

Part No. 060117-10, Rev. B  
January 2002

# **OmniStack<sup>®</sup> 8008**

## *Users Guide*

An Alcatel service agreement brings your company the assurance of 7x24 no-excuses technical support. You'll also receive regular software updates to maintain and maximize your Alcatel product's features and functionality and on-site hardware replacement through our global network of highly qualified service delivery partners. Additionally, with 24-hour-a-day access to Alcatel's Service and Support web page, you'll be able to view and update any case (open or closed) that you have reported to Alcatel's technical support, open a new case or access helpful release notes, technical bulletins, and manuals. For more information on Alcatel's Service Programs, see our web page at [www.ind.alcatel.com](http://www.ind.alcatel.com), call us at 1-800-995-2696, or email us at [support@ind.alcatel.com](mailto:support@ind.alcatel.com).

**This Manual documents OmniStack® 8008 hardware and software.  
The functionality described in this Manual is subject to change without notice.**

Copyright© 2002 by Alcatel Internetworking, Inc. All rights reserved. This document may not be reproduced in whole or in part without the express written permission of Alcatel Internetworking, Inc. Alcatel® and the Alcatel logo are registered trademarks of Compagnie Financière Alcatel, Paris, France. OmniSwitch® and OmniStack® are registered trademarks of Alcatel Internetworking, Inc. Omni Switch/Router™, SwitchExpertSM, the Xylan logo are trademarks of Alcatel Internetworking, Inc. All other brand and product names are trademarks of their respective companies.



26801 West Agoura Road  
Calabasas, CA 91301  
(818) 880-3500 FAX (818) 880-3505  
[info@ind.alcatel.com](mailto:info@ind.alcatel.com)  
US Customer Support-(800) 995-2696  
International Customer Support-(818) 878-4507  
Internet-<http://www.ind.alcatel.com>

## **Warning**

This equipment has been tested and found to comply with the limits for Class B 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 equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions in this guide, may cause interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user will be required to correct the interference at his own expense.

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user's authority to operate this equipment. It is suggested that the user use only shielded and grounded cables to ensure compliance with FCC Rules.

This digital apparatus does not exceed the Class B limits for radio noise emissions from digital apparatus set out in the radio interference regulations of the Canadian department of communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la Class B prescrites dans le règlement sur le brouillage radioélectrique édicté par le ministère des communications du Canada.



# Contents

---

---

<b>Chapter 1: Switch Management</b>	<b>1-1</b>
Configuration Options	1-1
Required Connections	1-1
Console Port (Out-of-Band) Connections	1-1
In-Band Connections	1-2
<b>Chapter 2: Console Interface</b>	<b>2-1</b>
Log-in Screen	2-1
Main Menu	2-2
System and Switch Information	2-5
Displaying System Information	2-6
Displaying Switch Version	2-7
Management Setup Menu	2-8
Changing the Network Configuration	2-9
IP Configuration	2-10
IP Connectivity Test (Ping)	2-11
HTTP Configuration	2-12
Configuring the Serial Port	2-13
Assigning SNMP Parameters	2-14
Configuring Community Names	2-15
Configuring IP Trap Managers	2-16
Console Login Configuration	2-17
Downloading System Software	2-18
Using TFTP Protocol to Download Over the Network	2-18
Saving the System Configuration	2-19
Managing the Switch	2-20
Configuring the Banner Message	2-21
Configuring the Switch	2-22
Configuring Port Parameters	2-24
Viewing the Current Port Configuration	2-25
Using the Spanning Tree Algorithm	2-26
Configuring Bridge STA	2-27
Configuring STA for Ports	2-28
Viewing the Current Spanning Tree Information	2-30
Displaying the Spanning Tree Bridge State	2-31
Displaying the Spanning Tree Port State	2-32
Using a Mirror Port for Analysis	2-33
Configuring Port Trunks	2-34
IGMP Multicast Filtering	2-36
Configuring IGMP	2-37

Configuring Broadcast Storm Control	2-38
Port Security Configuration	2-39
Configuring Bridge MIB Extensions	2-40
Configuring Traffic Classes	2-41
Port Priority Configuration	2-42
802.1P Port Traffic Class Information	2-43
Configuring Virtual LANs	2-44
802.1Q VLAN Base Information	2-44
802.1Q VLAN Current Table Information	2-45
802.1Q VLAN Static Table Configuration	2-46
802.1Q VLAN Port Configuration	2-48
Monitoring the Switch	2-49
Displaying Port Statistics	2-50
Displaying RMON Statistics	2-51
Displaying the Unicast Address Table	2-53
Displaying the IP Multicast Registration Table	2-54
Configuring Static Unicast Addresses	2-55
Resetting the System	2-56
Logging Off the System	2-56
<b>Chapter 3: Web Interface</b>	<b>3-1</b>
Web-Based Configuration and Monitoring	3-1
Navigating the Web Browser Interface	3-2
Home Page	3-2
Configuration Options	3-3
Panel Display	3-4
Port State Display	3-4
Configuring the Serial Port	3-5
Main Menu	3-6
System Information	3-7
Switch Information	3-8
Main Board	3-8
IP Configuration	3-9
SNMP Configuration	3-10
SNMP Community	3-10
Trap Managers	3-11
Security Configuration	3-11
Change Password	3-11
Firmware Upgrade Options	3-12
Web Upload Management	3-12
TFTP Download Management	3-13
Configuration Save and Restore	3-14
Configuration Upload Management	3-14
Configuration Download Management	3-14
Address Table Configuration	3-15

STA (Spanning Tree Algorithm)	3-16
Spanning Tree Information	3-16
Spanning Tree	3-16
Ports	3-17
Spanning Tree Configuration	3-18
Switch	3-18
When the Switch Becomes Root	3-19
STA Port Configuration	3-20
Configuring Bridge MIB Extensions	3-21
Bridge Capability	3-21
Bridge Settings	3-22
Priority	3-23
Port Priority Configuration	3-23
Port Traffic Class Information	3-24
Configuring Virtual LANs	3-25
VLAN Basic Information	3-25
VLAN Current Table	3-26
VLAN Static List	3-27
VLAN Static Table	3-27
VLAN Static Membership by Port	3-29
VLAN Port Configuration	3-30
IGMP Multicast Filtering	3-31
Configuring IGMP	3-31
IP Multicast Registration Table	3-32
Port Menus	3-33
Port Information	3-33
Port Configuration	3-34
Port Broadcast Storm Protect Configuration	3-35
Port Security Configuration	3-36
Using a Port Mirror for Analysis	3-37
Port Trunk Configuration	3-37
Port Statistics	3-39
Etherlike Statistics	3-39
RMON Statistics	3-40
<b>Chapter 4: Advanced Topics</b>	<b>4-1</b>
Layer 2 Switching	4-1
Spanning Tree Algorithm	4-1
Virtual LANs	4-2
Assigning Ports to VLANs	4-3
Port Overlapping	4-3
Automatic VLAN Registration (GVRP)	4-3
Forwarding Traffic with Unknown VLAN Tags	4-4
Forwarding Tagged/Untagged Frames	4-4
Connecting VLAN Groups	4-4

## Contents

Multicast Filtering	4-5
IGMP Snooping	4-5
IGMP Protocol	4-5
Class-of-Service (CoS) Support	4-6
Port Trunks	4-6
SNMP Management Software	4-6
Remote Monitoring	4-7
<b>Appendix A: Troubleshooting</b>	<b>A-1</b>
Troubleshooting Chart	A-1
Upgrading Firmware via the Serial Port	A-2
<b>Appendix B: Pin Assignments</b>	<b>B-1</b>
Console Port Pin Assignments	B-1
DB-9 Port Pin Assignments	B-1
Console Port to 9-Pin COM Port on PC	B-1
Console Port to 25-Pin DTE Port on PC	B-2
<b>Glossary</b>	
<b>Index</b>	

# Chapter 1: Switch Management

## Configuration Options

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

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

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

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

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

## Required Connections

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

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

When attaching to a PC, set terminal emulation type to VT100, specify the port used by your PC (i.e., COM 1~4), and then set communications to 8 data bits, 1 stop bit, no parity, and 9600 bps (for initial configuration). Also be sure to set flow control to "none." (Refer to "Configuring the Serial Port" on page 2-13 for a complete description of configuration options.)

**Note:** If the default settings for the management agent's serial port have been modified and you are having difficulty making a console connection, you can display or modify the current settings using a Web browser as described under "Configuring the Serial Port" on page 3-5.

## In-Band Connections

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

**Note:** By default BOOTP is disabled and the IP address is set to 192.168.10.1. See "IP Configuration" on page 2-10.

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

- Notes:**
1. This switch supports four concurrent Telnet sessions.
  2. The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software.

## Chapter 2: Console Interface

### Log-in Screen

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

```
Alcatel OmniStack 8008

Alcatel Internetworking
26801 West Agoura Road
Calabasas, CA, 91301
(818) 880-3500

Alcatel OmniStack
Copyright (c), 2000 Alcatel and its licensors.
All rights reserved.
OmniStack is a trademark of Alcatel registered in
the United States Patent and Trademark Office.

Username :
Password :
```

**Note:** A banner message may be configured to appear before the Login screen. The banner message is a login security alert. (See “Configuring the Banner Message” on page 2-21.)

If this is your first time to log into the configuration program, then the default user names are “admin” and “guest,” with the password “switch.” The Administrator has Read/Write access to all configuration parameters and statistics, while the Guest has Read Only access to the management program.

You should define a new administrator password, record it and put it in a safe place. Select Console Login Configuration from the Management Setup Menu and enter a new password for the administrator. Note that passwords can consist of up to 11 alphanumeric characters and are not case sensitive.

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

## Main Menu

The Main Menu is the first screen seen after successfully logging into the system.

```

Alcatel OmniStack 8008

    < Main Menu >

About this product
Management Setup Menu
Switch Configuration Menu
Network Monitor Menu
Reset System Menu
Quit Current Session

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

Selection	Description
About this product	
System Information	Provides basic system description, including contact information.
Switch Information	Shows hardware/firmware version numbers and power status of the switch.
Management Setup Menu	
Network Configuration	Includes IP setup, Ping facility, HTTP (Web server) setup, Telnet configuration, and MAC address.
Serial Port Configuration	Sets communication parameters for the serial port, including management mode, baud rate, console time-out, and screen data refresh interval.
SNMP Configuration	Activates traps; and configures communities and trap managers.
Console Login Configuration	Sets user names and passwords for system access, as well as the invalid password threshold and lockout time.
TFTP Download New Software	Downloads new version of firmware to update your system (in-band).
Configuration Save and Restore	Saves the switch configuratin to a file on the TFTP server. This file can be later downloaded to restore the configuration.
Management Configuration	Allows management access of the switch from all VLANs or only from a specified VLAN.

<b>Selection</b>	<b>Description</b>
Banner Message Configuration	Configures a login security alert message.
Switch Configuration Menu	
Port Configuration	Enables any port, enables/disables flow control, and sets communication mode to auto-negotiation, full duplex or half duplex.
Port State	Displays operational status, including link state, flow control method, and duplex mode.
Spanning Tree Configuration	Enables Spanning Tree Algorithm; also sets parameters for hello time, maximum message age, switch priority, and forward delay; as well as port priority and path cost.
Spanning Tree Information	Displays full listing of parameters for the Spanning Tree Algorithm.
Mirror Port Configuration	Sets the source and target ports for mirroring.
Port Trunking Configuration	Specifies ports to group into aggregate trunks.
IGMP Configuration	Configures IGMP multicast filtering.
BStorm Control Configuration	Allows you to enable/disable broadcast storm control on a per-port basis and set the packet-per-second threshold.
Port Security Configuration	Allows you to enable and configure port security for the switch.
Extended Bridge Configuration	Displays/configures extended bridge capabilities provided by this switch, including support for traffic classes, GMRP* multicast filtering, and VLAN extensions.
802.1P Configuration	Configures default port priorities and queue assignments.
802.1Q VLAN Base Information	Displays basic VLAN information, such as VLAN version number and maximum VLANs supported.
802.1Q VLAN Current Table Information	Displays VLAN groups and port members.
802.1Q VLAN Static Table Configuration	Configures VLAN groups via static assignments, including setting port members, or restricting ports from being dynamically added to a port by the GVRP protocol.
802.1Q VLAN Port Configuration	Displays/configures port-specific VLAN settings, including PVID, ingress filtering, and GVRP*.
Network Monitor Menu	
Port Statistics	Displays statistics on network traffic passing through the selected port.
RMON Statistics	Displays detailed statistical information for the selected port such as packet type and frame size counters.
Unicast Address Table	Provides full address listing, as well as search and clear functions.

---

<b>Selection</b>	<b>Description</b>
IP Multicast Registration Table	Displays all the multicast groups active on this switch, including multicast IP addresses and corresponding VLAN IDs.
Static Unicast Address Table Configuration	Used to manually configure host MAC addresses in the unicast table.
Reset system menu	Restarts system with options to use POST, or to retain factory defaults, IP settings, or user authentication settings.
Quit current session	Exits the configuration program.

---

\* Not implemented in the current firmware release.

## System and Switch Information

Use the "About this product" menu to display a basic description of the switch, including contact information, and hardware/firmware versions.

```

Alcatel OmniStack 8008

< About this product >

System Information
Switch Information

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

```

Selection	Description
System Information	Provides basic system description, including contact information.
Switch Information	Shows hardware/firmware version numbers and power status of the switch.

## Displaying System Information

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

```

Alcatel OmniStack 8008

< System Information >

System Description : Alcatel OmniStack 8008
System Object ID   : 1.3.6.1.4.1.800.3.1.1.13
System Up Time     : 8302069 (0 day 23 hr 3 min 40 sec)
Network Host Name  : OmniStack 8008
System Contact     :
System Location    :

<APPLY>           <OK>           <CANCEL>
Use <TAB> or arrow keys to move, other keys to make changes.
    
```

Parameter	Description
System Description	System hardware description.
System Object ID	MIB II object identifier for switch's network management subsystem.
System Up Time	Length of time the current management agent has been running. (Note that the first value is 1/100 seconds.)
Network Host Name*	Name assigned to the switch system.
System Contact*	Contact person for the system.
System Location*	Specifies the area or location where the system resides.

\* Maximum string length is 255, but the screen only displays 45 characters. You can use the arrow keys to browse the whole string.

## Displaying Switch Version

Use the Switch Information screen to display hardware/firmware version numbers for the switch, as well as the power status of the system.

```

Alcatel OmniStack 8008

< Switch Information >

Main Board

Label
P/N :          S/N :          Revision :

Hardware Version      : V3.0 (860 CPU)
Firmware Version     : V2.5
POST ROM Version     : V1.02
Serial Number        : 00-00-11-11-43-21
Port Number          : 8
Internal Power Status : Active
Redundant Power Status : Inactive

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

```

Parameter	Description
Main Board	
P/N	Part number of the main board.
S/N	Serial number of the main board.
Revision	Revision number of the main board.
Hardware Version	Hardware version of the main board.
Firmware Version	System firmware version in Flash ROM.
POST ROM Version	Power-On Self-Test version number.
Serial Number	MAC address associated with the main board.
Port Number	Number of ports on the switch.
Internal Power Status	Power status for the switch.
Redundant Power Status	Redundant power status for the switch.

## Management Setup Menu

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

```

Alcatel OmniStack 8008

< Management Setup Menu >

Network Configuration
Serial Port Configuration
SNMP Configuration
Console Login Configuration
TFTP Download New Software
Configuration Save & Restore
Management Configuration
Banner Message Configuration

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

Selection	Description
Network Configuration	Includes IP setup, Ping facility, HTTP (Web server) setup, Telnet configuration, and MAC address.
Serial Port Configuration	Sets communication parameters for the serial port, including management mode, baud rate, console time-out, and screen data refresh interval.
SNMP Configuration	Activates traps; and configures communities and trap managers.
Console Login Configuration	Sets user names and passwords for system access, as well as the invalid password threshold and lockout time.
TFTP Download New Software	Downloads new version of firmware to update your system (in-band).
Configuration Save & Restore	Saves the switch configuration to a file on a TFTP server. This file can be later downloaded to restore the configuration.
Management Configuration	Allows management access of the switch from all VLANs or only from a specified VLAN.
Banner Message Configuration	Configures a banner message. The banner message is a login security alert message.

