate of HyperTerminal back to 9600 bps.
8. Disconnect and reconnect.
9. Log in to the switch.
10. From the main menu, select **Switch Information** and press **Enter**. Verify the firmware version.

Switch Management and Operating Concepts 3

This chapter describes many of the concepts you need to understand to configure and manage the switch. It also describes many of the features available for managing the switch. The instructions for configuring the switch are in chapter 4 (Telnet Console) and chapter 5 (Web Console).

Managing the Switch

The ZT8101 switch has three methods for configuring switch parameters and viewing switch status and statistics:

- **Serial**—The switch's serial port on the front panel allows a terminal or a PC running terminal emulation software to be connected to the switch and configure the switch. It uses the same application that is used over Telnet. The serial port is usually used only for initial set up, such as configuring the switch's IP address, or when the network is down. It can also be used to upgrade the switch's firmware with Zmodem.
- **Telnet**—The switch's embedded Telnet server allows users from remote systems, which are running a Telnet application over TCP/IP, to log in to the switch, configure it, and view the status of and statistics from the ports. The current implementation allow eight 8 Telnet sessions to be active at the same time.
- **Web**—The switch's embedded Web server allows users from remote systems, which are running a Web browser, to log in to the switch, configure it, and view the status of and statistics from the ports. The current implementation allows five HTTP sessions to be active at the same time.

The switch also contains the following utilities:

- **Ping**—The Ping utility invokes the ICMP echo request and echo reply messages. A host or gateway sends an ICMP echo request message to a specified destination. Any computer that receives an echo request formulates an echo reply and transmits it to the original sender. The echo request and associated reply can be used to test whether a destination is reachable and responding. Five ping sessions can be supported simultaneously.
- **TFTP**—This protocol is used to transfer files without any kind of authentication. It runs on top of UDP, using timeout and retransmission to ensure that data arrives. The switch's TFTP client allows users to copy files from and to a remote system that is running the TFTP server protocol. The TFTP client allows only one user to access it and transfer files.

  You can use the TFTP client to do the following:

  — Download firmware.

  — Download or upload a switch configuration file.

  — Upload the switch's history log.

  Some TFTP servers cannot determine when a transaction is aborted. In these cases, you must reboot the switch, which restarts the TFTP server and re-initializes the TFTP transaction.

- **Switch diagnostics**—The PROM loader automatically runs memory diagnostics each time the switch is booted.
- **Reset to factory defaults**—The switch includes an option that allows you to reset the configuration to the factory defaults. You can select to reset the IP address or save your configured IP address.

Switch IP and MAC Addresses

Each switch must be assigned its own IP Address. The switch's default IP address is 10.90.90.90. You can change the default switch IP address to meet the specification of your networking address scheme.

The switch is also assigned a unique MAC address by the factory. You cannot change this MAC address.

In addition, you can also set an IP address for a gateway router. This becomes necessary when the network management station is located on a different IP network from the switch, making it necessary for management packets to go through a router to reach the network manager, and vice versa.

For security, you can list the IP addresses of the network management stations that you want to manage the switch. If you list IP addresses, only those workstations have access; all others will be denied.

You can also configure a VLAN for the network that the management stations are on, and then configure the switch for this VLAN.

Port Configurations

By default, the switch is configured to use auto-negotiation to determine each port's speed and duplex setting. The user can modify this and configure a port to use a specified configuration. The Ethernet ports have the following characteristics:

Ethernet Port	Link Speed	Duplex
Fast Ethernet (10/100)	10/100 Mbps	Half, Full
Gigabit Ethernet	100/1000 Mbps	Full

Flow Control

All ports have a traffic limit because they have a limited buffer space to receive incoming frames. Upon reaching the limit, a port either starts dropping packets or triggers flow control. The ZT8101 switch uses the following methods for flow control:

- **802.3x flow control**—The switch sends PAUSE frames, which request remote ports to delay sending packets for a period of time. Sending ports suspend further frame transmission until the specified time period has elapsed.
- **802.3x compliant flow control**—The switch does not send PAUSE frames, but it does respond to them.

- **Back pressure**—The switch fakes a collision and then transmits a jam sequence to ensure all stations are notified of the “collision.” This causes the sending ports to trigger their back-off routines and reduces the amount of traffic on the port.

The port type and duplex mode determine which type of flow control is used. The following table lists the port types and their flow control methods.

Port Type	Duplex Mode	Flow Control
Fast Ethernet (10/100)	Half	Back pressure
Fast Ethernet (10/100)	Full	802.3x compliant
Gigabit Ethernet	Full	802.3x

Port Security and MAC Address Learning

For security purposes, you can disable MAC address learning on one or more ports. When MAC address learning is disabled, a port cannot discover MAC addresses. The port receives only broadcast traffic and packets with destination MAC addresses that match the port's MAC address.

The default value for each port is learning enabled.

SNMP

The switch has an embedded Simple Network Management Protocol (SNMP) agent which is compliant with SNMPv1. This agent monitors the status of the board’s hardware and the traffic passing through its ports. A computer attached to the network, called a management station, can access this information. The switch uses the following features to control access to its information:

- **Community strings**—You can configure up to four community strings so that only authorized management stations can access the agent. You can set each string to grant either read only or read/write access.
- **IP address**—You can restrict access to specified IP addresses. You can enter up to three IP addresses which restricts access to these specified management stations.

You can also specify which management agents receive the trap messages generated by the SNMP agent. These trap messages are status messages that alert you of events such as authentication failure, STP topology changes, and link status changes on the port.

BOOTP/DHCP Relay

BOOTP and DHCP allow stations to obtain boot and TCP/IP information dynamically. The relay agent allows them to obtain this information when the BOOTP/DHCP server is not on the same IP interface as the end station. You can configure the switch so that the messages are forwarded from one interface to the appropriate server on another interface.

DNS Relay

The Domain Name System (DNS) is used to map names to IP addresses. DNS relay enables the switch to act as a DNS cache or proxy. It forwards DNS requests to DNS servers only if it can't resolve the name from its cache.

If you enable DNS relay on the switch, you can specify a primary and secondary DNS server to forward requests that the switch cannot resolve. You can also specify that requests destined for specific DNS servers should be first serviced by looking in the switch's table.

Packet Forwarding

The switch maintains a forwarding table. This table contains the relationship between a destination MAC or IP addresses and the Ethernet port or gateway router the destination resides on. This information is then used to forward packets. This reduces the traffic congestion on the network, because packets, instead of being transmitted to all ports, are transmitted to the destination port only. For example, if Port 1 receives a packet destined for a station on Port 2, the switch transmits that packet through Port 2 only, and transmits nothing through the other ports. This process is referred to as "learning" the network topology.

You can configure forwarding rules for the following:

- MAC address aging
- MAC address forwarding
- IP address to a specified gateway
- IP address to a specified MAC address

MAC Address Aging Time

The aging time affects the learning process of the switch. Dynamic forwarding table entries, which are made up of the source and destination MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time.

The aging time can be 10 — 1,000,000 seconds with a default value of 300 seconds. A very long aging time can result in dynamic forwarding table entries that are out-of-date or no longer exist. This may cause incorrect packet forwarding decisions by the switch.

If the aging time is too short, however, many entries may be aged out too soon. This will result in a high percentage of received packets whose source addresses cannot be found in the forwarding table, in which case the switch will broadcast the packet to all ports, negating many of the benefits of having a switch.

Static forwarding entries are not affected by the aging time.

MAC Address Forwarding

The switch allows you to configure how unicast and multicast packets are forwarded.

- For unicast packets, you specify the MAC address and then either select the port that they will be forwarded to or have them dropped (called “BlackHole”).
- For multicast packets, you specify the MAC address and then select the ports they can be forwarded to.

Storm Control

You can also set thresholds to control broadcast and multicast storms. When the threshold is exceeded, the switch drops the multicast or broadcast traffic. When traffic levels drop below the threshold, the switch resumes forwarding the traffic again.

The thresholds are applied to all Ethernet ports and cannot be set for individual ports. The threshold specifies in thousands the number of broadcast or multicast packets per second a port can receive before triggering a storm control response. The possible range is 0 — 255 KB packets per second. This threshold can be configured to apply to broadcast packets, to multicast packets, or to both.

Traffic Control

You can also set thresholds for the amount of traffic a port can handle before triggering flow control. The flow control threshold sets the limit for the maximum amount of memory a port can use to hold packets. When a port reaches this limit, the port sends a signal to slow down the packets coming in:

- Ports in half-duplex mode assert a jamming signal.
- Ports in full-duplex mode send PAUSE frames.

You can set the flow control thresholds for individual ports and then monitor the status.

IP Forwarding

You can configure how packets are forwarded, based on their IP address, by configuring entries for the ARP table and the routing table.

ARP Table

The ARP table maintains the mappings from Internet addresses (IP) to hardware addresses (MAC). There are two types of ARP entries: dynamic and static.

When a static ARP entry is added to the switch’s ARP table, the switch does not send an ARP query to the configured IP address. This allows the switch to connect to devices that have not implement ARP.

The ARP table has the following characteristics:

- Static entries have higher precedence than dynamic entries. Therefore, a static entry will not be overwritten by a dynamic entry.
- The aging time for dynamic entries is 20 minutes. This value is not configurable.
- The table can be up to 2 KB in size.
- Up to 32 static entries are allowed in the table.

Router Ports

Router ports allow multicast packets to be propagated throughout the network. Router ports can be either static or dynamic. Static router ports are special routes that you manually enter into the switch's routing table. Usually it is a port that has a router attached to it, and the router has a connection to a WAN or to the Internet. Static router ports should be used sparingly, because when a network failure occurs, they do not change. However, they can reduce network traffic by eliminating the need for a routing protocol on a local network. For example, a local network, which has only one link to the network, is an ideal candidate for a static route. You can also use them to restrict the transmission path a datagram must follow, based on the datagram's destination address. You can add up to 32 static entries into the routing table.

Dynamic router ports are added by the switch. The switch monitors each port for UDP multicast packets and IGMP multicast group membership reports. When these packets are detected on a port, that port is dynamically assigned as a router port.

Priority

MAC address priority is a Layer 2 Class of Service. It allows certain frames, based on their MAC address, to receive special handling.

The frames can be prioritized based on where the MAC address appears:

- The source only
- The destination only
- Both the source and destination

Frames that match the criteria are given a priority tag. The switch supports only four hardware priority levels per egress port, so the eight levels are mapped to four as listed in the table below.

Priority in Frames	Priority Queue of ASIC
0 - 1	0
2 - 3	1
4 - 5	2
6 - 7	3

After an Ethernet frame has been prioritized, the switch forwards the Ethernet frame using the strict priority-based scheduling algorithm. With this policy, any packets residing in a higher priority queue are always transmitted first. Only when these queues are empty are packets in lower priority queues transmitted.

Filtering

A filtering database is used to segment the network and control communication between segments. It can also filter packets off the network for intrusion control. Static filtering entries can be made by MAC or IP addresses.

Each port on the switch is a unique collision domain, and the switch filters (discards) packets whose destination lies on the same port as where it originated. This keeps local packets from disrupting communications on other parts of the network.

The switch does some filtering automatically:

- **Dynamic filtering**—The switch automatic learns and ages MAC addresses and their location on the network. Filtering occurs to keep local traffic confined to its segment.
- **Filtering done by the Spanning Tree Protocol**—STP filters packets based on topology, ensuring that signal loops don't occur.
- **Filtering done for VLAN integrity**—The switch filters packets from a member of a VLAN (VLAN 2, for example) destined for a device on another VLAN (VLAN 3).

You can also manually configure the switch to drop packets from specified MAC and IP addresses. Whenever a switch encounters a packet originating from, or destined to, a MAC address or an IP address entered into the filter table, the switch discards the packet.

MAC Address Filtering

When filtering by MAC address, you have two options:

- **Static**—This option allows you to specify which port handles the packets from the specified MAC address.
- **BlackHole**—This option allows you to have the switch drop the packets from, or to, a specified MAC address.

IP Address Filtering

When filtering by IP address, you have three options. You can have the switch drop the packet based on where the IP address appears:

- In the source
- In the destination
- In both the source and destination

The table can contain 32 entries, and two table entries are needed to configure a bi-direction filter.

Port Mirroring

Port mirroring allows the traffic on a particular port to be monitored by sending copies of the packets to a target port. You can then attach a logic analyzer or a RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner. You can configure only one port to be a target port, but you can select multiple ports to be mirrored to this target port. For optimum performance, you should mirror three or fewer ports at any given time.

You can select which traffic is mirrored. For a given mirrored port (or source port), you can select to mirror only incoming traffic, only outgoing traffic, or both.

When mirroring ports, remember the following:

- The source port cannot be the target port.

- The target port cannot belong to a link aggregation group.
- The target port should be operating at the same or higher speed than the source port. If the target port is operating at a lower speed than the source port, packets will be lost.

Spanning Tree Protocol

The IEEE 802.1D Spanning Tree Protocol allows for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link.

It is possible to cause serious degradation of network performance if the Spanning Tree is incorrectly configured. The switch's default global setting should be used by the majority of installations.

The ZT8101 switch performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees from any combination of ports contained within a single switch, in user-specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

STP Levels and Parameters

The ZT8101 switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.

- On the switch level, STP calculates the Bridge Identifier for each switch and then sets the Root Bridge and the Designated Bridges.
- On the port level, STP sets the Root Port and the Designated Ports.

The factory default settings should cover the majority of installations. Setting up STP using values other than the defaults can be complex. Therefore, we recommend that you keep the default factory settings, and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the Priority setting, or influencing STP to choose a particular port to block using the Port Priority and Port Cost settings is, however, relatively simple.

For example, if all switches have STP enabled with default settings, the switch with the lowest MAC address in the network becomes the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

STP Parameters for the Switch Level

The following are the user-configurable STP parameters for the switch level.

Parameter	Description	Default Value
Bridge Identifier	Specifies the combination of the user-set priority and the switch's MAC address. The bridge identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address. The only portion that a user can configure is the priority.	32768 + MAC address
Priority	Specifies the relative priority for each switch. Lower numbers specify a higher priority and a greater chance of a given switch being elected as the root bridge	32768
Hello Time	Specifies the length of time between broadcasts of the hello message by the switch. It can be set from 1 — 10 seconds. This interval is not used until the switch becomes (if ever) the root bridge. The Hello Time parameter cannot be longer than the Max Age parameter.	2 seconds
Max Age	Measures the age of a received BPDU for a port, and ensures that the BPDU is discarded when its age exceeds the value of the Max Age parameter. It can be set from 6 — 40 seconds.	20 seconds
Forward Delay	Specifies the time a port can remaining in the listening state while moving from the blocking state to the forwarding state. It can be set from 4 — 30 seconds.	15 seconds

Use the following formulas when setting these parameters:

- Max Age = 2 x (Forward Delay -1second)
- Mag Age = 2 x (Hello Time + 1 second)

STP Parameters for the Port Level

The following are the user-configurable STP parameters for the port or port group level.

Variable	Description	Default Value
Port Priority	A relative priority for each port. Lower numbers specify a higher priority and a greater chance of a given port being elected as the root port	32768
Port Cost	A value used by STP to evaluate paths. STP calculates path costs and selects the path with the minimum cost as the active path.	• 100 for 10 Mbps Fast Etherenet ports • 19 for 100 Mbps Fast Ethernet ports • 4 for 1000 Mbps Gigabit Ethernet ports

Link Aggregation

Link aggregation allows several ports to be grouped so that they can act as a single port. This is done to either increase the bandwidth of a network connection or to ensure fault recovery. The group has the following assignments:

- **Master port**—This port is the Ethernet port with the lowest port number. All member ports are configured to use its port settings and become members of its VLAN.
- **Anchor port**—This port is in charge of sending control packets, such as spanning tree BPDUs, and also the flooding of multicast frames. When a link change event occurs in the group, the anchor port may be re-elected.

When a link aggregation group is deleted or disabled, the ports retain their reassigned port settings. They do not recover their original port settings. For example, suppose that Port 1 belongs to VLAN1 and Port 2 belongs to VLAN2. When you create a group with a starting point of Port 1 and a width of 2, Port 2 will be added to VLAN1 and removed from VLAN2 automatically. If you delete or disable the group later, the Port 2 will still be assigned to VLAN1.

The switch also assigns the group a anchor port. This port is in charge of sending control packets and also the flooding of multicast frames. When a link change event occurs in the group, the anchor port may be re-elected.

The ZT8101 supports six link aggregation groups, which may include from 2 — 8 switch ports each, except for a gigabit link aggregation group, which consists of the two gigabit Ethernet ports on the front panel.

Remember the following guidelines when creating a link aggregation group:

- The ports used in a group must all be of the same media type (10/100 Mbps fiber or 100/1000 Mbps fiber).
- The ports used for each group must all be on the same switch.
- The ports in a group must be contiguous (they must have sequential port numbers).
- Ports can only be assigned to one link aggregation group.
- None of the ports in a group can be configured as a mirror source port or a mirror target port.
- All of the ports in a group must be treated as a whole when added to or deleted from a VLAN.
- STP will use the port parameters of the base port in the calculation of port cost and in determining the state of the link aggregation group. The following formula is used to calculate the path cost:

  path cost of master port - the number of ports in the group
- STP treats all ports in a link aggregation group as a single port and will block the entire group if it is a redundant link.
- Data transmitted to a specific host (destination address) will always be transmitted over the same port in the group. This allows packets in a data stream to arrive in the same order they were sent.
- The configuration of the lowest numbered port in the group becomes the configuration for all of the ports in the aggregation group. This port is called the base port of the group, and all configuration options—including the VLAN configuration—that can be applied to the base port are applied to the entire link aggregation group.

- Load balancing is automatically applied to the links in the aggregation group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.
- Switches that use a load-balancing scheme that sends the packets of a host-to-host data stream over multiple ports cannot have a trunk connection with the ZT8101 switch.
- Enable the group prior to connecting any cable between the switches to avoid creating a data loop. Disconnect all link aggregation cables or disable the ports before removing a link aggregation group to avoid creating a data loop.

VLANs

VLANs allow you to group some physical ports as if they were on the same LAN. VLAN can be created either statically or dynamically.

- **Static VLAN**—Ports are assigned to a specific VLAN.
- **Dynamic VLAN**—Using GVRP (GARP VLAN Registration Protocol), ports are allowed to dynamically join a VLAN group.

VLANs reduce traffic because traffic between VLANs is restricted. Bridges forward unicast, multicast, and broadcast traffic only on LAN segments that serve the VLAN to which the traffic belongs.

For static VLAN configuration, the switch supports two kinds of VLANs:

- **Static port**—Uses untagged frames.
- **Static IEEE 802.1Q VLAN**—Uses tagged or untagged frames. Ports that use tagged frames can belong to more than one VLAN.

By default, all ports belong to a special VLAN called “default.” This default VLAN is a static IEEE802.1Q VLAN, which has the following unique characteristics:

- The name and the type fields are read-only.
- It cannot be deleted.
- It can contain no VLAN members.
- Its VID is 1, which cannot be changed.

All user-configured VLANs have the following characteristics:

- The size of VLAN name field is 32 bytes.
- Ingress checking is set to on.
- Up to 32 static VLANs can be configured.

The switch supports a maximum of 255 VLANs (64 static, the rest dynamic).

Static Port-Based VLANs

A port-based VLAN is the easiest type to configure on the switch because you only need to specify the following:

- VLAN name

- Member ports

The complexity of the VLAN configuration is hidden. The switch applies the following rules when it creates the VLAN:

- Tagged frames are discarded. With port-based VLANs, frames are assumed to be untagged, so that the VLAN members do not receive frames coming from another VLAN.
- VLAN ID is assigned using an internal algorithm. The switch allocates the largest free VLAN ID that is smaller than 4095 (for example, 4094, 4093, 4092).
- The member port's PVID is assigned as the VLAN ID.
- A port can only belong to one port-based VLAN.

Static IEEE 802.1Q VLANs

IEEE 802.1Q VLANS have the following characteristics:

- Use filtering to assign packets to VLANs.
- Assume the presence of a single global spanning tree.
- Use an explicit tagging scheme with one-level tagging.

A static IEEE 802.1Q VLAN is more complex than a port-based VLAN, but it is also more flexible. You can configure ports to be tagged, untagged, or forbidden.

- **Tagged Member Port**—Ports with tagging enabled put the VID number, priority and other VLAN information into the header of all packets that flow into and out of it. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q-compliant devices on the network to make packet forwarding decisions. The tagging feature allows VLANs to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally. Tagged ports can belong to more than one 802.1Q VLAN.
- **Untagged Member Port**—Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into and out of it. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device and allow VLANs to work with legacy switches that don't recognize VLAN tags in packet headers. The receiving port can only forward untagged packets to the VLAN it belongs to.
- **Forbidden Port**—The forbidden flag designates the port as not being a member of the VLAN and prevents packets tagged with the VLAN's VID from entering the port.

You can enable or disable the following per port for IEEE 802.1Q VLANs:

- GVRP
- Ingress Checking

GVRP

GVRP (Group VLAN Registration Protocol) must be enabled globally on the switch before individual ports can be enabled.

A global flag controls the switch's ability to participate in dynamically configured VLANs. If the GVRP flag is enabled, ports can dynamically register to be a member of a VLAN. If the flag is disabled, only statically configured ports can be members of VLANs.

The default value is disabled.

Ingress Checking

An ingress port is a port on a switch where packets are flowing into the switch and VLAN forwarding decisions must be made. Packets are forwarded according to the following rules:

- If ingress checking is disabled on a port, the switch forwards all incoming tagged frames, even when the receiving port is not a member of the destination VLAN of the frame.
- If ingress checking is enabled on a port, the switch examines the VLAN information in the packet header (if present) and decides whether to forward the packet.

When ingress checking is enabled, the switch uses different rules based on whether the incoming packet is tagged. If the packet is tagged with VLAN information, the ingress port uses the following rules to determine whether to forward the packet.

- It determines if the ingress port itself is a member of the tagged VLAN. If it is not, the packet is dropped.
- If the ingress port is a member of the 802.1Q VLAN, the switch determines if the destination port is a member of the 802.1Q VLAN. If it is not, the packet is dropped.
- If the destination port is a member of the 802.1Q VLAN, the packet is forwarded, and the destination port transmits it to its attached network segment.

If the packet is not tagged with VLAN information, the ingress port tags the packet with its own PVID as a VID (if the port is a tagging port). It then uses the following rules to determine whether to forward the packet:

- If the destination port is a member of the same VLAN (has the same VID) as the ingress port, the packet is forwarded, and the destination port transmits it on its attached network segment.
- If it is not a member of the same VLAN, the packet is dropped.

