Accton

Making Partnership Work

CheetahSwitch Workgroup-4508 Management Guide

Accton

Making Partnership Work

Management Guide

CheetaSwitch Workgroup-4508

Intelligent Gigabit Ethernet Switch
with 8 1000BASE-SX (SC) Ports

Accton

International Headquarters
No. 1 Creation Road III,
Science-based Industrial Park
Hsinchu 300, Taiwan, R.O.C.
Phone: 886-3-5770-270
FAX: 886-3-5770-267
Internet: support@accton.com.tw

USA Headquarters
6 Hughes
Irvine, CA 92618
Phone Numbers -
Sales: 800-926-9288
Support: 888-398-4101 or 949-707-4847
RMA: 800-762-4968
FAX: 949-707-2460

ES4508
E022000-R01
150065-102

Contents

Chapter 1: Managing the Switch

Configuration Options

The CheetahSwitch Workgroup-4508 provides a menu-driven system configuration program that can be accessed through a direct console connection or modem connection to the serial port on the switch's rear panel (out-of-band), or by a Telnet connection over the network (in-band).

The switch 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 switch's management agent is based on SNMP (Simple Network Management Protocol). This SNMP agent allows the switch to be managed from any PC on the network using in-band management software, such as Accton's AccView/Open.

Once you have connected a terminal or PC to the serial port on the switch, you can perform the following tasks:

- Enable/disable any port
- Set the communication mode for any port
- Configure SNMP parameters
- Configure the switch to join a Spanning Tree
- Add ports to VLAN groups
- Mirror data from a target port to an analysis port
- Display system information or statistics
- Download system firmware
- Restart the system

Making Connections for System Configuration

The switch includes a menu-driven configuration program. The ASCII interface to this program can be accessed by making a direct connection to the serial port on the rear panel, or by a Telnet connection to the switch over the network.

This section describes how to access the menu-driven configuration program via:

- **Onsite connection**
  A terminal or workstation connected to the serial port on the rear panel
- **Modem connection**
  A workstation connected to the serial port of a remote switch via modems
- **Telnet connection**
  A workstation connected to a remote switch via a Telnet connection

It also describes how to access the embedded Web agent over the network using any standard browser, or with AccView network management software or other third-party management software.

Onsite Connection

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 the back of this guide.

When attaching to a PC, set terminal emulation type to VT100, specify the port used by your PC (i.e., COM 1~4), and then set communications to 8 data bits, 1 stop bit, no parity, and 19200 bps (for initial configuration). Also be sure to set both handshaking and flow control to "none."

Modem Connection

Configure the Switch Site: Connect the switch's DB-9 serial port to the modem's serial port using standard cabling. For most modems, which use a 25-pin port, you will have to provide an RS-232 cable with a 9-pin connector on one end and a 25-pin connector on the other end. You do not have to set the modem at the switch's site, because the switch will automatically configure it to auto-answer mode.

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

Telnet Connection

Prior to accessing the switch via an in-band Telnet connection, you must first configure it with a valid IP address, subnet mask, and default gateway using an out-of-band connection or BOOTP protocol. After configuring the switch's IP parameters, you can access the on-board configuration program from anywhere within the attached network.

Note: Up to four Telnet sessions are supported.

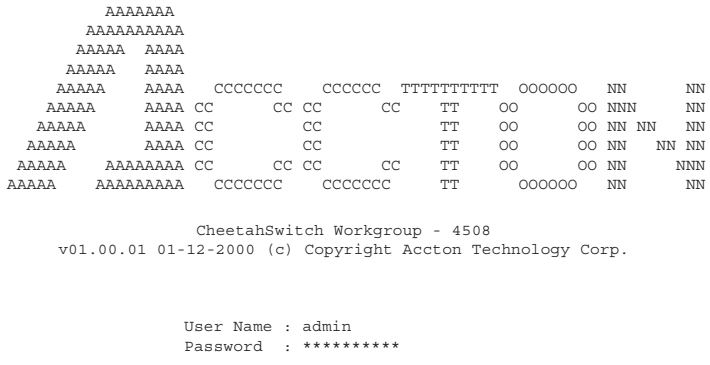
In-Band Network Connection

The on-board configuration program can be accessed using Telnet or a Web browser (Internet Explorer 4.0 or above, or Netscape Navigator 4.0 or above) from any computer attached to the network. It can also be managed from a network computer using management software such as AccView.

Notes:
1. Prior to accessing the switch via a direct network connection, first configure it with a valid IP address, subnet mask, and default gateway using an out-of-band connection or BOOTP protocol.
2. The on-board 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. Accton provides a Windows-based SNMP software package called AccView/Open. If you require this software, please contact your Accton distributor. Also note that AccView's CheetahSwitch Manager module can be easily integrated into most third-party management platforms.

Chapter 2: Using the System Configuration Program

Once a direct connection to the serial port or a Telnet connection is established, the login screen for the on-board configuration program appears as shown below.



If this is your first time to log into the configuration program, then the default user names are “admin” and “guest,” and the passwords are null. The administrator has Read/Write access to all configuration parameters and statistics, while the guest has Read Only access. To open the Main Menu, type “admin” for the user name and press <Enter> for the password.

You should define a password, record it, and put it in a safe place. If you have not already done so, select Security Configuration and enter a password. Note that passwords can consist of up to 15 alphanumeric characters and are not case sensitive.