## Changing the Network Configuration

Use the Network Configuration menu to set the bootup option, configure the switch's Internet Protocol (IP) parameters, enable the on-board Web server, or to set the number of concurrent Telnet sessions allowed. The screen shown below is described in the following table.

```

Alcatel OmniStack 8008

< Network Configuration >

IP Configuration
IP Connectivity Test (Ping)
HTTP Configuration
MAX Number of allowed Telnet sessions (1-4) : 4
Physical Address : 00-00-11-11-43-21

<APPLY>                <OK>                <CANCEL>
Use <TAB> or arrow keys to move. <Enter> to select.

```

Parameter	Description
IP Configuration	Screen used to set the bootup option, or configure the switch's IP parameters.
IP Connectivity Test	Screen used to test IP connectivity to a (Ping) specified device.
HTTP Configuration	Screen used to enable the Web server.
MAX Number of Allowed Telnet Sessions	The maximum number of Telnet sessions allowed to simultaneously access the switch.
Physical Address	MAC address of the switch.

## IP Configuration

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

```

Alcatel OmniStack 8008

< IP Configuration >

Interface Type : Ethernet

IP Address      : 192.168.10.1

Netmask        : 255.255.255.0

Default Gateway :

IP State       : USER-CONFIG

<APPLY>                <OK>                <CANCEL>
Use <TAB> or arrow keys to move, other keys to make changes.
    
```

Parameter	Default	Description
Interface Type	Ethernet	Indicates IP over Ethernet.
IP Address	192.168.10.1	IP address of the switch you are managing when accessing it over the network. The switch supports SNMP over UDP/IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the switch must have an IP address. Valid IP addresses consist of four decimal numbers, of 0 to 255, separated by periods. Anything outside of this format will not be accepted by the configuration program.
Subnet Mask	255.255.255.0	Subnet mask of the switch. This mask identifies the host address bits used for routing to specific subnets.
Default Gateway		The gateway that the switch's agent uses to pass data to the management station. Note that the gateway must be defined if the management station is located in a different IP segment.
IP State	USER-CONFIG	Specifies whether IP functionality is enabled via manual configuration, or set by Boot Protocol (BootP). Options include: USER-CONFIG -IP functionality is enabled based on the default or user specified IP configuration. BOOTP-GET-IP - IP is enabled but will not function until a BootP reply has been received. BootP requests will be broadcast 10 times, once every second, in an effort to learn its IP address. If no response is received, the switch will use the default IP setting in NVRAM. (BootP values can include the IP address, default gateway, and subnet mask.)

## IP Connectivity Test (Ping)

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

```

Alcatel OmniStack 8008

< IP Connectivity Test (Ping) >

IP Address :

Test Times : 1           Interval : 3
Success    : 0           Failure   : 0

[Start]

                                <OK>
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
IP Address	IP address of the site you want to ping.
Test Times	The number of ICMP echo requests to send to the specified site. Range: 1~9999
Interval	The interval (in seconds) between pinging the specified site. Range: 1~10 seconds
Success/Failure	The number of times the specified site has responded or not to pinging.

## HTTP Configuration

Use the HTTP Configuration screen to enable/disable the on-board Web server, and to specify the TCP port that will provide HTTP service. The screen shown below is described in the following table.

```

Alcatel OmniStack 8008

< HTTP Configuration >

HTTP Server      : ENABLED
HTTP Port Number : 80

<APPLY>          <OK>          <CANCEL>
Use <TAB> or arrow keys to move, <Space> to scroll options.
    
```

Parameter	Description
HTTP Server	Enables/disables access to the on-board Web server.
HTTP Port Number	Specifies the TCP port that will provide HTTP service. Range : 0-65535 Default : Port 80 (Telnet Port 23 is prohibited.)

## Configuring the Serial Port

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

```

Alcatel OmniStack 8008

< Serial Port Configuration >

Management Mode           : CONSOLE MODE

Baud rate                 : 9600
Data bits                 : 8
Stop bits                 : 1
Parity                   : NONE
Time-Out (in minutes)    : 10

<APPLY>                   <OK>                   <CANCEL>
Use <TAB> or arrow keys to move, <Space> to scroll options.

```

Parameter	Default	Description
Management Mode	Console Mode	Indicates that the console port settings are for direct console connection.
Baud Rate	9600	The rate at which data is sent between devices. Options : 2400, 4800, 9600, 19200 bps, and Auto detection
Data bits	8 bits	Sets the data bits of the RS-232 port. Options : 7, 8
Stop bits	1 bit	Sets the stop bits of the RS-232 port. Options : 1, 2
Parity	none	Sets the parity of the RS-232 port. Options : none/odd/even
Time-Out	10 minutes	If no input is received from the attached device after this interval, the current session is automatically closed. Range : 0 - 100 minutes; 0: disabled

### Assigning SNMP Parameters

Use the SNMP Configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP). The switch includes an 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 switch are controlled by community strings. To communicate with the switch, the NMS must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following sections.

```

Alcatel OmniStack 8008

< SNMP Configuration >

Send Authentication Fail Traps : ENABLED

SNMP Security

IP Trap Managers

<APPLY>           <OK>           <CANCEL>
Use <TAB> or arrow keys to move, <Space> to scroll options.
    
```

Parameter	Description
Send Authentication Fail Traps	Issue a trap message to specified IP trap managers whenever authentication of an SNMP request fails. (The default is enabled.)
SNMP Security	Assigns SNMP access based on specified strings.
IP Trap Managers	Specifies management stations that will receive authentication failure messages or other trap messages from the switch.

### Configuring Community Names

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

```

Alcatel OmniStack 8008

< SNMP Security >

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

<APPLY>           <OK>           <CANCEL>
Use <TAB> or arrow keys to move, other keys to make changes.

```

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

**Note:** The default community strings are “public” with Read Only access, and “private” with Read/Write access.

### Configuring IP Trap Managers

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

```

Alcatel OmniStack 8008

      < IP Trap Managers >

      IP Address      Community Name      Status
1.  10.1.0.23      public            DISABLED
2.
3.
4.
5.

      <APPLY>          <OK>                <CANCEL>
Use <TAB> or arrow keys to move, <Space> to scroll options.
    
```

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

## Console Login Configuration

Use the Management Setup: Console Login Configuration to restrict management access based on specified user names and passwords, or to set the invalid password threshold and timeout. There are only two user types defined, ADMIN (Administrator) and GUEST, but you can set up to five different user names and passwords. Only Administrators have write access for parameters governing the switch. You should therefore assign a user name and password to the default Administrator as soon as possible, and store it in a safe place. (If for some reason your password is lost, or you cannot gain access to the system configuration program, contact Alcatel Technical Support for assistance.) The parameters shown on this screen are indicated in the following figure and table.

```

Alcatel OmniStack 8008

< Console Login Configuration >

Password Threshold           : 3
Lock-out Time (in minutes) : 0

User Type      User Name      Password      Confirm password
-----
1. ADMIN      admin          *****      *****
2. GUEST      guest
3.
4.
5.

<APPLY>           <OK>           <CANCEL>
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Default	Description
Password Threshold	3	Sets the password intrusion threshold which limits the number of failed logon attempts. Range : 0-65535
Lock-out Time	0	Time (in minutes) the management console will be disabled, Range : 0-65535
Admin*	name: admin password: switch	Administrator has access privilege of Read/Write for all screens.
Guest*	name: user password: switch	Guest has access privilege of Read Only for all screens.

\* Passwords can consist of up to 11 alphanumeric characters and are not case sensitive.

## Downloading System Software

### Using TFTP Protocol to Download Over the Network

Use the TFTP Download menu to load software updates into the switch. The download file should be an OmniStack 8008 file from Alcatel; otherwise the switch will not accept it. The success of the download operation depends on the accessibility of the TFTP server and the quality of the network connection. After downloading the new software, the switch will automatically restart itself.

Parameters shown on this screen are indicated in the following figure and table.

```

Alcatel OmniStack 8008

< TFTP Download New Software >

Download Server IP :

Agent Software Upgrade      : ENABLED
Download Filename           :
Download Mode                : PERMANENT

[Process TFTP Download]

Download status : Complete

<APPLY>                <OK>                <CANCEL>
Use <TAB> or arrow keys to move, other keys to make changes.
    
```

Parameter	Description
Download Server IP	IP address of a TFTP server.
Agent Software Upgrade	Indicates that the switch is enabled for software upgrades.
Download Filename	The binary file to download to the switch.
Download Mode	Downloads to permanent flash ROM.
[Process TFTP Download]	Issues a request to the TFTP server to download the specified file.
Download Status	Indicates if a download is "Complete" or "In Progress."

## Saving the System Configuration

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

```

Alcatel OmniStack 8008

    < Configuration Upload >

        Upload Server IP      :
        Upload Filename       :

    [Process TFTP Upload]

    Upload status   : Complete

    < Configuration Download >

        Download Server IP    :
        Download Filename     :

    [Process TFTP Download]

    Download status : Complete

    <Apply>           <OK>           <Cancel>
    Use <TAB> or arrow keys to move, other keys to make changes.
  
```

Parameter	Description
<i>Configuration Upload</i>	
Upload Server IP	IP address of a TFTP server.
Upload Filename	The name of the file to contain the switch configuration settings.
[Process TFTP Upload]	Issues a request to upload the configuration settings to the specified file on the TFTP server.
Upload Status	Indicates if an upload is "Complete" or "In Progress."
<i>Configuration Download</i>	
Download Server IP	IP address of a TFTP server.
Download Filename	The name of the file that contains the switch configuration settings you wish to restore.
[Process TFTP Download]	Issues a request to the TFTP server to download the specified file.
Download Status	Indicates if a download is "Complete" or "In Progress."

### Managing the Switch

Use the Management Configuration screen to configure the management access of the switch.

```
Alcatel OmniStack 8008

< Management Configuration >

Management VLAN   : ONE
VLAN              : 1

<Apply>          <Ok>          <Cancel>
Use <TAB> or arrow keys to move, <Space> to scroll options.
```

---

Parameter	Description
Management VLAN	Allows management access of the switch from all VLANs or only from a specified VLAN. If this field is set to "ONE" then the single VLAN with management access must be set in the "VLAN" field.
VLAN	The ID of the only VLAN with management access to the switch when the "Management VLAN" field is set to "ONE."

---

## Configuring the Banner Message

The Banner Message is a login security alert message. It will be presented to a user attempting to log into the switch via console or Telnet, before prompting for a user name and password. Use the Banner Message Configuration screen to write and set the Banner Message.

You can type, or paste, the banner message into the screen one row at a time, using the arrow keys to move from one row to the next. For example, to paste text using Windows HyperTerminal, select "Paste to Host" from the Edit menu in the menu bar. Note that the maximum line length in the screen is 80 characters. The first page of a sample Banner Message is shown below.

```

Alcatel OmniStack 8008

< Banner Message Configuration >

SECURITY ALERT
This is an Organization Z computer system. This computer system,
including all related equipment, networks, and network devices
(specifically including Internet access and access to restricted sites)
is provided only for authorized use. Organization Z computer systems may
be monitored for all lawful purposes, including to ensure that their use
is authorized for management of the system, to facilitate protection
against unauthorized access, and to verify security procedures,
survivability, and operational security. Monitoring includes active
attacks by authorized Organization Z entities to test or verify the
security of this system. During monitoring, information may be examined,
recorded, copied and used for authorized purposes. All information,
including personal information, placed or sent over this system may be
monitored.
Use of this Organization Z computer system, authorized or unauthorized,
constitutes consent to monitoring of this system. Unauthorized use may
subject you to criminal prosecution.

Page : 1      Total 4 Pages
<Apply>      <Ok>          <Cancel>      <Prev Page>   <Next Page>
Use <TAB> or arrow keys to move, <Space> to scroll options.

```

**Note:** After entering text, use <Apply> to confirm the text that you have entered or <OK> to confirm the text and return to the Management Setup menu. Use <Cancel> to cancel the text that you have just entered and return to the Management Setup menu. Use <Prev Page> and <Next Page> to scroll through the banner message.

## Configuring the Switch

The Switch Configuration Menu is used to control a broad range of functions, including port configuration, Spanning Tree support for redundant switches, port mirroring, multicast filtering, and Virtual LANs. Each of the setup screens provided by these configuration menus is described in the following sections.

```

Alcatel OmniStack 8008

< Switch Configuration Menu >

Port Configuration           Extended Bridge Configuration
Port State                  802.1P Configuration
Spanning Tree Configuration 802.1Q VLAN Base Information
Spanning Tree Information   802.1Q VLAN Current Table Information
Mirror Port Configuration   802.1Q VLAN Static Table Configuration
Port Trunking Configuration 802.1Q VLAN Port Configuration
IGMP Configuration         Port GARP Configuration
BStorm Control Configuration Port GMRP Configuration
Port Security Configuration

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

Selection	Description
Port Configuration	Sets communication parameters for ports.
Port State	Displays current port settings and port status.
Spanning Tree Configuration	Configures the switch and its ports to participate in a local Spanning Tree.
Spanning Tree Information	Displays the current Spanning Tree configuration for the switch and its ports.
Mirror Port Configuration	Sets the source and target ports for mirroring.
Port Trunking Configuration	Specifies ports to group into aggregate trunks.
IGMP Configuration	Configures IGMP multicast filtering.
BStorm Control Configuration	Allows you to enable/disable broadcast storm control on a per-port basis and set the packet-per-second threshold.
Port Security Configuration	Allows you to enable and configure port security for the switch.

Selection	Description
Extended Bridge Configuration	Displays/configures extended bridge capabilities provided by this switch, including support for traffic classes, and VLAN extensions.
802.1P Configuration	Configures default port priorities and queue assignments.
802.1Q VLAN Base Information	Displays basic VLAN information, such as VLAN version number and maximum VLANs supported.
802.1Q VLAN Current Table Information	Displays VLAN groups and port members.
802.1Q VLAN Static Table Configuration	Configures VLAN groups via static assignments, including setting port members, or restricting ports from being dynamically added to a port by the GVRP protocol.
802.1Q VLAN Port Configuration	Displays/configures port-specific VLAN settings, including PVID, ingress filtering, and GVRP.
Port GARP Configuration*	Configures generic attribute settings used in the Spanning Tree Algorithm, VLAN registration, and multicast filtering.
Port GMRP Configuration*	Configures GMRP multicast filtering.

\* Not implemented in the current firmware release.

### Configuring Port Parameters

Use the Port Configuration menus to set or display communication parameters for any port on the switch.

```

Alcatel OmniStack 8008

< Port Configuration >

Flow Control mode of all ports : [Enable] [Disable]

Port      Type      Admin      Flow Control      Speed and Duplex
-----
 1    1000SX    ENABLED    DISABLED          AUTO
 2    1000SX    ENABLED    DISABLED          1000_FULL
 3    1000SX    ENABLED    DISABLED          AUTO
 4    1000SX    ENABLED    DISABLED          AUTO
 5    1000SX    ENABLED    DISABLED          AUTO
 6    1000SX    ENABLED    DISABLED          AUTO
 7    1000SX    ENABLED    DISABLED          AUTO
 8    1000SX    ENABLED    DISABLED          AUTO

<APPLY>                <OK>                <CANCEL>
Use <TAB> or arrow keys to move. <Enter> to select
    
```

Parameter	Default	Description
Flow Control mode of all ports	DISABLED	Allows you to enable or disable flow control for all ports on the switch.
Type		Shows port type as 1000SX (1000BASE-SX)
Admin	ENABLED	Allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable a port for security reasons.
Flow Control	DISABLED	Used to enable or disable flow control. Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. Back pressure is used for half duplex and IEEE 802.3x for full duplex.
Speed and Duplex	AUTO	Used to set the current port speed, duplex mode, and auto-negotiation.

**Note:** If you experience problems establishing a port link using auto-negotiation, try forcing the setting of the port to 1000\_FULL or 1000\_HALF.

## Viewing the Current Port Configuration

The Port State screen displays the port type, status, link state, and flow control in use, as well as the communication speed and duplex mode. To change any of the port settings, use the Port Configuration menu.

```

Alcatel OmniStack 8008

< Port State >

Port  Type  Operational Link  FlowControl  Speed and
      InUse  Duplex InUse
-----
1.   1000SX  YES      UP      NONE      1000-FULL
2.   1000SX  YES      UP      NONE      1000-FULL
3.   1000SX  YES      UP      NONE      1000-FULL
4.   1000SX  YES      UP      NONE      1000-FULL
5.   1000SX  YES      UP      NONE      1000-FULL
6.   1000SX  YES      UP      NONE      1000-FULL
7.   1000SX  YES      UP      NONE      1000-FULL
8.   1000SX  YES      UP      NONE      1000-FULL

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

```

Parameter	Description
Type	Shows port type as 1000SX (1000BASE-SX).
Operational	Shows if the port is functioning or not.
Link	Indicates if the port has a valid connection to an external device.
FlowControl InUse	Shows the flow control type in use. Flow control can eliminate frame loss by "blocking" traffic from end stations connected directly to the switch. Back pressure is used for half duplex and IEEE 802.3x for full duplex.
Speed and Duplex InUse	Displays the current port speed and duplex mode used.

## Using the Spanning Tree Algorithm

The Spanning Tree Algorithm can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network. For a more detailed description of how to use this algorithm, refer to "Spanning Tree Algorithm" on page 4-1.