This process is used to conserve bandwidth within the switch by dropping packets that are not on the same VLAN as the ingress port at the point of reception. This eliminates the subsequent processing of packets that will just be dropped by the destination port.

Broadcast Storm Control and VLANs

The ZT8101 switch has broadcast sensors and filters built into each port to control broadcast storms, but VLANs can also be used to segment broadcast domains. They do this by forwarding packets only to ports that are members of the same VLAN. Other parts of the network are effectively shielded. Thus, the smaller the broadcast domain, the smaller effect a broadcast storm will have. Because VLANs are implemented at each switch port, they can be quite effective in limiting the scope of broadcast storms.

Layer 3-Based VLANs

Layer 3-based VLANs use network-layer addresses (subnet address for TCP/IP) to determine VLAN membership. These VLANs are based on Layer 3 information, but this does not constitute a "routing" function.

Note: The ZT8101 allows an IP subnet to be configured for each 802.1Q VLAN that exists on the switch.

Even though a switch inspects a packet's IP address to determine VLAN membership, no route calculation is performed, the RIP protocol is not employed, and packets traversing the switch are bridged using the Spanning Tree algorithm.

A switch that implements Layer 3 (or subnet) VLANs without performing any routing function between these VLANs is referred to as performing "IP switching."

- IP switching does not allow packets to cross VLANs (in this case, IP subnets) without a network device performing a routing function between the VLANs (IP subnets).
- The ZT8101 switch does not directly support IP switching; however, you can configure the switch to imitate this behavior by assigning IP subnets to configured VLANs and then disabling the Routing Information Protocol (RIP). This prevents packets from crossing IP subnets without going through an external router.

Multi-Netting

In legacy networks, multi-netting is commonly used to configure a physical router port with more than one IP interface. In a Layer 3 switch, an IP interface is bound to a single VLAN. To accommodate multi-netting, you must configure two or more tagged VLANs to span the same physical ports and then assign each VLAN a different IP address.

The VLANs must include tagged ports, because untagged ports can only belong to one VLAN.

IP Interfaces

An IP interface associates an IP address with a specific VLAN, which allows the VLAN to be configured for RIP and multicasting protocols. Each VLAN must be configured prior to setting up the corresponding IP interface. The switch has one pre-configured IP interface. You can add additional IP interfaces for each user-defined VLAN.

System IP Interface

The switch's pre-configured IP interface is called **System**. This name cannot be modified. By default, the System IP interface is bound to the default VLAN (VID=1). This VLAN contains all the switch's Ethernet ports.

You can assign or change the IP address of the System IP interface with a manual assignment, BOOP, or DHCP. The switch uses the IP address assigned to the switch as the IP address for the System IP interface.

Note: BOOTP and DHCP are only available for the System IP interface.

Additional IP Interfaces

To add an IP interface to the switch, you must first configure a VLAN and then associate an IP address (subnet mask and gateway) with the VLAN. These user-defined IP interfaces differ from the System IP interface in the following ways:

- They cannot use BOOTP/DHCP to get a dynamic IP address. They must be assigned a manual IP address.
- They can be renamed. However, when the change is applied, all other settings for the IP interface are changed to their default values. This includes the settings for RIP and the IP multicast protocols.

IP Addressing Scheme

An IP addressing scheme must be established and implemented when the IP interfaces are set up on the switch.

For example:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineering	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4
Backbone	6	25, 26

In this case, six IP interfaces (or six subnets) are required, so a CIDR notation of 10.32.0.0/11 (or a 11-bit) addressing scheme will work. This addressing scheme will give a subnet mask of 11111111.11100000.00000000.00000000 (binary) or 255.224.0.0 (decimal).

A10.xxx.xxx.xxx IP address notation provide six network addresses. For example:

VLAN Name	VID	Network Address
System (default)	1	10.32.0.0
Engineering	2	10.64.0.0
Marketing	3	10.96.0.0
Finance	4	10.128.0.0
Sales	5	10.160.0.0
Backbone	6	10.192.0.0

The six IP interfaces, each with an IP address listed in the table above and a subnet mask of 255.224.0.0, can be entered into the Setup IP Interface form.

IP interfaces consist of two parts—a subnet mask and an IP address.

Each IP interface listed above provides a maximum of 2,097,150 unique IP addresses per interface (assuming the 10.xxx.xxx.xxx notation).

Multicasting

Multicasting is a group of protocols and tools that enable a single source point to send packets to groups of multiple destination points with persistent connections that last for some amount of time. The main advantage of multicasting, when compared to broadcasting, is a decrease in the network load.

- Broadcast packets are sent to all devices on a subnetwork.
- Unicast packets are sent from a single network device to another single network device.
- Multicast packets are sent to a group of network devices.

The following table lists some of the permanently assigned multicast addresses.

Address	Description
224.0.0.0	Base Address (reserved)
224.0.0.1	All Systems on this subnet
224.0.0.2	All Routers on this subnet
224.0.0.3	Unassigned
224.0.0.4	DVMRP Routers
224.0.0.5	OSPF IGP Routers
224.0.0.6	OSPF IGP Designated Routers
224.0.0.7	ST Routers
224.0.0.8	ST Hosts
224.0.0.9	All RIP2 Routers
224.0.0.10	All IGRP Routers
224.0.0.11	Mobile Agents
224.0.0.12	DHCP Servers and Relay Agents
224.0.0.13	All PIM Routers
224.0.0.14	RSVP Encapsulation
224.0.0.15	All CBT Routers
224.0.0.16	Designated Sbm
224.0.0.17	All Sbms
224.0.0.18	VRRP
224.0.0.19 through 224.0.0.225 except 224.0.0.21	Unassigned
224.0.0.21	DVMRP on MOSPF

Internet Group Management Protocol (IGMP)

Multicasting relies on the concept of nodes joining and leaving multicast groups. Nodes use IGMP to join and then leave a multicast group. Based on the IGMP reports the switch receives from the nodes, it can decide whether to forward a multicast packet on a particular interface.

The ZT8101 switch supports both IGMPv1 and IGMPv2. You can select which version to use on a particular VLAN.

IGMPv2 is an enhancement to the original IGMP and includes a few extensions such as a procedure for the election of the multicast querier for each LAN, explicit leave messages for faster pruning, and group-specific query messages.

IGMP Queriers

An IGMP querier sends IGMP Query packets periodically to help to maintain the multicast group information for a VLAN. When IGMP Snooping is enabled for a VLAN, the switch uses the following states to determine whether the VLAN becomes a querier:

- **Non-Querier**—Prevents the VLAN from becoming a querier.
- **V1 Querier**—Enables the sending of IGMPv1 query packets. If no querier is present in the VLAN or the VLAN's IP address is smaller than current V1 querier, the switch becomes the querier for the VLAN. IGMPv2 group-specific query and leave packets are not handled.
- **V2 Querier**—If a V1 querier is present in the VLAN, the switch remains silent. If no querier is present in the VLAN or the VLAN's IP address is smaller than current V2 querier, the switch becomes the querier for the VLAN. The switch then handles IGMPv2 group-specific query and leave packets.

When receiving an IGMPv2 leave packet, the IGMP interface issues an IGMPv2 group specific query packet immediately and waits one second to check if any IGMP reports are received on the ports. If not, the port is removed from the IGMP group member list, and the group's multicast data is not forwarded to this port until an IGMP report is received again.

If the IGMP interface is designated as the IGMP querier, the switch uses the following intervals for sending query packets:

- When you enable IGMP snooping or boot the switch with the querier option enabled, the first query packet will not be sent for 255 seconds. This time delay is non-standard.
- The second query packet will be sent after the Startup Querier Interval, which is one fourth of the Query Interval. By default, this is 31 seconds.
- The next query packets will be sent periodically according to the Query Interval. The default Query Interval is 125 seconds.

IGMP Snooping

IGMP Snooping is a feature that reduces the flooding of IP multicast traffic. The default behavior for handling a multicast packet is to flood the packet to all members of a VLAN. With IGMP Snooping, only the active member ports receive the data.

All groups learned by IGMP Snooping are recorded in an internal group table with the VLAN ID and Multicast Group Address used as the table's index. The table's port list stores the active member ports for this group. This table can contain a maximum of 128 groups. If the active multicast groups exceed this limit, the new group's data will be flooded in the VLAN.

You can globally enable or disable IGMP Snooping on the switch. You can also enable or disable the snooping for a specific VLAN. You must enable IGMP globally for it to be enabled on a specific VLAN. By default, the IGMP global flag is off and VLAN flag is on. Thus, when you enable IGMP globally, it is enabled on all VLANs.

You can configure the switch to snoop and to keep track of IGMP groups. These two interact in the following ways:

- If the IP interface has IGMP Snooping configured for the associated VLAN, the configuration of IGMP Snooping will be overwritten by the IGMP group settings. On such VLANs, the per-VLAN flag is the only available configurable option on the IGMP Snooping screen.
- If the IGMP group settings are disabled on the interface, IGMP Snooping on the VLAN becomes configurable and the switch uses these settings for the VLAN.

Note: The switch supports a maximum of 255 VLANs and a maximum of 128 IGMP Snooping groups. If you create more than 128 VLANs with IGMP Snooping enabled, some of those VLANs will not be added to the IGMP Snooping table and the group's data will be flooded in the VLAN.

IGMP Group Settings

An IP host uses IGMP to register its IP multicast group membership with the switch. Periodically, the switch queries the multicast group to see if the group is still in use and takes one of the following actions:

- If the group is still active, a single IP host responds to the query, and the group registration is maintained.
- If the group is inactive and a report is not received within the time limit for a response, the group registration is removed.

Routing Protocols

This section presents an overview of routing protocols that the switch supports.

RIP

The Routing Information Protocol (RIP) is a distance-vector protocol that uses hop count as its criteria for making routing decisions. The ZT8101 switch supports both RIP v1 and RIP v2. You can configure the following RIP options:

- Enable or disable RIP on the switch
- Enable or disable transmitting RIP packets on a specific IP interface
- Enable or disable receiving RIP packets on a specific IP interface

Distance Vector Multicast Routing Protocol (DVMRP)

The Distance Vector Multicast Routing Protocol (DVMRP) is a hop-based method of building multicast delivery trees from multicast sources to all network nodes. Because the delivery trees are "pruned" and use the "shortest path," DVMRP is relatively efficient. Because multicast group membership information is forwarded by a distance-vector algorithm, propagation is slow. DVMRP is optimized for high delay (high latency) and relatively low bandwidth networks, and it can be considered as a "best-effort" multicasting protocol.

The switch supports DVMRP v3.

Protocol-Independent Multicast - Dense Mode (PIM-DM)

The Protocol Independent Multicast - Dense Mode (PIM-DM) protocol should be used in networks with a low delay (low latency) and high bandwidth because PIM-DM is optimized to guarantee delivery of multicast packets, not to reduce overhead. The switch supports PIM-DM v2.

The PIM-DM multicast routing protocol assumes that all downstream routers want to receive multicast messages and relies on explicit prune messages from downstream routers to remove branches from the multicast delivery tree that do not contain multicast group members.

PIM-DM has no explicit “join” messages. It relies on periodic flooding of multicast messages to all interfaces. It then waits for the following:

- A timer to expire (the join/prune interval)
- The downstream routers to transmit explicit “prune” messages indicating that there are no multicast members on their respective branches.

PIM-DM then removes these branches (“prunes” them) from the multicast delivery tree.

Because a member of a pruned branch of a multicast delivery tree may want to join a multicast delivery group (at some point in the future), the protocol periodically removes the prune information from its database and floods multicast messages to all interfaces on that branch. The interval for removing prune information is the join/prune interval.

Using the Telnet Console 4

Your ZT8101 Fast Ethernet Switch supports a console management interface that allows you to set up and control your switch, either with an ordinary terminal (or terminal emulator) or over a TCP/IP network using a Telnet application. This chapter describes how to use the Telnet Console to access the switch, change its settings, and monitor its operation.

Note: Switch configuration settings that are saved with **APPLY** are only active until the switch is rebooted. Settings that are saved to non-volatile RAM (with the **Save Changes** option from the Main Menu) are retained.

Before You Start

The ZT8101 switch supports a wide array of functions and provides great flexibility and increased network performance by eliminating the routing bottleneck between networks: the WAN, the Internet, and the intranet. This new generation switch performs routing functions in hardware rather than software. To take full advantage of this flexibility and rich feature set, you need to carefully plan a deployment strategy that will maximize the potential of the ZT8101 switch.

This plan should include a

- "General Deployment Strategy"
- "VLAN Layout"
- "IP Addressing Scheme for VLANs"
- "Static Route Assessment"

General Deployment Strategy

- **Determine how to segment the network—**This involves creating VLANs in an existing Layer 2 switched network.
- **Develop an IP addressing scheme—**This involves allocating a block of IP addresses to each network segment. Each network subnet is then assigned a network address and a subnet mask.
- **Determine which network resources must be shared by the subnets and how they will be shared—**You can connect shared resources directly to the Layer 3 switch, if need be. Or you can set up static routes to make the shared resources accessible.
- **Determine how each subnet will communicate with the WAN or Internet—**Again, static routes should be determined and default gateways identified.
- **Develop a security scheme—**Some subnets on the network need more security or should be isolated from the other subnets. You can use MAC and IP filtering. You can also configure one or more VLANs on the Layer 3 switch without an IP subnet. Without a subnet mask, these VLANs function as a Layer 2 VLAN and require an external router to connect to the rest of the network.
- **Develop a policy scheme—**Some subnets will have a greater need for multicasting bandwidth, for example. A policy is a mechanism to alter the normal packet forwarding in a

network device, and can be used to intelligently allocate bandwidth to time-critical applications such as the integration of voice, video, and data on the network.

- **Develop a redundancy scheme—** Planning redundant links and routes to network-critical resources can save valuable time in case a link or a device fails. You can use the Spanning Tree Protocol to block the redundant link until it is needed.

VLAN Layout

VLANs on the ZT8101 switch have more functions than on a traditional Layer 2 switch and must therefore be laid-out and configured with more care. Layer 3 VLANs could be thought of as network links rather than as a collection of associated end users. Further, Layer 3 VLANs are assigned an IP network address and subnet mask to enable IP routing between them.

Layer 3 VLANs must be configured on the switch before they can be assigned IP subnets. Also, the static VLAN configuration is specified on a per port basis. On the ZT8101 switch, a VLAN can consist of end nodes, just like a traditional Layer 2 switch. But a VLAN can also consist of one or more Layer 2 switches, each of which is connected to multiple end nodes or network resources.

For example, a Layer 3 VLAN, consisting of four ports, could be connected to four switches. If these switches each have 24 ports, then the Layer 3 VLAN would contain 96 (4 x 24) end nodes. Assigning an IP subnet to the Layer 3 VLAN would allow wire-speed IP routing from the WAN to each end node and between end nodes.

Therefore, the IP subnets for a network must be determined first, and the VLANs configured on the switch to accommodate the IP subnets. Finally, the IP subnets can be assigned to the VLANs.

IP Addressing Scheme for VLANs

The ZT8101 switch allows the assignment of IP subnets to individual VLANs. Any VLAN configured on the switch that is not assigned an IP subnet will behave as a Layer 2 VLAN and will not be capable of IP routing.

Developing an IP addressing scheme is a complex subject. As you are developing your scheme, remember that the switch requires a unique IP address for all the anticipated end nodes on each Layer 3 VLAN. The switch treats a VLAN with an IP network address and subnet mask as an IP interface in an IP routing mode.

Static Route Assessment

You need to define static routes for the following types of subnets:

- Subnets not accessible through the default route
- Subnets that the switch does not already know about internally
- Subnets not learned through the dynamic routing protocols

You determine how these packets are routed by entering static routes into the switch’s static/default routing table.

Getting Started

This section describes the conventions (function keys and entry fields) and explains how to log in to the switch for the first time.

Console Usage Conventions

You can use the following function keys with the Telnet Console.

Key	Action
Arrows	Moves the cursor around the screen.
Tab	Moves the cursor to the next menu or field.
Backspace	Moves the cursor to the previous menu or field.
Esc	Returns to the previous screen.
CTRL+T	Returns to the Main Menu.
CTRL+R	Refreshes the current screen.
CTRL+A	Applies the settings. This is the same as highlighting **APPLY** and pressing **Enter**.
CTRL+P	Displays the previous page of information.
CTRL+N	Displays the next page of information.
Spacebar	Shows the next available option in a selection box.

You use the following fields to enter or select items.

Field	Description
[Entry]	Allows you to input a string or integer value.
<Toggle>	Allows you to use the spacebar to toggle though a list of options.
BUTTON	Allows the user to highlight it and press Enter to perform the designated action such as **APPLY** or **SAV**E.

The default mode for an Edit field is insert. You can use the **Insert** key to toggle between insert and overstrike.

The **APPLY** button (or CTRL+A) only applies for the current session. Use Save Changes from the Main Menu for permanent changes. Save Changes enters the current switch configuration into non-volatile RAM for use the next time the switch is rebooted.

Connecting to the Switch

You can use this interface by connecting an RS-232C serial cable to the switch's front panel serial port and to a VT100-compatible terminal or to a computer running an ordinary terminal emulator program (for example, the terminal program included with the Windows operating system). Set the terminal parameters to these values:

- VT-100/ANSI compatible

- 9,600 baud
- 8 data bits
- No parity
- One stop bit
- No flow control

You can also access the same functions over a Telnet interface. Once you have set an IP address for your switch, you can use a Telnet program (in VT-100 compatible terminal mode) to access and control the switch. All of the screens are identical, whether accessed from the serial port or from a Telnet interface.

To log in to the switch the first time

The passwords used to access the switch are case sensitive; therefore, “S” is not the same as “s.”

When you first connect to the switch, a login screen appears.

1. In a command window, enter **Telnet <IP_address>**.
   Replace <IP_address> with the address assigned to the switch.
2. In the Username field press **Enter.** There is no initial username.
3. In the Password field, press **Enter**. There is no initial password. The Main Menu appears.

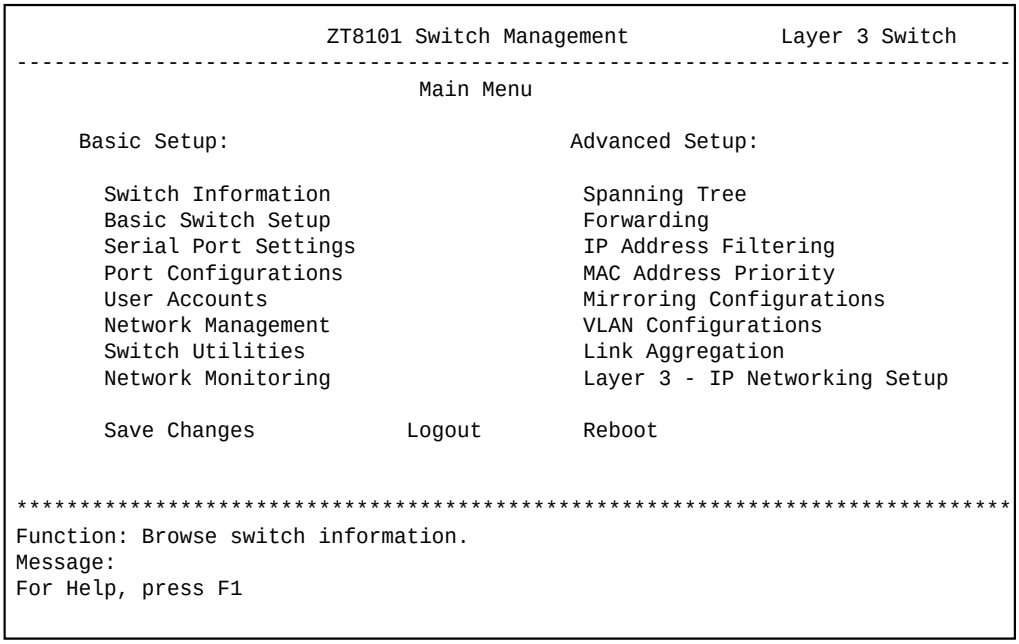
The first created user automatically has Admin privileges. One of your first configuration tasks should be to create at least one Admin-level user for the switch to protect it from unauthorized users.

Press CTRL+R to refresh the screen. This command can be used at any time to force the console program in the switch to refresh the console screen.

Note: If the arrow keys don’t work, check your terminal preferences and make sure you have enabled VT 100 Arrows.

Main Menu

The Main Menu has these options.



- **Basic Setup**
  - **Switch Information**—Display information about the switch's hardware and firmware.
  - **Basic Switch Setup**—Configure the switch's IP address.
  - **Serial Port Settings**—Configure the switch's serial port that is used for Telnet communication and terminal sessions.
  - **Port Configurations**—Enable/disable individual ports and set their speed and duplex state.
  - **User Accounts**—Set up user accounts, change their passwords, and modify their access rights.
  - **Network Management**—Set up SNMP traps and community strings.
  - **Switch Utilities**—View the history log, ping other devices, and manage firmware and configuration files.
  - **Network Monitoring**—View various statistics by port or protocol and to view various routing tables.
- **Advanced Setup**
  - **Spanning Tree**—Enable/disable the Spanning Tree Protocol (STP) for the switch and on individual ports.
  - **Forwarding**—Reduce traffic congestion on the network by configuring MAC address aging, unicast packet forwarding, storm control, and static IP routes.

  - — **IP Address Filtering**—Configure filters to drop packets from specified IP addresses or MAC addresses.
  - — **MAC Address Priority**—Configure specified MAC addresses for priority handling on source address, destination address, or both.
  - — **Mirroring Configurations**—Configure a source port to send a copy of its data to a target port for monitoring and troubleshooting.
  - — **VLAN Configurations**—Set up and administer VLANs on the switch.
  - — **Link Aggregation**—Combine ports on the switch to increase bandwidth.
  - — **Layer 3 - IP Networking Setup**—Configure IP interfaces, RIP, and multicast routing protocols.
- **Save Changes**—Save the switch's current settings in non-volatile RAM (NV_RAM) so that they are not lost when the switch is rebooted.
- **Logout**—Returns you to the login screen and closes your account.
- **Reboot**—Select which configuration file is used when the switch restarts.

Creating User Accounts

Access to the console is controlled via user accounts. You can create up to six accounts, one of which must be an Admin-level account. The other five accounts can be any combination of Admin-level and User-level accounts.

To create a new user account

1. From the Main Menu, select **User Accounts** and press **Enter**.
2. Use the spacebar to toggle the Action field to **Add**.
3. Enter the new username, assign an initial password, and then confirm the new password. Determine whether the new user should have Admin or User privileges. Use the spacebar to toggle between these options. (The next section describes the differences between these levels.)