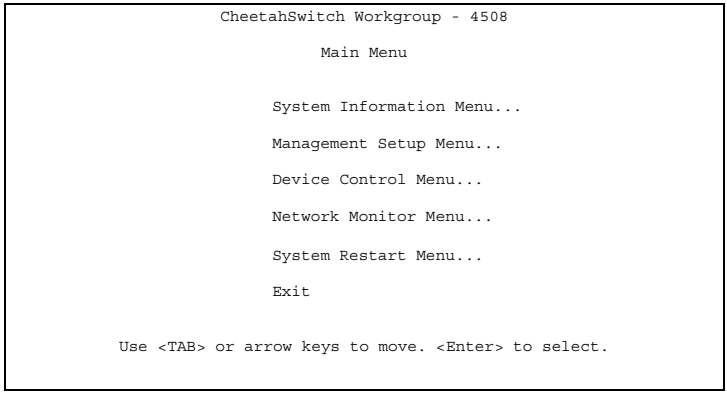
Configuration parameters are described in the following section.

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.

Main Menu

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

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



Parameter	Description
System Information Menu	
System Information	Provides basic system description, including contact information.
Switch Information	Shows hardware/firmware version numbers, and power status.
Management Setup Menu	
Network Configuration	Includes IP setup, Ping facility, Access Host configuration, HTTP (Web agent) 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	Enables/disables SNMP access, 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	Downloads new version of firmware to update your system (in-band).
Device Control Menu	
Port Configuration	Enables any port, enables/disables flow control, and sets communication mode to auto-negotiation or full duplex.

Parameter	Description
Port Information	Displays operational status, including link state, flow control method, speed 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, path cost and Fast STA mode.
Spanning Tree Information	Displays full listing of parameters for the Spanning Tree Algorithm.
Mirror Port Configuration	Sets the source and target ports for mirroring.
IGMP Configuration	Configures IGMP multicast filtering.
Broadcast Storm Control	Sets the broadcast-rate threshold at which broadcast packets are discarded.
Extended Bridge Configuration	Displays/configures extended bridge capabilities provided by this switch.
802.1P Configuration	Configures default port priorities and queue assignments.
802.1Q VLAN Base Information	Displays basic VLAN information, such as VLAN version number, maximum VLAN ID, maximum VLANs supported, and the current number of VLANs configured.
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.
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.
System Restart	Restarts system with options to use POST, or to retain factory defaults, IP settings, or user authentication settings.
Exit	Exits the configuration program.

System Information Menu

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

```
                    CheetahSwitch Workgroup - 4508

                        System Information Menu

                        System Information ...

                        Switch Information ...


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

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.

```
                    CheetahSwitch Workgroup - 4508

                          System Information


  System Description : Gigabit Ethernet Switch ES4508

  System Object ID   : 1.3.6.1.4.1.259.6.17

  System Up Time     : 48067 (0 day, 1 hr, 2min, 34 sec)

  System Name        :

  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.)
System Name[1]	Name assigned to the switch system.
System Contact[1]	Contact person for the system.
System Location[1]	Specifies the area or location where the system resides.