```
Alcatel OmniStack 8008

< Spanning Tree Configuration Menu >

Spanning Tree Bridge Configuration
Spanning Tree Port Configuration

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

## Configuring Bridge STA

The following figure and table describe Bridge STA configuration.

```

Alcatel OmniStack 8008

< Spanning Tree Bridge Configuration >

Spanning Tree Protocol      : On
Bridge Priority              : 32768
Hello Time (in seconds)    : 2
Max Age (in seconds)       : 20
Forward Delay (in seconds) : 15

<APPLY>          <OK>          <CANCEL>
Use <TAB> or arrow keys to move, <Space> to scroll options.

```

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

Parameter	Default	Description
Max (Message) Age	20	<p>The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.</p> <p>The minimum value is the higher of 6 or <math>[2 \times (\text{Hello Time} + 1)]</math>.</p> <p>The maximum value is the lower of 40 or <math>[2 \times (\text{Forward Delay} - 1)]</math>.</p>
Forward Delay	15	<p>The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.</p> <p>The maximum value is 30.</p> <p>The minimum value is the higher of 4 or <math>[(\text{Max. Message Age} / 2) + 1]</math>.</p>

### Configuring STA for Ports

The following figure and table describe STA configuration for ports.

```

Alcatel OmniStack 8008

  < Spanning Tree Port Configuration >

Fast forwarding mode of all ports : [Enable]  [Disable]
Port      Type      Priority  Cost    FastForwarding
-----
1         1000SX      128      4       ENABLED
2         1000SX      128      4       ENABLED
3         1000SX      128      4       ENABLED
4         1000SX      128      4       ENABLED
5         1000SX      128      4       ENABLED
6         1000SX      128      4       ENABLED
7         1000SX      128      4       ENABLED
8         1000SX      128      4       ENABLED

<APPLY>                <OK>                    <CANCEL>
Use <TAB> or arrow keys to move. <Enter> to select
    
```

Parameter	Default	Description
Fast forwarding mode of all ports	ENABLED	Allows you to enable or disable fast forwarding for all ports on the switch.
Type		Shows the port type as 1000SX (1000Base-SX).
Priority	128	Defines the priority for the use of a port in the STA algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the spanning tree. When more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is 0 - 255.
(Path) Cost	100/19/4	This parameter is used by the STA algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) The default and recommended range is: Ethernet: 100 (50-600) Fast Ethernet: 19 (10-60) Gigabit Ethernet: 4 (3-10) The full range is 0 - 65535.
FastForwarding	ENABLED	This parameter is used to enable/disable the Fast Spanning Tree mode for the port. In this mode, ports skip the Blocked, Listening and Learning states and proceed straight to Forwarding. FastForwarding enables end-node workstations and servers to overcome time-out problems when the Spanning Tree Algorithm is implemented in a network. Therefore, FastForwarding should only be enabled for ports that are connected to an end-node device.

### Viewing the Current Spanning Tree Information

The Spanning Tree Information screen displays a summary of the STA information for the overall bridge or for a specific port. To make any changes to the parameters for the Spanning Tree, use the Spanning Tree Configuration menu.

```
Alcatel OmniStack 8008

< Spanning Tree Information Menu >

Spanning Tree Bridge State
Spanning Tree Port State

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

## Displaying the Spanning Tree Bridge State

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

```

Alcatel OmniStack 8008

< Spanning Tree Bridge State >

Bridge Priority           : 32768
Hello Time (in seconds)  : 2
Max Age (in seconds)    : 20
Forward Delay (in seconds) : 5
Hold Time (in seconds)   : 1
Designated Root         : 128.0000E800E800
Root Cost                : 4
Root Port               : 8
Configuration Changes    : 152
Topology Up Time        : 112844 (0 day 0 hr 18 min 48 sec)

<OK>
<Enter> to select.

```

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

### Displaying the Spanning Tree Port State

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

```

Alcatel OmniStack 8008
< Spanning Tree Port State >
Port      Type      Status      Designated      Designated      Designated
          Type      Status      Cost            Bridge          Port
-----
1      1000SX  NO LINK      4      32768.0010B54C1EB6      128.1
2      1000SX  NO LINK      4      32768.0010B54C1EB6      128.2
3      1000SX  NO LINK      4      32768.0010B54C1EB6      128.3
4      1000SX  NO LINK      4      32768.0010B54C1EB6      128.4
5      1000SX  NO LINK      4      32768.0010B54C1EB6      128.5
6      1000SX  NO LINK      4      32768.0010B54C1EB6      128.6
7      1000SX  NO LINK      4      32768.0010B54C1EB6      128.7
8      1000SX  NO LINK      4      32768.0010B54C1EB6      128.8

          <Ok>
Use <TAB> or arrow keys to move. <Enter> to select.
    
```

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

## Using a Mirror Port for Analysis

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a network sniffer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, note that the target port must be configured in the same VLAN as the source port (see “Configuring Virtual LANs” on page 2-44).

You can use the Mirror Port Configuration screen to designate a single port pair for mirroring as shown below:

```

Alcatel OmniStack 8008

< Mirror Port Configuration >

Mirror Source Port : Port 1

Mirror Target Port : Port 2

Status                : DISABLED

<APPLY>                <OK>                <CANCEL>
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
Mirror Source Port	The port whose traffic will be monitored.
Mirror Target Port	The port that will duplicate or “mirror” all the traffic happening on the monitored port.
Status	Enables or disables the mirror function.

## Configuring Port Trunks

Port trunks can be used to increase the bandwidth of a network connection or to ensure fault recovery. You can configure up to four trunk connections (combining 2~4 ports into a fat pipe) between any two OmniStack 8008 switches. However, before making any physical connections between devices, use the Trunk Configuration menu to specify the trunk on the devices at both ends. When using a port trunk, note that:

- Ports can only be assigned to one trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- The ports at both ends of a trunk must be configured in an identical manner, including duplex mode, and VLAN assignments.
- None of the ports in a trunk can be configured as a mirror source port or mirror target port.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Algorithm will treat all the ports in a trunk as a whole.
- Enable the trunk prior to connecting any cable between the switches to avoid creating a loop.
- Disconnect all trunk port cables or disable the trunk ports before removing a port trunk to avoid creating a loop.

You can use the Port Trunking Configuration screen to set up port trunks as shown below. Remember that you must "Enable" a new configuration before it will take effect.

```

Alcatel OmniStack 8008

      < Port Trunking Configuration >

Trunk ID  Status          Member List
-----  -
      1      2      3      4
-----  -
  --  -----  Port : --  Port : --  Port : --  Port : --

  --  -----  Port : --  Port : --  Port : --  Port : --

  --  -----  Port : --  Port : --  Port : --  Port : --

Trunk ID : 1          Trunk ID : 1  Member Port : 1

[Show]      [More]
[Enable]    [Disable]          [Add]      [Delete]

      <OK>

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

```

Parameter	Description
Trunk ID	Configure up to four trunks per switch (ID of 1~4).
Port	Select from 2~4 ports per trunk.
[Show]	Displays trunk settings, where the first trunk listed is specified by "Sorted by Trunk ID."
[More]	Scrolls through the list of configured trunks.
[Enable] [Disable]	Enables/disables the selected trunk.

## **IGMP Multicast Filtering**

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

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts who want to receive a specific multicast service. The switch looks up the IP Multicast Group used for this service and adds any port which received a similar request to that group. It then propagates the service request on to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. (For more information, see "IGMP Snooping" on page 4-5.)

## Configuring IGMP

This protocol allows a host to inform its local switch/router that it wants to receive transmissions addressed to a specific multicast group. You can use the IGMP Configuration screen to configure multicast filtering shown below:

```

Alcatel OmniStack 8008

< IGMP Configuration >

IGMP Status                : DISABLED
IGMP Query Count           : 2
IGMP Report Delay (Seconds) : 10

<APPLY>                <OK>                <CANCEL>
Use <TAB> or arrow keys to move, <Space> to scroll options.

```

Parameter	Description
IGMP Status	If enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.
IGMP Query Count	The maximum number of queries issued for which there has been no response before the switch takes action to solicit reports.
IGMP Report Delay	The time (in seconds) between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list.

**Note:** The default values are indicated in the sample screen.

### Configuring Broadcast Storm Control

Use the Broadcast Storm Control Configuration screen to enable broadcast storm control for any port on the switch, as shown below.

```

Alcatel OmniStack 8008

< Broadcast Storm Control Configuration >

Broadcast control on all ports :      [Enable]  [Disable]
Port      Threshold      Broadcast Control
-----
1          500             ENABLED
2          500             ENABLED
3          500             ENABLED
4          500             ENABLED
5          500             ENABLED
6          500             ENABLED
7          500             ENABLED
8          500             ENABLED

<Apply>                <OK>                <Cancel>
Use <TAB> or arrow keys to move. <Enter> to select
    
```

Parameter	Description
Broadcast control on all ports	Allows you to enable/disable broadcast storm control for all ports on the switch.
Threshold	The packet-per-second threshold for broadcast packets on the port. (Default is 500 pps.)
Broadcast Control	Enables/disables broadcast control for the port. When enabled, the switch will employ a broadcast-control mechanism if the packet-per-second threshold is exceeded. This mechanism limits the amount of broadcasts passed by the port to half of the received packet-per-second count. The control mechanism remains in effect until the number of received broadcasts falls back below the packet-per-second threshold. (Default is Enabled.)

## Port Security Configuration

Use the Port Security Configuration screen to enable and configure port security for the switch. Port Security allows you to configure each port with a list of MAC addresses of devices that are authorized to access the network through that port.

```

Alcatel OmniStack 8008

  < Port Security Configuration >

MAC Address          MAC Address
-----
-----

Secure address count : 0

Port : 1              MAC : 00-00-00-00-00-00
[Show]               [More]           [Add] [Delete]
Mode:DISABLE         [Apply]          [Clear]

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

```

Parameter	Description
MAC Address	A list of the authorized MAC addresses that can access the network through the specified port.
Secure address count	The number of authorized MAC addresses for the specified port.
Port	Numeric identifier for switch port.
[Show]	Displays authorized MAC addresses for the specified port.
[More]	Displays more MAC addresses for the port.
Mode	Port security can be set to three states: Static, Disable, or Learning. When set to Static, the switch will drop packets from the port if the source MAC address does not match one of the addresses in the MAC Address list. If set to Learning, the switch will add the source MAC address of all packets received on the port to the authorized MAC Address list.
[Apply]	Applies a change of Mode to the port.
MAC	A specific MAC address to be added or deleted from the list.
[Add]	Adds a new MAC address to the current list.
[Delete]	Removes a MAC address from the current list.
[Clear]	Clears all the MAC addresses for the current port.

## Configuring Bridge MIB Extensions

The Bridge MIB includes extensions for managed devices that support Traffic Classes, Multicast Filtering and Virtual LANs. To configure these extensions, use the Extended Bridge Configuration screen as shown below:

```

Alcatel OmniStack 8008

< Extended Bridge Configuration >

Bridge Capability : (Read Only)
  Extended Multicast Filtering Services : NO
  Traffic Classes                       : YES
  Static Entry Individual Port          : YES
  VLAN Learning                        : IVL
  Configurable PVID Tagging            : YES
  Local VLAN Capable                   : NO

Bridge Settings :
  Traffic Classes                       : TRUE
  GMRP                                  : DISABLED
  GVRP                                  : DISABLED

<APPLY>                <OK>                <CANCEL>
Use <TAB> or arrow keys to move, <Space> to scroll options.

```

Parameter	Description
Bridge Capability	
Extended Multicast Filtering Services	Indicates that the switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol). Note that this function is not implemented for the current firmware release.
Traffic Classes	Indicates that the switch provides mapping of user priorities to multiple traffic classes. (Refer to 802.1P Configuration.)
Static Entry Individual Port	Indicates that the switch allows static filtering for unicast and multicast addresses. (Refer to Network Monitor Menu / Static Unicast Address Table Configuration and Static Multicast Address Table Configuration.)
VLAN Learning	This switch uses Independent VLAN Learning (IVL), whereby each port maintains its own VLAN filtering database.
Configurable PVID Tagging	Indicates that the switch allows you to override the default PVID setting (Port VLAN ID used in frame tags) and its egress status (VLAN-Tagged or Untagged) on each port. (Refer to 802.1Q VLAN Port Configuration.)
Local VLAN Capable	This switch does not support multiple local bridges (that is, multiple Spanning Trees).

Parameter	Description
Bridge Settings	
Traffic Class*	Multiple traffic classes are supported by this switch as indicated under Bridge Capabilities. However, you can disable this function by setting this parameter to False.
GMRP*	GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. The Internet Group Management Protocol (IGMP) is currently used by this switch to provide automatic multicast filtering.
GVRP*	GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports across the network. This function should be enabled to permit VLANs groups which extend beyond the local switch.

\* Not implemented in the current firmware release.

### Configuring Traffic Classes

IEEE 802.1p defines up to 8 separate traffic classes. This switch supports Quality of Service (QoS) by using two priority queues, with Weighted Fair Queuing for each port. You can use the 802.1P Configuration menu to configure the default priority for each port, or to display the mapping for the traffic classes as described in the following sections.

```

Alcatel OmniStack 8008

      < 802.1P Configuration >

802.1P Port Priority Configuration
802.1P Port Traffic Class Information

                                <Ok>
Use <TAB> or arrow keys to move. <Enter> to select.

```

### Port Priority Configuration

The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in the low priority output queue. Default priority is only used to determine the output queue for the current port; no priority tag is actually added to the frame. You can use the 802.1P Port Priority Configuration menu to adjust default priority for any port as shown below:

```

Alcatel OmniStack 8008

< 802.1P Port Priority Configuration >

Port          Default Ingress   Number of Egress
              User Priority Traffic Class
-----
1             0                 2
2             0                 2
3             0                 2
4             0                 2
5             0                 2
6             0                 2
7             0                 2
8             0                 2

<APPLY>          <OK>          <CANCEL>
Use <TAB> or arrow keys to move, other keys to make changes.
    
```

Parameter	Description
Port	Numeric identifier for switch port.
Default Ingress User Priority	Default priority can be set to any value from 0~7, where 0~3 specifies the low priority queue and 4~7 specifies the high priority queue.
Number of Egress Traffic Classes	Indicates that this switch supports two priority output queues.

**802.1P Port Traffic Class Information**

This switch provides two priority levels with weighted fair queuing for port egress. This means that any frames with a default or user priority from 0~3 are sent to the low priority queue "0" while those from 4~7 are sent to the high priority queue "1" as shown in the following screen:

```

Alcatel OmniStack 8008

< 802.1P Port Traffic Class Information >

Port                               User Priority
      0      1      2      3      4      5      6      7
-----
1  0      0      0      0      1      1      1      1
2  0      0      0      0      1      1      1      1
3  0      0      0      0      1      1      1      1
4  0      0      0      0      1      1      1      1
5  0      0      0      0      1      1      1      1
6  0      0      0      0      1      1      1      1
7  0      0      0      0      1      1      1      1
8  0      0      0      0      1      1      1      1

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

```

Parameter	Description
Port	Numeric identifier for switch port.
User Priority	Shows that user priorities 0~3 specify the low priority queue and 4~7 specify the high priority queue.

## Configuring Virtual LANs

You can use the VLAN configuration menu to assign any port on the switch to any of up to 256 LAN groups. In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle a lot of IPX and NetBEUI traffic. By using IEEE 802.1Q compliant VLANs and GARP VLAN Registration Protocol, you can organize any group of network nodes into separate broadcast domains, confining broadcast traffic to the originating group. This also provides a more secure and cleaner network environment. For more information on how to use VLANs, see “Virtual LANs” on page 4-2. The VLAN configuration screens are described in the following sections.

### 802.1Q VLAN Base Information

The 802.1Q VLAN Base Information screen displays basic information on the VLAN type supported by this switch.

```

Alcatel OmniStack 8008

< 802.1Q VLAN Base Information >

VLAN Version Number           : 1
MAX VLAN ID                   : 2048
MAX Supported VLANs           : 256
Current Number of 802.1Q VLANs Configured : 1

                                <OK>
                                <Enter> to select.