   The first user you create must be assigned Admin privileges.
4. Highlight **APPLY** and press **Enter** to make the user addition effective.

   A listing of all user accounts and access levels is shown below the user setup menu. This list is updated when Apply is executed.
5. To delete a user, toggle the Action field to **Delete**, enter the username, highlight **APPLY,** and press **Enter**.

   You must enter an account's password to delete it.
6. To modify a user's password or privileges, toggle the Action field to **Update**, enter the username, the old password, and then modify the New Password and/or the Access Level fields. Highlight **APPLY** and press **Enter**.

Note: Remeber that **APPLY** makes changes to the switch configuration for the current session only. All changes (including user additions or updates) must be entered into non-volatile RAM using the **Save Changes** command on the Main Menu, if you want these changes to be permanent.

Admin, User+ and Normal User Privileges

The switch uses two levels of user privileges: Admin and User. Some menu selections available to users with Admin privileges may not be available to those with User privileges.

The table summarizes the Admin and User privileges:

	Admin	**User**
Switch Configuration Management		
Configuration	Yes	Read Only
Network Monitoring	Yes	Read Only
SNMP Community Strings and Trap Stations	Yes	Read Only
Update Firmware and Configuration Files	Yes	No
Switch Utilities	Yes	Ping; Read Only access to BOOTP/DHCP Relay and DNS Relay.
Factory Reset	Yes	No
Reboot Switch	Yes	No
Advanced Setup	Yes	Read Only
User Account Management		
Add/Update/Delete User Accounts	Yes	No
View User Accounts	Yes	No

To log in once you have created a registered user

1. From the Login screen, type in your username and press Enter.
2. Type in your password and press **Enter**.

The main menu screen will be displayed based on your access level or privilege.

Saving Changes

The ZT8101 switch has two levels of memory: normal RAM and non-volatile or NV-RAM. Configuration changes are made effective by highlighting **APPLY** and pressing **Enter**. When you do this, the settings are immediately applied to the switch software in RAM and immediately take effect.

Some settings, though, require you to restart the switch before they will take effect. Restarting the switch erases all settings in RAM and reloads the stored settings from the NV-RAM. Thus, it is necessary to save all setting changes to NV-RAM before rebooting the switch.

To save changes to NV-RAM

1. To retain any configuration changes permanently, from the Main Menu select **Save Changes** and press **Enter**.
2. Answer Yes to the confirmation prompt.

Reboot

1. From the Main Menu, select **Reboot** and press **Enter**.
2. Highlight one of these options and press **Enter**.

Option	Description
Reboot	Restarts the switch. Any configuration settings not saved using Save Changes from the Main Menu will be lost. The switch's configuration will be restored to the last configuration saved in NV-RAM.
Save Configuration & Reboot	Saves the current configuration to NV-RAM (identical to using Save Changes) and then restarts the switch.
Reboot & Load Factory Default Configuration	Restarts the switch using the default factory configuration. All custom configuration data will be lost.
Reboot & Load Factory Default Configuration Except IP Address	Restarts the switch using the default factory configuration, except the user configured IP address will be retained. All other configuration data will be lost.

3. Highlight Yes on the confirmation prompt and press **Enter**.

Basic Settings

This section explains some of the basic options for configuring the switch.

Condition	Task
Using SNMP for network management.	Configure the options in the Network Management Setup screens.
Installing more than one switch.	Use the Switch Utilities to save configurations for use on multiple switches.
Testing communication with other devices.	Use the Ping Test utility from the Switch Utilities menu.
Need to set the port settings for the serial port to values other than the default values.	Configure the options with the Serial Port Settings screen.

Switch Information

The Switch Information screen displays descriptive information about the switch.

From the Main Menu, select **Switch Information**. This screen contains the following information.

Field	Description
Device Type	Specifies the product name: ZT8101 Fast-Ethernet Switch.
MAC Address	Specifies the unique MAC address assigned to the switch. This address is not configurable.
Boot PROM Version	Specifies the version of the switch's boot code.
Firmware Version	Specifies the version of the firmware installed on the switch. You can update this using a switch utility.
Hardware Version	Specifies the hardware version of the main board.
Device S/N	Specifies the serial number of the device.
Name	Specifies the name assigned to the switch system. If you are installing multiple switches, you should give each a unique name.
Location	Specifies the area or location where the switch resides.
Contact	Specifies the contact person for the switch.
Spanning Tree	Indicates whether STP is enabled or disabled.
GVRP	Indicates whether the Group VLAN Registration Protocol is enabled or disabled.
IGMP Snooping	Indicates whether the Internet Group Management Protocol Snooping is enabled or disabled.
RIP	Indicates whether the Routing Information Protocol is enabled or disabled.
PIM-DM	Indicates whether Protocol Independent Multicast - Dense Mode is enabled or disabled.
DVMRP	Indicates whether the Distance Vector Multicast Routing Protocol is enabled or disabled.

Basic Switch Setup

Use the Basic Network Setup menu to set the boot-up operation for obtaining an IP address or to manually assign the IP address for the switch.

1. From the Main Menu, select **Basic Network Setup** and press **Enter**.
2. To configure the IP address, use the Arrow keys or the Tab key to modify the settings in the New Switch IP Settings column.

Parameter	Default	Description
Get IP From	Manual	Specifies the method for assigning the switch an IP address. Use the spacebar to toggle to **Manual**, **DHCP**, or **BOOTP.** (For more information about these options, see the descriptions below.)
IP Address	10.90.90.90	Specifies the IP address assigned to the switch. Only available for the Manual option.

Parameter	Default	Description
Subnet Mask	255.0.0.0	Specifies the subnet mask assigned to the switch and to the other devices on this segment of the network. Only available for the Manual option.
Default Gateway	0.0.0.0	Specifies the IP address of the device that routes to different networks. A gateway must be defined if the workstation you are going to use for switch management is located on a different IP segment than the switch. Only available for the Manual option.
VLAN Name	default	Specifies the name of the VLAN that the switch resides in. This VLAN must already exist.

3. To configure a name and contact information for the switch, enter information in these fields.

Parameter	Description
Name	Specifies the name assigned to the switch. If you are installing multiple switches, you should give each a unique name.
Location	Specifies the physical location of the switch.
Contact	Specifies the name of the person responsible for the switch.

4. Highlight **APPLY** and press **Enter**.

Get IP From Description

The switch uses the Get IP From setting to determine where to get its IP address. You must use the Manual option if you want to configure multiple IP interfaces. The manual option is also more convenient if you are going to manage the switch with Telnet Console or Web Console. Both of these consoles require you to know the IP address, and although BOOTP/DHCP usually assign the same IP address when a device reboots, there is no guarantee.

- **BOOTP**—The switch sends out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the switch looks first for a BOOTP server to provide it with this information.
- **DHCP**—The switch sends out a DHCP broadcast request when it is powered up. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the switch looks first for a DHCP server to provide it with this information.
- **Manual**—The switch uses the entered IP address, Subnet Mask, and Default Gateway. These entries should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal form) between 0—255. This option requires entries in these fields:
  - **IP Address**—This address should be a unique address on the network assigned to the switch by the network administrator.
  - **Subnet Mask**—This is a bitmask that determines the extent of the subnet that the switch is on. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.
  - **Default Gateway**—This IP address determines where packets with a destination address outside the current subnet are sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the switch to be accessible outside your local network, you can leave this field unchanged.

Network Management Setup

You use the Network Management Setup screens to display and modify parameters for the Simple Network Management Protocol (SNMP). The switch includes an on-board SNMP agent that monitors the status of its hardware, as well as the traffic passing through its ports. A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the on-board agent are controlled by community strings. To communicate with the switch, the NMS must first submit a valid community string for authentication.

To configure SNMP

You can configure up to four community strings.

1. From the Main Menu, select **Network Management** | **SNMP Configurations** and press **Enter**.
2. Configure these fields.

Field	Description
Community String	Specifies a string of up to 20 characters used for authentication of clients wanting access to the switch's SNMP agent.
Rights	Specifies the level of access for an authorized client. Use the spacebar to toggle between **Read** and **R/W** (read-write).
Status	Specifies whether the current string is Enabled or Disabled. This is used to temporarily limit access to the switch's SNMP agent. Use the spacebar to toggle between **Enabled** and **Disabled**.

3. Highlight **APPLY** and press **Enter**.

To configure trap recipients

The Trap Recipient Setup screen allows you to specify which management stations receive authentication failure messages or other trap messages from the switch. Up to three trap recipients may be entered.

1. From the Main Menu, select **Network Management | SNMP Configurations | Trap Recipients Setup** and press **Enter**.
2. Configure these fields.

Field	Description
IP Address	Specifies the IP address of the management station that will receive traps generated by the switch.
SNMP Community String	Specifies a string of up to 20 characters used for authentication of users wanting to receive traps from the switch's SNMP agent. This is similar to a password in that stations that do not know the correct string cannot receive or request SNMP information from the switch.
Status	Enables or disables the selected community string. This is used to temporarily limit a station from receiving traps generated by the switch. Use the spacebar to toggle between **Enabled** and **Disabled**.

3. Highlight **APPLY** and press **Enter**.

To configure the access list

You can specify the IP addresses of up to three management stations that will be allowed access to the management agent of the switch. If you enter IP addresses in this form, only the management stations with those IP addresses are allowed to access the management agent of the switch. All other IP addresses will be blocked.

1. From the Main Menu, select **Network Management | Access List Setup** and press **Enter**.
2. Configure these fields.

Field	Description
IP Address	Specifies the IP addresses of the management stations that you want to access to the switch's management agent.
Port	Specifies the ZT8101 switch port that the management station will use for access. Enter a number from 1—26.

3. Highlight **APPLY** and press **Enter**.

Serial Port Settings

The Serial Port Settings screen allows the configuration of the switch's serial port, which is on the front panel. Terminals must match these settings to connect to the switch.

1. From the Main Menu, select **Serial Port Settings** and press **Enter**.
2. Configure these fields.

Field	Description
Baud Rate	Sets the serial bit rate that will be used for communication the next time the switch is restarted. This setting applies only when the serial port is being used for out-of-band management. Available speeds are 9600, 19,200, 38,400 and 115,200 bits per second. The default setting is 9600.
Auto-Logout	Sets the time the interface can be idle before the switch automatically logs out the user. The options are Never, 2, 5, 10, or 15 minutes.

   Values for data bits (the number of bits used to represent one character of data) and stop bits (the number of bits used to mark the end of a unit of transmission) are displayed but are not configurable.

3. Highlight **APPLY** and press **Enter**.

Port Configurations

You can enable or disable a specific port and set its speed and duplex state.

1. From the Main Menu, select **Port Configurations** and press **Enter**.
2. Using the spacebar, toggle the View Ports field to view the ports you want to configure.
3. To configure a specific port, in the Configure Port field enter the port number or a range of ports. To configure a single port, enter that port number in both the To and From field.

4. Use the spacebar to toggle these fields to the appropriate value.

Field	Description
State	Enables or disables the currently selected ports.
Speed/Duplex	Specifies the speed and full- or half-duplex state of the ports. For 100 Mpbs ports the choices are **Auto, 10/Half, 10/Full, 100/Half**, and **100/Full**. For gigabit ports, the choices are **Auto,1000/Full**, and **100/Full**.
Flow Control	Specifies the flow control mode for the port.
Learn	Enables or disables dynamic learning of MAC addresses. You can disable MAC learning to increase the security of a specific port. Such ports only receive broadcast traffic and packets that have a destination MAC address that matches the port's MAC address.

5. Highlight **APPLY** and press **Enter**.

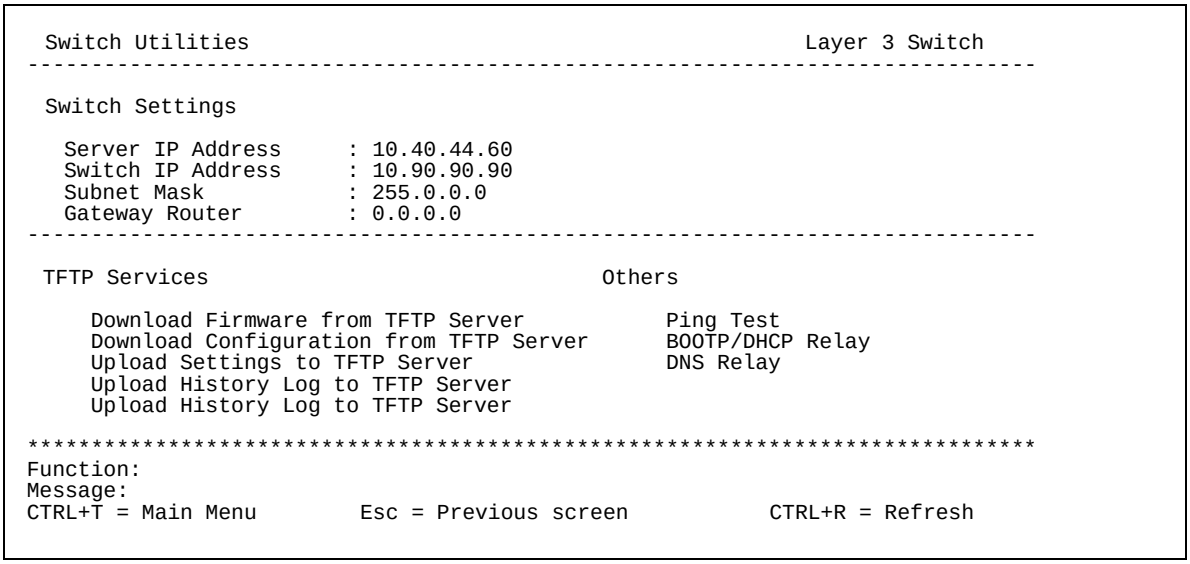
Switch Utilities

You can upgrade the switch's firmware by transferring a new firmware file from an TFTP (Trivial File Transfer Protocol) server to the switch. You can also load a configuration file into the switch from an TFTP server or save the switch's configuration file and a history log to an TFTP server.

The TFTP server must be running TFTP server software to perform the file transfer. TFTP server software is a part of many network management software packages, or can be obtained as a separate program.

The switch utilities also allow you to ping stations and to configure DNS relay and BOOTP/DHCP relay.

To access these utilities, from the Main Menu select **Switch Utilities** and press **Enter**.



To update firmware

The switch is rebooted after new firmware is downloaded. If you have any current settings that you have not saved to non-volatile RAM, use the Save Changes option on the Main Menu before starting these steps.

1. From the Main Menu, select **Switch Utilities | Download Firmware from TFTP Server** and press **Enter**.
2. In the Server IP Address field, enter the IP address of the TFTP server.
3. In the Path\Filename field, enter the path and the filename to the firmware file on the TFTP server., based from the root of the server.
4. Highlight **SAVE SETTINGS** and press **Enter**. This saves the IP address of the TFTP server so that the next time you access this screen, you won't have to enter the address or the path\filename.
5. To start the download, highlight **DOWNLOAD** and press **Enter**.

When the download is completed, the switch automatically reboots and executes the new runtime firmware.

Note: If FLASH becomes corrupted because you lose power when upgrading the firmware, you must use Zmodem to fix the problem. See "Upgrading Firmware through Zmodem" on page 19.

To download a configuration file

1. From the Main Menu, select **Switch Utilities | Download Configuration from TFTP Server** and press **Enter**.
2. In the Server IP Address field, enter the IP address of the TFTP server.
3. In the Path\Filename field, enter the path and the filename to the file on the TFTP server.
4. To start the download, highlight **DOWNLOAD** and press **Enter**.

When the download is completed, the switch saves the configuration in NV-RAM and automatically reboots.

To upload a configuration file

1. From the Main Menu, select **Switch Utilities | Upload Settings to TFTP Server** and press **Enter**.
2. In the Server IP Address field, enter the IP address of the TFTP server.
3. In the Path\Filename field, enter the path on the TFTP server and the filename.
4. Highlight **SAVE SETTINGS** and press **Enter**. This saves the IP address of the TFTP server so that the next time you access this screen, you won't have to enter the address.
5. To start the file transfer to the TFTP server, highlight **UPLOAD** and press **Enter**.

To upload a history log file

1. From the Main Menu, select **Switch Utilities | Upload History Log to TFTP Server** and press **Enter**.

2. In the Server IP Address field, enter the IP address of the TFTP server.
3. In the Path\Filename field, enter the path on the TFTP server and the filename.
4. Highlight **SAVE SETTING**S and press **Enter**. This saves the IP address of the TFTP server so that the next time you access this screen, you won't have to enter the address.
5. To start the file transfer to the TFTP server, highlight **UPLOAD** and press **Enter**.

To test connectivity with ping

1. From the Main Menu, select **Switch Utilities | Ping Test** and press **Enter**.
2. Configure these fields.

Field	Description
IP Address	Specifies the IP address of the network device to ping.
Number of Repetitions	Specifies the number of test packets to send. Three is the usual number.
Default timeout	Specifies the number of seconds to wait between sending the packets.

3. To start the test, highlight **START** and press **Enter**.

BOOTP/DHCP Relay

BOOTP/DHCP relay agent enables end stations to use a BOOTP or DHCP server to obtain TCP/IP configuration information or boot files to be loaded into memory, even if the servers are not on the local IP interface. The following conditions determine whether you need to enable BOOTP/DHCP relay:

- If the BOOTP or DCHP server and end station are on the same IP interface, no relay agent is necessary.
- If the servers and the end stations are on different IP interfaces, a relay agent is necessary for the switch to forward the messages.

The relay agent forwards these packets between IP interfaces, and therefore must know the IP addresses of the BOOTP and DHCP servers and their respective subnet names (or IP interface names).

When the switch receives packets destined for a BOOTP or DHCP server, it forwards them to specific servers as defined in the following configuration. The switch also forwards packets from the BOOTP or DHCP servers to the appropriate subnets.

To enable the BOOTP/DHCP relay agent

1. From the Main Menu, select **Switch Utilities | BOOTP/DHCP Relay** and press **Enter**.

2. Configure these fields.

Field	Description
BOOTP/DHCP Relay Status	Enables or disables the BOOTP/DHCP relay function.
BOOTP HOPS Count Limit	Sets the maximum number of hops (routers) that the BOOTP messages can be relayed through. If a packet's hop count is more than the hop count limit, the packet is dropped. The range is between 1—16 hops. The default value is 4.
BOOTP/DHCP Relay Time Threshold	Sets the minimum time (in seconds) that the switch will wait before forwarding a request packet. If the value in the seconds field of the packet is less than the relay time threshold, the packet will be dropped. The range is between 1—9999 seconds. The default value is 0 seconds.

3. Highlight **APPLY** and press **Enter**.
4. If you enabled BOOTP/DHCP Relay, highlight **BOOTP/DHCP Relay Interface Configuration** and press **Enter**.
5. Toggle the Action field to **Add** and configure these fields.

Field	Description
Interface Name	Specifies the subnet name (IP interface name) of the network that the BOOTP or DHCP server is located on.
BOOTP/DHCP Server	Specifies the IP address of the BOOTP or DHCP relay server. Multiple servers may be entered for a given subnet name (IP interface name).

6. Highlight **APPLY** and press **Enter** to make the change current.
7. To modify an entry in the table, toggle the Action field to **Modify**, enter the changes, highlight **APPLY**, and press **Enter**.
8. Use **Save Changes** on the Main Menu to enter the table into NV-RAM.

DNS Relay

DNS relay enables the switch to act as a DNS cache or proxy and to forward DNS requests to the DNS server only when required. Whether you enable DNS relay depends upon whether you want to

- Save a DNS server or a linking WAN extraneous or repetitive traffic.
- Try to shorten the response time for a DNS request on a slow or long WAN.
- Change or control the IP response for a series of DNS requests.
- Control which servers are used for DNS.

When the switch receives packets destined for a DNS server and the requests are not statically defined in the switch or previously cached, the switch forwards them to the servers as defined in the following configuration. The switch also forwards packets from the DNS servers back to the appropriate subnets.

To configure DNS Relay services

1. From the Main Menu, select **Switch Utilities | DNS Relay** and press **Enter**.

2. Configure these fields.

Field	Description
DNS Relay State	Enables or disables DNS relay on the switch.
Name Server [1]	Specifies the IP address of the primary DNS server.
Name Server [2]	Specifies the IP address of a secondary DNS server.
DNS Relay Cache Status	Enables or disables the DNS cache on the switch.
DNS Static Table Lookup Status	Enables or disables the DNS Static Table Lookup function on the switch.

3. Highlight **APPLY** and press **Enter**.
4. If you enabled DNS Static Table Lookup, highlight **Static Table Configuration** and press **Enter**.
5. Toggle the Action field to **Add** and configure these fields.

Field	Description
Domain Name	Specifies the name of the DNS server.
IP Address	Specifies the IP address of the DNS relay server.
Status	Enables or disables the entry for static look up.

6. Highlight **APPLY** and press **Enter** to make the change current.
7. To modify an entry in the table, toggle the Action field to **Modify**, enter the changes, highlight **APPLY**, and press **Enter**.
8. Use **Save Changes** on the Main Menu to enter the table into NV-RAM.

Network Monitoring

This section explains how to monitor the following aspects of the switch:

- "Port Statistics" (packets, errors, and utilization)
- "Address Tables" (MAC, IP, routing, and ARP)
- "Status" (switch history, router port table, IP multicast forwarding table, and other such tables)

Port Statistics

To view port utilization

1. From the Main Menu, select **Network Monitoring | Port Utilization** and press **Enter**.
2. To change the refresh interval, toggle the Refresh Interval field to a new value.
3. To clear the statistics and gather new information, highlight **CLEAR COUNTERS** and press **Enter**.

The Port Utilization screen displays these statistics.

Column	Description
Port	Identifies the port.
TX/sec	Displays the number of packets transmitted per second.
RX/sec	Displays the number of packets received per second.
%Util.	Displays the calculated percentage of the bandwidth being used by the device attached to the port.

To view port error statistics

1. From the Main Menu, select **Network Monitoring | Port Error Packets** and press **Enter**.
2. In the Port field, enter the port number to view.
3. Toggle the Interval field to suspend or a value from 2 seconds to 1 minute. This field sets the interval at which the error statistics are updated.
4. To clear the statistics and gather new, highlight **CLEAR COUNTERS** and press **Enter**.

The screen displays these statistics.