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

Displaying Version Information

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

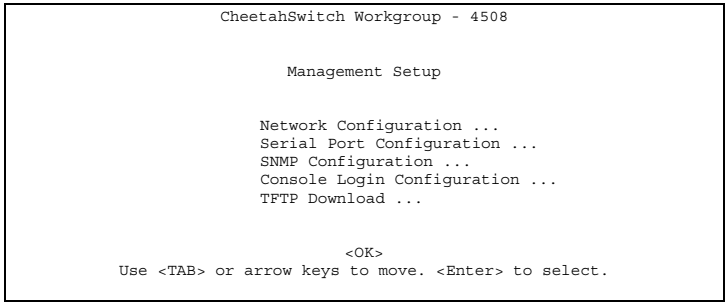
```
                CheetahSwitch Workgroup - 4508


                      Switch Information

              Hardware Version       : V1.0
              POST ROM Version       : V01.00.00
              Firmware Version       : V01.00.01
              Serial Number          :
              Port Number            : 8
              Internal Power Status  :
              Redundant Power Status :



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

Parameter	Description
Hardware Version	Hardware version of the main board.
POST ROM Version	Power-On Self-Test version number.
Firmware Version	System firmware version in ROM.
Serial Number[1]	Serial number of the main board.
Port Number	Number of ports.
Internal Power Status[1]	Indicates if the primary power is active or inactive.
Redundant Power Status[1]	Indicates if the redundant power is active or inactive.

1: These parameters are not supported by the current hardware version.

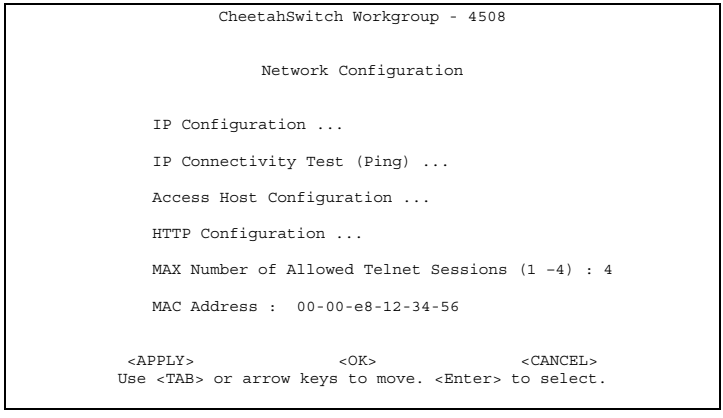
Management Setup Menu

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



Changing the Network Configuration

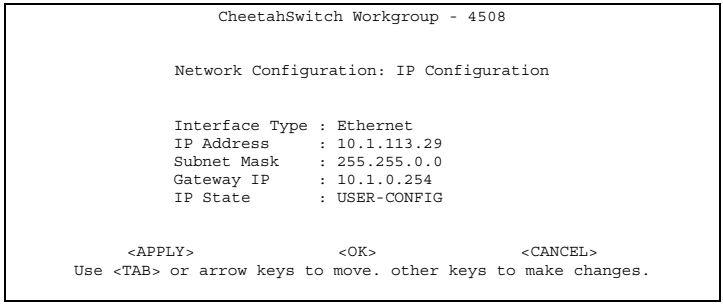
Use the Network Configuration menu to set the bootup option, configure the switch's Internet Protocol (IP) parameters, enable the on-board Web agent, or enable Telnet access. The screen shown below is described in the following table.



Parameter	Description
IP Configuration	Screen used to set the bootup option, or configure the switch's IP parameters for the Ethernet interface.
IP Connectivity Test (Ping)	Screen used to test IP connectivity to a specified device.
Access Host Configuration	Screen used to restrict access to the host switch to specified subnets.
HTTP Configuration	Screen used to enable/disable the Web agent.
MAX Number of Allowed Telnet Sessions	The maximum number of Telnet sessions allowed to simultaneously access the SNMP agent. Up to four sessions are supported.
MAC Address	Physical address of the SNMP agent.

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.

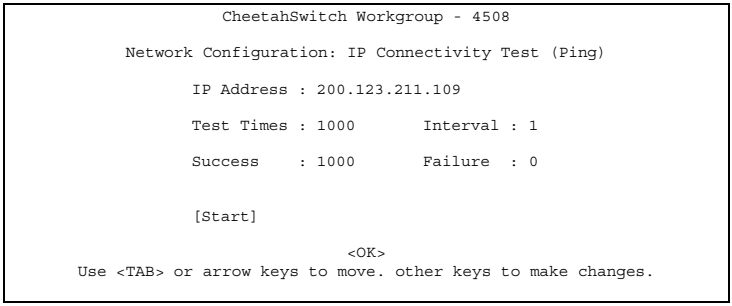


Parameter	Description
Interface Type	Indicates IP over Ethernet.
IP Address[1]	IP address of the switch you are managing when accessing the SNMP agent over the network. The management agent supports SNMP over UDP/IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the agent (or running AccView) are assigned an IP address. Valid IP addresses consist of four numbers, of 0 to 255, separated by periods. Anything outside of this format will not be accepted by the configuration program.
Subnet Mask[1]	Subnet mask of the SNMP agent. This mask identifies the host address bits used for routing to specific subnets.
Default Gateway[1]	Gateway used to pass trap messages from the switch's agent to the management station. Note that the gateway must be defined if the management station is located in a different IP segment.
IP State	Specifies whether IP functionality is enabled via manual configuration, or set by Boot Protocol (BOOTP). Options include: USER-CONFIG - IP functionality is enabled based on the default or user specified IP Configuration. (This is the default setting.) BOOTP Get IP - IP is enabled but will not function until a BOOTP reply has been received. BOOTP requests will be periodically broadcast by the switch in an effort to learn its IP address.

1: The default value is null.

IP Connectivity Test (Ping)

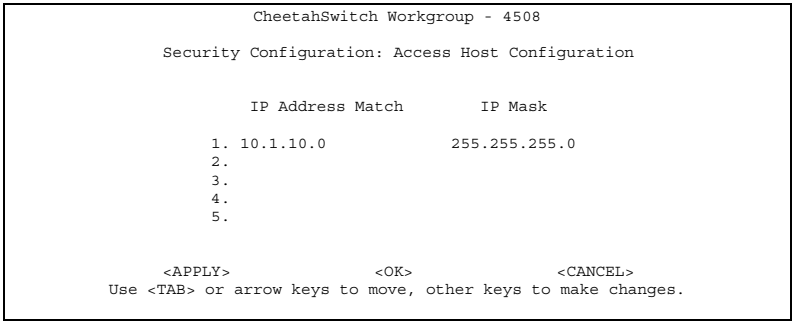
Use the IP Connectivity Test to see if another site on the Internet can be reached. The screen shown below is described in the following table.



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. (1~1000)
Interval	The interval (in seconds) between pinging the specified site. (1~ 10 seconds)
Success/Failure	The number of times the specified site has responded or not to pinging.

Access Host Configuration

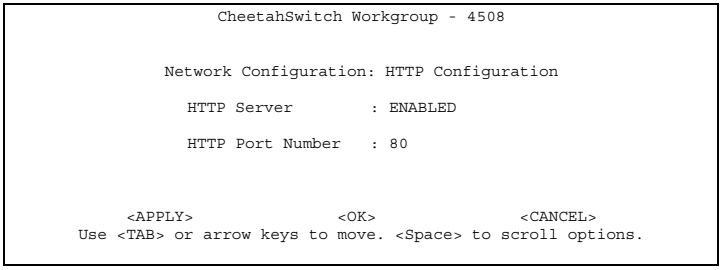
Use the Access Host Configuration screen to restrict management access to the host switch to specified subnets. The screen shown below is described in the following table.



Parameter	Description
IP Address Match	IP address of a subnet that is allowed management access to the host switch. Up to five subnets can be specified.
IP Mask	The IP mask that identifies the subnet.

HTTP Configuration

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



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

Configuring the Serial Port

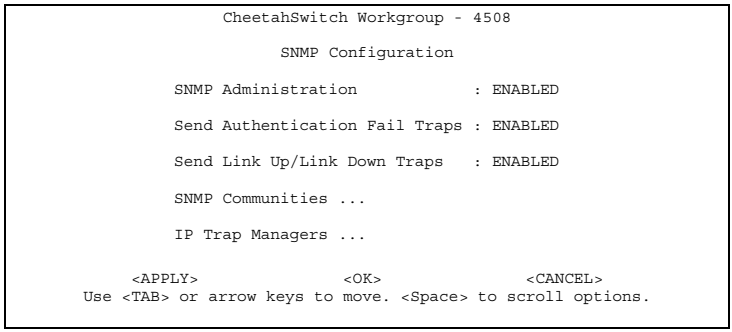
You can access the on-board configuration program by attaching a VT100 compatible device to the switch's serial port. For more information on connecting to this port, refer to the section on Making the Connections Required for System Configuration on page 9. The communication parameters for this port are accessed from the Serial Port Configuration screen seen below and described in the following table.