```

Parameter	Description
VLAN Version Number	The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
MAX VLAN ID	Maximum VLAN ID recognized by this switch.
MAX Supported VLANs	Maximum number of VLANs that can be configured on this switch.
Current Number of VLANs Configured	The number of VLANs currently configured on this switch.

**Note:** All ports are assigned only to VLAN 1 by default.

### 802.1Q VLAN Current Table Information

This screen shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can assign ports to the same untagged VLAN (page 2-48). The current configuration is shown in the following figure.

```

Alcatel OmniStack 8008

< 802.1Q VLAN Current Table Information >

Deleted VLAN Entry Counts : 0

VID                Creation Time                Status
-----
1      0 (0 day 0 hr 0 min 0 sec)          Permanent

Current Egress Ports      Current Untagged Ports
11111111                 11111111

Sorted by VID : 1
[Show]  [More]
Use <TAB> or arrow keys to move. <Enter> to select

```

Parameter	Description
Deleted VLAN Entry Counts	The number of times a VLAN entry has been deleted from this table.
VID	The ID for the VLAN currently displayed.
Creation Time	The value of sysUpTime (System Up Time) when this VLAN was created.
Status	Shows how this VLAN was added to the switch: Dynamic GVRP: Automatically learned via GVRP. Permanent: Added as a static entry.
Current Egress Ports	Shows the ports which have been added to the displayed VLAN group, where "1" indicates that a port is a member and "0" that it is not.
Current Untagged Ports	If a port has been added to the displayed VLAN (see Current Egress Ports), its entry in this field will be "1" if the port is untagged or "0" if tagged.
[Show]	Displays the members for the VLAN indicated by the "Sorted by VID" field.
[More]	Displays any subsequent VLANs if configured.

### 802.1Q VLAN Static Table Configuration

Use this screen to create a new VLAN or modify the settings for an existing VLAN. You can add/delete port members for a VLAN, or prevent a port from being automatically added to a VLAN via the GVRP protocol. (Also, note that all ports can only belong to one untagged VLAN. This is set to VLAN 1 by default, but can be changed via the 802.1Q VLAN Port Configuration screen on page 2-48.)

```

Alcatel OmniStack 8008
< 802.1Q VLAN Static Table Configuration >
VID      VLAN Name      Status
-----
1
Egress Ports      Forbidden Egress Ports
11111111         00000000
Untagged Ports
11111111         VID : 1
                  [Show]
                  [More]
                  [New]
<APPLY>          <OK>          <CANCEL>
Use <TAB> or arrow keys to move, other keys to make changes.
    
```

Parameter	Description
VID	The ID for the VLAN currently displayed. Range: 1-2048
VLAN Name	A user-specified symbolic name for this VLAN. String length: Up to 8 alphanumeric characters
Status	Sets the current editing status for this VLAN as: Not in Service, Destroy, or Active.
Egress Ports	Set the entry for any port in this field to "1" to add it to the displayed VLAN, or "0" to remove it from the VLAN.
Forbidden Egress Ports	Prevents a port from being automatically added to this VLAN via GVRP.
Untagged Ports	Set the entry for any port in this field to "1" to add it to the displayed VLAN as an untagged port.
[Show]	Displays settings for the specified VLAN.
[More]	Displays consecutively numbered VLANs.
[New]	Sets up the screen for configuring a new VLAN.

**Note:** No VLANs are statically configured by default.

For example, the following screen displays settings for VLAN 2, which includes tagged ports 1-4, and forbidden port 8.

```
Alcatel OmniStack 8008
< 802.1Q VLAN Static Table Configuration >
      VID      VLAN Name      Status
      -----
      2
Egress Ports          Forbidden Egress Ports
11110000              00000001

Untagged Ports
00000000

VID : 2
[Show]
[More]
[New]

<APPLY>          <OK>          <CANCEL>
Use <TAB> or arrow keys to move, other keys to make changes.
```

### 802.1Q VLAN Port Configuration

Use this screen to configure port-specific settings for IEEE 802.1Q VLAN features.

```

Alcatel OmniStack 8008

< 802.1Q VLAN Port Configuration >

Port  PVID    Acceptable  Ingress    GVRP      GVRP Failed  GVRP Last
      PVID    Frame Type  Filtering  Status     Registrations PDU Origin
-----
 1     1         All         FALSE      DISABLED    0           00-00-00-00-00-00
 2     1         All         FALSE      DISABLED    0           00-00-00-00-00-00
 3     1         All         FALSE      DISABLED    0           00-00-00-00-00-00
 4     1         All         FALSE      DISABLED    0           00-00-00-00-00-00
 5     1         All         FALSE      DISABLED    0           00-00-00-00-00-00
 6     1         All         FALSE      DISABLED    0           00-00-00-00-00-00
 7     1         All         FALSE      DISABLED    0           00-00-00-00-00-00
 8     1         All         FALSE      DISABLED    0           00-00-00-00-00-00

      <APPLY>                <OK>                <CANCEL>
Use <TAB> or arrow keys to move, other keys to make changes.
    
```

Parameter	Description
PVID	The VLAN ID assigned to untagged frames received on this port. Use the PVID to assign ports to the same untagged VLAN.
Acceptable Frame Type <sup>1</sup>	This switch accepts "All" frame types, including VLAN tagged or VLAN untagged frames. Note that all VLAN untagged frames received on this port are assigned to the PVID for this port.
Ingress Filtering <sup>1</sup>	If set to "True," incoming frames for VLANs which do not include this port in their member set will be discarded at the inbound port.
GVRP Status <sup>2</sup>	Enables or disables GVRP for this port. When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. Note that GVRP must be enabled for the switch before this setting can take effect. (See Switch Configuration Menu / Extended Bridge Configuration.)
GVRP Failed Registrations <sup>2</sup>	The total number of failed GVRP registrations, for any reason, on this port.
GVRP Last PDU Origin <sup>2</sup>	The Source MAC Address of the last GVRP message received on this port.

1. This control does not affect VLAN independent BPDU frames, such as GVRP or STP. However, it does affect VLAN dependent BPDU frames, such as GMRP.

2. GVRP is not available for the current firmware release.

## Monitoring the Switch

The Network Monitor Menu provides access to port statistics, RMON statistics, IP multicast addresses, and the static (unicast) address table. Each of the screens provided by these menus is described in the following sections.

```

Alcatel OmniStack 8008

< Network Monitor Menu >

Port Statistics
RMON Statistics
Unicast Address Table
Multicast Address Registration Table
IP Multicast Registration Table
Static Unicast Address Table Configuration
Static Multicast Address Table Configuration

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

```

Parameter	Description
Port Statistics	Displays statistics on network traffic passing through the selected port.
RMON Statistics	Displays detailed statistical information for the selected port such as packet type and frame size counters.
Unicast Address Table	Provides full listing of all unicast addresses stored in the switch, as well as sort, search and clear functions.
Multicast Address Registration Table*	Displays the ports that belong to each GMRP Multicast group.
IP Multicast Registration Table	Displays the ports that belong to each IP Multicast group.
Static Unicast Address Table Configuration	Allows you to display or configure static unicast addresses.
Static Multicast Address Table Configuration*	Allows you to display or configure static GMRP multicast addresses.

\* Not implemented in the current firmware release.

### Displaying Port Statistics

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

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

```

Alcatel OmniStack 8008

      < Port Statistics > Port  1

Ether Like Counter :

Alignment Errors      : 0          Late Collisions      : 0
FCS Errors           : 0          Excessive Collisions : 0
Single Collision Frames : 0      Internal Mac Transmit Errors: 0
Multiple Collision Frames: 0      Carrier Sense Errors  : 0
SQE Test Errors      : 0          Frame Too Longs       : 0
Deferred Transmissions : 0      Internal Mac Receive Errors : 0

      [Refresh Statistics]          [Reset Counters]

      <OK>          <PREV PORT>          <NEXT PORT>
      Use <TAB> or arrow keys to move. <Enter> to select
    
```

Parameter	Description
Alignment Errors	The number of frames received that are not an integral number of octets in length and do not pass the FCS check.
FCS Errors	The number of frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames*	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames*	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
SQE Test Errors*	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer.
Deferred Transmissions*	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.

Parameter	Description
Excessive Collisions*	The number of frames for which transmission failed due to excessive collisions.
Internal Mac Transmit Errors*	The number of frames for which transmission failed due to an internal MAC sublayer transmit error.
Carrier Sense Errors*	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Frame Too Longs	The number of frames received that exceed the maximum permitted frame size.
Internal Mac Receive Errors	The number of frames for which reception failed due to an internal MAC sublayer receive error.

\* The reported values will always be zero because these statistics are not supported by the internal chip set.

## Displaying RMON Statistics

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

```

Alcatel OmniStack 8008

      < RMON Statistics > Port  1

Drop Events      : 4                Jabbers          : 0
Received Bytes   : 438387005        Collisions       : 0
Received Frames  : 2470786          64 Byte Frames  : 715132
Broadcast Frames : 2180266          65-127 Byte Frames : 868284
Multicast Frames : 237352           128-255 Byte Frames : 502964
CRC/Alignment Errors : 0           256-511 Byte Frames : 379998
Undersize Frames : 172              512-1023 Byte Frames : 671
Oversize Frames  : 0                1024-1518 Byte Frames : 3565
Fragments       : 0

      [Refresh Statistics]                [Reset Counters]

<OK>                <PREV PORT>                <NEXT PORT>
Use <TAB> or arrow keys to move. <Enter> to select

```

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

## Displaying the Unicast Address Table

The Address Table contains the MAC addresses and VLAN identifier associated with each port (that is, the source port associated with the address and VLAN), sorted by MAC address or VLAN ID. You can search for a specific address, clear the entire address table, or information associated with a specific address, or set the aging time for deleting inactive entries. The information displayed in the Address Table is indicated in the following figure and table.

```

Alcatel OmniStack 8008
< Unicast Address Table >

Aging Time : 300      Dynamic Counts : 146      Static Counts : 0
  MAC          VID      Port Status      MAC          VID      Port Status
-----
00-00-24-B3-28-83  1      8 D  00-00-E8-00-00-02  1      8 D
00-00-E2-12-F9-F8  1      8 D  00-00-E8-00-00-05  1      8 D
00-00-E2-16-C5-82  1      8 D  00-00-E8-00-00-96  1      8 D
00-00-E2-20-C3-D5  1      8 D  00-00-E8-00-01-01  1      8 D
00-00-E2-21-74-D0  1      8 D  00-00-E8-07-12-5E  1      8 D
00-00-E2-2A-59-9A  1      8 D  00-00-E8-11-03-51  1      8 D
00-00-E2-2E-FD-F6  1      8 D  00-00-E8-11-11-33  1      8 D
00-00-E8-00-00-00  1      8 D  00-00-E8-12-12-12  1      8 D

Sorted by : MAC + VID      Cleared by : MAC + VID
VLAN ID   : 1              VLAN ID     : 1
MAC       : 00-00-00-00-00-00  MAC         : 00-00-00-00-00-00
[Show]    [More]            [Clear]     [Clear Dynamic]

<APPLY>      <OK>      <CANCEL>
Use <TAB> or arrow keys to move, other keys to make changes.

```

Parameter	Description
Aging Time	Time-out period in seconds for aging out dynamically learned forwarding information. Range: 10 - 65534 seconds; Default: 300 seconds
Dynamic Counts	The number of dynamically learned addresses in the table.
Static Counts	The number of static addresses in the table.
MAC	The MAC address of a node.
VID	The VLAN(s) associated with this address or port.
Port	The port whose address table includes this MAC address.
Status	Indicates address status as: D: Dynamically learned, or P: Fixed permanently by SNMP network management software.
[Show]	Displays the address table based on specified VLAN ID, and sorted by primary key MAC or VID.
[More]	Scrolls through the entries in the address table.

Parameter	Description
[Clear]	Clears the specified MAC address.
[Clear Dynamic]	Clears all dynamically learned MAC addresses in the table.

### Displaying the IP Multicast Registration Table

Use the IP Multicast Registration Table to display all the multicast groups active on this switch, including multicast IP addresses and the corresponding VLAN ID.

```

Alcatel OmniStack 8008

< IP Multicast Registration Table >

VID      Multicast IP      Dynamic Port Lists      Learned by
-----
1        224.0.0.2         00000001                IGMP
1        224.0.0.9         00000001                IGMP
1        224.0.1.22        00000001                IGMP
1        224.0.1.24        00000001                IGMP
1        224.1.2.9         00000010                IGMP

Sorted by      : VID + Multicast IP
VID            : 1
Multicast IP   : 224.0.0.2
[Show]         [More]

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

Parameter	Description
VID	VLAN ID assigned to this multicast group.
Multicast IP	IP address for specific multicast services.
Dynamic Port Lists	The switch ports registered for the indicated multicast service.
Learned by	Indicates if the ports were learned dynamically or via IGMP.
[Show]	Displays the address table sorted on VID and then Multicast IP.
[More]	Scrolls through the entries in the address table.

## Configuring Static Unicast Addresses

Use the Static Unicast Address Table Configuration screen to manually configure host MAC addresses in the unicast table. You can use this screen to associate a MAC address with a specific VLAN ID and switch port as shown below.

```

Alcatel OmniStack 8008

< Static Unicast Address Table Configuration >

VID          MAC Address          Port      Status
-----
1           00-00-00-E8-43-12         1         Permanent

Sorted by : VID + MAC          VID   : 1   MAC   : 00-00-00-00-00-00
VID      : 1                   Port   : 1
MAC      : 00-00-00-00-00-00   Status : Permanent

[Show]      [More]              [Set]

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

```

Parameter	Description
VID	The VLAN group this port is assigned to.
MAC Address	The MAC address of a host device attached to this switch.
Port	The port the host device is attached to.
Status	The status for an entry can be set to: Permanent: This entry is currently in use and will remain so after the next reset of the switch. DeleteOnReset: This entry is currently in use and will remain so until the next reset. Invalid: Removes the corresponding entry. DeleteOnTimeOut: This entry is currently in use and will remain so until it is aged out. (Refer to Address Table Aging Time on page 2-53.) Other: This entry is currently in use but the conditions under which it will remain so differ from the preceding values.
[Show]	Displays the static address table sorted on VID as the primary key and MAC address as secondary key.
[More]	Scrolls through entries in the static address table.
[Set]	Adds the specified entry to the static address table, such as shown in the following example: VID : 1      MAC : 00-00-00-e8-34-22 Port : 1 Status : Permanent

## Resetting the System

Select the Reset System Menu under the Main Menu to reset the switch. The reset screen includes options as shown in the following figure and table.

```

Alcatel OmniStack 8008

      < Reset System Menu >

Restart Option :

      POST                               : YES
      Reload Factory Defaults           : NO
      Keep IP Setting                   : NO
      Keep User Authentication          : NO

      [Restart]

      <APPLY>           <OK>           <CANCEL>
Use <TAB> or arrow keys to move, <Space> to scroll options.
    