Field	Description
Rx Frames—Received packets	
CRC Error	Alignment. For 10 Mbps ports, the counter records CRC errors (Frame Check Sequence (FCS) and alignment errors). For 100 Mbps ports, the counter records the sum of CRC errors and code errors (frames received with rxerror signal).
Undersize	Small. The total number of frames received that were shorter than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize	Long. The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragment	Small with alignment error. The total number of frames received that were shorter than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or an alignment error.
Jabber	Long with alignment error. The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or an alignment error.
Drop Pkts	Total dropped. The total number of events in which packets were dropped due to a lack of resources.
Tx Frames—Transmitted packets	
ExDefer	Delayed. The number of frames for which the first transmission attempt on a particular interface was delayed because the medium was busy.
CRC Error	Alignment. For 10 Mbps ports, the counter records CRC errors (FCS or alignment errors). For 100 Mbps ports, the counter records the sum of CRC errors and code errors (frames received with rxerror signal).
Late Coll.	Late Collisions. The number of times that a collision is after the allowable the detection period.

Field	Description
Ex. Coll.	Excessive Collisions. The number of frames for which transmission failed due to excessive collisions.
Single Coll.	Single Collision Frames. The number of successfully transmitted frames for which transmission is inhibited by more than one collision.
Coll.	Total Collisions. An estimate of the total number of collisions on this network segment.

To view an analysis of packet sizes and types

1. From the Main Menu, select **Network Monitoring | Port Packet Analysis** and press **Enter**.
2. In the Port field, enter the port number to be analyzed.
3. Toggle the Interval field to suspend or to a value from 2 seconds to 1 minute. This field sets the interval at which the statistics are updated.
4. To clear the statistics and gather new, highlight **CLEAR COUNTERS** and press **Enter**.

The screen displays these statistics (RX indicates received and TX indicates transmitted)**.**

Column	Description
Frame Size or Type	The size in octets (bytes) of frames or the type of frame transferred through the switch.
Frame Counts	The total number of frames transferred through the switch, of the corresponding size or type.
Frames/sec	The number of frames per second transferred through the switch, of the corresponding size or type.
Total	The total number of bytes or frames received or transmitted.
Total/sec	The total number of bytes or frames received or transmitted per second.

Address Tables

To view the MAC address table

1. From the Main Menu, select **Network Monitoring | MAC Address Table** and press **Enter**.
2. Toggle the Browse By field to **ALL, MAC Address, Port**, or **VLAN**. This sets a filter to determine which MAC addresses to display. The ALL option specifies no filter.
   - The MAC Address option allows you to enter a specific address.
   - The Port option allows you to enter a port number
   - The VLAN option allows you to enter a VLAN name.
3. Highlight **BROWSE** and press **Enter** to populate the table.

The following information is displayed for each MAC address.

Column	Description
VID	The VLAN ID of the VLAN the port is a member of.
VLAN Name	The name of the VLAN.
MAC Address	The MAC address.
Port	The port corresponding to this MAC address. CPU is used to identify the MAC address for the switch.
Type	How the switch discovered the MAC address. The possible entries are Dynamic, Self, and Static. Self is used to identify the MAC address for the switch.

4. To clear all entries and force the switch to rebuild the table, highlight **CLEAR ALL** and press **Enter**. If you have selected to browse by port, you will have the option of clearing all the entries for the specified port.

To view the IP address table

1. From the Main Menu, select **Network Monitoring | IP Address Table** and press **Enter.**
2. To find a particular IP address, enter the IP address in the Jump to IP Address field, highlight **FIND**, and press **Enter**. To find all IP address known by the switch, enter 0.0.0.0 for the IP address.

The following information is displayed about each IP address.

Column	Description
Interface	The name of the IP interface corresponding to the IP address.
IP Address	The IP address corresponding to the IP interface name.
Port	The port the IP address is associated with.
Learned	The method the switch used to discover the IP address, either Dynamic or Static.

To view the routing table

1. From the Main Menu, select **Network Monitoring | Routing Table** and press **Enter**.
2. To find a particular IP address, enter the following in the appropriate fields: the IP address, the subnet mask, and the gateway. Highlight **FIND**, and press **Enter**.

   The following information is displayed in the table.

Column	Description
IP Address	The IP address corresponding to the subnet mask and gateway.
Subnet Mask	The subnet mask corresponding to the IP address.
Gateway	The gateway used to reach the IP address.
Interface Name	The IP interface name corresponding to the IP address.
Hops	The number of hops (routers) between the switch and the IP address.
Protocol	The routing protocol used to link the switch to the IP address.

To view the ARP table

1. From the Main Menu, select **Network Monitoring | ARP Table** and press **Enter.**
2. Enter the IP interface name and the IP address, highlight **FIND**, and press **Enter**.
   The following information is displayed in the table.

Column	Description
Interface	The IP interface name corresponding to the IP address.
IP Address	The IP address that corresponds to the MAC address.
MAC Address	The MAC address that corresponds to the IP address.
Type	The method that was used to enter the IP address and MAC address pair into the ARP table. The possible entries are Static, Dynamic, and Local.

3. To delete an entry from the table, enter its information in the fields, highlight **CLEAR**, and press **Enter**.

Status

To view GVRP status

From the Main Menu, select **Network Monitoring | GVRP** and press **Enter.** The GVRP Status screen contains the following information.

Field	Description
Number of IEEE 802.1Q VLANs	The number of VLANs that have been defined for the switch.
IEEE 802.1Q VLAN ID	The ID assigned to the currently displayed VLAN.
Current Egress Ports	The ports in the VLAN that are egress ports.
Current Untagged Ports	The ports in the VLAN that are untagged.
Status	The status of the VLAN, whether it is a permanent definition or whether the ports dynamically joined the VLAN.
Creation time since switch power up	The time the VLAN was created or last modified, relative to when the switch was last booted.

Note: If more than one IEEE 802.1Q VLAN has been defined for the switch, use CTRL+N to view the status of the other VLANs.

To view the router ports

Router ports can be either static or dynamic. Static ports are ports that you manually configure to route UDP multicast packets. Dynamic ports are added by the switch when the switch detects UDP multicast packets and IGMP multicast group membership reports on a port.

1. From the Main Menu, select **Network Monitoring | Router Ports** and press **Enter.**
2. In the VLAN Name field, enter the name of the VLAN to search for router ports. Highlight **FIND** and press **Enter**.

The Router Port table contains the VLAN name, and under the port groupings (1 to 8, 9 to 16, 17 to 24, and 25 to 26), a port is assigned an “S” if the port is a static router port, a “D” if the port has been dynamically assigned to be a router port, or a “-” if the port is not a router port.

To view the IGMP snooping status

You can view IGMP group information for each VLAN.

1. From the Main Menu, select **Network Monitoring | IGMP Snooping Status** and press **Enter.**
2. In the VLAN Name field, enter the name of the VLAN to retrieve IGMP snooping information. Highlight **FIND** and press **Enter**.

   The IGMP Snooping Status screen contains the following information.

Column	Description
Multicast group	The IP address of a multicast group learned by IGMP snooping.
MAC address	The corresponding MAC address learned by IGMP snooping.
Reports	The number of IGMP reports for the listed source.

To view the IP multicast forwarding table

You can browse the IP multicast forwarding table for static and dynamic (learned) entries. You can also search the table using a combination of a multicast group IP address, a multicast source IP address, and a subnet mask.

1. From the Main Menu, select **Network Monitoring | IP Multicast Forwarding Table** and press **Enter**.
2. Enter the following: a multicast group address, a source IP address, and a source subnet mask address. To find all multicast groups known to the switch, use 0.0.0.0 for all the addresses.
3. Highlight **FIND** and press **Enter**.

   The IP Multicast Forwarding Table contains the following information.

Column	Description
Multicast Group	The IP address of a multicast group used in the search for a specific entry.
Source IP Addr.	The IP address of a multicast source used in the search for a specific entry.
Source Mask	The subnet mask of a multicast source used in the search for a specific entry.
Upstream Neighbor	The IP address of the next hop router between the multicast group and the source.
Expire Time	The number of seconds the packets from the multicast source can live.
Prot.	The multicast routing protocol used by the current source.

To view the IGMP group table

You can view IGMP information for an IP interface name and a multicast group IP address.

1. From the Main Menu, select **Network Monitoring | IGMP Group Table** and press **Enter**.
2. Enter the name of an IP interface and the IP address of a multicast group. To find all multicast groups, use 0.0.0.0 for the address.

3. Highlight **FIND** and press **Enter**.
   The IGMP Group table contains the following information.

Column	Description
Interface Name	The IP interface associated with the multicast group.
Multicast Group	The IP address of the multicast group associated with the IP interface.
Last Reporter IP	The IP address of the member that responded with the last report.
Querier IP	The IP address of the member elected to be the querier for the group.
Expire	The time when the next report is due.

To view the DVMRP routing table

You can search the DVMRP routing table with an IP address and subnet mask combination.

1. From the Main Menu, select **Network Monitoring | DVMRP Routing Table** and press **Enter**.
2. Enter an IP address and a subnet mask.
3. Highlight **FIND** and press **Enter**.
   The DVMRP Routing Table contains the following information:

Column	Description
Source Address	The source IP address used to retrieve this information.
Source Mask	The source subnet mask used to retrieve this information.
Next-hop Router	The IP address of the next hop router for the source address.
Hop	The number of hops (routers) between the multicast group member and the switch.
Learned	The method the switch used to discover the source address, either Static or Dynamic.
Interface	The IP interface name of the source address.
Exp	The number of seconds before the entry expires. Expired entries display H-D (hold down) for 120 seconds before they are removed.

To view the switch's history log

From the Main Menu, select **Network Monitoring | Switch History** and press **Enter**. The Switch History screen contains the following information.

Column	Description
Seq. #	A counter incremented whenever an entry to the switch's history log is made. The table displays the last entry (highest sequence number) first.
Time	The time the history log entry was made. The time is specified in days, hours, and minutes since the switch was last restarted.
Log Text	The text describing the event that triggered the history log entry.

Advanced Setup

Most of the following options can be configured independently of the other options. However, you must configure a VLAN before you can configure an IP interface for it.

Spanning Tree

The Spanning Tree Protocol (STP) prevents loops in a network by allowing only one active path between any two network devices at a time. (For more information about using this protocol, refer to “Spanning Tree Concepts” in chapter 3.)

STP operates on two levels. On the switch level, the settings are globally implemented. On the port level, the settings are implemented on a user-defined group basis. STP must be enabled on the switch for it to be enabled on a particular port.

To configure global STP switch settings

1. From the Main Menu, select **Spanning Tree** and press **Enter**.
2. Using the spacebar, toggle the Status field to **Enabled** or **Disabled**.

   The factory default settings should cover the majority of installations, and most installations should keep these default settings.
3. To change the factory default settings, configure these fields.

Field	Default	Description
Max Age	20	Specifies the maximum time (in seconds) the switch will wait for a configuration message from the root bridge. At the end of this time, the switch will start sending out its own configuration messages for permission to become the root bridge. The device with the lowest bridge identifier becomes the root bridge (see the Priority field). Max Age must be set within the following range: • The minimum value is the higher of 6 or [2 x (Hello Time +1)] • The maximum value is the lower of 40 or [2 x (Forward Delay -1)]
Hello Time	2	Specifies the time interval (in seconds) between two configuration messages. The root bridge sends these messages at this interval to inform all other devices that it is the root bridge. This time will be used if and when your switch becomes the root bridge. It can be set from 1—10 seconds. The Hello Time cannot be longer than the Max Age. Otherwise, a configuration error occurs.

Field	Default	Description
Forward Delay	15	Specifies the maximum time (in seconds) the root device will wait before changing states (for example, from listening to blocking, from blocking to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward packets. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. • Maximum value is 30 • Minimum value is the higher of 4 or [(Max. Age / 2) +1]
Priority	32768	Priority is used in selecting the root bridge, root port, and designated port. The device with the highest priority becomes the STP root bridge. The lower the numeric value, the higher the priority. If all devices have the same priority, the device with the lowest MAC address will become the root bridge. Range: 0 to 65535.

4. Highlight **APPLY** and press **Enter**.

The following information is displayed about STP.

Field	Description
Designated Root Bridge	The IP address of the current root bridge for the STP group.
Root Priority	The current value of the bridge priority for the group.
Cost to Root	The currently assigned cost for the route from the designated STP-group port to the root bridge.
Root Port	The port number of the root port.
Last Topology Change	The time (in seconds) since the last change in the root bridge or designated STP-group port.
Topology Change Count	The number of topology changes since the switch was last restarted.

To define the port members of an STP group

The switch allows you to configure Spanning Tree Groups that consist of a group of ports that will be handled as though they were a single spanning tree device. An STP group uses the switch-level parameters entered above, with the addition of port priority and port cost.

An STP group spanning tree works in the same way as the switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected (on the basis of port priority and port cost) to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the switch level.

An STP port group should correspond to a VLAN group of ports.

1. From the Main Menu, select **Spanning Tree | Port Settings** and press **Enter**.

2. Configure these fields.

Field	Description
View Ports	Specifies the range of ports to view. The Fast Ethernet ports are displayed for configuration in groups of 12, and the two gigabit Ethernet ports are displayed together.
Configure Port	Specifies a specific port or range of ports to configure. To configure a specific port, enter the port number in both the from and to field.
Port Cost	Specifies the port cost. It can be set between 1—65535. The lower the cost, the greater the probability the port will be chosen as the designated port (chosen to forward packets). The default value for the 10/100 ports is 19, and for the 100/1000 ports it is 4.
Priority	Specifies the port priority. It can be set between 0—255. The default is 128. The lower the priority, the greater the probability the port will be chosen as the root port. If two ports have the same priority, the port with the lowest port number is selected. For example, STP chooses port 1 instead of port 5 if they both have the same priority.
State	Enables or disables STP on the specified port or range of ports.

3. Highlight **APPLY** and press **Enter**.
   The table displays this additional information about the port.

Column	Description
Connection	Displays the port's speed, duplex mode, and flow control method.
Status	Displays whether the port is Disabled or Forwarding.
STP Name	Displays the assigned STP group name for the port.

Forwarding

Forwarding reduces traffic congestion on the network because packets are transmitted only to the destination port rather than to all ports. The switch maintains a number of static forwarding tables which you can manually configure for MAC, IP, and ARP forwarding.

This section explains how to configure

- MAC address aging
- MAC forwarding (unicast MAC address, multicast MAC address, and storm control)
- IP forwarding (static and default routes, static ARP)

To configure MAC address aging

A very long MAC address aging time can result in out-of-date dynamic entries that may cause incorrect packet filtering and forwarding decisions. A very short aging time may cause entries to be aged out too soon, which results in a high percentage of received packets whose source addresses cannot be found in the address table. In this case, the switch must broadcast the packet to all ports, negating many of the benefits of having a switch.

1. From the Main Menu, select **Forwarding** and press **Enter**.
2. In the MAC Address Aging Time field, specify the length of time a learned MAC address can remain in the forwarding table without being accessed (that is, how long a learned MAC

Address is allowed to remain idle). The aging time can be set to any value between 10—1,000,000 seconds. The default is 300 seconds (5 minutes).

3. Highlight **APPLY** and press **Enter**.

To configure unicast MAC address forwarding

Unicast addresses are used to transmit messages from a single network device to another, single network device. You can specify to have these addresses statically forwarded to a specified port or to have the switch drop them.

1. From the Main Menu, select **Forwarding | Unicast MAC Address Settings** and press **Enter.**
2. Toggle the Action field to **Add/Modify** and configure these fields.

Field	Description
MAC Address	Specifies the unicast MAC address in the packets.
Type	Specifies whether to forward the packets (Static) or to drop the packets (BlackHole).
Port	Specifies which port to use for forwarding the packets. This option is not available if BlackHole is specified as the type.
VLAN Name	Specifies the VLAN to which the MAC address belongs.

3. Highlight **APPLY** and press **Enter**.
4. To delete an entry, toggle the Action field to **Delete**, enter the MAC address, highlight **APPLY**, and press **Enter**.

To configure multicast MAC address forwarding

The multicast MAC address settings configure the switch to forward multicast packets from a specific MAC address to a specified VLAN. The port settings determine which ports can join the VLAN to forward the multicast packets.

1. From the Main Menu, select **Forwarding | Multicast MAC Address Settings** and press **Enter.**
2. Toggle the Action field to **Add/Modify** and configure these fields.

Field	Description
VLAN Name	Specifies the VLAN to which the multicast MAC packets are forwarded.
Multicast MAC Address	Specifies the MAC address of the source of multicast packets.
Port	Specifies how the port can join the multicast group. You can enter the values for the individual ports directly from the keyboard or you can use the spacebar to toggle between **E, F**, and **-**. • **E** (Engress)—Specifies that the port is a static member of the multicast group. • **F** (Forbidden)—Restricts the port from joining the multicast group. • **-** (None)—Specifies that the port has no restrictions and that it can join the multicast group dynamically.

3. Highlight **APPLY** and press **Enter**.

4. To modify an entry, toggle the Action field to **Add/Modify,** enter the VLAN Name and MAC address, configure the ports, highlight **APPLY**, and press **Enter**.
5. To delete an entry, toggle the Action field to **Delete**, enter the VLAN Name and MAC address, highlight **APPLY**, and press **Enter**.

To configure storm control

The storm control settings allow you to specify thresholds for broadcast or multicast traffic that will activate storm control. When the threshold is exceeded, the switch drops the broadcast or multicast traffic. When the traffic level drops below the threshold, the switch resumes forwarding the traffic again.

1. From the Main Menu, select **Forwarding | Broadcast/Multicast Storm Control** and press **Enter**.
2. Configure these fields for each port group.

Field	Description
Upper Threshold (Kpps)	Specifies, in thousands, the number of broadcast or multicast packets per second a port can receive before triggering a storm control response.
Broadcast Storm Mode	Enables or disables storm control for broadcast packets.
Multicast Storm Mode	Enables or disables storm control for multicast packets.

3. Highlight **APPLY** and press **Enter**.

To configure advanced traffic control

Advance traffic control sets the threshold for the amount of traffic a port can handle before triggering flow control. You must enable flow control on the ports before you can set a flow control threshold.

1. From the Main Menu, select **Forwarding | Advance Traffic Control** and press **Enter**.
2. Toggle the View Ports field to the group of ports you want to configure.
3. In the field, enter a port or a range of ports to configure. To configure a single port, enter that port number in both the to and from field.
4. In the Flow Control Threshold field, enter a value from 2—57344.
5. Highlight **APPLY** and press **Enter**.

   The table displays the following information about the ports:

Field	Description
Port	The port number.
Flow Control Threshold	The current value of the flow control threshold.
Drop Packet	A status field that indicates whether the port is currently dropping packets.
Flow Control Status	A status field that indicates whether the port is currently implementing flow control.
Port Connection	A status filed that indicates the port's speed, duplex mode, and flow control mode.

To configure static IP routes

1. From the Main Menu, select **Forwarding | Static/Default Routes** and press **Enter**.
2. Toggle the Action field to **Add** and configure these fields.

Field	Description
IP Address	Specifies the IP address to be statically entered into the IP forwarding table.
Subnet Mask	Specifies the corresponding subnet mask for the IP address.
Gateway IP	Specifies the address of the next hop gateway for the IP address. This is usually a router with a connection to a WAN or the Internet.
Metric	Specifies the Routing Information Protocol (RIP) metric. This is the number of hops between the IP address and the Gateway. This is a number between 1 and 15.

3. Highlight **APPLY** and press **Enter.**
4. To delete a route, toggle the Action field to **Delete**, enter the route information in the fields, highlight **APPLY**, and press **Enter**.

To configure static ARP

The ARP table maps an IP address to a device's MAC address.

1. From the Main Menu, select **Forwarding | Static ARP** and press **Enter.**
2. Toggle the Action field to **Add/Modify** and configure these fields.

Field	Description
Interface Name	Specifies the IP interface of the IP address that you are adding to the static ARP table.
IP Address	Specifies the IP address of the end node or station.
MAC Address	Specifies the MAC address corresponding to the IP address.

3. Highlight **APPLY** and press **Enter.**
4. To delete an entry, toggle the Action field to **Delete**, enter the entry's information in the fields, highlight **APPLY**, and press **Enter.**

IP Address Filtering

You can manually configure the switch to drop packets from specified MAC and IP addresses. For information about specifying MAC addresses to drop, see the **Forwarding | Unicast MAC Address Setting** screen.

To specify an IP address for filtering

1. From the Main Menu, select **Filtering | IP Address Filtering** and press **Enter.**
2. Toggle the Action field to **Add/Modify**.

3. Configure these fields.

Field	Description
IP Address	Specifies the IP address of the packets you want dropped.
Source/Destination	Specifies the condition for filtering the packets: • **Dst.** (destination)—Packets with the above IP address as their destination will be dropped. • **Src.** (source)—Packets with the above IP address as their source will be dropped. • **Either**—All packets with the above IP address will be dropped.

4. Highlight **APPLY** and press **Enter**.
5. To remove an entry, toggle the Action field to **Delete**, enter the IP address and the direction, highlight **APPLY**, and press **Enter**.

MAC Address Priority

You can specify a MAC address so that packets with this address are given special handling, either a higher or lower priority than normal traffic.

Note: If flow control is enabled, a small of amount of low priority traffic may be forwarded before high priority traffic.

1. From the Main Menu, select **MAC Address Priority** and press **Enter**.
2. Toggle the Action field to **Add/Modify** and configure these fields.

Field	Description
VLAN Name	Specifies the name of VLAN on which this MAC address resides.
MAC Address	Specifies the MAC address to set a priority for.
User Priority	Specifies the priority for this MAC address. The levels are 0 —7, with 7 being the highest priority.
Source/Destination	Specifies the state under which the above priority will be active. The options are • **Dst.** (destination)—Packets with the above MAC address as their destination will be given the selected priority. • **Src.** (source)—Packets with the above MAC address as their source will be given the selected priority. • **Either**—All packets with the above MAC address will be given the selected priority.

3. Highlight **APPLY** and press **Enter.**
4. To delete an entry, toggle the Action field to **Delete**, enter the MAC address, highlight **APPLY**, and press **Enter**.

Mirroring Configurations

Incoming or outgoing traffic from any source port can be mirrored for real-time analysis. A logic analyzer or a RMON probe can then be attached to study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, remember these conditions:

- The target port should be operating at the same or higher speed than the source port. If the target port is operating at a lower speed than the source port, packets will be lost.
- For optimum performance, you should mirror three or fewer ports at any given time.

To configure a port for mirroring

1. From the Main Menu, select **Mirroring Configurations** and press **Enter**.
2. Configure these fields.

Field	Description
Target Port	Specifies the port where information will be duplicated and sent for capture and network analysis. This is the port where a network analyzer would be attached to capture packets duplicated from the source port.
Mirrored Port	Specifies which port to be mirror and which packets to be mirror. This port is the source of the packets. Use one of these values: • R—Mirror incoming packet • **T**—Mirror outgoing packets • **B**—Mirror both incoming and outgoing packets • **-** (none)—Do not mirror Use the spacebar to toggle these values for a specific port. If the port has an X, this port cannot be selected for mirroring.