```
                    CheetahSwitch Workgroup - 4508


                      Serial Port Configuration

                       Management Mode            : Console Mode
                       Baudrate                   : 19200
                       Databits                   : 8
                       Stopbits                   : 1
                       Parity                     : NONE
                       Time-Out (in minutes)      : 10
                       Auto Refresh (in seconds)  : 180


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

Parameter	Default	Description
Management Mode	Console Mode	Indicates if the console port settings are for direct console connection.
Baud Rate	19200	The rate at which data is sent between devices. (Options: 2400, 4800, 9600, 19200, 38400, 57600, 115200 bps, and Auto detection). Note that when Auto is selected, you must first press the Enter key once to set the data rate and initialize the connection.
Databits	8 bits	Sets the data bits of the RS-232 port. (Options: 7, 8)
Stopbits	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	0 minutes	If no input is received from the attached device after this interval (in minutes), the current session is automatically closed. (Range: 0 -100 minutes; where 0 indicates disabled.)
Auto Refresh	0 sec.	Sets the interval before a console session will auto refresh the console information, including Spanning Tree Information, Port Configuration, Port Statistics, and RMON Statistics. (Range: 0, or 5 - 255 seconds; where 0 indicates disabled.)

Assigning SNMP Parameters

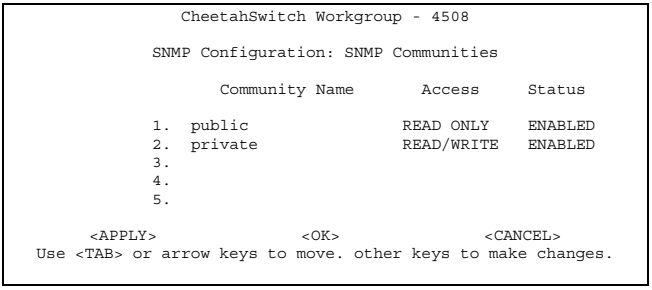
Use the SNMP Configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP). The switch includes an on-board SNMP agent which monitors the status of its hardware, as well as the traffic passing through its ports. A computer attached to the network, called a Network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



Parameter	Description
SNMP Administration	Enables/disables the SNMP function of the agent.
Send Authentication Fail Traps	Issue a trap message to specified IP trap managers whenever authentication of an SNMP request fails. (The default is disabled.)
Send Link Up/Link Down Traps	Issue a trap message to specified IP trap managers whenever a link changes its up/down state. (The default is enabled.)
SNMP Communities	Assigns SNMP access based on specified community 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 trap management access. All community strings used for IP Trap Managers must be listed in this table. Up to 5 community names may be entered.

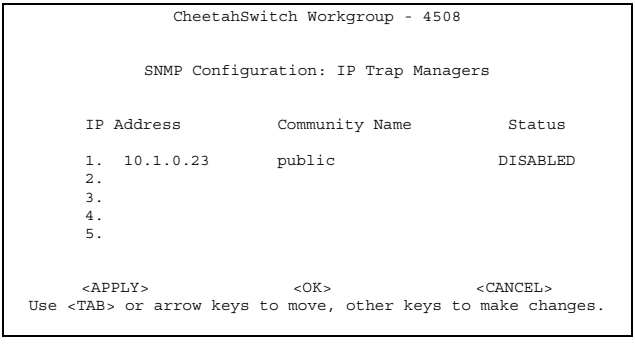


Parameter	Description
Community Name	A community entry authorized for trap management access. (The maximum string length is 20 characters).
Access	Management access is restricted to Read Only or Read/Write.
Status	Sets administrative status of entry to enabled or disabled.

Note: This switch has default community strings of “public” with read only access and “private” with read/write access.