```

Parameter	Description
POST	Runs the Power-On Self-Test
Reload Factory Defaults	Reloads the factory defaults
Keep IP Setting	Retains the settings defined in the IP Configuration menu.
Keep User Authentication	Retains the user names and passwords defined in the Console Login Configuration menu.

## Logging Off the System

Use the Quit Current Session command under the Main Menu to exit the configuration program and terminate communications with the switch for the current session.

## **Chapter 3: Web Interface**

### **Web-Based Configuration and Monitoring**

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

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

1. Configure it with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection or BOOTP protocol.
2. Set a user name and password using an out-of-band serial connection. Access to the Web agent is controlled by the same user name and password as the onboard configuration program.

## Navigating the Web Browser Interface

To access the Web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name for the administrator is “admin,” with the password “switch.”

### Home Page

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

The screenshot shows the Alcatel OmniStack 8008 Manager web interface. On the left is a navigation menu with the following items: System (selected), Switch, IP, SNMP, Security, Upgrade, Configure, Address Table, STA, Bridge Extension, Priority, VLAN, IGMP, Port, Mirror, Trunk, and Statistics. Below the menu are 'Apply', 'Revert', and 'Help' buttons. The main content area is titled 'Alcatel OmniStack 8008 Manager' and contains a table with the following data:

System Name	OmniStack 8008
IP Address	10.2.34.97
Object ID	1.3.6.1.4.1.800.3.1.1.13
Location	
Contact	
System Up Time	0 d 0 h 29 min 34 s

Below the table are three links: [Telnet](#) - Connect to textual user interface, [Support](#) - Send mail to technical support, and [Contact](#) - Connect to ALCATEL Web page. At the top right, there is a 'Mode:' dropdown menu set to 'Active' and a status bar with 'Link Up' and 'Link Down' indicators.

If this is your first time to access the management agent, you should define a new Administrator password, record it and put it in a safe place. From the Main Menu, select Security and enter a new password for the Administrator. Note that passwords can consist of up to 11 alphanumeric characters and are not case sensitive.

**Note:** Based on the default configuration, a user is allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated. See “Console Login Configuration” on page 2-17.

## Configuration Options

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the “Apply” button at the bottom of the page to confirm the new setting. The following table summarizes the Web page configuration buttons.

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

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

## Panel Display

The Web agent displays an image of the switch's ports, showing port links and activity. Clicking on the image of a port displays statistics and configuration information for the port. Clicking on the image of the serial port (labeled "Mgmt") displays the Console Configuration screen. Clicking on any other part of the front panel displays Switch Information as described on page 3-7.



## Port State Display

Click on any port to display a summary or port status as shown below, as well as Etherlike statistics (page 3-39) and RMON statistics (page 3-40).

Type	1000Base-SX
Admin Status	Enabled
Link Status	Up
Speed Status	1000M
Duplex Status	Full
Flow Control Status	IEEE 802.3x
VLAN	1

Parameter	Description
Type	Shows port type as 1000BASE-SX
Admin Status	Shows if the port is enabled, or has been disabled due to abnormal behavior or for security reasons. See "Port Configuration" on page 3-34.
Link Status	Indicates if the port has a valid connection to an external device.
Speed Status	Indicates the current port speed.
Duplex Status	Indicates the port's current duplex mode.
Flow Control Status	Shows the flow control type in use. Flow control can eliminate frame loss by "blocking" traffic from end stations connected directly to the switch.
VLAN	The VLAN ID assigned to untagged frames received on this port. Use the PVID (page 3-30) to assign ports to the same untagged VLAN.

## Configuring the Serial Port

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

Baud rate	9600
Time-Out	10 minutes
Data bits	8
Stop bits	1
Parity	None
Auto-Refresh Time	5 seconds

Parameter	Default	Description
Baud Rate	9600	The rate at which data is sent between devices. Options : 2400, 4800, 9600, 19200 bps, and Auto detection.
Time-Out	10 minutes	If no input is received from the attached device after this interval, the current session is automatically closed. Range : 0 - 100 minutes; where 0 indicates disabled
Data Bits	8 bits	Sets the data bits of the RS-232 port. Options : 7, 8
Stop Bits	1 bit	Sets the stop bits of the RS-232 port. Options : 1, 2
Parity	None	Sets the parity of the RS-232 port. Options : none/odd/even
Auto Refresh Time	5 second	Sets the interval before a console session will auto refresh the console information, such as Spanning Tree Information, Port Configuration, Port Statistics, and RMON Statistics. Range : 0, or 5-255 seconds; where 0 indicates disabled

## Main Menu

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

Function	Description
System	Provides basic system description, including contact information.
Switch	Shows hardware/firmware version numbers and power status of the switch.
IP	Includes boot state, IP address, and Telnet session count.
SNMP	Configures communities and trap managers; and activates traps.
Security	Sets password for system access.
Upgrade	Downloads new version of firmware to update your system.
Configure	Saves the switch configuration to a file on a TFTP server. This file can be later downloaded to restore the configuration
Address Table	Provides full listing or unicast addresses, sorted by address or VLAN.
STA	Enables Spanning Tree Algorithm; also sets parameters for switch priority, hello time, maximum message age, and forward delay; as well as port priority and path cost.
Bridge Extension	Displays/configures extended bridge capabilities provided by this switch, including support for traffic classes, GMRP* multicast filtering, and VLAN extensions.
Priority	Configures default port priorities and queue assignments.
VLAN	Configures VLAN group members, automatic registration with GVRP*, and other port-specific VLAN settings.
IGMP	Configures IGMP multicast filtering.
Port	Enables any port, sets communication mode to auto-negotiation, full duplex or half duplex, and enables/disables flow control.
Mirror	Sets the source and target ports for mirroring.
Trunk	Specifies ports to group into aggregate trunks.
Statistics	Displays statistics on network traffic passing through the selected port.

\* Not implemented in the current firmware release.

## System Information

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

System Name	OmniStack 8008
IP Address	10.1.10.98
Object ID	1.3.6.1.4.1.800.3.1.1.13
Location	
Contact	
System Up Time	1 d 17 h 12 min 44 s

Parameter	Description
System Name <sup>1</sup>	Name assigned to the switch system.
IP Address <sup>2</sup>	IP address of the switch you are managing. The switch's management supports SNMP over UDP/IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the switch must have an IP address. Valid IP addresses consist of four decimal numbers, of 0 to 255, separated by periods. Anything outside of this format will not be accepted by the configuration program.
Object ID	MIB II object identifier for switch's network management subsystem.
Location <sup>1</sup>	Specifies the area or location where the system resides.
Contact <sup>1</sup>	Contact person for the system.
System Up Time	Length of time the current management software has been running.

<sup>1</sup> Maximum string length is 255, but the screen only displays 45 characters. You can use the arrow keys to browse the whole string.

<sup>2</sup> The default value is 192.168.10.1

## Switch Information

Use the Switch Information screen to display hardware/firmware version numbers for the switch, as well as the power status of the system.

### Main Board

Serial Number	00-10-B5-0A-CB-24
Number of Ports	8
Hardware Version	V3.0 (860 CPU)
Firmware Version	V2.5
POST ROM Version	V1.02
Internal Power Status	Active
Redundant Power Status	Inactive

Parameter	Description
Serial Number	Serial number of the main board.
Number of Ports	Number of ports on the switch.
Hardware Version	Hardware version of the main board.
Firmware Version	System firmware version in ROM.
POST ROM Version	Management's Power-On Self-Test version.
Internal Power Status	Power status for the switch.
Redundant Power Status	Redundant power status for the switch.

## IP Configuration

Use the IP Configuration screen to set the bootup option, configure the Ethernet IP address for the switch, or set the number or concurrent Telnet sessions allowed. The screen shown below is described in the following table.

IP State	User-Configured ▼
IP Address	10.1.10.98
Subnet Mask	255.255.0.0
Gateway IP Address	10.1.0.254
MAC Address	00-00-11-11-43-21
Maximum Number of Telnet Sessions (1-4)	4

Parameter	Default	Description
IP State	USER-CONFIG	Specifies whether IP functionality is enabled via manual configuration, or set by Boot Protocol (BootP). Options include:  BOOTP Get IP - IP is enabled but will not function until a BootP reply has been received. BootP requests will be periodically broadcast by the switch in an effort to learn its IP address. (BootP values include the IP address, default gateway, and subnet mask.)  USER-CONFIG - IP functionality is enabled based on the default or user specified IP Configuration. (This is the default setting.)
IP Address	192.168.10.1	IP address of the switch you are managing. The switch supports SNMP over UDP/IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the switch are assigned an IP address. Valid IP addresses consist of four decimal numbers, of 0 to 255, separated by periods. Anything outside of this format will not be accepted by the configuration program.
Subnet Mask	255.255.255.0	Subnet mask of the switch. This mask identifies the host address bits used for routing to specific subnets.
Gateway IP Address	0.0.0.0	The gateway that the switch's agent uses to pass data to the management station. Note that the gateway must be defined if the management station is located in a different IP segment.
MAC Address		Physical address of the switch.
Maximum Number of Telnet sessions	4	Sets the number of concurrent Telnet sessions allowed to access the switch.

## SNMP Configuration

Use the SNMP Configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP). The switch includes an 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 switch are controlled by community strings. To communicate with the switch, the NMS must first submit a valid community string for authentication. The options for configuring community strings and related trap functions are described in the following figures and table.

### SNMP Community

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

#### SNMP Community Capability: 5

Current:                      New:

public RO private RW	<input type="button" value=" &lt;&lt; Add"/> <input type="button" value=" Remove"/>	<table border="1" style="width: 100%;"> <tr> <td style="width: 150px;">Community String</td> <td><input type="text"/></td> </tr> <tr> <td>Access Mode</td> <td>Read-Only ▾</td> </tr> </table>	Community String	<input type="text"/>	Access Mode	Read-Only ▾
Community String	<input type="text"/>					
Access Mode	Read-Only ▾					

Parameter	Description
SNMP Community Capability	Up to 5 community strings may be used.
Add/Remove	Add/remove strings from the active list.
Community String	A community entry authorized for management access. (The maximum string length is 19 characters).
Access Mode	Management access is restricted to Read Only or Read/Write.

## Trap Managers

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

### Trap Manager Capability: 5

Current:		New:	
(none)	<< Add	Trap Manager IP address	<input type="text"/>
	Remove	Trap Manager Community String	<input type="text"/>

Enable Authentication Traps:

Parameter	Description
Trap Manager Capability	Up to 5 trap managers may be used.
Trap Manager IP Address	IP address of the trap manager.
Trap Manager Community String	A community authorized to receive trap messages.
Add/Remove	Add/remove strings from the active list.
Enable Authentication Traps	Issues a trap message to specified IP trap managers whenever authentication of an SNMP request fails. Default: enabled

## Security Configuration

Use the Security Configuration screen to restrict management access based on a specified password. The Administrator has write access for parameters governing the switch. You should therefore assign a password to the Administrator as soon as possible, and store it in a safe place. (If for some reason your password is lost, or you cannot gain access to the system's configuration program, contact Alcatel Technical Support for assistance.)

### Change Password

Old Password	<input type="text"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/>

This password is for the system Administrator, with access privilege of Read/Write for all screens. Passwords can consist of up to 11 alphanumeric characters and are not case sensitive.

(User name: admin; default password: switch)

## Firmware Upgrade Options

You can upgrade system firmware by performing a Web upload or a TFTP download. Note that you can also upgrade by a direct connection to the console port (see “Upgrading Firmware via the Serial Port” on page A-2).

### Web Upload Management

Use the Web Upload Management menu to load software updates into the switch. The upload file should be an Omnistack® 8008 binary file from Alcatel; otherwise the switch will not accept it. The success of the upload operation depends on the quality of the network connection. After uploading the new software, the switch will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table.

Upload Mode	Permanent
File Name	<input type="text"/> <input type="button" value="Browse..."/>

Parameter	Description
Upload Mode	Uploads to permanent flash ROM.
File Name	The Omnistack® 8008 binary file to download. Use the browse button to locate the file on your local network.
Start Web Upload	Starts uploading the file over the network.

## TFTP Download Management

Use the TFTP Download Management menu to load software updates into the switch. The download file should be an Omnistack® 8008 binary file from Alcatel; otherwise the switch will not accept it. The success of the download operation depends on the accessibility of the TFTP server and the quality of the network connection. After downloading the new software, the switch will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table.

Server IP Address	<input type="text" value="0.0.0.0"/>
Download Mode	Permanent
File Name	<input type="text"/>

Start TFTP Download

Parameter	Description
Server IP Address	IP address of a TFTP server.
Download Mode	Downloads to permanent flash ROM.
File Name	The Omnistack® 8008 binary file to download.
Start TFTP Download	Issues request to TFTP server to download the specified file.

## Configuration Save and Restore

Use the Configure screen to save the switch configuration settings to a file on a TFTP server. The file can be later downloaded to the switch to restore the switch's settings. The success of the operation depends on the accessibility of the TFTP server and the quality of the network connection.

### Configuration Upload Management

Use the Configuration Upload Management to save the switch configuration to a file on a TFTP sever. Parameters shown on this screen are indicated in the figure and table.

Server IP Address	<input type="text" value="0.0.0.0"/>
File Name	<input type="text"/>

Start Configuration TFTP Upload

Parameter	Description
Server IP Address	IP address of a TFTP server.
File Name	The name of the file to contain the switch configuration settings.
Start Configuration TFTP Upload	Issues a request to upload the configuration settings to the specified file on the TFTP server.

### Configuration Download Management

Use the Configuration Download Management to restore switch configuration settings from a file on a TFTP sever. Parameters shown on this screen are indicated in the following figure and table

Server IP Address	<input type="text" value="0.0.0.0"/>
File Name	<input type="text"/>

Start Configuration TFTP Download

Parameter	Description
Server IP Address	IP address of a TFTP server.
File Name	The name of the file that contains the switch configuration settings you wish to restore.
Start Configuration TFTP Download	Issues a request to the TFTP server to download the specified file.

## Address Table Configuration

The Address Table contains the unicast MAC addresses and VLAN identifier associated with each port (that is, the source port associated with the address and VLAN), sorted by MAC address or VLAN. You can also clear the entire address table, or information associated with a specific address; or set the aging time for deleting inactive entries. The information displayed in the Address Table is indicated in the following figure and table.

Aging Time (10-415):	<input type="text" value="300"/> seconds
Dynamic Address Counts:	107
Static Address Counts:	0

Address Table Sort Key:

Address Table:

000024-B32883, VLAN 1, Port 8, Dynamic
0000E2-12F9F8, VLAN 1, Port 8, Dynamic
0000E2-16C582, VLAN 1, Port 8, Dynamic
0000E2-20C3D5, VLAN 1, Port 8, Dynamic
0000E2-2174D0, VLAN 1, Port 8, Dynamic
0000E2-2EFD6, VLAN 1, Port 8, Dynamic
0000E8-000002, VLAN 1, Port 8, Dynamic
0000E8-000096, VLAN 1, Port 8, Dynamic
0000E8-000101, VLAN 1, Port 8, Dynamic
0000E8-00E803, VLAN 1, Port 8, Dynamic
0000E8-111133, VLAN 1, Port 8, Dynamic
0000E8-18096B, VLAN 1, Port 8, Dynamic

New Static Address:

<< Add	MAC	<input type="text"/>
Remove	Address	<input type="text"/>
Clear Table	VLAN (1-2048)	<input type="text"/>
	Port	<input type="text" value="1"/>

Parameter	Description
Aging Time	Time-out period in seconds for aging out dynamically learned forwarding information. Range: 10 - 415 secs; default: 300 secs.
Dynamic Address Counts	The number of dynamically learned addresses currently in the table.
Static Address Counts	The number of static addresses currently in the table.
Address Table	All entries, sorted by address or VLAN ID.
Address Table Sort Key	The system displays the MAC address of each node and port whose address table includes this MAC address, the associated VLAN(s), and the address status (i.e., dynamic or static).
New Static Address	Use these fields to add or remove a static entry to the address table. Indicate the address, port and VLAN group when adding a new entry.
Add/Remove	Adds/removes selected address.
Clear Table	Removes all addresses from the address table.

## STA (Spanning Tree Algorithm)

The Spanning Tree Algorithm can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network. For a more detailed description of how to use this algorithm, refer to “Spanning Tree Algorithm” on page 4-1.

### Spanning Tree Information

The Spanning Tree Information screen displays a summary of the STA information for the overall bridge or for a specific port. To make any changes to the parameters for the Spanning Tree, use the STA Configuration and STA Port Configuration screens.

### Spanning Tree

The parameters shown in the following figure and table describe the current bridge STA Information.

Spanning Tree State	Enabled	Designated Root	128.0000E800E800
Bridge ID	32768.000011114321	Root Port	8
Max Age	20 seconds	Root Path Cost	4
Hello Time	2 seconds	Configuration Changes	175
Forward Delay	5 seconds	Last Topology Change	0 d 14 h 49 min 23 s

Parameter	Description
Spanning Tree State	Shows if the switch is enabled to participate in an STA-compliant network.
Bridge ID	A unique identifier for this bridge, consisting of bridge priority plus MAC address (where the address is normally taken from Port 1).
Max Age	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure.
Hello Time	The time interval (in seconds) at which the root device transmits a configuration message.
Forward Delay	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding).
Root Port	The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the spanning tree network.
Designated Root	The priority and MAC address of the device in the spanning tree that this switch has accepted as the root device.
Root Path Cost	The path cost from the root port on this switch to the root device.
Configuration Changes	The number of times the spanning tree has been reconfigured.
Last Topology Change	The time since the spanning tree was last reconfigured.

## Ports

The parameters shown in the following figure and table are for port STA Information (Port 1~8).

Port	Port Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port
1	No Link	2	23	1000.0010B5BB8A83	128.1
2	No Link	0	23	1000.0010B5BB8A83	128.2
3	No Link	0	23	1000.0010B5BB8A83	128.3
4	No Link	0	23	1000.0010B5BB8A83	128.4
5	No Link	0	23	1000.0010B5BB8A83	128.5
6	No Link	1	23	1000.0010B5BB8A83	128.6