3. Highlight **APPLY** and press **Enter**.
4. To modify a target port in the table of current settings, enter the port number in the Target Port field, change the mirror port value, highlight **APPLY**, and press **Enter**.

VLAN Configuration

The switch allows the assignment of an IP interface to each VLAN. A VLAN must be configured before setting up its IP interface. You can create either a port-based or an IEEE 802.1Q VLAN. By default, all ports belong to an IEEE 802.1Q VLAN called “default.” Although this VLAN cannot be deleted, all member ports can be assigned to other VLANs.

To configure GVRP globally

The global GVRP flag determines whether GVRP (GARP VLAN Registration Protocol) is enabled on the switch so that the switch can share VLAN information with other switches, and VLANs can span multiple switches. When this flag is disabled, VLANs are confined to the physical connections of the switch. By default, this flag is disabled.

1. From the Main Menu, select **VLAN Configurations** and press **Enter**.
2. Use the spacebar to toggle the Switch GVRP field to **Enabled** or **Disabled**.
3. Highlight **APPLY** and press **Enter**.

To create or modify a port-based VLAN

1. From the Main Menu, select **VLAN Configurations | Configure VLAN Settings** and press **Enter**.
2. Toggle the Action field to **Add/Modify** and configure these fields.

Field	Description
VLAN Name	Specifies the name of the VLAN for which ports are to be configured. The name can be up to 32 characters. Once created, a VLAN name cannot be modified.
VLAN Type	Specifies the type of VLAN. Use the spacebar to toggle the type to **Port Based VLAN**.
Membership	Specifies the status of the port. You can enter the status indicators of individual ports directly from the keyboard or you can use the spacebar to toggle between **M** and **-**. • **M** (member)—Designates the port as a static member. • **-** (non-member)—Designates the port as not being a member of the VLAN.

3. Highlight **APPLY** and press **Enter**.

To create or modify an 802.1Q VLAN

1. From the Main Menu, select **VLAN Configurations | Configure VLAN Settings** and press **Enter**.
2. Using the spacebar, toggle the Action field to **Add/Modify**.
3. Configure these fields.

Field	Description
VLAN Name	Specifies the name of the VLAN for which ports are to be configured. The name can be up to 32 characters. Once created, the name cannot be modified.

Field	Description
VLAN Type	Specifies the type of VLAN. Use the spacebar to toggle the type to **1Q VLAN**.
VID	Specifies an identifier for the VLAN. Enter a number from 2—4094.
Membership	Specifies the status of the port. You can enter the status indicators of individual ports directly from the keyboard or you can use the spacebar to toggle between **U, T, F,** and **-** . • **U** (Untagged)—Designates the port as an untagged member of the VLAN. When an untagged packet is transmitted by the port, the packet header remains unchanged. When a tagged packet exits the port, the tag is stripped and the packet is changed to an untagged packet. If the port is attached to a device that is not IEEE 802.1Q VLAN compliant (VLAN-tag unaware), then the port should be set to U - Untagged. • **T** (Tagged)—Designates the port as a tagged member of the VLAN. When an untagged packet is transmitted by the port, the packet header is changed to include the 32-bit tag associated with the PVID (Port VLAN Identifier). When a tagged packet with a different VID exits the port, the packet header is unchanged. If the port is attached to a device that is IEEE 802.1Q VLAN compliant, (VLAN-tag aware), then the port can be set to T - Tagged. • **F** (Forbidden)—Designates the port as not being a member of the VLAN and prevents packets tagged with the VLAN's VID from entering the port. • **-** (non-member)—Designates the port as not being a member of the VLAN.

4. Highlight **APPLY** and press **Enter**.
5. To enter the change into non-volatile RAM, highlight **Save Changes** from the Main Menu and press **Enter**.

To configure the member ports of an 802.1Q VLAN

1. From the Main Menu, select **VLAN Configurations | IEEE 802.1Q Port Settings** and press **Enter**.
2. Highlight the Configure Port field and enter the range of port numbers you want to configure. To configure a single port, enter that port number in both the to and from field.
3. Configure these fields.

Field	Description
Ingress Checking	Enables or disables ingress filter checking. Ingress Filtering allows the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet. Use the spacebar to toggle between **On** and **Off**.
GVRP	Enables or disables GVRP (Group VLAN Registration Protocol). This allows the switch to share VLAN information with other switches so that a VLAN can span multiple switches.

4. Highlight **APPLY** and press **Enter**.

Link Aggregation

Link aggregation allows several ports to be grouped together so that they can act as a single port. This is done to either increase the bandwidth of a network connection or to increase fault tolerance.

Link Aggregation is most commonly used to link a bandwidth-intensive network device or devices —such as a server or server farm—to the backbone of a network.

You can configure up to six aggregation groups, each using from two to eight ports between any two ZT8101 switches or other switches that support Etherchannel. Etherchannel is only required for this first release. In the second release, the ports can be from any switch that is compliant with 802.1ad.

To configure a link aggregation group

1. From the Main Menu, select **Link Aggregation** and press **Enter**.
2. Configure these fields.

Field	Description
Group ID	Specifies one of the six possible link aggregation groups configurable on the switch.
Starting Port	Specifies the first port in the group. This port is called the master port.
Group Width	Specifies the number of ports, in sequential order from the master port, that will be included in the link aggregation group.
Status	Enables or disables the link aggregation group.

3. Highlight **APPLY** and press **Enter**.
   The table displays the following additional information.

Column	Description
Master	Specifies which member port is the master port. The master port is always the lowest numbered port. All member ports are configured to use its settings and become members of its VLAN.
Anchor	Specifies which member port is the anchor port. The anchor port is responsible for the flooding of multicast frames and for sending control packets.

Layer 3 IP Networking

This section describes how to configure:

- IP Interfaces
- RIP
- Multicast routing protocols

Setting Up IP Interfaces

Each IP interface on the switch corresponds to a VLAN. A VLAN, which does not have a corresponding IP interface defined for it, will function as a Layer 2-only VLAN.

The switch allows ranges of IP addresses (OSI Layer 3) to be assigned to VLANs (OSI Layer 2). Each VLAN must be configured prior to setting up the corresponding IP interface.

To set up IP Interfaces on the switch

1. From the Main Menu, select **Layer 3 - IP Networking Setup | IP Interface Settings** and press **Enter**.
2. Toggle the Action field to **Add/Modify**.
3. Configure these fields.

Field	Description
Interface Name	Specifies the name of the IP interface. The default VLAN interface name is System.
IP Address	Specifies the IP address of the IP interface (sometimes referred to as a network address).
Subnet Mask	Specifies the subnet mask for the IP address.
VLAN Name	Specifies the VLAN that is assigned to this IP interface. This VLAN must already exist. The IP interface gets its port membership from the VLAN.
State	Enables or disables the IP interface.

4. Highlight **APPLY** and press **Enter**.

The Action field can be toggled between **Add/Modify** and **Delete** using the space bar. This enables the addition/modification of a new or existing IP interface entry or the deletion of an existing entry.

If you modify an existing IP interface and apply the changes, the RIP and IP multicast interface configurations are reset to default values.

RIP Configuration

The Routing Information Protocol (RIP) is a distance-vector protocol that uses the hop count as its criteria for making routing decisions. RIP is an Interior Gateway Protocol (IGP), which means that it performs routing within a single autonomous system.

To configure RIP

1. From the Main Menu, select **Layer 3 - IP Networking Setup | RIP Configurations** and press **Enter**.
2. Using the space bar, toggle the RIP Status field to **Enabled** or **Disabled**. This function allows the RIP protocol to be turned on or off without changing the RIP setup.
3. Highlight **APPLY** and press **Enter**.
4. On the RIP Configurations menu, select **RIP Interface Settings**.

5. Configure these fields.

Field	Description
Interface Name	Specifies the name of the IP interface on which RIP is to be set up. This interface must be previously configured on the switch.
TX Mode	Specifies which version of the RIP protocol will be used to transmit RIP packets. This field toggles between **Disabled, V1 Only, V1 Compatible**, and **V2 Only**. Disabled prevents the transmission of RIP packets.
RX Mode	Specifies which version of the RIP protocol will be used to interpret received RIP packets. This field toggles between **Disabled, V1 Only, V2 Only,** and **V1 and V2**. Disabled prevents the reception of RIP packets.
Authentication	Enables or disables authentication between routers. When authentication is enabled, a password is used to authenticate communication between routers on the network. Authentication is only supported when RIP is in V1 Compatible or V2 mode.
Password	Specifies the password to be used to authenticate communication between routers on the network.

6. Highlight **APPLY** and press **Enter**.

Multicast Global Configurations

The Multicast Global Configurations screen is only for globally enabling or disabling the multicast routing protocols on the switch. Each VLAN or IP Interface uses these global values unless you configured it to use specialized settings. The protocol must be enabled globally before you can enable it on a specific VLAN or IP interface. (RIP is globally set up with the RIP Configuration option.)

To configure globally the multicast protocols

1. From the Main Menu, select **Layer 3 - IP Networking Setup | Multicast Global Configurations** and press **Enter**.
2. Configure these fields.

Field	Description
Switch IGMP Snooping	Enables or disables, globally, Internet Group Management Protocol (IGMP) snooping. This protocol allows the switch to forward multicast traffic intelligently on the switch.
DVMRP State	Enables or disables, globally, the Distance-Vector Multicast Routing Protocol (DVMRP).
PIM-DM State	Enables or disables, globally, the Protocol Independent Multicasting - Dense Mode (PIM-DM) multicasting protocol.
DVMRP Include Report From Unknown Neighbors	Enables or disables receiving DVMRP reports from unknown neighbors.

3. Highlight **APPLY** and press **Enter**.

Each protocol has a corresponding configuration screen. You access these screens from the **Layer 3 - IP Networking Setup** screen.

IGMP Configuration

The Internet Group Management Protocol (IGMP) allows the switch to forward multicast traffic intelligently on the switch. The switch “snoops” the IGMP query and report messages and forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

IGMP requires a network device that learns about the presence of multicast groups on its subnets and that keeps track of group membership. Multicasting is not connection oriented, so data is delivered to the requesting hosts on a best-effort level of service.

The switch has two configuration screens for IGMP:

- The IGMP snooping screen allows you to configure the switch for snooping and querying.
- The IGMP interface screen allows you to configure the switch to keep track of IGMP groups.

To configure IGMP snooping

1. From the Main Menu, select **Layer 3 - IP Networking Setup | IGMP Snooping Configurations** and press **Enter**.
2. Using the spacebar, toggle the Action field to either **Add/Modify** or **Delete** and configure these fields.

Field	Description
VLAN Name	Specifies the name of the VLAN you want to configure.
Querier Version	Specifies whether this VLAN should respond to IGMP queries. Three options are available: • **No**—Prevents this VLAN from becoming a querier. • **V1**—Enables the sending of IGMP query packets when needed. • **V2**—Enables the sending of IGMP query and leave packets according to the IGMP V2 specification. Use the spacebar to toggle between the options.
Robustness Variable	Specifies the permitted packet loss on a link. Enter a value between 2—255. The default is 2.
Query Interval	Specifies the time that can elapse between general IGMP queries. Enter a value between 1—65535 seconds. The default is 125.
Max Response Time	Specifies the maximum time the switch can wait for IGMP member reports. Enter a value between 1—25. The default is 10 seconds.
State	Enables or disables learning about IGMP groups. If enabled, the switch limits multicast forwarding to active member ports.

3. Highlight **APPLY** and press **Enter** to make the changes.

These conditions affect the fields on the IGMP snooping screen:

- The switch IGMP snooping flag must be enabled for these settings to have any effect.
- If the IGMP settings have been enabled for the IP interface associated with the VLAN you select, the only field available on the IGMP snooping screen is the State field.

To configure IGMP for an IP interface

1. From the Main Menu, select **Layer 3 - IP Networking Setup | IGMP Interface Configurations** and press **Enter**.
2. Configure these fields.

Field	Description
Interface Name	Specifies the name of the IP interface you want to configure. The IP address field displays the address which corresponds to the entered IP interface.
Version	Specifies the version number of IGMP to be used with the IP interface. Use the spacebar to toggle between **1 and 2**.
Query Interval	Specifies the time (in seconds) between the transmission of IGMP query packets. Enter a value between 1—65535 seconds. The default is 125.
Max Response Time	Specifies the maximum time the switch can wait for reports from members. Enter a value between 1—25. The default is 10 seconds.
Robustness Variable	Specifies the permitted packet loss on a link. Enter a value between 1—255. The default is 2.
State	Enables or disables IGMP on this IP interface.

3. Highlight **APPLY** and press **Enter**.

Note: When IGMP is enabled on an interface, the switch IGMP snooping flag is set to Enabled and becomes a read-only parameter.

DVMRP Interface Configuration

The Distance Vector Multicast Routing Protocol (DVMRP) is a hop-based method of building multicast delivery trees from multicast sources to all nodes of a network. Because the delivery trees are “pruned” and use the “shortest path,” DVMRP is relatively efficient. Because multicast group membership information is forwarded by a distance-vector algorithm, propagation is slow. DVMRP is optimized for high delay (high latency) and relatively low-bandwidth networks, and it can be considered as a “best-effort” multicasting protocol.

To configure DVMRP for an IP interface

1. From the Main Menu, select **Layer 3 - IP Networking Setup | DVMRP Interface Configurations** and press **Enter**.
2. Configure these fields.

Field	Description
Interface Name	Specifies the name of the interface to configure. This must be a previously defined IP interface.
Neighbor Timeout Interval	Specifies the maximum interval the switch will wait to hear from a neighbor. If this interval expires, the switch assumes that this neighbor is down. Enter a value from 1—65535. The default is 35.
Probe Interval	Specifies the interval between probes. A probe is a query to other routers to determine if a multicast group is present on a given router subnetwork. Enter a value from 1—65535 seconds. The default is 10.

Field	Description
Metric	Specifies the cost for this path. The higher the assigned cost, the less likely it is that multicast packets will be routed over this interface (provided that other path options exist). Enter a value between 1—31. The default is 1.
State	Enables or disables DVMRP for this interface.

3. Highlight **APPLY** and press **Enter**.

PIM-DM Interface Configurations

The Protocol Independent Multicast - Dense Mode (PIM-DM) protocol should be used in networks with a low delay (low latency) and high bandwidth because PIM-DM is optimized to guarantee delivery of multicast packets, not to reduce overhead.

To configure PIM-DM for an IP interface

1. From the Main Menu, select **Layer 3 - IP Networking Setup | PIM-DM Interface Configurations** and press **Enter**.
2. Configure these fields.

Field	Description
Interface Name	Specifies the name of an IP interface that you want to configure for PIM-DM. This must be a previously-defined IP interface. The IP Address field displays the address associated with the IP interface.
Hello Interval	Specifies the interval between sending Hello packets to other routers on the network. The Hello messages are used by the router to determine whether it is the root router on the delivery tree or not. If the router does not receive a Hello message within the Hello Interval, it will begin transmitting Hello messages to advertise its availability to become the root router. The range is between 1—65535 seconds. The default is 30 seconds.
State	Disables or enables PIM-DM for this IP interface.
Join-Prune Interval	Specifies the interval for performing these tasks: • Removing prune information from a branch of a multicast delivery tree. • Flooding multicast messages to all branches of that delivery tree. These two actions are equivalent. The range is between 1— 65535 seconds. The default is 60 seconds.

3. Highlight **APPLY** and press **Enter**.

Static Router Port

A static router port allows UDP multicast and IGMP packets to be forwarded to a designated port regardless of VLAN configuration.

A router port functions within Layer 2 of the OSI model. A static router port is a port that has a router attached to it. Generally, this router would have a connection to a WAN or to the Internet. Establishing a router port will allow multicast packets coming from the router to be propagated through the network. It also allows multicast messages coming from the network to be propagated to the router.

The purpose of a router port is to enable UDP multicast packets and IGMP multicast group membership messages to reach multiple ports of a multi-port router. Routers do not implement IGMP snooping or transmit/forward IGMP report packets. Thus, forwarding all IP UDP multicast packets to a static router port on the ZT8101 switch guarantees that all ports of a multi-port router, which are attached to the switch, can reach all multicast group members through the attached router's other ports.

A router port interacts with multicast packets in these ways:

- All IGMP report packets will be forwarded to the router port.
- IGMP queries (from the router port) will be flooded to all ports.
- All UDP multicast packets will be forwarded to the router port. Because routers do not send IGMP reports or implement IGMP snooping, a multi-port router connected to the router port of the Layer 3 switch would not be able to receive UDP data streams from its ports unless the UDP multicast packets were all forwarded to the router port.

A router port will be dynamically configured when IGMP query packets, RIPv2 multicast, DVMRP multicast, PIM-DM multicast packets are detected flowing into a port.

To configure a static router port

1. From the Main Menu, select **Layer 3 - IP Networking Setup | Static Router Port Settings** and press **Enter**.
2. Toggle the Action field to **Add/Modify** and configure these fields.

Field	Description
VLAN Name	Specifies the name of the VLAN the static router port resides on.
Router Port	Specifies the ports that you want to set up as static router ports. Each port can be set individually as a router port by highlighting the port's entry using the Arrow keys. Use the spacebar to toggle between M (member) and **-** (non-member).

3. Highlight **APPLY** and press **Enter**.
4. To delete an entry, toggle the Action field to **Delete** and enter the VLAN name of the VLAN for which the router port table entry is to be deleted. Highlight **APPLY** and press **Enter**.

Using the Web Console 5

The ZT8101 switch has an embedded Web server that allows you to manage the switch from anywhere on the network through a standard browser such as Netscape* Navigator or Microsoft* Internet Explorer. The Web browser communicates directly with the switch using the HTTP protocol.

The Web Console program and the Telnet Console are different ways to access the same internal switching software and configure it. Thus, all settings found in the Web Console are the same as those found in the Telnet Console.

Note: The Web Console does not accept Chinese language input (or other languages requiring 2 bytes per character).

Before You Start

The ZT8101 switch supports a wide array of functions and provides great flexibility and increased network performance by eliminating the routing bottleneck between networks: the WAN, the Internet, and the intranet. This new generation switch performs routing functions in hardware rather than software. To take full advantage of this flexibility and rich feature set, you need to carefully plan a deployment strategy that will maximize the potential of the ZT8101 switch.

This plan should include a

- "General Deployment Strategy"
- "VLAN Layout"
- "IP Addressing Scheme for VLANs"
- "Static Route Assessment"

General Deployment Strategy

- **Determine how to segment the network—**This involves creating VLANs in an existing Layer 2 switched network.
- **Develop an IP addressing scheme—**This involves allocating a block of IP addresses to each network segment. Each network subnet is then assigned a network address and a subnet mask. See the "IP Addressing and Subnetting" section in Chapter 3 for more information.
- **Determine which network resources must be shared by the subnets and how they will be shared—**You can connect shared resources directly to the Layer 3 switch, if need be. Or you can set up static routes to make the shared resources accessible.
- **Determine how each subnet will communicate with the WAN or Internet—**Again, static routes should be determined and default gateways identified.
- **Develop a security scheme—** Some subnets on the network need more security or should be isolated from the other subnets. You can use MAC and IP filtering. You can also configure one or more VLANs on the Layer 3 switch without an IP subnet. Without a subnet mask, these

VLANs function as a Layer 2 VLAN and require an external router to connect to the rest of the network.

- **Develop a policy scheme—**Some subnets will have a greater need for multicasting bandwidth, for example. A policy is a mechanism to alter the normal packet forwarding in a network device, and can be used to intelligently allocate bandwidth to time-critical applications such as the integration of voice, video, and data on the network.
- **Develop a redundancy scheme—**Planning redundant links and routes to network-critical resources can save valuable time in case a link or device fails. You can use the Spanning Tree Protocol to block the redundant link until it is needed.

VLAN Layout

VLANs on the ZT8101 switch have more functions than on a traditional Layer 2 switch and must therefore be laid-out and configured with a more care. Layer 3 VLANs could be thought of as network links rather than as a collection of associated end users. Further, Layer 3 VLANs are assigned an IP network address and subnet mask to enable IP routing between them.

Layer 3 VLANs must be configured on the switch before they can be assigned IP subnets. Also, the static VLAN configuration is specified on a per port basis. On the ZT8101 switch, a VLAN can consist of end-nodes, just like a traditional Layer 2 switch. But a VLAN can also consist of one or more Layer 2 switches, each of which is connected to multiple end nodes or network resources.

For example, a Layer 3 VLAN, consisting of four ports, could be connected to four switches. If these switches each have 24 ports, then the Layer 3 VLAN would contain 96 (4 x 24) end nodes. Assigning an IP subnet to the Layer 3 VLAN would allow wire-speed IP routing from the WAN to each end node and between end nodes.

Therefore, the IP subnets for a network must be determined first, and the VLANs configured on the switch to accommodate the IP subnets. Finally, the IP subnets can be assigned to the VLANs.

IP Addressing Scheme for VLANs

The ZT8101 switch allows the assignment of IP subnets to individual VLANs. Any VLAN configured on the switch that is not assigned an IP subnet will behave as a Layer 2 VLAN and will not be capable of IP routing.

Developing an IP addressing scheme is a complex subject. As you are developing your scheme, remember that the switch requires a unique IP addreess for all the anticipated end nodes on each Layer 3 VLAN. The switch treats a VLAN with an IP network address and subnet mask as an IP interface in an IP routing mode.

Static Route Assessment

You need to define static routes for the following types of subnets:

- Subnets not accessible through the default route
- Subnets that the switch does not already know about internally
- Subnets not learned through the dynamic routing protocols

You determine how these packets are routed by entering static routes into the switch's static/default routing table.

Getting Started

The first step required to use the Web Console for the first time is to secure a browser such as Netscape Navigator or Microsoft Internet Explorer.

The second step is to configure the IP address of the switch. This must be done manually through the serial port. See chapter 2 for instructions.

Note: If you are using the Web Console on an isolated network without a DHCP server, ensure that your workstation's subnet mask matches the subnet mask you assigned to the switch.

Logging In

1. To begin managing your switch simply, start the browser you have installed on your computer.
2. Enter the IP address you have defined for the switch. The URL in the address bar should read something like: http://123.123.123.123, where the numbers 123 represent the IP address of the switch.

   The Factory default IP address for the switch is 10.90.90.90.
3. In the page that opens, enter the name and password of an Admin user if an account has been created, or click the fields and press Enter if no user accounts have been created.