Configuring IP Trap Managers

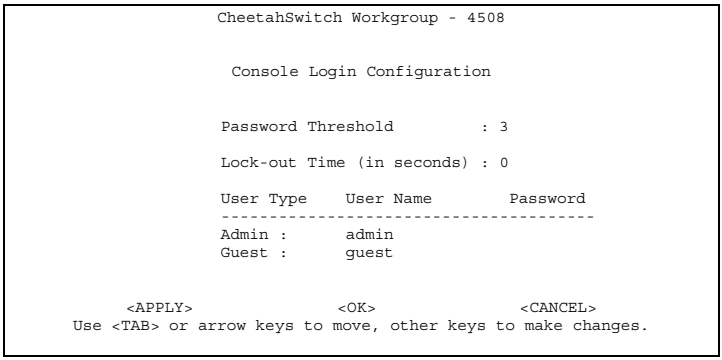
The following figure and table describe how to specify management stations that will receive authentication failure messages or other trap messages from the switch. Note that all community strings used for IP Trap Managers must be listed in the SNMP Communities table. Up to 5 trap managers may be entered.



Parameter	Description
IP Address	IP address of the trap manager.
Community Name	A community specified in the SNMP Communities table.
Status	Sets administrative status of 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 two user types, Administrator and Guest. Only the Administrator has write access for parameters governing the SNMP agent. You should therefore assign a user name and password to the Administrator as soon as possible, and store it in a safe place. (If for some reason your password is lost, or you can not gain access to the System Configuration Program, contact your Accton distributor for assistance.) The parameters shown on this screen are indicated in the following figure and table.



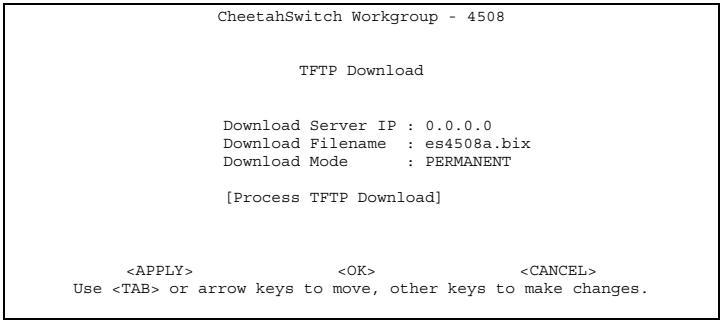
Parameter	Default	Description
Password Threshold	3	Sets the password intrusion threshold which limits the number of failed logon attempts. (Range: 0~65535)
Lock-out Time	0	The time (in seconds) the management console will be disabled due to an excessive number of failed logon attempts. (Range: 0~65535)
Admin[1]	name: admin password: null	Administrator has access privilege of Read/Write for all screens.
Guest[1]	name: guest password: null	Guest has access privilege of Read Only for all screens.

1: Passwords can consist of up to 15 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 ES4508 binary file from Accton; otherwise the agent will not accept it. The success of the download operation depends on the accessibility of the TFTP server and the quality of the network connection. After downloading the new software, the agent will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table.

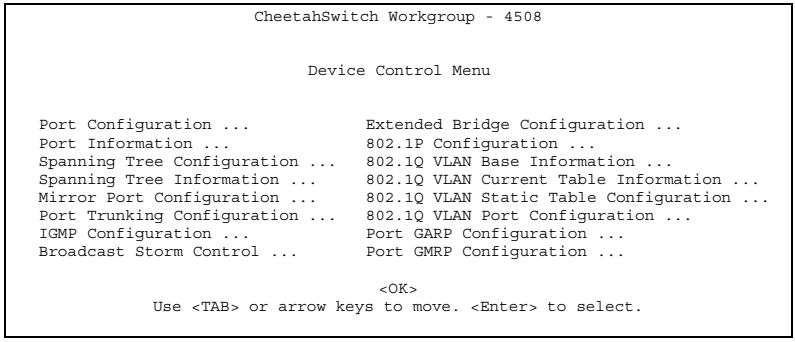


Parameter	Description
Download Server IP	IP address of a TFTP server.
Download Filename	The binary file to download to the SNMP agent.
Download Mode	You can download to “Permanent” flash ROM or “Temporary” storage in RAM (for test purposes). Note that if you download to temporary memory, this firmware will be lost upon power off.
Process TFTP Download	Issues request to TFTP server to download the specified file.

Note: You can also download firmware using the Web agent (see page 3-10) or a direct console connection (see page A-1).

Configuring the Switch

The Device Control menu is used to set the communication parameters for individual ports, and to fine-tune the performance of your switch by adjusting the forwarding mode, flow control, and specific Spanning Tree parameters. Configuration menus are also provided for advanced functions, such as Virtual LANs, and port mirroring. Each of the setup screens provided by the configuration menus is described in the following sections.