7	No Link	1	23	1000.0010B5BB8A83	128.7
8	Forwarding	2	19	32768.000000AAAA00	128.4

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

## Spanning Tree Configuration

The following figures and tables describe Bridge STA configuration.

### Switch

Usage	Enabled ▾
Priority	32768

---

Parameter	Default	Description
Usage	Enabled	Enable this parameter to participate in an STA-compliant network.
Priority	32,768	Device priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. (Remember that the lower the numeric value, the higher the priority.) However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Range: 0 - 65535

---

**When the Switch Becomes Root**

Hello Time	2	seconds
Maximum Age	20	seconds
Forward Delay	15	seconds

Parameter	Default	Description
Hello Time	2	<p>The time interval (in seconds) at which the root device transmits a configuration message.</p> <p>The minimum value is 1.</p> <p>The maximum value is the lower of 10 or <math>[(\text{Max. Message Age} / 2) - 1]</math>.</p>
Max (Message) Age	20	<p>The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.</p> <p>The minimum value is the higher of 6 or <math>[2 \times (\text{Hello Time} + 1)]</math>.</p> <p>The maximum value is the lower of 40 or <math>[2 \times (\text{Forward Delay} - 1)]</math>.</p>
Forward Delay	15	<p>The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result.</p> <p>Maximum value is 30.</p> <p>Minimum value is the higher of 4 or <math>[(\text{Max. Message Age} / 2) + 1]</math>.</p>

## STA Port Configuration

The following figure and table describe STA configuration for ports.

Fast forwarding mode:

Port	Priority	Path Cost	Fast Forward
1	128	4	<input checked="" type="checkbox"/> Enable
2	128	4	<input checked="" type="checkbox"/> Enable
3	128	4	<input checked="" type="checkbox"/> Enable
4	128	4	<input checked="" type="checkbox"/> Enable
5	128	4	<input checked="" type="checkbox"/> Enable
6	128	4	<input checked="" type="checkbox"/> Enable
7	128	4	<input checked="" type="checkbox"/> Enable
8	128	4	<input checked="" type="checkbox"/> Enable

Parameter	Default	Description
Fast forwarding mode	ENABLED	Allows you to enable or disable fast forwarding for all ports on the switch.
Priority	128	<p>Defines the priority for the use of a port in the STA algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the spanning tree. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.</p> <p>The range is 0 - 255.</p>
(Path) Cost	100/19/4	<p>This parameter is used by the STA algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.</p> <p>The default and recommended range is:</p> <p>Standard Ethernet: 100 (50~600)                      Fast Ethernet: 19 (10~60)                      Gigabit Ethernet: 4 (3~10)</p> <p>The full range is 0 - 65535.</p> <p>Note: Path cost takes precedence over port priority.</p>
FastForwarding	ENABLED	<p>This parameter is used to enable/disable the Fast Spanning Tree mode for the port. In this mode, ports skip the Blocked, Listening and Learning states and proceed straight to Forwarding.</p> <p>FastForwarding enables end-node workstations and servers to overcome time-out problems when the Spanning Tree Algorithm is implemented in a network. Therefore, FastForwarding should only be enabled for ports that are connected to an end-node device.</p>

## Configuring Bridge MIB Extensions

The Bridge MIB includes extensions for managed devices that support Traffic Classes, Multicast Filtering and Virtual LANs. To configure these extensions, use the Extended Bridge Configuration screen as shown below:

### Bridge Capability

Extended Multicast Filtering Services	No
Traffic Classes	Yes
Static Entry Individual Port	Yes
VLAN Learning	IVL
Configurable PVID Tagging	Yes
Local VLAN Capable	No

Parameter	Description
Extended Multicast Filtering Services	Indicates that the switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol). Note that this function is not implemented in the current firmware release.
Traffic Classes	Indicates that the switch provides mapping of user priorities to multiple traffic classes. (Refer to the Priority menu on page 3-23.)
Static Entry Individual Port	Indicates that the switch allows the static filtering of unicast and multicast addresses. (Refer to the Address Table Configuration on page 3-14.)
VLAN Learning	This switch uses Independent VLAN Learning (IVL), whereby each port maintains its own VLAN filtering database.
Configurable PVID Tagging	Indicates that the switch allows you to override the default PVID setting (Port VLAN ID used in frame tags) and its egress status (VLAN-Tagged or Untagged) on each port. (Refer to VLAN Port Configuration on page 3-30.)
Local VLAN Capable	This switch does not support multiple local bridges (that is, multiple Spanning Trees).

## Bridge Settings

Traffic Classes	<input checked="" type="checkbox"/> Enable
GMRP	<input type="checkbox"/> Enable
GVRP	<input type="checkbox"/> Enable

Parameter	Description
Traffic Class*	Multiple traffic classes are supported by this switch as indicated under Bridge Capabilities. However, you can disable this function by clearing this checkbox.
GMRP*	GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. Note that this function is not implemented in the current firmware release.  The Internet Group Management Protocol (IGMP) is currently used by this switch to provide automatic multicast filtering.
GVRP*	GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports across the network. This function should be enabled to permit VLAN groups which extend beyond the local switch.

\* Not implemented in the current firmware release.

## Priority

IEEE 802.1p defines up to 8 separate traffic classes. This switch supports Quality of Service (QoS) by using two priority queues, with weighted fair queuing for each port. You can use the Priority menu to configure the default priority for each port, or to display the mapping for the traffic classes as described in the following sections.

### Port Priority Configuration

The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in the low priority output queue. Default priority is only used to determine the output queue for the current port; no priority tag is actually added to the frame. You can use the Port Priority Configuration screen to adjust default priority for any port as shown below:

Port	Default Ingress User Priority	Number of Egress Traffic Classes
1	0	2
2	0	2
3	0	2
4	0	2
5	0	2
6	0	2
7	0	2
8	0	2

Parameter	Description
Port	Numeric identifier for switch port.
Default Ingress User Priority	Default priority can be set to any value from 0~7, where 0~3 specifies the low priority queue and 4~7 specifies the high priority queue.
Number of Egress Traffic Classes	Indicates that this switch supports two priority output queues.

### Port Traffic Class Information

This switch provides two priority levels with weighted fair queuing for port egress. This means that any frames with a default or user priority from 0~3 are sent to the low priority queue “0” while those from 4~7 are sent to the high priority queue “1” as shown in the following screen:

Port	Priority 0	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5	Priority 6	Priority 7	Class Range
1	0	0	0	0	1	1	1	1	0-1
2	0	0	0	0	1	1	1	1	0-1
3	0	0	0	0	1	1	1	1	0-1
4	0	0	0	0	1	1	1	1	0-1
5	0	0	0	0	1	1	1	1	0-1
6	0	0	0	0	1	1	1	1	0-1
7	0	0	0	0	1	1	1	1	0-1
8	0	0	0	0	1	1	1	1	0-1

---

Parameter	Description
Port	Numeric identifier for switch port.
User Priority	Shows that user priorities 0~3 specify the low priority queue and 4~7 specify the high priority queue.

---

## Configuring Virtual LANs

You can use the VLAN configuration menu to assign any port on the switch to any of up to 256 VLAN groups. In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle a lot of IPX and NetBEUI traffic. By using IEEE 802.1Q compliant VLANs and GARP VLAN Registration Protocol, you can organize any group of network nodes into separate broadcast domains, confining broadcast traffic to the originating group. This also provides a more secure and cleaner network environment. For more information on how to use VLANs, see “Virtual LANs” on page 4-2. The VLAN configuration screens are described in the following sections.

### VLAN Basic Information

The VLAN Basic Information screen displays basic information on the VLAN type supported by this switch.

VLAN Version Number	1
Maximum VLAN ID	2048
Maximum Number of Supported VLANs	256
Current Number of 802.1Q VLANs Configured	1

Parameter	Description
VLAN Version Number	The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
Maximum VLAN ID	Maximum VLAN ID recognized by this switch.
Maximum Number of Supported VLANs	Maximum number of VLANs that can be configured on this switch.
Current Number of 802.1Q VLANs Configured	The number of VLANs currently configured on this switch.

**Note:** All ports are assigned only to VLAN 1 by default.

### VLAN Current Table

This screen shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can assign ports to the same untagged VLAN see “VLAN Port Configuration” on page 3-30. The current configuration is shown in the following screen.

VLAN Entry Delete Count: 0

VLAN ID:  ▼

Up Time at Creation	0 d 0 h 0 min 0 s
Status	Permanent

**Egress Ports**

- Port 1
- Port 2
- Port 3
- Port 4
- Port 5
- Port 6
- Port 7
- Port 8

**Untagged Ports**

- Port 1
- Port 2
- Port 3
- Port 4
- Port 5
- Port 6
- Port 7
- Port 8

Parameter	Description
VLAN Entry Delete Count	The number of times a VLAN entry has been deleted from this table.
VLAN ID	The ID for the VLAN currently displayed.
Up Time at Creation	The value of sysUpTime (System Up Time) when this VLAN was created.
Status	Shows how this VLAN was added to the switch: Dynamic GVRP: Automatically learned via GVRP. Permanent: Added as a static entry.
Egress Ports	Shows the ports which have been added to the displayed VLAN group.
Untagged Ports	Shows the untagged VLAN port members.

## VLAN Static List

Use this screen to create or remove VLAN groups.

Current:	New:						
<div style="border: 1px solid black; padding: 5px;">           1., Enabled            3., Enabled         </div>	<div style="border: 1px solid black; padding: 5px;"> <table border="1"> <tr> <td>VLAN ID (1-2048)</td> <td><input type="text"/></td> </tr> <tr> <td>VLAN Name</td> <td><input type="text"/></td> </tr> <tr> <td>Status</td> <td><input type="checkbox"/> Enable</td> </tr> </table> </div>	VLAN ID (1-2048)	<input type="text"/>	VLAN Name	<input type="text"/>	Status	<input type="checkbox"/> Enable
VLAN ID (1-2048)	<input type="text"/>						
VLAN Name	<input type="text"/>						
Status	<input type="checkbox"/> Enable						
<input type="button" value=" &lt;&lt; Add"/>							
<input type="button" value=" Remove"/>							

Parameter	Description
Current	Lists all the current VLAN groups created for this system. Up to 256 VLAN groups can be defined. To allow this switch to participate in external VLAN groups, you must use the VLAN ID for the concerned external groups.
New	Allows you to specify the name and numeric identifier for a new VLAN group. (The VLAN name is only used for management on this system; it is not added to the VLAN tag.)
Status	Enables/disables the specified VLAN.
Add	Adds a new VLAN group to the current list.
Remove	Removes a VLAN group from the current list. If any port is assigned to this group as untagged, it will be reassigned to VLAN group 1 as untagged.

**Note:** No VLANs are statically configured by default.

## VLAN Static Table

Use this screen to modify the settings for an existing VLAN. You can add/delete port members for a VLAN, disable or enable VLAN tagging for any port, or prevent a port from being automatically added to a VLAN via the GVRP protocol. (Note that VLAN 1 is fixed as an untagged VLAN containing all ports on the switch, and cannot be modified via this screen.)

VLAN:  ▼

Name	<input type="text"/>
Status	<input checked="" type="checkbox"/> Enable

Parameter	Description
VLAN	The ID for the VLAN currently displayed. Range: 1-2048
Name	A user-specified symbolic name for this VLAN. String length: 8 alphanumeric characters
Status	Enables/disables the specified VLAN.

Use the screens shown below to assign ports to the specified VLAN group as an IEEE 802.1Q tagged port. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices. If the port is connected to VLAN-unaware devices, frames will be passed to the untagged VLAN group to which this port has been assigned under the VLAN Port Configuration screen (page 3-30).

**Egress Ports**

Members:		Non-Members:
Port 1 Port 2 Port 3 Port 4 Port 5 Port 6 Port 7 Port 8	<< Add Remove >>	(none)

**Forbidden Egress Ports**

Members:		Non-Members:
(none)	<< Add Remove >>	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6 Port 7 Port 8

**Untagged Ports**

Members:		Non-Members:
Port 1 Port 2 Port 3 Port 4 Port 5 Port 6 Port 7 Port 8	<< Add Remove >>	(none)

Parameter	Description
Egress Ports	Adds ports to the specified VLAN.
Forbidden Egress Ports	Prevents a port from being automatically added to this VLAN via GVRP.
Untagged Ports	Adds untagged ports to the specified VLAN.

## VLAN Static Membership by Port

Use the screen shown below to assign VLAN groups to the selected port. To perform detailed port configuration for a specific VLAN, use the VLAN Static Table (page 3-27).

Port Number:

Member:

<< Add

Remove >>

Non-Member:

Parameter	Description
Port Number	Port number on the switch selected from the upper display panel.
Add/Remove	Add or remove selected VLAN groups for the port indicated in the Port Number field.

## VLAN Port Configuration

Use this screen to configure port-specific settings for IEEE 802.1Q VLAN features.

Port	PVID (1-2048)	Acceptable Frame Type	Ingress Filtering	GVRP Status	GVRP Failed Registrations	GVRP PDU Origin
1	<input type="text" value="1"/>	All	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	0	00-00-00-00-00-00
2	<input type="text" value="1"/>	All	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	0	00-00-00-00-00-00
3	<input type="text" value="1"/>	All	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	0	00-00-00-00-00-00
4	<input type="text" value="1"/>	All	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	0	00-00-00-00-00-00
5	<input type="text" value="1"/>	All	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	0	00-00-00-00-00-00
6	<input type="text" value="1"/>	All	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	0	00-00-00-00-00-00
7	<input type="text" value="1"/>	All	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	0	00-00-00-00-00-00
8	<input type="text" value="1"/>	All	<input type="checkbox"/> Enable	<input type="checkbox"/> Enable	0	00-00-00-00-00-00

Parameter	Description
PVID	The VLAN ID assigned to untagged frames received on this port. Use the PVID to assign ports to the same untagged VLAN.
Acceptable Frame Type <sup>1</sup>	This switch accepts "All" frame types, including VLAN tagged or VLAN untagged frames. Note that all VLAN untagged frames received on this port are assigned to the PVID for this port.
Ingress Filtering <sup>1</sup>	If set to "True," incoming frames for VLANs which do not include this port in their member set will be discarded at the inbound port.
GVRP Status <sup>2</sup>	Enables or disables GVRP for this port. When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports.  Note that, before this port setting takes effect, GVRP must be enabled for the switch (see Configuring Bridge MIB Extensions on page 3-21).
GVRP Failed Registrations <sup>2</sup>	The total number of failed GVRP registrations, for any reason, on this port.
GVRP PDU Origin <sup>2</sup>	The Source MAC Address of the last GVRP message received on this port.

1. This control does not affect VLAN independent BPDU frames, such as GVRP or STP. However, it does affect VLAN dependent BPDU frames, such as GMRP.

2. GVRP is not available for the current firmware release.

## IGMP Multicast Filtering

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

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts who want to receive a specific multicast service. The switch looks up the IP Multicast Group used for this service and adds any port which received a similar request to that group. It then propagates the service request on to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service. (For more information, see “IP Multicast Filtering” in the Users Guide.)

### Configuring IGMP

This protocol allows a host to inform its local switch/router that it wants to receive transmissions addressed to a specific multicast address group. Use the IGMP Configuration screen to set key parameters for multicast filtering as shown below.

IGMP Status	<input type="checkbox"/> Enable
IGMP Query Count (2-10)	2
IGMP Report Delay (5-30)	10 seconds

Parameter	Description
IGMP Status	If enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.
IGMP Query Count	The maximum number of queries issued for which there has been no response before the switch takes action to solicit reports.
IGMP Report Delay	The time (in seconds) between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out that port and removes the entry from its list.

**Note:** The default values are indicated in the sample screen.

### IP Multicast Registration Table

Use the IP Multicast Registration Table to display all the multicast groups active on this switch, including multicast IP addresses and the corresponding VLAN ID.

**VLAN ID:**

**Multicast IP Address:**

**Learned by:** Dynamic

Multicast Group Port List:

- Port 1
- Port 2
- Port 3
- Port 4
- Port 5
- Port 6
- Port 7
- Port 8

Parameter	Description
VLAN ID	VLAN ID assigned to this multicast group.
Multicast IP Address	IP address for specific multicast services.
Learned by	Indicates the manner in which this address was learned: dynamic or IGMP.
Multicast Group Port List	The switch ports registered for the indicated multicast service.

## Port Menus

### Port Information

The Port Information screen displays the port status, link state, the communication speed and duplex mode, as well as the flow control in use. To change any of the port settings, use the Port Configuration menu. The parameters shown in the following figure and table are for the RJ-45 ports.

Port	Admin Status	Link Status	Speed Status	Duplex Status	Flow Control Status
1	Enabled	Up	1000M	Full	IEEE 802.3x
2	Enabled	Down	10M	Half	Disabled
3	Enabled	Down	10M	Half	Disabled
4	Enabled	Down	10M	Half	Disabled
5	Enabled	Down	10M	Half	Disabled
6	Enabled	Down	10M	Half	Disabled
7	Enabled	Down	10M	Half	Disabled
8	Enabled	Up	1000M	Full	IEEE 802.3x

Parameter	Description
Admin Status	Shows if the port is enabled or not.
Link Status	Indicates if the port has a valid connection to an external device.
Speed Status	Shows the port speed (1000M).
Duplex Status	Displays the current duplex mode.
Flow Control Status	Shows the flow control type in use. Flow control can eliminate frame loss by "blocking" traffic from end stations connected directly to the switch. Back pressure is used for half duplex and IEEE 802.3x for full duplex.

**Note:** The port information displayed is not valid if the link status is down.

## Port Configuration

Use the Port Configuration menus to configure any port on the switch.

Flow control mode:

Port	Admin Status	Duplex Status	Flow Control Status
1	<input checked="" type="checkbox"/> Enable	1000M Full-Duplex ▾	Enabled ▾
2	<input checked="" type="checkbox"/> Enable	Auto-Negotiation ▾	Enabled ▾
3	<input checked="" type="checkbox"/> Enable	Auto-Negotiation ▾	Enabled ▾
4	<input checked="" type="checkbox"/> Enable	Auto-Negotiation ▾	Enabled ▾
5	<input checked="" type="checkbox"/> Enable	Auto-Negotiation ▾	Enabled ▾
6	<input checked="" type="checkbox"/> Enable	Auto-Negotiation ▾	Enabled ▾
7	<input checked="" type="checkbox"/> Enable	Auto-Negotiation ▾	Enabled ▾
8	<input checked="" type="checkbox"/> Enable	Auto-Negotiation ▾	Enabled ▾

Parameter	Default	Description
Flow Control Mode	DISABLED	Allows you to enable or disable flow control for all ports on the switch.
Admin Status	Enable	Allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable a port for security reasons.
Duplex Status	Auto-Negotiation	Used to set the current port duplex mode or auto-negotiation. The default is auto-negotiation.
Flow Control status	Disabled	Used to enable or disable flow control. Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. Back pressure is used for half duplex and IEEE 802.3x for full duplex. Note that flow control should not be used if a port is connected to a hub.

## Port Broadcast Storm Protect Configuration

Use the Port Broadcast Storm Protect Configuration screen to configure broadcast storm control for any port on the switch

Port	Protect Status	Threshold
1	<input checked="" type="checkbox"/> Enable	500
2	<input checked="" type="checkbox"/> Enable	500
3	<input checked="" type="checkbox"/> Enable	500
4	<input checked="" type="checkbox"/> Enable	500
5	<input checked="" type="checkbox"/> Enable	500
6	<input checked="" type="checkbox"/> Enable	500
7	<input checked="" type="checkbox"/> Enable	500
8	<input checked="" type="checkbox"/> Enable	500

Parameter	Default	Description
Broadcast Storm Protect Mode	Enabled	Allows you to enable/disable broadcast storm control for all ports on the switch.