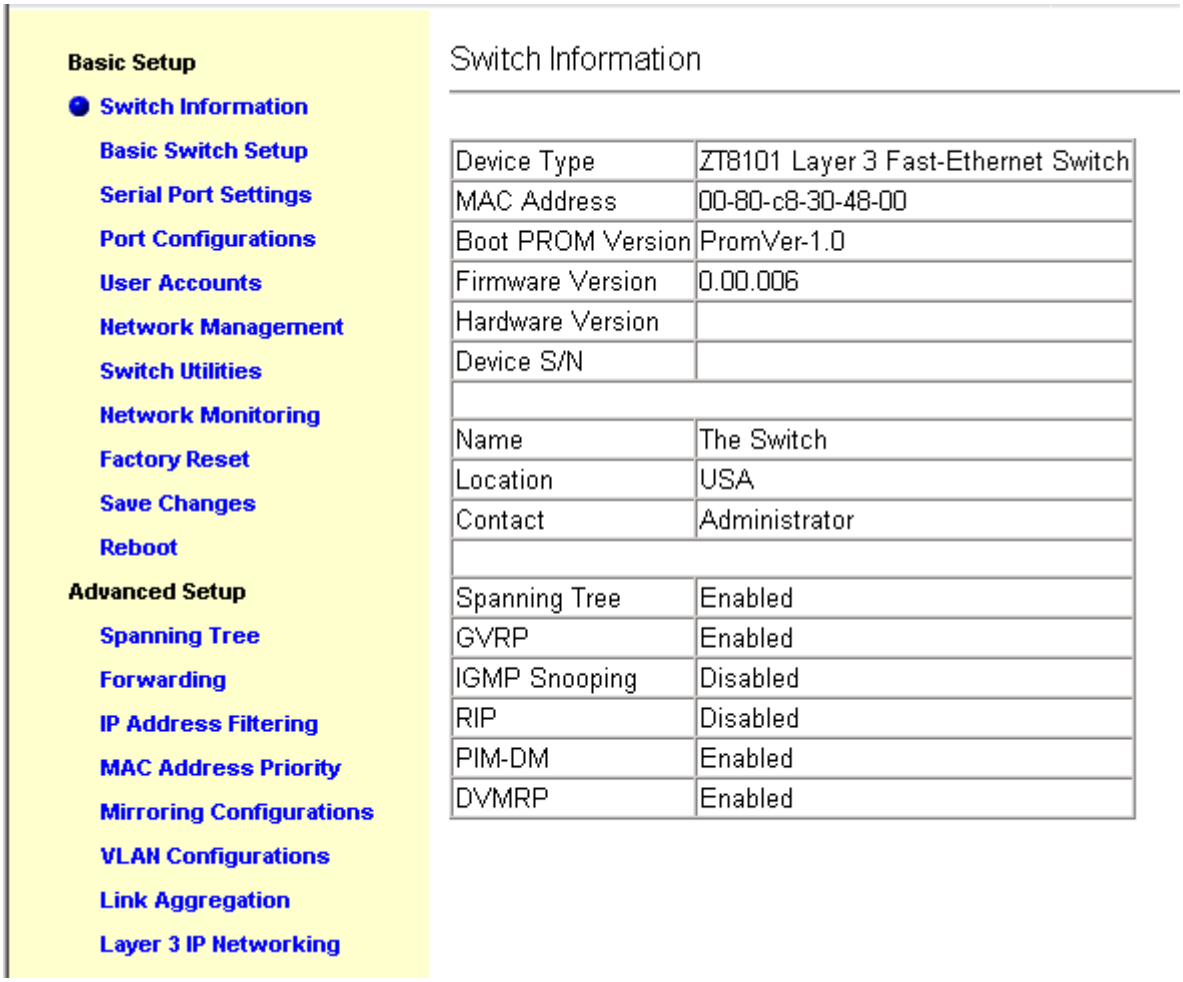
   The Switch Information screen appears.

This chapter describes the switch management features that are available from the Web Console. The immediate sections below describe some basics about user accounts, saving changes, and resetting the switch to factory default settings. The subsequent sections describe the basic and advanced features.

If no user accounts have been created, one of your first configuration tasks should be to create at least one Admin-level user to protect the switch from unauthorized users.

Configuration Options

The left panel has these options.



- **Basic Setup**
  - — **Switch Information**—Display information about the switch's hardware, firmware, and protocol configuration.
  - — **Basic Switch Setup**—Configure the switch's IP address.
  - — **Serial Port Settings**—Configure the switch's serial port that is used for Telnet communication and terminal sessions.
  - — **Port Configurations**—Enable/disable individual ports and set their speed and duplex state.
  - — **User Accounts**—Set up user accounts, change their passwords, and modify their access rights.
  - — **Network Management**—Set up SNMP traps and community strings.

  - **Switch Utilities**—View the history log, ping other devices, and manage firmware and configuration files.
  - **Network Monitoring**—View various statistics by port or protocol and to view various routing tables.
  - **Factory Reset**—Restart the switch using the default factory configuration.
  - **Save Changes**—Save the switch's current settings in non-volatile RAM (NV_RAM) so that they are not lost when the switch is rebooted.
  - **Reboot**—Restart the switch.
- **Advanced Setup**
  - **Spanning Tree**—Enable/disable the Spanning Tree Protocol (STP) for the switch and on individual ports.
  - **Forwarding**—Reduce traffic congestion on the network by configuring MAC address aging, unicast packet forwarding, storm control, and static IP routes.
  - **IP Address Filtering**—Configure filters to drop packets from specified IP addresses or MAC addresses.
  - **MAC Address Priority**—Configure specified MAC addresses for priority handling on source address, destination address, or both.
  - **Mirroring Configurations**—Configure a source port to send a copy of its data to a target port for monitoring and troubleshooting.
  - **VLAN Configurations**—Set up and administer VLANs on the switch.
  - **Link Aggregation**—Combine ports on the switch to increase bandwidth.
  - **Layer 3 IP Networking**—Configure IP interfaces, RIP, and multicast routing protocols.

User Accounts

Access to the console is controlled via user accounts. You can create up to six accounts, one of which must be an Admin-level account. The other five accounts can be any combination of Admin-level and User-level accounts.

1. Under Basic Setup in the left panel, click **User Accounts**.
2. Click **New** to add a user.
3. Enter a new username, assign an initial password, and then confirm the new password. Determine whether the user should have Admin or User privileges. (The next section describes the differences.) The first user created must be granted Admin privileges.
4. Click **Apply** to make the user addition effective.

The Apply button makes changes to the switch configuration for the current session only. If you want these changes to be permanent, all changes (including user additions or updates) must be entered into non-volatile ram using the **Save Changes** option in the left panel.

Admin and User Privileges

There are two levels of user privileges: Admin and User. Some menu selections available to users with Admin privileges may not be available to those with User privileges.

The table summarizes the Admin and User privileges:

	Admin	User
Switch Configuration Management		
Configuration	Yes	Read Only
Network Monitoring	Yes	Read Only
SNMP Community Strings and Trap Stations	Yes	Read Only
Update Firmware and Configuration Files	Yes	No
Switch Utilities	Yes	Ping; Read Only access to BOOTP/DHCP Relay and DNS Relay.
Factory Reset	Yes	No
Reboot Switch	Yes	No
Advanced Setup	Yes	Read Only
User Account Management		
Add/Update/Delete User Accounts	Yes	No
View User Accounts	Yes	No

After establishing a User Account with Admin-level privileges, highlight **Save Changes** and press **Enter**. The switch will save any changes to its non-volatile RAM. You can now log in as that user and continue configuring the switch.

Saving Changes

The ZT8101 has two levels of memory; normal RAM and non-volatile or NV-RAM. Configuration changes are made effective when you click the **Apply** button. When you do this, the settings are immediately applied to the switching software in RAM and immediately take effect.

Some settings, though, require you to restart the switch before they will take effect. Restarting the switch erases all settings in RAM and reloads the stored settings from the NV-RAM. Thus, it is necessary to save all setting changes to NV-RAM before rebooting the switch.

To retain any configuration changes permanently

1. In the left panel, click **Save Changes**.
2. Click **Save Configuration**.

A message appears verifying that your new settings have been saved to NV-RAM.

Once the switch configuration settings have been saved to NV-RAM, they become the default settings for the switch. These settings will be used every time the switch is rebooted. You can use the **Factory Reset** option to return the switch to its factory configured settings.

Restart

1. To restart the switch, in the left panel click **Reboot**.
2. Click **Yes** to save the current switch configuration to non-volatile RAM (flash RAM), or **No** if you want to restart the switch using the last-saved (previous) configuration.
3. Click **Restart**.

Factory Reset

The Factory Reset option is used to restart the switch using only the configuration that was supplied by the factory. A factory reset returns all configuration options to their default values and restores the switch's configuration to the factory settings.

All user-entered configuration information is lost.

To reset the switch to factory default values

1. In the left panel, click **Factory Reset**.
2. Click **Yes** if you want the switch to retain its current IP address, or **No** to reset the switch's IP address to the factory default of 10.90.90.90.
3. Click **Reboot**.

Basic Settings

This section describes how to perform common monitoring and configuration tasks on the switch.

Condition	Task
Using SNMP for network management	Configure the options in the Network Management Setup screens.
Installing more than one switch	Use the Switch Utilities to save configurations for use on multiple switches.
Testing communication with other devices	Use the Ping Test utility from the Switch Utilities menu.
Need to set the port settings for the serial port to values other than the default values	Configure the options with the Serial Port Settings screen.

Switch Information

The Switch Information screen displays descriptive information about the switch.

In the left panel, click **Switch Information**. This screen contains the following information.

Field	Description
Device Type	Specifies the product name: ZT8101 Fast-Ethernet Switch.
MAC Address	Specifies the unique MAC address assigned to the switch. This address is not configurable.
Boot PROM Version	Specifies the version of the switch's boot code.
Firmware Version	Specifies the version of the firmware installed on the switch. You can update this using a switch utility.
Hardware Version	Specifies the hardware version of the main board.
Device S/N	Specifies the serial number of the device.
Name	Specifies the name assigned to the switch system. If you are installing multiple switches, you should give each a unique name.
Location	Specifies the area or location where the switch resides.
Contact	Specifies the contact person for the switch.
Spanning Tree	Indicates whether STP is enabled or disabled.
GVRP	Indicates whether the Group VLAN Registration Protocol is enabled or disabled.
IGMP Snooping	Indicates whether the Internet Group Management Protocol Snooping is enabled or disabled.
RIP	Indicates whether the Routing Information Protocol is enabled or disabled.
PIM-DM	Indicates whether Protocol Independent Multicast - Dense Mode is enabled or disabled.
DVMRP	Indicates whether the Distance Vector Multicast Routing Protocol is enabled or disabled.

Basic Switch Setup

Use the Basic Switch Setup screen to set the boot-up option for obtaining an IP address or to manually assign an IP address for the switch.

1. In the left panel, click **Basic Switch Setup**.

   This screen displays the current settings and allows you to configure these fields in the New Switch IP Settings form.

2. To configure the IP address, configure these fields.

Parameter	Default	Description
Get IP From	Manual	Specifies the method for assigning the switch an IP address. Use the drop-down menu to select Manual, DHCP, or BOOTP. (For more information about these options, see the descriptions below.)
IP Address	10.90.90.90	Specifies the IP address assigned to the switch.

Parameter	Default	Description
Subnet Mask	255.0.0.0	Specifies the subnet mask assigned to the switch and to the other devices on this segment of the network.
Default Gateway	0.0.0.0	Specifies the IP address of the device that routes to different networks. A gateway must be defined if the workstation you are going to use for switch management is located on a different IP segment than the switch.
VLAN Name	default	Specifies the name of the VLAN that the switch resides in. This VLAN must already exist.

3. To configure a name and contact information for the switch, enter information in these fields.

Parameter	Description
Name	Specifies the name assigned to the switch. If you are installing multiple switches, you should give each a unique name.
Location	Specifies the physical location of the switch.
Contact	Specifies the name of the person responsible for the switch.

4. Click **Apply**.

Get IP From Description

The switch uses the Get IP From setting to determine where to get its IP address. You must use the Manual option if you want to configure multiple IP interfaces. The manual option is also more convenient if you are going to manage the switch with Telnet Console or Web Console. Both of these consoles require you to know the IP address, and although BOOTP/DHCP usually assign the same IP address when a device reboots, there is no guarantee.

- **BOOTP**—The switch sends out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the switch looks first for a BOOTP server to provide it with this information.
- **DHCP**—The switch sends out a DHCP broadcast request when it is powered up. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the switch looks first for a DHCP server to provide it with this information.
- **Manual**—The switch uses the entered IP address, Subnet Mask, and Default Gateway. These entries should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal form) between 0 and 255. The fields that require entries under this option are as follows:
  - **IP Address**—This address should be a unique address on the network assigned to the switch by the network administrator.
  - **Subnet Mask**—This is a bitmask that determines the extent of the subnet that the switch is on. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.
  - **Default Gateway**—This IP address determines where packets with a destination address outside the current subnet are sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the switch to be accessible outside your local network, you can leave this field unchanged.

Serial Port Settings

The Serial Port Settings screen allows the configuration of the switch's serial port, which is on the front panel. Terminals must match these settings to connect to the switch.

1. In the left panel, click **Serial Port Settings**.
2. Configure these fields.

Field	Description
Baud Rate	Sets the serial bit rate that will be used for communication the next time the switch is restarted. This setting applies only when the serial port is being used for out-of-band management. Available speeds are 9600, 19,200, 38,400, and 115,200 bits per second. The default setting is 9600.
Auto-Logout	Sets the time the interface can be idle before the switch automatically logs out the user. The options are Never, 2, 5, 10, or 15 minutes.

   Values for data bits (the number of bits used to represent one character of data) and stop bits (the number of bits used to mark the end of a unit of transmission) are displayed but are not configurable.

3. Click **Apply.**

Port Configurations

You can enable or disable a specific port and set its speed and duplex state.

1. In the left panel, click **Port Configurations**.
2. Use the drop-down menu to select the port you want to configure.
   The Port Type and Connection fields will display the port's current information.
3. Configure these fields.

Field	Description
State	Enables or disables the currently selected ports.
Speed/Duplex	Specifies the speed and full- or half-duplex state of the ports. For 100 Mpbs ports, the choices are **Auto, 10/Half, 10/Full, 100/Half,** or **100/Full**. For gigabit ports, the choices are **Auto,1000/Full**, or **100/Full**.
Flow Control	Specifies the flow control mode for the port.
Learn	Enables or disables dynamic learning of MAC addresses. You can disable MAC learning to increase the security of a specific port. Such ports only receive broadcast traffic and packets that have a destination MAC address that matches the port's MAC address.
Configure Ports from to	Allows you to apply the configuration for multiple ports.

4. Click **Apply**.

Network Management

You use the Network Management screens to display and modify parameters for the Simple Network Management Protocol (SNMP). The switch includes an on-board SNMP agent which monitors the status of its hardware, as well as the traffic passing through its ports. A computer

attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the on-board agent are controlled by community strings. To communicate with the switch, the NMS must first submit a valid community string for authentication.

To configure SNMP community strings

You can configure up to four community strings for SNMP authentication.

1. In the left panel, click **Network Management**.
2. In the top panel, click **SNMP Community Setup**.
3. Configure these fields.

Field	Description
Community String	Specifies a string of up to 20 characters used for authentication of users wanting access to the switch's SNMP agent.
Rights	Specifies the level of access for an authorized user. The level can be Read-Only or Read-Write.
Status	Specifies whether the current string is Enabled or Disabled. This is used to temporarily limit access to the switch's SNMP agent.

4. Click **Apply**.

To configure trap recipients

The trap recipient screen allows you to specify which management stations will receive authentication failure messages or other trap messages from the switch. Up to three trap recipients may be entered.

1. In the left panel, click **Network Management**.
2. In the top panel, click **SNMP Trap Recipients**.
3. Configure these fields.

Field	Description
IP Address	Specifies the IP address of the management station that will receive traps generated by the switch.
SNMP Community String	Specifies a string of up to 20 characters used for authentication of users wanting to receive traps from the switch's SNMP agent. This is similar to a password in that stations that do not know the correct string cannot receive or request SNMP information from the switch.
Status	Enables or disables the selected community string. This is used to temporarily limit a station from receiving traps generated by the switch.

4. Click **Apply**.

To configure management station IP addresses

You can specify the IP addresses of up to three management stations that will be allowed access to the management agent of the switch. If you enter IP addresses in this form, only the management stations with those IP addresses are allowed to access the management agent of the switch. All other IP addresses will be blocked.

1. In the left panel, click **Network Management**.
2. In the top panel, click **Management Station IP Addresses**.
3. Configure the following fields.

Field	Description
IP Address	Specifies the IP addresses of the management stations that you want to access to the switch's management agent.
Port	Specifies the ZT8108 switch port used for access.

4. Click **Apply**.

Switch Utilities

Trivial File Transfer Protocol (TFTP) services enable these maintenance tasks:

- Upgrading the switch’s firmware by downloading a new firmware file from a TFTP server to the switch.
- Downloading a configuration file from a TFTP server to the switch
- Saving the switch’s settings to a TFTP server.
- Saving the switch’s history log to a TFTP server.

The TFTP server must be running TFTP server software to perform the file transfer. TFTP server software is a part of many network management software packages, or can be obtained as a separate program.

The switch utilities also allow you ping stations and configure DNS relay and BOOTP/DHCP relay. The following sections describe how to perform these tasks.

To update firmware

1. In the left panel, click **Switch Utilities.**
2. In the top panel under TFTP Services, click **Download Firmware from TFTP Server**.
3. In the Server IP Address field, enter the IP address of the TFTP server.
4. In the Path \ Filename field, enter the full path with filename of the new firmware file on the TFTP server, based from the root of the server.
5. To save this configuration information, click **Save Settings.** This saves the IP address of the TFTP server so that the next time you access this screen, you won’t have to enter the address or the path \ filename.
6. To start the download, click **Download**.

When the download is completed, the switch automatically reboots and executes the new runtime firmware.

To download a configuration file

1. In the left panel, click **Switch Utilities.**
2. In the top panel under TFTP Services, click **Download Configuration from TFTP Server.**
3. In the Server IP Address field, enter the IP address of the TFTP server.
4. In the Path\ Filename field, enter the full path with filename of the configuration file on the TFTP server.
5. To start the download, click **Download**.

When the download is completed, the switch saves the configuration in NV-RAM and automatically reboots.

Note: If FLASH becomes corrupted because you lose power when upgrading the firmware, you must use Zmodem to fix the problem. See “Upgrading Firmware through Zmodem” on page 19.

To upload a configuration file

You can save the switch's current settings to a TFTP Server. This saved file can then be used to reconfigure the switch or to configure another switch.

1. In the left panel, click **Switch Utilities.**
2. In the top panel under TFTP Services, click **Upload Settings to TFTP Server**.
3. In the Server IP Address field, enter the IP address of the TFTP server.
4. In the Path\ Filename field, enter the location on the TFTP server to save the configuration. Include the full path and the filename in this field.
5. To save this configuration information, click **Save Settings.** This saves the IP address of the TFTP server so that the next time you access this screen, you won’t have to enter the address or the path \ filename.
6. To start the upload, click **Upload**.

To upload a history log file

1. In the left panel, click **Switch Utilities.**
2. In the top panel under TFTP Services, click **Upload History Log to TFTP Server.**
3. In the Server IP Address field, enter the IP address of the TFTP server.
4. In the Path\ Filename field, enter the location on the TFTP server to save the history log. Include the full path and the filename in this field.
5. To save this configuration information, click **Save Settings.** This saves the IP address of the TFTP server so that the next time you access this screen, you won’t have to enter the address.
6. To start the upload, click **Upload**.

To test connectivity with ping

1. In the left panel, select **Switch Utilities.**
2. In the top panel under Others, click **Ping Test**.
3. Configure these fields.

Field	Description
Target IP Address	Specifies the IP address of the network device to ping.
Number of Repetitions	Specifies the number of test packets to send. Three is the usual number.
Default timeout	Specifies the number of seconds to wait between sending the packets.

4. To start the test, click **Start**.

   A window appears to display the results of the test. If you selected a large number of repetitions, you can select to stop and then resume the test.

BOOTP/DHCP Relay Agent

BOOTP/DHCP relay agent enables end stations to use a BOOTP or DHCP server to obtain TCP/IP configuration information or boot files to be loaded into memory, even if the servers are not on the local IP interface. These conditions determine whether you need to enable BOOTP/DHCP relay:

- If the BOOTP or DCHP server and end station are on the same IP interface, no relay agent is necessary.
- If the servers and the end stations are on different IP interfaces, a relay agent is necessary for the switch to forward the messages.

The relay agent forwards these packets between IP interfaces, and therefore must know the IP addresses of the BOOTP and DHCP servers and their respective subnet names (or IP interface names).

When the switch receives packets destined for a BOOTP or DHCP server, it forwards them to specific servers as defined in the following configuration. The switch also forwards packets from the BOOTP or DHCP servers to the appropriate subnets.

To enable the BOOTP/DHCP relay agent, you must configure both the BOOT/DHCP Relay form and the Static Setup form.

To configure the BOOTP/DHCP relay agent

You must configure the relay agent so it can determine whether or not to forward a given BOOTP/DCHP packet.

1. In the left panel, click **Switch Utilities.**
2. In the top panel under Others, click **BOOTP/DHCP Relay**.

3. Configure these fields.

Field	Description
BOOTP/DHCP Relay Status	Enables or disables the BOOTP/DHCP relay function.
BOOTP Hops Count Limit	Sets the maximum number of hops (routers) that the BOOTP messages can be relayed through. If a packet's hop count is more than the hop count limit, the packet is dropped. The range is between 1—16 hops. The default value is 4.
BOOTP/DHCP Relay Time Threshold	Sets the minimum time (in seconds) that the switch will wait before forwarding a BOOTREQUEST packet. If the value in the seconds field of the packet is less than the relay time threshold, the packet will be dropped. The range is between 1—9999 seconds. The default value is 4 seconds.

4. Click **Apply**.

To configure the static BOOTP relay setup

You must configure the BOOTP/DCHP relay agent so that it knows the servers' IP addresses and subnet names (IP interface names).

1. In the left panel, click **Switch Utilities**.
2. In the top panel under Others, click **BOOTP/DHCP Relay Interface Configurations.**
3. Click **New** and configure these fields.

Field	Description
Interface Name	Specifies the subnet name (IP interface name) of the network that the BOOTP or DHCP server is located on.
BOOTP/DHCP Server	Specifies the IP address of the BOOTP or DHCP relay server. Multiple servers may be entered for a given subnet name (IP interface name).

4. Click **Apply**.
   The server is added to the BOOTP/DHCP Relay Setup list.
5. To add another server, repeat steps 2 and 3. Each IP interface can be configured for four servers.
6. To remove a server, select the server and click **Delete**.