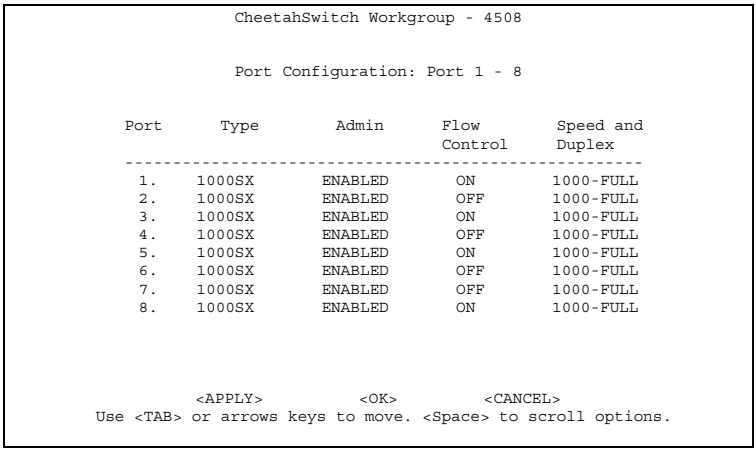


Parameter	Description
Port Configuration	Sets communication parameters for ports.
Port Information	Displays current port settings and port status.
Spanning Tree Configuration	Configures the switch and its ports to participate in a Spanning Tree.
Spanning Tree Information	Displays the current Spanning Tree configuration for the switch.
Mirror Port Configuration	Sets the source and target ports for mirroring.
IGMP Configuration	Configures IGMP multicast filtering.
Broadcast Storm Control	Configures the threshold at which broadcast packets are discarded.
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.
802.1Q VLAN Port Configuration	Displays/configures port-specific VLAN settings, including PVID and ingress filtering.

Note: This switch does not support trunking, GVRP or GMRP. Therefore, the Port Trunking, Port GARP, and Port GMRP configuration menus are not accessible from this screen.

Configuring Port Parameters

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



Parameter	Default	Description
Type		Shows port type as 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	ON	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.
Speed and Duplex	1000-FULL	Indicates the current port speed and duplex mode (1000-FULL or AUTO). Although ports on the switch can be set for auto-negotiation, operation is restricted to 1000 Mbps, full duplex.

Viewing the Current Port Configuration

The Port Information screen displays the port type, status, link state, and flow control in use. To change any of the port settings, use the configuration menu.

```
                    CheetahSwitch Workgroup - 4508

                      Port Information: Port 1 - 8

Port  Type  Operational Link   FlowControl  Speed and
                               InUse        Duplex InUse
-------------------------------------------------------------
 1.  1000SX    YES      DOWN   802.3x       1000-FULL
 2.  1000SX    YES      DOWN   NONE         1000-FULL
 3.  1000SX    YES      UP     802.3x       1000-FULL
 4.  1000SX    YES      DOWN   NONE         1000-FULL
 5.  1000SX    YES      DOWN   802.3x       1000-FULL
 6.  1000SX    YES      UP     NONE         1000-FULL
 7.  1000SX    YES      DOWN   NONE         1000-FULL
 8.  1000SX    YES      UP     802.3x       1000-FULL

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

Parameter	Description
Type	Shows port type as 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. IEEE 802.3x flow control is used for full duplex.
Speed and DuplexInUse	Displays the current port speed and duplex mode used.

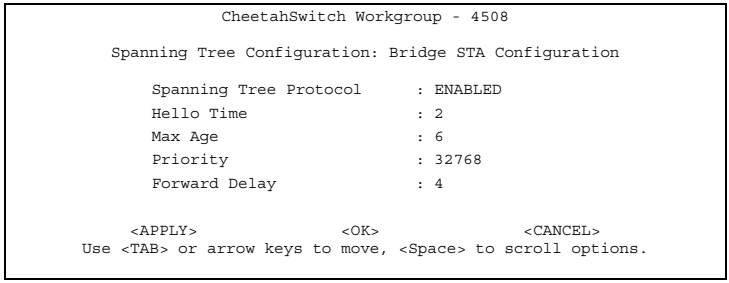
Using the Spanning Tree Algorithm

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, 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" in Chapter 4.

```
                    CheetahSwitch Workgroup - 4508

              Spanning Tree Configuration: Selection Menu

                 STA Bridge Configuration ...

                 STA Port Configuration ...

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

Configuring Bridge STA

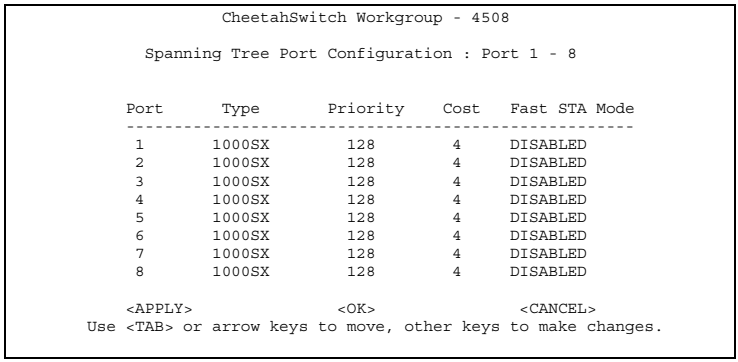
The following figure and table describe Bridge STA configuration.



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

Configuring STA for Ports

The following figure and table describe STA configuration for ports.



Parameter	Default	Description
Type		Shows port type as 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. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. The range is 0 - 255.
(Path) Cost	100/19/4	This parameter is used by the STA algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. The default and recommended range is: Standard Ethernet: 100 (50~600) Fast Ethernet: 19 (10~60) Gigabit Ethernet: 4 (3~10) The full range is 0 - 65535. Note: Path cost takes precedence over port priority.
Fast STA Mode	DISABLED	This parameter is used to enable/disabled the Fast Spanning Tree mode. In this mode, ports skip the Blocked, Listening and Learning states and proceed straight to Forwarding. The Fast STA Mode enables end-node workstations and servers to overcome time-out problems when the Spanning Tree Algorithm is implemented in a network. Therefore, the Fast STA Mode should only be enabled for ports that are connected to an end-node device.