Protect Status	Enabled	Enables/disables broadcast control for the port. When enabled, the switch will employ a broadcast-control mechanism if the packet-per-second threshold is exceeded. This mechanism limits the amount of broadcasts passed by the port to half of the received packet-per-second count. The control mechanism remains in effect until the number of received broadcasts falls back below the packet-per-second threshold.
Threshold	500	The packet-per-second threshold for broadcast packets on the port.

## Port Security Configuration

Use the Port Security Configuration screen to enable and configure port security for the switch. Port Security allows you to configure each port with a list of MAC addresses of devices that are authorized to access the network through that port.

Port Number:

Status:

MAC Address List:

New Address:

Parameter	Description
Port Number	The port number on the unit.
Status	Port security can be set to three states; Static, Disable, or Learning. When set to Static, the switch will drop packets from the port if the source MAC address does not match one of the addresses in the MAC Address list. If set to Learning, the switch will add the source MAC address of all packets received on the port to the authorized MAC Address list.
MAC Address List	A list of the authorized MAC addresses that can access the network through the specified port.
New Address	A specific MAC address to be added to the list.
Add	Adds a new specified MAC address to the current list.
Remove	Removes a MAC address from the current list.
Clear All	Clears all the MAC addresses for the current port.

## Using a Port Mirror for Analysis

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a network sniffer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, note that the target port must be configured in the same VLAN and be operating at the same duplex mode as the source port (see VLAN Static List on page 3-27).

You can use the port mirror configuration screen to designate a single port pair for mirroring as shown below:

Status	<input type="checkbox"/> Enable
Mirror Source Port	1 ▾
Mirror Target Port	2 ▾

Parameter	Description
Status	Enables/disables port mirroring.
Mirror Source Port	The port whose traffic will be monitored.
Mirror Target Port	The port that will duplicate or "mirror" all the traffic happening on the monitored port.

## Port Trunk Configuration

Port trunks can be used to increase the bandwidth of a network connection or to ensure fault recovery. You can configure up four trunk connections (combining 2~4 ports into a fat pipe) between any two Omnistack® 8008 switches. However, before making any physical connections between devices, use the Trunk Configuration menu to specify the trunk on the devices at both ends. When using a port trunk, note that:

- Ports can only be assigned to one trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- The ports at both ends of a trunk must be configured in an identical manner, including duplex mode and VLAN assignments.
- None of the ports in a trunk can be configured as a mirror source port or mirror target port.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Algorithm will treat all the ports in a trunk as a whole.
- Enable the trunk prior to connecting any cable between the switches to avoid creating a loop.
- Disconnect all trunk port cables or disable the trunk ports before removing a port trunk to avoid creating a loop.

## Web Interface

Use the Port Trunking Configuration screen to set up port trunks as shown below. Remember that you must “Enable” a new configuration before it will take effect.

### Status List:

Trunk	Status
1	<input checked="" type="checkbox"/> Enable

### Member List:

Current:

Trunk 1, Port 2
Trunk 1, Port 3

New:

Parameter	Description
Trunk Number	A unique identifier for this trunk. You can configure up to four trunks per switch.
Port	The port members of this trunk. Select from 2~4 ports per trunk.

## Port Statistics

Use the Port Statistics menu to display Etherlike or RMON statistics for any port on the switch. Select the required port. The statistics displayed are indicated in the following figure and table.

### Etherlike Statistics

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

Port Number:

Alignment Errors	<input type="text" value="0"/>	Late Collisions	<input type="text" value="0"/>
FCS Errors	<input type="text" value="514069"/>	Excessive Collisions	<input type="text" value="119434"/>
Single Collision Frames	<input type="text" value="0"/>	Internal MAC Transmit Errors	<input type="text" value="0"/>
Multiple Collision Frames	<input type="text" value="4043438"/>	Carrier Sense Errors	<input type="text" value="0"/>
SQE Test Errors	<input type="text" value="0"/>	Frames Too Long	<input type="text" value="0"/>
Deferred Transmissions	<input type="text" value="16979915"/>	Internal MAC Receive Errors	<input type="text" value="21"/>

Parameter	Description
Alignment Errors	The number of frames received that are not an integral number of octets in length and do not pass the FCS check.
FCS Errors	The number of frames received that are an integral number of octets in length but do not pass the FCS check.
Single Collision Frames*	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames*	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
SQE Test Errors*	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer.
Deferred Transmissions*	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
Excessive Collisions*	The number of frames for which transmission failed due to excessive collisions.
Internal Mac Transmit Errors*	The number of frames for which transmission failed due to an internal MAC sublayer transmit error.
Carrier Sense Errors*	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
Frames Too Long	The number of frames received that exceed the maximum permitted frame size.
Internal Mac Receive Errors	The number of frames for which reception failed due to an internal MAC sublayer receive error.

\* The reported values will always be zero because these statistics are not supported by the internal chip set.

### RMON Statistics

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

Port Number:

Drop Events	0	Jabbers	0
Received Bytes	0	Collisions	0
Received Frames	0	64 Bytes Frames	0
Broadcast Frames	0	65-127 Bytes Frames	0
Multicast Frames	0	128-255 Bytes Frames	0
CRC/Alignment Errors	0	256-511 Bytes Frames	0
Undersize Frames	0	512-1023 Bytes Frames	0
Oversize Frames	0	1024-1518 Bytes Frames	1
Fragments	0		

Parameter	Description
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	The number of frames received with CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.

---

<b>Parameter</b>	<b>Description</b>
64 Byte Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames	The total number of frames (including bad packets) received and transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
512-1023 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518 Byte Frames	The total number of packets (including bad packets) received and transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

---



## Chapter 4: Advanced Topics

The Alcatel OmniStack® 8008 supports Layer 2 switching and other advanced features, which are described in this chapter.

### Layer 2 Switching

When a frame enters a port, its destination MAC address is checked in the address database to see which port leads to this destination. If the destination address belongs to the incoming port, the frame is dropped or “filtered” because it is addressed to the local segment. If the destination address is found on another port, the frame is forwarded to that port and queued for output. But, if the destination address is **not** found in the address database, the frame is sent to one or more output ports based on the rules for handling tagged or untagged VLAN frames.

If the source MAC address of the frame was not found in the address database, it is recorded along with the incoming port number where it entered the switch. This information is then used to make later decisions for frame forwarding.

Switching involves the following steps:

- VLAN Classification
- Learning
- Filtering
- Forwarding
- Aging

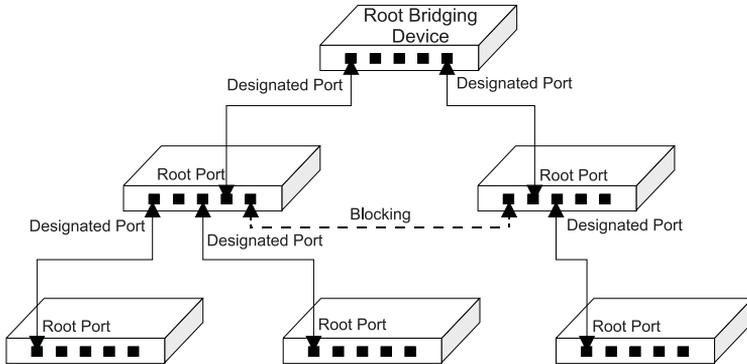
### Spanning Tree Algorithm

The Spanning Tree Algorithm (that is, the STA configuration algorithm as outlined in IEEE 802.1D) can be used to detect and disable network loops, and to provide link backup. This allows the switch to interact with other bridging devices (including STA-compliant switches, bridges or routers) in your network to ensure that only one route exists between any two stations on the network. If redundant paths or loops are detected, one or more ports are put into a blocking state (stopped from forwarding packets) to eliminate the extra paths. Moreover, if one or more of the paths in a stable spanning tree topology fail, this algorithm will automatically change ports from blocking state to forwarding state to reestablish contact with all network stations.

The STA uses a distributed algorithm to select a bridging device (STA-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

The following figure gives an illustration of how the Spanning Tree Algorithm assigns bridging device ports.



## Virtual LANs

Switches do not inherently support broadcast domains, which can lead to broadcast storms in large networks that handle a lot of IPX or NetBEUI traffic. In conventional networks with routers, broadcast traffic is split up into physically separate domains to confine broadcast traffic to the originating group and provide a much cleaner network environment. This switch creates segregated broadcast domains based on easily configurable VLANs, these VLANs are then linked, as required, using a router or Layer 3 switch.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as video conferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, but also allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security, since traffic must pass through a Layer 3 switch or a router to reach a different VLAN.

This switch supports the following VLAN features:

- Up to 256 VLANs can be configured based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging
- Port trunking with VLANs

### **Assigning Ports to VLANs**

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) it will participate in. (By default all ports are assigned to VLAN 1 as untagged ports.) Add a port as a tagged port (that is, a port attached to a VLAN-aware device) if you want it to carry traffic for one or more VLANs and the device at the other end of the link also supports VLANs. Then assign the port at the other end of the link to the same VLAN(s). However, if you want a port on this switch to participate in one or more VLANs, but the device at the other end of the link does not support VLANs, then you must add this port as an untagged port (that is, a port attached to a VLAN-unaware device).

Port-based VLANs are tied to specific ports. The switch's forwarding decision is based on the destination MAC address and its associated port. Therefore, to make valid forwarding and flooding decisions, the switch learns the relationship of the MAC address to its related port—and thus to the VLAN—at run-time. When the switch receives a frame, it assigns the frame to the port's default VLAN if the frame is untagged (determined by the PVID of the receiving port), or maps it for output to the broadcast domain associated with the frame's VLAN tag.

### **Port Overlapping**

Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them using a router or Layer 3 switch.

### **Automatic VLAN Registration (GVRP)**

GVRP defines a system whereby the switch can automatically learn the VLANs each endstation should be assigned to. If an endstation (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network.

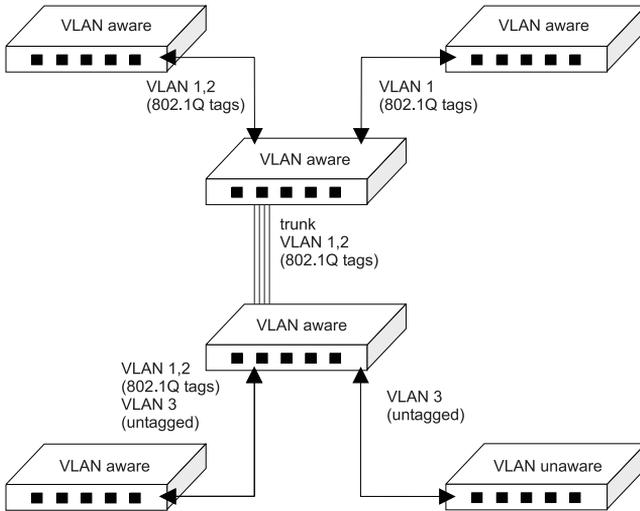
This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on endstation requests.

### Forwarding Traffic with Unknown VLAN Tags

This switch only supports 256 VLANs with VLAN IDs ranging from 1 to 2048, but the IEEE 802.1Q VLAN standard allows for VLAN IDs from 1 to 4094. Therefore, if this switch is attached to endstations that issue VLAN registration requests, it will have to forward unknown VLAN tags. This traffic can only be propagated to the rest of the network if automatic VLAN registration is enabled on your switch.

### Forwarding Tagged/Untagged Frames

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. To forward a frame from a VLAN-aware device to a VLAN-unaware device, the switch first decides where to forward the frame, and then strips off the VLAN tag. However, to forward a frame from a VLAN-unaware device to a VLAN-aware device, the switch first decides where to forward the frame, and then inserts a VLAN tag reflecting this port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed (see page 2-48 or page 3-30).



### Connecting VLAN Groups

The switch supports intra-VLAN communication using wire-speed switching. However, if you have devices in separate VLANs that must communicate, and it is not practical to include these devices in a common VLAN, then the VLANs can be connected via a Layer 3 switch or router.

## Multicast Filtering

Multicasting sends data to a group of nodes instead of a single destination. The simplest way to implement multicasting is to broadcast data to all nodes on the network. However, such an approach wastes a lot of bandwidth if the target group is small compared to overall the broadcast domain.

Since applications such as video conferencing and data sharing are more widely used today, efficient multicasting has become vital. A common approach is to use a group registration protocol that lets nodes join or leave multicast groups. A switch or router can then easily determine which ports contain group members and send data out to those ports only. This procedure is called multicast filtering.

The purpose of multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches instead of flooding to all ports in the subnet (VLAN). The OmniStack® 8008 supports multicast filtering by passively monitoring IGMP Query and Report messages.

### IGMP Snooping

A Layer 2 switch can passively snoop on IGMP Query and Report packets transferred between IP Multicast Routers/Switches and IP Multicast host groups to learn the IP Multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures multicast filters accordingly. IGMP Snooping generates no additional network traffic, allowing you to significantly reduce the multicast traffic passing through your switch.

### IGMP Protocol

The Internet Group Management Protocol (IGMP) runs between hosts and their immediately neighboring multicast router/switch. IGMP is a multicast host registration protocol that allows any host to inform its local router that it wants to receive transmissions addressed to a specific multicast group.

A router, or multicast-enabled switch, can periodically ask its hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the responsibility of querying the LAN for group members.

Based on the group membership information learned from IGMP, a router/switch can determine which (if any) multicast traffic needs to be forwarded to each of its ports. At Layer 3, multicast routers use this information, along with a multicast routing protocol such as DVMRP, to support IP multicasting across the Internet.

Note that IGMP neither alters nor routes any IP multicast packets. A multicast router/switch must be used to deliver IP multicast packets across different subnetworks.

## **Class-of-Service (CoS) Support**

The OmniStack® 8008 provides two transmit queues on each port, with a Weighted Fair Queuing scheme. This function can be used to provide independent priorities for various types of data such as real-time video or voice, and best-effort data.

Priority assignment to a packet in the OmniStack® 8008 can be accomplished in any of the following ways:

- Priority can be explicitly assigned by end stations which have applications that require a higher priority than best-effort. This switch utilizes the IEEE 802.1p and 802.1Q tag structure to decide priority assignments for the received packets.
- A port may be manually configured as high priority. In this case, when any other port receives traffic from a high-priority port, that traffic is automatically placed in the high-priority output queue.

## **Port Trunks**

Ports can be combined into an aggregate link to increase the bandwidth of a network connection or ensure fault recovery. You can group ports into trunks that consist of two, three or four ports, creating an aggregate bandwidth of up to 8 Gbps. Besides balancing the load across each port in the trunk, the additional ports provide redundancy by taking over the load if another port in the trunk should fail.

When using port trunks, remember that:

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

## **SNMP Management Software**

SNMP (Simple Network Management Protocol) is a communication protocol designed specifically for managing devices or other elements on a network. Network equipment commonly managed with SNMP includes hubs, switches, bridges, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as monitor them to evaluate performance and detect potential problems.

## Remote Monitoring

Remote Monitoring (RMON) provides a cost-effective way to monitor large networks by placing embedded or external probes on distributed network equipment (hubs, switches or routers). Network management software can access the probes embedded in recent Alcatel network products to perform traffic analysis, troubleshoot network problems, evaluate historical trends, or implement proactive management policies. RMON has already become a valuable tool for network managers faced with a quickly changing network landscape that contains dozens or hundreds of separate segments. RMON is the only way to retain control of the network and analyze applications running at multi-megabit speeds. It provides the tools you need to implement either reactive or proactive policies that can keep your network running based on real-time access to key statistical information.

This switch provides support for basic RMON which contains the four key groups required for basic remote monitoring. These groups include:

**Statistics:** Includes all the tools needed to monitor your network for common errors and overall traffic rates. Information is provided on bandwidth utilization, peak utilization, packet types, errors and collisions, as well as the distribution of packet sizes.

**History:** Can be used to create a record of network utilization, packet types, errors and collisions. You need a historical record of activity to be able to track down intermittent problems. Historical data can also be used to establish normal baseline activity, which may reveal problems associated with high traffic levels, broadcast storms, or other unusual events. Historical information can also be used to predict network growth and plan for expansion before your network becomes too overloaded.

**Alarms:** Can be set to test data over any specified time interval, and can monitor absolute or changing values (such as a statistical counter reaching a specific value, or a statistic changing by a certain amount over the set interval). Alarms can be set to respond to either rising or falling thresholds.

**Events:** Defines the action to take when an alarm is triggered. The response to an alarm can include recording the alarm in the Log Table or sending a message to a trap manager. Note that the Alarm and Event Groups are used together to record important events or immediately respond to critical network problems.



# Appendix A: Troubleshooting

## Troubleshooting Chart

Troubleshooting Chart	
Symptom	Action
Cannot connect using Telnet, Web browser, or SNMP software	<ul style="list-style-type: none"><li>• Be sure you have configured the agent with a valid IP address, subnet mask and default gateway.</li><li>• Check that you have a valid network connection to the switch and that the port you are using has not been disabled.</li><li>• Check network cabling between the management station and the switch.</li><li>• If you cannot connect using Telnet, there may already be another active session. Try connecting again at a later time.</li></ul>
Cannot access the on-board configuration program via a serial port connection	<ul style="list-style-type: none"><li>• Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and 9600 bps.</li><li>• Check that the null-modem serial cable conforms to the pin-out connections provided in Appendix B.</li></ul>
Forgot or lost the password	<ul style="list-style-type: none"><li>• Contact Alcatel's technical support for help.</li></ul>

## Upgrading Firmware via the Serial Port

You can upgrade system firmware by connecting your computer to the serial port on the switch, and using a console interface package that supports the XModem protocol. (See “Required Connections” on page 1-1.)

1. Restart the system by using the Restart System command; or by pulling out the power cord to reset the power, waiting five seconds, and plugging it back in.
2. When the system initialization screen appears as shown below, press “D” to download system firmware, and then indicate the code type (<1> Runtime image or <2> POST image).