DNS Relay

DNS relay enables the switch to act as a DNS cache or proxy and to forward DNS requests to the DNS server only when required. Whether you enable DNS relay depends upon whether you want to

- Ssave a DNS server or the linking WAN extraneous or repetitive traffic.
- Try to shorten the response time for a DNS request on a slow or long WAN.
- Change or control the IP response for a series of DNS requests.
- Control which servers are used for DNS.

When the switch receives packets destined for a DNS server and the requests are not statically defined in the switch or previously cached, the switch forwards them to the servers as defined in the following configuration. The switch also forwards packets from the DNS servers back to the appropriate subnets.

To configure DNS Relay

1. In the left panel, click **Switch Utilities.**
2. In the top panel under Others, click **DNS Relay.**
3. Configure these fields.

Field	Description
DNS Relay State	Enables or disables DNS relay on the switch.
Name Server [1}	Specifies the IP address of the primary DNS server.
Name Server [2]	Specifies the IP address of a secondary DNS server.
DNS Relay Cache Status	Enables or disables the DNS cache on the switch.
DNS Static Table Lookup Status	Enables or disables the DNS Static Table Lookup function on the switch.

4. Click **Apply**.

To configure the static DNS table

The second task is to tell the DNS relay agent where the servers are located in terms of IP addresses and subnet names (IP interface names).

1. In the left panel, click **Switch Utilities.**
2. In the top panel under Others, click **DNS Relay - Static Table Configurations**.
3. Click **New** and configure these fields:

Field	Description
Domain Name	Specifies the name of the DNS server.
IP Address	Specifies the IP address of the DNS relay server.
Status	Enables or disables the entry for static look up.

4. Click **Apply**.
5. To remove an entry, highlight it in the DNS Static Table and click **Delete**.

Network Monitoring

This section explains how to monitor the following aspects of the switch:

- “Port Statistics” (packets, errors, and utilization)
- “Address Tables” (MAC, IP, Routing, and ARP)
- “Status” (switch history, router port table, IP multicast forwarding table, and other such tables)

Port Statistics

To view port utilization

1. In the left panel, click **Network Monitoring.**
2. In the top panel under Statistics, click **Port Utilization**.
3. To change the refresh interval, select a value from the drop-down menu.
4. To clear the gathered statistics, click **Clear**.

The screen displays these statistics.

Column	Description
Port	Identifies the port.
Tx/sec	Displays the number of packets transmitted per second
Rx/sec	Displays the number of packets received per second
%Utilization	Displays the calculated the percentage of the total bandwidth being used by the device attached to the port.

To view port error statistics

1. In the left panel, click **Network Monitoring.**
2. In the top panel under Statistics, click **Port Error Packets**.
3. In the Port field, select the port to view.
4. In the Interval field, select the interval for updating the statistics.
5. To clear the statistics and gather new information, click **Clear.**

The screen displays these statistics.

Field	Description
Rx Frames—Received packets	
CRC Error	Alignment. For 10 Mbps ports, the counter records CRC errors (FCS or alignment errors). For 100 Mbps ports, the counter records the sum of CRC errors and code errors (frames received with rxerror signal).
Undersize	Small. The total number of frames received that were shorter than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize	Long. The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragment	Small with alignment error. The total number of frames received that were shorter than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or an alignment error.
Jabber	Long with alignment error. The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or an alignment error.
Drop Pkts	Total dropped. The total number of events in which packets were dropped due to a lack of resources.

Field	Description
Tx—Transmitted packets	
ExDefer	Delayed. The number of frames for which the first transmission attempt on a particular interface was delayed because the medium was busy.
CRC Error	Alignment. For 10 Mbps ports, the counter records CRC errors (FCS or alignment errors). For 100 Mbps ports, the counter records the sum of CRC errors and code errors (frames received with rxerror signal).
Late Coll.	Late Collisions. The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Ex. Coll.	Excessive Collisions. The number of frames for which transmission failed due to excessive collisions.
Single Coll.	Single Collision Frames. The number of successfully transmitted frames for which transmission is inhibited by more than one collision.
Coll.	Total Collisions. An estimate of the total number of collisions on this network segment.

To view an analysis of packet sizes and types

1. In the left panel, click **Network Monitoring.**
2. In the top panel under Statistics, click **Port Packet Analysis.**
3. In the Port field, select the port to view.
4. In the Interval field, select the interval for updating the statistics.
5. To clear the statistics and gather new, click **Clear.**

The tables contain the following information.

Field	Description
Frame Size	The size in octets (bytes) of frames transmitted through the switch.
Frame Type	The type of frame being transmitted
Frame Counts	The total number of frames transmitted through the switch of the corresponding size indicated.
Frames/sec	The number of frames per second transmitted through the switch of the corresponding size indicated.
Packet Type	Either received (Rx) or transmitted (Tx) packets.
Total	The total number of bytes or frames transmitted or received.
Total/sec	The total number of bytes or frames received or transmitted per sec.

Address Tables

To view the MAC address table

1. In the left panel, click **Network Monitoring.**
2. In the top panel under Tables, click **MAC Address Table.**
3. Select how you want to view the MAC addresses:
   - **Search Table By VLAN—**Allows you to enter a VLAN name and find all known MAC addresses on that VLAN.
   - **Search Table By MAC Address—**Allows you to enter a specific MAC address or 00-00-00-00-00-00 to list all known MAC addresses.
   - **Search Table By Port**—Allows you to enter a port number and find all MAC addresses known by that port.
4. Click **Find**.

The following information is displayed about each MAC address.

Field	Description
VID	The VLAN ID of the VLAN the port is a member of.
VLAN Name	The name of the VLAN corresponding to the MAC address.
MAC Address	The MAC address of a device.
Port	The port corresponding to the MAC address.
Learned	How the switch discovered the MAC address. The possible entries are Dynamic, Self, and Static. Self is used to identify the switch.

To view the IP address table

1. In the left panel, click **Network Monitoring.**
2. In the top panel under Tables, click **IP Address Table.**
3. In the Start IP Address field, enter the IP address that you want the table to display first. The default value is 0.0.0.0 which displays all IP addresses in numerical order.
4. Click **Find** to populate the table.

The following information is displayed about each IP address.

Field	Description
Interface	The name of the IP Interface corresponding to the IP address.
IP Address	The IP address corresponding to the IP interface name.
Port#	The port the IP address is associated with.
Learned	How the switch discovered the IP interface. The possible entries are Dynamic and Static.

To view the routing table

1. In the left panel, click **Network Monitoring.**
2. In the top panel under Tables, click **Routing Table.**
3. In the entry boxes, enter the following information

Field	Description
Destination Address	IP address of a learned or statically entered destination.
Mask	The subnet mask corresponding to the above destination IP address.
Gateway	The default or next hop gateway to reach the destination.

   To find all known routes, enter 0.0.0.0 for all the addresses.

4. Click **Find.**
   The following information is displayed in the table.

Field	Description
IP Address	The IP address corresponding to the subnet mask and gateway.
Netmask	The subnet mask corresponding to the IP address.
Gateway	The gateway used to reach the IP address.
Interface Name	Displays the IP interface name the destination resides on.
Hops	Displays the number of hops (routers) between the switch and the destination.
Protocol	Displays the routing protocol in use by the link to the destination.

To view the ARP table

The Address Resolution Protocol (ARP) table allows the switch to relate often used IP addresses to MAC addresses quickly, and without having to make ARP requests.

1. In the left panel, click **Network Monitoring.**
2. In the top panel under Tables, click **ARP Table.**
3. In the entry boxes, enter the following information.

Field	Description
Interface Name	Specifies the IP interface name to start the display of the ARP table.
IP Address	Specifies of an IP address to start the display of the ARP table. To find all entries associated with an IP interface, enter 0.0.0.0 for the IP address.

4. Click **Find.**

The following ARP information is displayed.

Field	Description
Interface Name	The IP interface name corresponding to the IP address.
IP Address	The IP address that corresponds to the MAC address.
MAC Address	The MAC address that corresponds to the IP address.
Type	The method that was used to enter the MAC address and IP address pair into the ARP table. The possible entries are Static, Dynamic, and Local.

Status

To view GVRP Status

1. In the left panel, click **Network Monitoring.**
2. In the top panel under Status, click **GVRP Status.**

The screen contains this information.

Field	Description
IEEE 802.1Q VLAN ID	The ID assigned to the currently displayed VLAN.
Status	The status of the VLAN, whether it is a permanent definition or whether the ports dynamically joined the VLAN.
Creation time since switch power up	The time the VLAN was created or last modified, relative to when the switch was last booted.
Current Egress Ports	The ports in the VLAN which are egress ports.
Current Untagged Ports	The ports in the VLAN which are untagged.
Number of IEEE 802.1Q VLANs	The number of VLANs that have been defined for the switch.

If more than one IEEE 802.1Q VLAN has been defined for the switch, click Next to view the status of the other VLANs.

To view router ports

Router ports can be either static or dynamic. Static ports are ports that you manually configure to route UDP multicast packets. Dynamic ports are added by the switch when the switch detects UDP multicast packets and IGMP multicast group membership reports on a port.

1. In the left panel, click **Network Monitoring.**
2. In the top panel under Status, click **Router Ports.**
3. In the VLAN field, enter the name of the VLAN to search for router ports.
4. Click **Find.**

   The Router Port table contains the VLAN name, and under the port groupings (1 to 8, 9 to 16, 17 to 24, and 25 to 26), a port is assigned an “S” if the port is a static router port, a “D” if the port has been dynamically assigned to be a router port, or a “-” if the port is not a router port.

To view IGMP snooping status

1. In the left panel, click **Network Monitoring.**
2. In the top panel under Status, click **IGMP Snooping Status.**
3. In the VLAN Name field, enter the name of the VLAN to retrieve IGMP snooping information.
4. Click **Find.**

   The table displays this information.

Field	Description
Multicast Group	The IP address of a multicast group learned by IGMP snooping.
MAC Address	The corresponding MAC address learned by IGMP snooping.
Port Map	Displays the ports that have forwarded multicast packets from the above source.
Reports	The number of IGMP reports for the listed source.

To view the IP multicast forwarding table

You can browse the IP multicast forwarding table for static and dynamic (learned) entries. You can also search the table using a combination of a multicast group IP address, a multicast source IP address, and a subnet mask.

1. In the left panel, click **Network Monitoring.**
2. In the top panel under Status, click **IP Multicast Forwarding Table.**
3. Enter a multicast group address, a source IP address, and a source subnet mask address. To find all multicast groups known to the switch, use 0.0.0.0 for all the addresses.
4. Click **Find**.

   The table displays this information.

Column	Description
Multicast Group	The IP address of a multicast group used in the search for a specific entry.
Source IP Address.	The IP address of a multicast source used in the search for a specific entry.
Source Mask	The subnet mask of a multicast source used in the search for a specific entry.
Upstream Neighbor	The IP address of the next hop router between the multicast group and the source.
Expire Time	The number of seconds the packets from the multicast source can live.
Protocol	The multicast routing protocol used by the current source.

To view the IGMP group table

You can search the IGMP table using a combination of an IP interface name and a multicast group IP address.

1. In the left panel, click **Network Monitoring.**
2. In the top panel under Status, click **IGMP Group Table**

3. In the Interface Name field, enter the name of an IP interface.
4. In the Multicast Group field, enter the IP address of a multicast group. To find all groups for the specified IP interface, use 0.0.0.0 for the address.
5. Click **Find**.
   The table displays this information.

Column	Description
Interface Name	The IP interface associated with the multicast group.
Multicast Group	The IP address of the multicast group associated with the IP interface.
Last Reporter IP	The IP address of the member which responded with the last report.
Querier IP	The IP address of the member elected to be the querier for the group.
Expire	The time when the next report is due.

To view the DVMRP routing table

You can search the DVMRP routing table with an IP address and subnet mask combination.

1. In the left panel, click **Network Monitoring.**
2. In the top panel under Status, click **DVMRP Routing Table.**
3. Enter an IP address and a subnet mask.
4. Click **Find**.
   The table displays this information:

Column	Description
Source Address	The source IP address used to retrieve this information.
Source Mask	The source subnet mask used to retrieve this information.
Next Hop Router	The IP address of the next hop router for the source address.
Hop	The number of hops (routers) between the multicast group member and the switch.
Learned	The method the switch used to discover the source address, either Static or Dynamic.
Interface Name	The IP interface name of the source address.
Expire	The number of seconds before the entry expires. Expired entries display H-D (hold down) for 120 seconds before they are removed.

To view the switch's history log

1. In the left panel, click **Network Monitoring.**
2. In the top panel under Status, click **Switch History.**

The Switch History screen contains this information

Field	Description
Sequence	A counter incremented whenever an entry to the switch's history log is made. The table displays the last entry (highest sequence number) first.
Time	The time the history log entry was made. The time is specified in days, hours, and minutes since the switch was last restarted.
Log Text	Text describing the event that triggered the history log entry.

Advanced Setup

Most of the following options can be configured independently of the other options. However, you must configure a VLAN before you can configure an IP interface for it.

Spanning Tree Protocol

The Spanning Tree Protocol (STP) prevents loops in a network by allowing only one active path between any two network devices at a time. (For more information about using this protocol, refer to "Spanning Tree Concepts" in chapter 3.)

STP operates on two levels. On the switch level, the settings are globally implemented. On the port level, the settings are implemented on a user-defined group basis. STP must be enabled on the switch for it to be enabled on a particular port.

To configure STP switch settings

1. In the left panel, click **Spanning Tree.**
2. In the top panel, click **STP Switch Settings.**
3. In the Status field, select to **Enabled** or **Disabled**.

4. Configure the following fields. The factory default settings should cover the majority of installations, and most installations should keep these default settings.

Field	Default	Description
Max Age	20	Specifies the maximum time (in seconds) the switch will wait for a configuration message from the root bridge. At the end of this time, the switch will start sending out its own configuration messages for permission to become the root bridge. The device with the lowest bridge identifier becomes the root bridge (see the Priority field). Max Age must be set within the following range: • The minimum value is the higher of 6 or [2 x (Hello Time +1)] • The maximum value is the lower of 40 or [2 x (Forward Delay -1)]
Hello Time	2	Specifies the time interval (in seconds) between two configuration messages. The root bridge sends these messages at this interval to inform all other devices that it is the root bridge. This time will be used if and when your switch becomes the root bridge. It can be set from 1—10 seconds. The Hello Time cannot be longer than the Max Age; otherwise, a configuration error occurs.
Forward Delay	15	Specifies the maximum time (in seconds) the root device will wait before changing states (for example, from listening to blocking, from blocking to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward packets. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. • Maximum value is 30 • Minimum value is the higher of 4 or [(Max. Age / 2) +1]
Priority	32768	Priority is used in selecting the root bridge, root port, and designated port. The device with the highest priority becomes the STP root bridge. The lower the numeric value, the higher the priority. If all devices have the same priority, the device with the lowest MAC address will become the root bridge. Range: 0—65535.

5. Click **Apply**.

The following information is displayed about STP.

Field	Description
Designated Root Bridge	The IP address of the current root bridge for the STP group.
Root Priority	The current value of the bridge priority for the group.
Cost to Root	The currently-assigned cost for the route from the designated STP-group port to the root bridge.
Root Port	The port number of the root port.
Last Topology Change	The time (in seconds) since the last change in the root bridge or designated STP-group port.
Topology Change Count	The number of topology changes since the switch was last restarted.

To define the port members of an STP group

The switch allows you to configure Spanning Tree Groups that consist of a group of ports that will be handled as though they were a single spanning tree device. An STP group uses the switch-level parameters entered above, with the addition of port priority and port cost.

An STP group spanning tree works in the same way as the switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected (on the basis of port priority and port cost) to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the switch level.

An STP port group should correspond to a VLAN group of ports.

1. In the left panel, click **Spanning Tree.**
2. In the top panel, click **STP Port Settings.**
3. Configure these fields.

Field	Description
Cost	Specifies the port cost. It can be set between 1—65535. The lower the cost, the greater the probability the port will be chosen as the designated port (chosen to forward packets). The default value for the 10/100 ports is 19, and for the 100/1000 ports it is 4.
Priority	Specifies the port priority. It can be set between 0—255. The default is 128. The lower the priority, the greater the probability the port will be chosen as the root port. If two ports have the same priority, the port with the lowest port number is selected. For example, STP chooses port 1 over port 5 if they both have the same priority.
State	Enables or disables STP on the specified port or range of ports.

4. Click **Apply**.
   The Status field displays whether the port is Disabled or Forwarding. The STP Name field displays the assigned STP group name for the port.

Forwarding

Forwarding reduces traffic congestion on the network because packets are transmitted only to the destination port rather than to all ports. The switch maintains a number of static forwarding tables which you can manually configure for MAC, IP, and ARP forwarding.

This section explains how to configure

- MAC address aging
- MAC forwarding (unicast MAC address, multicast MAC address, and storm control)
- IP forwarding (static and default routes, static ARP)

To configure MAC address aging

A very long MAC address aging time can result in out-of-date dynamic entries that may cause incorrect packet filtering and forwarding decisions. A very short aging time may cause entries to be aged out too soon, which results in a high percentage of received packets whose source addresses cannot be found in the address table. In this case, the switch must broadcast the packet to all ports, negating many of the benefits of having a switch.

1. In the left panel, select **Forwarding**.
2. In the top panel under MAC Forwarding, select **MAC Address Aging Time**.
3. In the MAC Address Aging Time field, specify the length of time a learned MAC address can remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). The aging time can be set to any value between 300—1,000,000 seconds. The default is 300 seconds (5 minutes).
4. Click Apply.

To configure unicast MAC address forwarding

1. In the left panel, click **Forwarding**.
1. In the top panel under MAC Forwarding, click **Unicast MAC Address Settings**.
2. Click **New** and configure these fields.

Field	Description
MAC Address	Specifies the unicast MAC address in the packets.
VLAN Name	Specifies the VLAN to which the MAC address belongs.
Type	Specifies whether to forward the packets (Static) or to drop the packets (BlackHole).
Port	Specifies which port to use for forwarding the packets. This option is not available if BlackHole is specified as the type.

3. Click **Apply**.
4. To remove an entry for the Entries list, select the entry and click **Delete**.

To configure multicast MAC address forwarding

The multicast MAC address settings configure the switch to forward multicast packets from a specific MAC address to a specified VLAN. The port settings determine which ports can join the VLAN to forward the multicast packets.

1. In the left panel, click **Forwarding**.
2. In the top panel under MAC Forwarding, click **Multicast MAC Address Settings**.

3. Click New and configure these fields.

Field	Description
MAC Address	Specifies the MAC address of the source of the multicast packets.
VLAN Name	Specifies which VLAN to forward the multicast packets to.
State	Specifies how the port can join the multicast group. • **Engress**—Specifies that the port is a static member of the multicast group. • **Forbidden**—Restricts the port from joining the multicast group. • **None**—Specifies that the port has no restrictions and that it can join the multicast group dynamically.

4. Click **Apply**.

To configure storm control

The storm control settings allow you to specify thresholds for broadcast or multicast traffic that will activate storm control. When the threshold is exceeded, the switch drops the broadcast or multicast traffic. When the traffic level drops below the threshold, the switch resumes forwarding the traffic again.

1. In the left panel, click **Forwarding**.
2. In the top panel under MAC Forwarding, click **Broadcast/Multicast Storm Control**.
3. Configure these following fields for each port group.

Field	Description
Upper Threshold (Kpps)	Specifies, in thousands, the number of broadcast or multicast packets per second a port can receive before triggering a storm control response.
Broadcast Storm Mode	Enables or disables storm control for broadcast packets.
Multicast Storm Mode	Enables or disables storm control for multicast packets.

4. Click **Apply**.

To configure advanced traffic control

Advance traffic control sets the threshold for the amount of traffic a port can handle before triggering flow control. You must enable flow control on the ports before you can set a flow control threshold.

1. In the left panel, click **Forwarding**.
2. In the top panel under MAC Forwarding, click **Advance Traffic Control**.
3. Select the port you want to configure and click **Edit.**
4. In the Flow Control Threshold field, enter a value from 2—57344.
5. If you want this setting to apply to more than the selected port, select a group of ports in the Configure Port from field.
6. Click **Apply**.

The table displays this information about the ports:

Field	Description
Port	The port number.
Flow Control Threshold	The current value of the flow control threshold.
Drop Packet	A status field that indicates whether the port is currently dropping packets.
Flow Control Status	A status field that indicates whether the port is currently implementing flow control.
Port Connection	A status filed that indicates the port's speed, duplex mode, and flow control mode.

To configure static IP routes

1. In the left panel, click **Forwarding**.
2. In the top panel under IP Forwarding, click **Static/Default Routes**.
3. Click **New** and configure these fields.

Field	Description
IP Address	Specifies the IP address to be statically entered into the IP forwarding table.
Subnet Mask	Specifies the corresponding subnet mask for the IP address.
Gateway IP	Specifies the address of the next hop gateway for the IP address. This is usually a router with a connection to a WAN or the Internet.
Metric	Specifies the Routing Information Protocol (RIP) metric. This is the number of hops between the IP address and the gateway. This is a number between 1—15.

4. Click **Apply**.
5. To delete a route, select the entry in the static/default route table and click **Delete**.

To configure static ARP

The ARP table maps an IP address to a device's MAC address.

1. In the left panel, click **Forwarding**.
2. In the top panel under IP Forwarding, click **Static ARP**.
3. Click **New** and configure these fields.

Field	Description
Interface Name	Specifies the IP interface of the IP address that you are adding to the static ARP table.
IP Address field	Specifies the IP address of the end node or station.
MAC Address	Specifies the MAC address corresponding to the IP address.

4. Click **Apply**.
5. To delete a route, select the entry in the static ARP table and click **Delete**.

IP Address Filtering

You can manually configure the switch to drop packets from specified MAC and IP addresses. For information about specifying MAC addresses to drop, see the **Forwarding | Unicast MAC Address Setting** screen

To specify an IP address for filtering

1. In the left panel, click **IP Address Filtering**.
2. Click **New** and configure these fields:

Field	Description
IP Address	Specifies the IP address of the packets you want dropped.
Source/Destination	Specifies the condition for filtering the packets: • **Destination**—Packets with the above IP address as their destination will be dropped. • **Source**—Packets with the above IP address as their source will be dropped. • **Either**—All packets with the above IP address will be dropped.

3. Click **Apply**.
   The entry is added to the table.
4. To remove an entry, select the entry in the table and click **Remove**.

MAC Address Priority

You can specify a MAC address so that packets with this address are given special handling, either a higher or lower priority than normal traffic.

Note: If flow control is enabled, a small of amount of low priority traffic may be forwarded before high priority traffic.