Viewing the Current Spanning Tree Configuration

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. Also note that this screen cannot be accessed unless you have already enabled the Spanning Tree Algorithm via the STA Bridge Configuration menu.

```
                    CheetahSwitch Workgroup - 4508

              Spanning Tree Information : Selection Menu


                 STA Bridge Information ...

                 STA Port Information ...


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

Displaying the Current Bridge STA

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

```
                    CheetahSwitch Workgroup - 4508

           Spanning Tree Information : Bridge STA Information

  Priority                    : 65535
  Hello Time (in seconds)     : 2
  Max Age (in seconds)        : 6
  Forward Delay (in seconds)  : 5
  Hold Time (in seconds)      : 2
  Designated Root             : 0.0000e8123456
  Root Cost                   : 10
  Root Port                   : 1
  Reconfig Counts             : 2
  Topology Up Time            : 0 day, 1 hr, 2min, 34 sec

                                <OK>
          Use <Tab> or arrow keys to move, <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).

Parameter	Description
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.
Reconfig Counts	The number of times the spanning tree has been reconfigured.
Topology Up Time	The time since the spanning tree was last reconfigured.

Displaying the Current STA for Ports

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

```
                    CheetahSwitch Workgroup - 4508

                       Spanning Tree Information


Port    Type        Status      Designated      Designated       Designated
                                Cost            Bridge           Port
 ------------------------------------------------------------------------
  1.  1000SX      forwarding      32768       128.0000e8123456       3
  2.  1000SX      forwarding      32768       128.0000e8123457       1
  3.  1000SX      forwarding      32768       128.0000e8123458       1
  4.  1000SX      forwarding      32768       128.0000e8123459       5
  5.  1000SX      listening       32768       128.0000e812345a       6
  6.  1000SX      learning        32768       128.0000e812345b       3
  7.  1000SX      forwarding      32768       128.0000e8123456       3
  8.  1000SX      forwarding      32768       128.0000e8123457       3



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

Parameter	Description
Type	Shows port type as 1000SX (1000BASE-SX).
Status	Displays the current state of this port within the spanning tree: Disabled — Port has been disabled by the user or has failed diagnostics. Blocked — Port receives STA configuration messages, but does not forward packets. Listening — Port will leave blocking state due to topology change, starts transmitting configuration messages, but does not yet forward packets. 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. Forwarding — The port forwards packets, and continues learning addresses. The rules defining port status are: • A port on a network segment with no other STA compliant bridging device is always forwarding. • 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. • All ports are blocked when the switch is booted, then some of them change state to listening, to learning, and then to forwarding.
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 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 logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner. When mirroring port traffic, note that the target port must be included in the same VLAN as the source port. (See Configuring Virtual LANs on page 2-41.)

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

```
                    CheetahSwitch Workgroup - 4508


                       Mirror Port Configuration


                  Analyzer Port      : Port 0

                  Monitored Port     : Port 0

                  Analyzer Port 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.

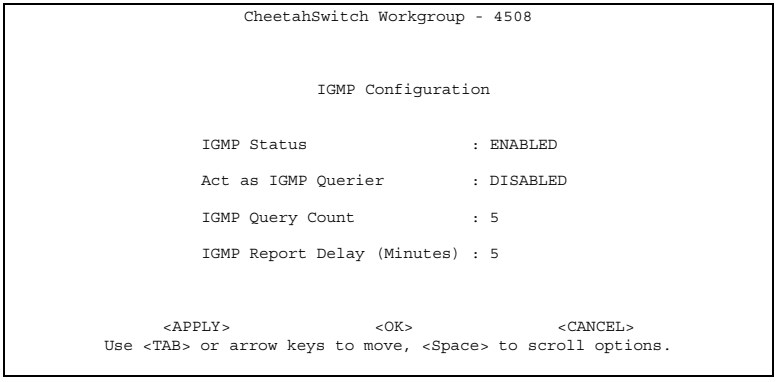
IGMP Multicast Filtering

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 and IP Multicast Filtering” in Chapter 4.)

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:

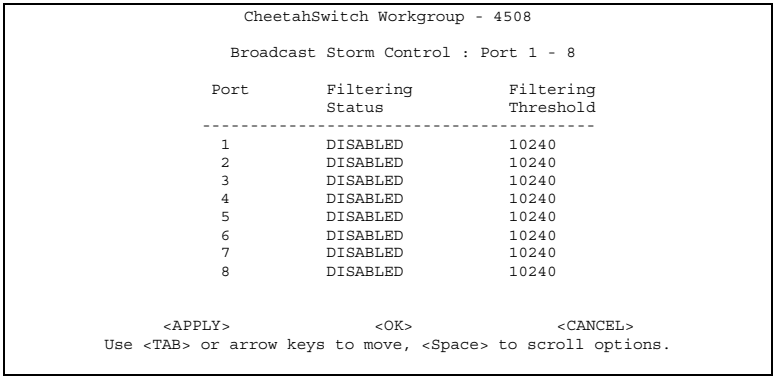


Parameter	Description
IGMP Status	If enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.
Act as IGMP Querier	If enabled, the switch can serve as the "querier," which is responsible for asking hosts is they want to receive multicast traffic. (Not implemented in the current firmware release.)
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 minutes) 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.