```
Alcatel OmniStack 8008
Alcatel OmniStack - Copyright (c), 2000 Alcatel and its licensors.
All rights reserved. OmniStack is a trademark of Alcatel registered
in the United States Patent and Trademark Office.
LOADER Version V1.02
POST Version V1.04

----- Performing the Power-On Self Test (POST) -----
EPROM Checksum Test ..... PASS
Testing the System SDRAM ..... PASS
CPU Self Test ..... PASS
EEPROM Checksum Test ..... PASS
MAC Address ..... 00-00-11-11-43-21
----- Power-On Self Test Completed -----

(D)ownload System Image or (S)tart Application: [S]

Select the Firmware Type to Download (1)Runtime (2)POST [1]: 1
Your Selection: Runtime Code
Change Baud Rate to 115200 and Press <ENTER> to Download.
```

3. Change your baud rate to 115200 bps, and press Enter to enable download. From the terminal emulation program, select the file you want to download, set the protocol to XModem, and then initialize downloading.

- Notes:**
1. If you use Windows HyperTerminal, disconnect , set the baud rate, and reconnect .
  2. The download file must be the correct binary file for the switch; otherwise the agent will not accept it.

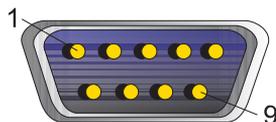
4. After the file has been downloaded, the console screen will display information similar to that shown below. Press Enter to download to permanent memory, change the baudrate back to 9600, press Enter to start decompressing the new firmware, and then press Enter to open the Logon screen.

```
XModem Download to DRAM buffer area 0x00200000: ..... SUCCESS !
Verifying image in DRAM download buffer 0x00200000... SUCCESS !
Update FlashROM Image at 0x02880000 ... SUCCESS !
(D)ownload another Image or (S)tart Application: [S]
Change Baud Rate to 9600 and Press <ENTER>.
```

For details on managing the switch, refer to Chapter 2 for information on the out-of-band console interface, or Chapter 3 for information on the Web interface.



# Appendix B: Pin Assignments



## Console Port Pin Assignments

The DB-9 serial port on the switch's rear panel is used to connect to the switch for out-of-band console configuration. The on-board menu-driven configuration program can be accessed from a terminal or from a PC running a terminal emulation program. The pin assignments used to connect to the serial port are provided in the following tables.

### DB-9 Port Pin Assignments

EIA Circuit	CCITT Signal	Description	Switch's DB9 DTE Pin #	PC DB9 DTE Pin #	Signal Direction DTE-DCE
CF	109	<b>DCD</b> (Data Carrier Detected)	1	1	<-----
BB	104	<b>RxD</b> (Received Data)	2	2	<-----
BA	103	<b>TxD</b> (Transmitted Data)	3	3	----->
CD	108.2	<b>DTR</b> (Data Terminal Ready)	4	4	----->
AB	102	<b>SG</b> (Signal Ground)	5	5	-----
CC	107	<b>DSR</b> (Data Set Ready)	6	6	<-----
CA	105	<b>RTS</b> (Request-to-Send)	7	7	----->
CB	106	<b>CTS</b> (Clear-to-Send)	8	8	<-----
CE	125	<b>RI</b> (Ring Indicator)	9	9	<-----

### Console Port to 9-Pin COM Port on PC

Switch's 9-Pin Serial Port	CCITT Signal	PC's 9-Pin COM Port
1 DCD	-----DCD -----	1
2 RXD	<-----TXD -----	3
3 TXD	-----RXD ----->	2
4 DTR	-----DSR ----->	6
5 SGND	-----SGND -----	5
6 DSR	-----DTR -----	4
7 RTS	-----CTS ----->	8
8 CTS	<-----RTS -----	7
9 RI	-----RI -----	9

**Console Port to 25-Pin DTE Port on PC**

Switch's 9-Pin Serial Port	Null Modem	PC's 25-Pin DTE Port
1 DCD	1 _____ 1	8 DCD
2 RXD	2 _____ 3	3 TXD
3 TXD	3 _____ 2	2 RXD
4 DTR	4 _____ 8	20 DTR
5 SGND	5  20	7 SGND
6 DSR	6 _____ 7	6 DSR
7 RTS	7 _____ 4	4 RTS
8 CTS	9 _____ 5	5 CTS
9 RI	20 _____ 6	22 RI

# Glossary

## **Bandwidth Utilization**

The percentage of packets received over time as compared to overall bandwidth.

## **BOOTP**

Boot protocol used to load the operating system for devices connected to the network.

## **GARP VLAN Registration Protocol (GVRP)**

Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

## **Generic Attribute Registration Protocol (GARP)**

GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment such that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. (Formerly called Group Address Registration Protocol.)

## **Group Address Registration Protocol**

*See Generic Attribute Registration Protocol.*

## **Internet Control Message Protocol (ICMP)**

An integral part of the Internet Protocol (IP) that handles error and control messages. ICMP also includes an echo request /reply used to test whether a destination is reachable and responding.

## **IEEE 802.1D**

Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

## **IEEE 802.1Q**

VLAN Tagging defines Ethernet frame tags which carry VLAN information. It allows switches to assign end-stations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

## **IEEE 802.3ac**

Defines frame extensions for VLAN tagging.

## **In-Band Management**

Management of the network from a station that is attached to the network.

## **Link Aggregation**

*See Port Trunk.*

## **MIB**

An acronym for Management Information Base. It is a set of database objects that contains information about the device. It defines variables needed by the SNMP protocol to monitor and control components in a network.

## **Out-of-Band Management**

Management of the network from a station that is not attached to the network.

## **Port Mirroring**

A method whereby data on a target port is mirrored to an analysis port for troubleshooting with a network sniffer or RMON probe. This allows data on the target port to be studied unobtrusively.

## **Port Trunk**

Defines network link aggregation and trunking standards which specify how to create a single high-speed logical link that combines several lower-speed physical links.

## **Remote Monitoring (RMON)**

RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific errors types.

## **Simple Network Management Protocol (SNMP)**

An application protocol offering network management services in the Internet suite of protocols.

## **Serial Line Internet Protocol (SLIP)**

A standard protocol for point-to-point connections using serial lines.

## **Spanning Tree Algorithm (STA)**

A technology that checks your network for any loops. A loop can often occur in complicated network systems or systems with redundant links. Spanning-tree detects and directs data along the shortest path, maximizing the performance and efficiency of the network.

## **Spanning Tree Protocol (STP)**

See Spanning Tree Algorithm.

**Telnet**

Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

**Trivial File Transfer Protocol (TFTP)**

The TCP/IP standard protocol for file transfer with minimal capability and minimal overhead. TFTP depends on the connectionless datagram delivery service, UDP.

**Virtual LAN (VLAN)**

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, allowing users to share information and resources as though located on the same LAN.

**XModem**

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.



# Index

## Numerics

- 802.1p port priority 4-6
- 802.1Q VLANs 4-2

## A

- address table, static unicast 3-15
- Administrator password, setting 3-11
- aging time of address table 3-15
- automatic VLAN registration 4-3

## B

- banner message configuration 2-21
- baud rate, configuring 3-5
- BOOTP, for IP configuration 1-2, 3-9
- bridge
  - capability 3-21
  - MIB extensions 2-40, 3-21
- Bridge Protocol Data Units (BPDUs) 4-2
- Broadcast Storm Control 2-38, 2-39

## C

- Class of Service (CoS) 4-6
- community strings, configuring 3-10
- connections
  - serial port 1-1
  - Web browser 1-2
- console login configuration 2-17
- console port
  - configuring 3-5
  - connections 1-1
  - pin assignments B-1

## D

- downloading software A-2

## F

- firmware
  - upgrades A-2
- firmware upgrade
  - TFTP download 3-13
  - Web upload 3-12
- firmware version 3-8

## G

- GVRP 4-3

## H

- hardware version 3-8
- HTTP
  - configuration 2-12
  - server 2-12

## I

- IGMP 3-31
  - multicast filtering 2-36
  - protocol 4-5
  - query 4-5
  - report 4-5
  - snooping 4-5
- in-band connections 1-2
- Internet Group Management Protocol,  
*see IGMP*
- IP
  - configuration 2-10, 3-9
  - multicast filtering 2-36

## L

- Layer 2 switching 4-1
- link aggregation 4-6
- log-in
  - console interface 2-1
  - Web interface 3-2

## M

- MAC address of agent 3-9
- main board information 3-8
- main menu 2-2, 3-6
  - description 3-6
- management
  - configuration 2-20
  - firmware upgrades 3-12
  - options 1-1
  - software, SNMP 4-6
  - using SNMP 3-10
- MIB extensions, configuring 3-21
- mirror port configuration 3-37
- multicast filtering 4-5
  - configuring 3-31

## N

- network management station
  - access 3-10

## O

out-of-band connection 1-1

## P

password configuration 3-11

pin assignments, console port B-1

Ping 2-11

port

configuration 3-34, 3-35

information 3-33

mirror 3-37

overlapping 4-3

priority 2-41

statistics 3-39

trunk configuration 2-34

trunks 3-37, 4-6

priority

port configuration 3-23

traffic class 3-24

problems, troubleshooting A-1

PVID 4-3

## Q

QoS configuration 2-41

Quality of Service (QoS) 3-23

## R

remote monitoring (RMON) 4-7

restoring switch configuration 3-14

RMON probes and mirror ports 3-37

## S

screen refresh 3-5

security configuration 3-11

serial number of main board 3-8

serial port

configuring 3-5

connections 1-1

XModem downloads A-2

Simple Network Management Protocol

see *SNMP*

SNMP

community 2-15, 3-10

configuration 3-10

management 1-2

software downloads A-2

software upgrades 3-12

Spanning Tree Algorithm, see *STA*

STA 2-26, 3-16, 4-1

statistics

Etherlike 3-39

RMON 3-40

switch information 2-7, 3-8

switching, Layer 2 4-1

system information 2-6, 3-7

## T

tagged

ports 4-3

VLANs 3-26, 3-28, 4-4

Telnet sessions, maximum number

of 3-9

TFTP

configuration for downloads 2-18

protocol 2-18

timeout, console 3-5

traffic classes configuration 2-41

traffic classes, configuring 4-6

trap managers, configuring 3-11

Traps, enabling 3-11

troubleshooting A-1

trunks, configuring 2-34, 3-37

## U

untagged

ports 4-3

VLANs 4-4

upgrading firmware 3-12

upgrading software A-2

user password 2-1

## V

Virtual LAN

see *VLAN*

VLAN

assigning ports 4-3

automatic registration 4-3

configuration 2-44, 3-25

connecting 4-4

port overlapping 4-3

static list 3-27

static membership by port 3-29

static table 3-27

static table configuration 2-46

tagged 3-26, 4-4

unknown tags 4-4

untagged 4-4

**W**

## Web

- access requirements 3-1
- browser connection 1-2

## Web interface

- configuration buttons 3-3
- home page 3-2
- panel display 3-4
- passwords 3-2

## Web server 2-12

## Weighted Fair Queuing 2-41

**X**

## XModem downloads A-2

[www.alcatel.com/enterprise](http://www.alcatel.com/enterprise)

**Alcatel**

26801 West Agoura Road  
Calabasas, CA 91301 USA

**Contact Center**

(800) 995-2612 US/Canada  
(818) 880-3500 Outside US

[www.alcatel.com/enterprise](http://www.alcatel.com/enterprise)

Product specifications contained in this document are subject to change without notice. Contact your local Alcatel representative for the most current information. Copyright © 2003 Alcatel Internetworking, Inc. All rights reserved. This document may not be reproduced in whole or in part without the expressed written permission of Alcatel Internetworking, Inc. Alcatel® and the Alcatel logo are registered trademarks of Alcatel. All other trademarks are the property of their respective owners.

P/N 060117-10, Rev. B 01/02

ARCHITECTS OF AN INTERNET WORLD