To set up a MAC address priority

1. In the left panel, click **MAC Address Priority.**
2. Click **New** and configure these fields.

Field	Description
MAC Address	Specifies the MAC address to set a priority for.

Field	Description
VLAN Name	Specifies the name of VLAN on which this MAC address resides.
User Priority	Specifies the priority for this MAC address. The levels are 0—7, with 7 being the highest priority.
Source/Destination	Specifies the state under which the above priority will be active. The options are • **Destination**—Packets with the above MAC address as their destination will be given the selected priority. • **Source**—Packets with the above MAC address as their source will be given the selected priority. • **Either**—All packets with the above MAC address will be given the selected priority.

3. Click **Apply**.
4. To remove an entry, select the entry in the table and click **Delete**.

Mirroring Configurations

Incoming or outgoing traffic from any source port can be mirrored for realtime analysis. A logic analyzer or a RMON probe can then be attached to study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, remember the following conditions:

- The target port should be operating at the same or higher speed than the source port. If the target port is operating at a lower speed than the source port, packets will be lost.
- For optimum performance, you should mirror three or fewer ports at any given time.

To configure a port for mirroring

1. In the left panel, click **Mirroring Configurations.**
2. Configure these fields.

Field	Description
Target Port	Specifies the port where information will be duplicated and sent for capture and network analysis. This is the port where a network analyzer would be attached to capture packets duplicated from the source port.
Mirrored Port	Specifies which port to be mirror and which packets to be mirror. This port is the source of the packets. Use one of the following values: • **Rx**—Mirror incoming packet. • **T**x—Mirror outgoing packets. • **Both**—Mirror both incoming and outgoing packets. • **None**—Do not mirror. If the port is grayed out, the port cannot be selected for mirroring.

3. Click **Apply**.
4. To remove an entry, select the port and click **None**.

VLAN Configurations

The switch allows the assignment of an IP interface to each VLAN. A VLAN must be configured before setting up its IP interface. You can create either a port-based or an IEEE 802.1Q VLAN. By default, all ports belong to an IEEE 802.1Q VLAN called “default.” Although this VLAN cannot be deleted, all member ports can be assigned to other VLANs.

To configure GVRP globally

The global GVRP flag determines whether GVRP (Group VLAN Registration Protocol) is enabled on the switch so that the switch can share VLAN information with other switches, and VLANs can span multiple switches. When this flag is disabled, VLANs are confined to the physical connections of the switch. By default, this flag is disabled.

1. In the left panel, click **VLAN Configurations**.
2. In the top panel, click **Switch GVRP**.
3. Use the drop-down menu to select **Enabled** or Disabled.
4. Click **Apply**.

To configure a port-based VLAN

Ports must be removed from another VLAN before they are available for assigning as static members of a port-based VLAN.

1. In the left panel, click **VLAN Configurations**.
2. In the top panel, click **Port-Based VLANs**.
3. Click **New** and configure these fields.

Field	Description
VLAN Name	Specifies the name of the VLAN for which ports are to be configured. The name can be up to 32 characters. Once created, a VLAN name cannot be modified.
Port Member	Specifies which ports are static members of the VLAN. Click a port’s check box to add a port to the VLAN.

4. Click **Apply**.
5. To modify a VLAN, select it from the list and click **Edit**.

To configure an 802.1Q VLAN

1. In the left panel, click **VLAN Configurations**.
2. In the top panel, click **802.1Q VLANs**.
3. Click **New** and configure these fields.

Field	Description
VLAN ID (VID)	Specifies an identifier for the VLAN. Enter a number from 2—4094.

Field	Description
VLAN Name	Specifies the name of the VLAN for which ports are to be configured. The name can be up to 32 characters. Once created, the name cannot be modified.
Membership	Specifies the port's membership status. Select the appropriate state by selecting a radial button for each port. Options which aren't available are grayed out. • **Untagged**—Designates the port as an untagged member of the VLAN. When an untagged packet is transmitted by the port, the packet header remains unchanged. When a tagged packet exits the port, the tag is stripped and the packet is changed to an untagged packet. If the port is attached to a device that is not IEEE 802.1Q VLAN compliant (VLAN-tag unaware), then the port should be set to U - Untagged. • **Tagged**—Designates the port as a tagged member of the VLAN. When an untagged packet is transmitted by the port, the packet header is changed to include the 32-bit tag associated with the PVID (Port VLAN Identifier). When a tagged packet with a different VID exits the port, the packet header is unchanged. If the port is attached to a device that is IEEE 802.1Q VLAN compliant, (VLAN-tag aware), then the port can be set to Tagged. • **Forbidden**—Designates the port as not being a member of the VLAN and prevents packets tagged with the VLAN's VID from entering the port. • **None**—Designates the port as not being a member of the VLAN.

4. Click **Apply**.

To configure member ports of an 802.1Q VLAN

1. In the left panel, click **VLAN Configurations**.
2. In the top panel, click **IEEE 802.1Q Port Settings**.
3. For each port, enable or disable the following:

Field	Description
GVRP	Specifies whether the port can dynamically become a member of a VLAN. This protocol allows the port to share VLAN information with other ports so that a VLAN can span multiple switches.
Ingress Checking	Specifies whether a port checks the VID of incoming packets against its VID or PVID. If the two are equal, the port will receive the packet. It the two are unequal, the port will drop the packet. This is used to limit traffic to a single VLAN.

4. Click **Apply**.

Link Aggregation

Link aggregation allows several ports to be grouped together so that they can act as a single port. This is done to either increase the bandwidth of a network connection or to increase fault tolerance.

Link Aggregation is most commonly used to link a bandwidth-intensive network device or devices —such as a server or server farm—to the backbone of a network.

You can configure up to six aggregation groups, each using from two to eight ports between any two ZT8101 switches or other switches that support Etherchannel. Etherchannel is only required for this first release. In the second release, the ports can be from any switch that is compliant with 802.1ad.

To configure a link aggregation group

1. In the left panel, click **Link Aggregation**.
2. Select a group to configure and click **Edit**.
3. Configure these fields for the group.

Field	Description
Starting Port	Specifies the first port in the group. This port's configuration (speed, full- or half-duplex, etc.) will be used by all of the ports in the group. This port becomes the master port.
Group Width	Specifies the number of ports, in sequential order from the master port, that will be included in the group.
Status	Enables or disables the group.

4. Click **Apply**.

In addition to the configuration information, the table displays which port has been assigned to be the anchor port. The anchor port is responsible for the flooding of multicast frames and for sending control packets.

Layer 3 - IP Networking

This section describes how to configure

- IP interfaces
- RIP
- Multicast routing protocols

Setting Up IP Interfaces

Each IP interface on the switch corresponds to a VLAN. A VLAN, which does not have a corresponding IP interface defined for it, will function as a Layer 2-only VLAN.

The switch allows ranges of IP addresses (OSI Layer 3) to be assigned to VLANs (OSI Layer 2). Each VLAN must be configured prior to setting up the corresponding IP interface.

To set up IP interfaces on the switch

1. In the left panel, click **Layer 3 IP Networking**.
2. In the top panel under IP Interface Settings, click **IP Interface Settings**.

3. Click **New** and configure these fields.

Field	Description
Interface Name	Specifies the name of the IP interface. The default VLAN interface name is System.
IP Address	Specifies the IP address of the IP interface (sometimes referred to as a network address).
Subnet Mask	Specifies the subnet mask for the IP address.
VLAN Name	Specifies the VLAN that is assigned to this IP interface. This VLAN must already exist. The IP interface gets its port membership from the VLAN.
Active	Enables or disables the IP interface.
Port Member	Specifies the ports which are to be members of this IP interface.

4. Click **Apply**.
5. To delete an IP interface, highlight the interface and click **Delete**.

If you modify an existing IP interface and apply the changes, the RIP and IP multicast interface configurations are reset to default values.

RIP Configuration

The Routing Information Protocol (RIP) is a distance-vector protocol that uses the hop count as its criteria for making routing decisions. RIP is an Interior Gateway Protocol (IGP), which means that it performs routing within a single autonomous system.

To globally enable or disable RIP

1. In the left panel, click **Layer 3 IP Networking**.
2. In the top panel under IP Interface Settings, click **RIP Status**.
3. In the RIP field, select either **Disabled** or **Enabled**.
4. Click **Apply**.

To configure RIP interface settings

An IP Interface must be defined before you can configure its RIP settings.

1. In the left panel, click **Layer 3 IP Networking**.
2. In the top panel under IP Interface Settings, click **RIP Interface Settings**.
3. Select the interface you want to configure and click **Edit**.

4. Configure these fields.

Field	Description
Tx Mode	Specifies which version of the RIP protocol will be used to transmit RIP packets. This field toggles between Disabled, V1 Only, V1 Compatible, and V2 Only. Disabled prevents the transmission of RIP packets.
Rx Mode	Specifies which version of the RIP protocol will be used to interpret received RIP packets. This field toggles between Disabled, V1 Only, V2 Only, and V1 and V2. Disabled prevents the reception of RIP packets.
Authentication.	Enables or disables authentication between routers. When authentication is enabled, a password is used to authenticate communication between routers on the network. Authentication is only supported when RIP is in V1 Compatible or V2 mode.
Password	Specifies the password to be used to authenticate communication between routers on the network.

5. Click **Apply**.

Multicast Global Configurations

The Multicast Global Configurations screen is only for globally enabling or disabling the multicast routing protocols on the switch. Each VLAN or IP Interface uses these global values unless you configured it to use specialized settings. The protocol must be enabled globally before you can enable it on a specific VLAN or IP interface. (RIP is globally set up with the RIP Configuration option.)

To configure globally the multicast protocols

1. In the left panel, click **Layer 3 IP Networking**.
2. In the top panel under IP Multicast Routing Protocols, click **Multicast Global Configurations**.
3. Configure these fields.

Field	Description
Switch IGMP Snooping	Enables or disables, globally, Internet Group Management Protocol (IGMP) snooping. This protocol allows the switch to forward multicast traffic intelligently on the switch.
DVMRP	Enables or disables, globally, the Distance-Vector Multicast Routing Protocol (DVMRP).
DVMRP Include Report From Unknown Neighbors	Enables or disables receiving DVMRP reports from unknown neighbors.
PIM-DM	Enables or disables, globally, the Protocol Independent Multicasting - Dense Mode (PIM-DM) multicasting protocol.

4. Click **Apply.** Each protocol has a corresponding configuration form.

IGMP Configurations

The Internet Group Management Protocol (IGMP) allows the switch to forward multicast traffic intelligently on the switch. The switch “snoops” the IRMP query and report messages and forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

IGMP requires a network device that learns about the presence of multicast groups on its subnets and keeps track of group membership. Multicasting is not connection oriented, so data is delivered to the requesting hosts on a best-effort level of service.

The switch has two configuration screens for IGMP:

- The IGMP snooping screen allows you to configure the switch for snooping and querying.
- The IGMP interface screen allows you to configure the switch to keep track of IGMP groups.

To configure IGMP snooping

1. In the left panel, click **Layer 3 IP Networking**.
2. In the top panel under IP Multicast Routing Protocols, click **IGMP Snooping Configurations**.
3. Select a VLAN and click **Edit**.
4. Configure these fields.

Field	Description
Querier State	Specifies whether this VLAN should respond to IGMP queries. Three options are available: • **No**—Prevents this VLAN from becoming a querier. • **V1**—Enables the sending of IGMP query packets when needed. • **V2**—Enables the sending of IGMP query and leave packets according to the IGMP V2 specification.
Query Interval	Specifies the time that can elapse between general IGMP queries. Enter a value between 1—65535 seconds. The default is 125.
Robustness Variable	Specifies the permitted packet loss on a link. Enter a value between 2—255. The default is 2.
Max Response	Specifies the maximum time the switch can wait for IGMP member reports. Enter a value between 1—25. The default is 10 seconds.
State	Enables or disables learning about IGMP groups. If enabled, the switch limits multicast forwarding to active member ports.

5. Click **Apply**.

The following conditions affect the fields on the IGMP snooping screen:

- The switch IGMP snooping flag must be enabled for these settings to have any effect.
- If the IGMP settings have been enabled for the IP interface associated with the VLAN you select, the only field available on the IGMP snooping screen is the State field.

To configure IGMP for an IP interface

1. In the left panel, click **Layer 3 IP Networking**.
2. In the top panel under IP Multicast Routing Protocols, click **IGMP Interface Configurations**.
3. Select an interface and click **Edit**.
4. Configure these fields.

Field	Description
Version	Specifies the version number of IGMP to be used with the IP interface. Select between 1 and 2.
Query Interval	Specifies the time (in seconds) between the transmission of IGMP query packets. Enter a value between 1—65535 seconds. The default is 125.
Max Response Time	Specifies the maximum time the switch can wait for reports from members. Enter a value between 1—25. The default is 10 seconds.
Robustness Variable	Specifies the permitted packet loss on a link. Enter a value between 1—255. The default is 2.
State	Enables or disables IGMP on this IP interface.

5. Click **Apply**.

DVMRP Interface Configurations

The Distance Vector Multicast Routing Protocol (DVMRP) is a hop-based method of building multicast delivery trees from multicast sources to all nodes of a network. Because the delivery trees are “pruned” and use the “shortest path,” DVMRP is relatively efficient. Because multicast group membership information is forwarded by a distance-vector algorithm, propagation is slow. DVMRP is optimized for high delay (high latency) and relatively low-bandwidth networks, and it can be considered as a “best-effort” multicasting protocol.

To configure DVMRP for an IP interface

1. In the left panel, click **Layer 3 IP Networking**.
2. In the top panel, click **DVMRP Interface Configurations**.
3. Select the interface and click **Edit.**
4. Configure these fields.

Field	Description
Neighbor Timeout Interval	Specifies the maximum interval the switch will wait to hear from a neighbor. If this interval expires, the switch assumes that this neighbor is down. Enter a value from 1—65535. The default is 35.
Probe Interval	Specifies the interval between probes. A probe is a query to other routers to determine if a multicast group is present on a given router subnetwork. Enter a value from 1—65535 seconds. The default is 10.
Metric	Specifies cost for this path. The higher the assigned cost, the less likely it is that multicast packets will be routed over this interface (provided that other path options exist). Enter a value between 1—31. The default is 1.
State	Enables or disables DVMRP for this interface.

5. Click **Apply**.

PIM-DM Setup

The Protocol Independent Multicast - Dense Mode (PIM-DM) protocol should be used in networks with a low delay (low latency) and high bandwidth because PIM-DM is optimized to guarantee delivery of multicast packets, not to reduce overhead.

To configure PIM-DM for an IP interface

1. In the left panel, click **Layer 3 IP Networking**.
2. In the top panel, click **PIM-DIM Interface Configurations.**
3. Select the interface and click **Edit.**
4. Configure these fields.

Field	Description
Hello Interval	Specifies the interval between sending Hello packets to other routers on the network. The Hello messages are used by the router to determine whether it is the root router on the delivery tree or not. If the router does not receive a Hello message within the Hello Interval, it will begin transmitting Hello messages to advertise its availability to become the root router. The range is between 1—65535 seconds. The default is 30 seconds.
Join/Prune Interval	Specifies the interval between transmitting (flooding to all interfaces) multicast messages to downstream routers, and automatically “pruning” a branch from the multicast delivery tree. This interval also determines the time interval the router uses to automatically perform the following: • Remove prune information from a branch of a multicast delivery tree. • Begin to flood multicast messages to all branches of that delivery tree. These two actions are equivalent. The range is between 1— 65535 seconds. The default is 60 seconds.
State	Disables or enables PIM-DM for this IP interface. The default is Disabled.

5. Click **Apply**.

Static Router Port Settings

A static router port allows UDP multicast and IGMP packets to be forwarded to a designated port regardless of VLAN configuration.

A router port functions within Layer 2 of the OSI model. A static router port is a port that has a router attached to it. Generally, this router would have a connection to a WAN or to the Internet. Establishing a router port will allow multicast packets coming from the router to be propagated through the network. It also allows multicast messages coming from the network to be propagated to the router.

The purpose of a router port is to enable UDP multicast packets and IGMP multicast group membership messages to reach multiple ports of a multi-port router. Routers do not implement IGMP snooping or transmit/forward IGMP report packets. Thus, forwarding all IP UDP multicast

packets to a static router port on the ZT8101 switch guarantees that all ports of a multi-port router, which are attached to the switch, can reach all multicast group members through the attached router's other ports.

A router port interacts with multicast packets in these ways:

- All IGMP report packets will be forwarded to the router port.
- IGMP queries (from the router port) will be flooded to all ports.
- All UDP multicast packets will be forwarded to the router port. Because routers do not send IGMP reports or implement IGMP snooping, a multi-port router connected to the router port of the Layer 3 switch would not be able to receive UDP data streams from its ports unless the UDP multicast packets were all forwarded to the router port.

A router port will be dynamically configured when IGMP query packets, RIPv2 multicast, DVMRP multicast, PIM-DM multicast packets are detected flowing into a port.

To configure a static router port

1. In the left panel, click **Layer 3 IP Networking**.
2. In the top panel, click **Static Router Port Settings.**
3. Click **New** and configure these fields.

Field	Description
VLAN Name	Specifies the name of the VLAN that you want to configure a static router port for.
Port Members	Specifies the ports that you want to set up as static router ports. To select a port, click the port.

4. Click **Apply**.
5. To delete an entry from the table, select the entry and click **Delete**.

Agency Approvals A

CE Certification

The ZT8101 meets the intent of Directive 89/336/EEC for Electromagnetic Compatibility & Low-Voltage Directive 73/23/EEC for Product Safety. The ZT8101 has been designed for NEBS/ETSI compliance.

Safety

UL/cUL 60950	Safety for Information Technology Equipment (UL File # E179737)
EN/IEC 60950	Safety for Information Technology Equipment
CB Report Scheme	CB Certificate and Report

Emissions Test Regulations

FCC Part 15, Subpart B

EN 55022

CISPR 22

Bellcore GR-1089

EN 50081-1 Emissions

GR-1089-CORE	Sections 2 and 3
EN 55022	Class A Radiated
EN 55022	Power Line Conducted Emissions
EN 61000-3-2	Power Line Harmonic Emissions
EN 61000-3-3	Power Line Fluctuation and Flicker

EN 55024 Immunity

GR-1089-CORE	GR-1089-CORE Sections 2 and 3
EN 61000 4-2	Electrostatic Discharge (ESD)
EN 61000 4-3	Radiated Susceptibility
EN 61000 4-4	Electrical Fast Transient Burst
EN 61000 4-5	Power Line Surge
EN 61000 4-6	Frequency Magnetic Fields
EN 61000 4-11	Voltage Dips, Variations, & Short Interruptions

Regulatory Information

FCC—Federal Communications Commission (USA)

This product has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This product generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Note: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution: If you make any modification to the equipment not expressly approved by Intel, you could void your authority to operate the equipment.

Industry Canada (Canada)

Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques", NMB-003 édictée par le Ministre Canadien des Communications.

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled: "Digital Apparatus," ICES-003 of the Canadian Department of Communications.

Product Safety Information

Safety Precautions

Review the following precautions to avoid injury and prevent damage to this product, or products to which it is connected. To avoid potential hazards, use the product only as specified.

Read all safety information provided in the component product user manuals and understand the precautions associated with safety symbols, written warnings, and cautions before accessing parts or locations within the unit.

Caution: To Avoid Electric Overload. To avoid electrical hazards (heat shock and/or fire hazard), do not make connections to terminals outside the range specified for that terminal.

See the product user manual for correct connections.

Caution: To Avoid the Risk of Electric Shock. When supplying power to the system, always make connections to a grounded main. Always use a power cable with a grounded plug (third grounding pin). Do not operate in wet, damp, or condensing conditions.

Caution: System Airflow Requirements. Platform components such as single board computers, Ethernet switches, etc., are designed to operate with external air flow.

Components can be destroyed if they are operated without external air flow. External air flow is normally provided by chassis fans when components are installed in compatible chassis.

Filler panels must be installed over unused chassis slots so that airflow requirements are met.

Refer to the product data sheet for airflow requirements if you are installing components in custom chassis.

Warning: Microprocessor Heatsinks May Become Hot During Normal Operation. To avoid burns, do not allow anything to touch processor heatsinks.

Caution: Do Not Operate Without Covers. To avoid electric shock or fire hazard, do not operate this product with any removed enclosure covers or panels.

Caution: Do Not Operate in an Explosive Atmosphere. To avoid injury, fire hazard, or explosion, do not operate this product in an explosive atmosphere.

Caution: If Your System Has Multiple Power Supply Sources. Disconnect all external power connections before servicing.

Warning: Power Supplies Must Be Replaced by Qualified Service Personnel Only.

Caution: Lithium batteries are not field-replacable units. There is a danger of explosion if a battery is incorrectly replaced or handled. Do not disassemble or recharge the battery. Do not dispose of the battery in fire. When the battery is replaced, the same type or an equivalent type recommended by the manufacturer must be used. Used batteries must be disposed of according to the manufacturer's instructions. Return the unit to Intel for battery service.

Product Safety Information

AC and/or DC Power Safety Warning (AC and/or DC Powered Units)

The AC and/or DC Power cord is your unit's main AC and/or DC disconnecting device, and must be easily accessible at all times. Auxiliary AC and/or DC On/Off switches and/or circuit breaker switches are for power control functions only (NOT THE MAIN DISCONNECT).

For your safety, use only a power cord with a grounded plug. The enclosure is also provided with a separate Earth ground connection/stud. The Earth ground connection should be installed prior to the application of power or peripheral connections and should never be disconnected while power or peripheral connections exist.

To reduce the possibility of electric shock from a telephone or Ethernet system, plug your enclosure into the power source before making these connects. Disconnect these connections before unplugging your enclosure from the power source.

Warning: Verify Power Cord and Outlet Compatibility. Check to ensure you are using the appropriate power cords for your power outlet configurations. Visit the following Web site for additional information: http://kropla.com/electric2.htm.

Rack Mount Enclosure Safety

Your enclosure may be intended for stationary rack mounting. Mount in a rack designed to meet the physical strength requirements of NEBS GR-63-CORE and NEBS GR 487. Your system may have multiple power sources. Disconnect all power sources and external connections/cables prior to installing or removing your system from a rack frame.

Prior to mounting, Intel recommends that you remove all hot-swappable equipment for optimum weight reduction. Be sure to mount your system in a way that ensures even loading of the rack. Uneven mechanical loading of weight can result in a hazardous condition. Secure all mounting bolts when installing the enclosure to the frame/rack.

Caution: Avoid Electric Overload. To avoid electric shock or fire hazard, only connect your system to an input voltage source as specified in the product user manual.