Broadcast Storm Control

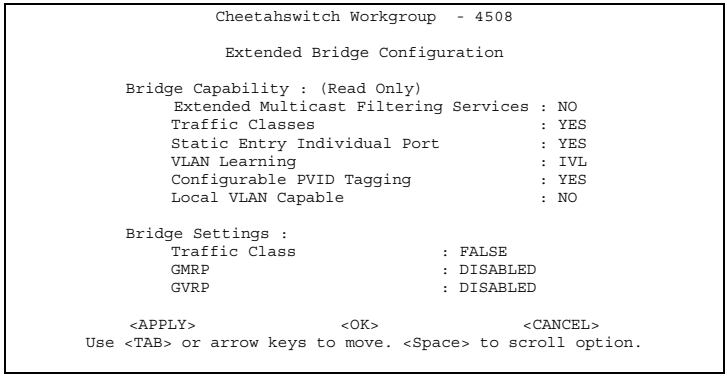
Use the Broadcast Storm Control menu to enable/disable broadcast suppression on a per-port basis. You can also set the packet-per-second threshold above which broadcast packets will be discarded. The parameters are shown in the following figure and table.



Parameter	Description
Filtering Status	Enables/disables Broadcast Storm Control for the port. When enabled, broadcast packets are discarded if the threshold rate is exceeded.
Filtering Threshold	The threshold rate above which broadcast packets are discarded. The default is 10240 packets per second. (Range is 1024 - 353,422 pps.)

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:



Parameter	Description
Bridge Capability	
Extended Multicast Filtering Services	This switch does not support filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
Traffic Classes	This switch provides the mapping of user priorities to multiple traffic classes. (Refer to 802.1P Configuration.)
Static Entry Individual Port	This 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	This 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).
Bridge Settings	
Traffic Class	Multiple traffic classes are supported by this switch as indicated under Bridge Capabilities. However, the switch supports just two priority queues and only the default port priority can be configured. The switch does not support the configuration of traffic class mapping. Therefore, this parameter under Bridge Settings is set to False and cannot be enabled.

Note: This switch does not support GVRP or GMRP. Therefore, the GVRP and GMRP parameters are always disabled.

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.

```
                CheetahSwitch Workgroup - 4508

            802.1P Configuration : Selection Menu

             802.1P Port Priority Configuration ...

             802.1P Port Traffic Class Information ...


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

Port Priority Configuration

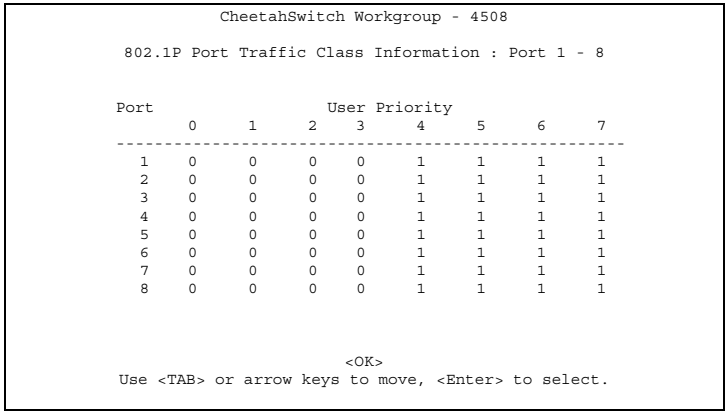
The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in the low priority output queue. Default priority is only used to determine the output queue for the current port; no priority tag is actually added to the frame. You can use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

```
                CheetahSwitch Workgroup - 4508

          802.1P Port Priority Configuration : Port 1 - 8


            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:



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 16 LAN groups. In conventional networks with routers, broadcast traffic is split up into separate domains. Switches do not inherently support broadcast domains. This can lead to broadcast storms in large networks that handle traffic such as IPX or NetBeui. By using IEEE 802.1Q compliant VLANs, you can organize any group of network nodes into separate broadcast domains, 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” in Chapter 4. The VLAN configuration screens are described in the following sections.

802.1Q VLAN Base Information

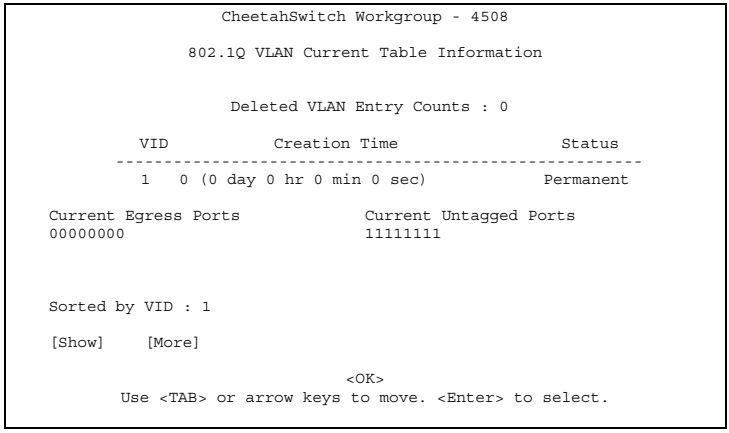
The 802.1Q VLAN Base Information screen displays basic information on the VLAN type supported by this switch.

```
                CheetahSwitch Workgroup - 4508

                 802.1Q VLAN Base Information


          VLAN Version Number                          : 1

          MAX VLAN ID                                  : 2048

          MAX Supported VLANs                          : 16

          Current Number of 802.1Q VLANs Configured    : 1


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

802.1Q VLAN Current Table Information

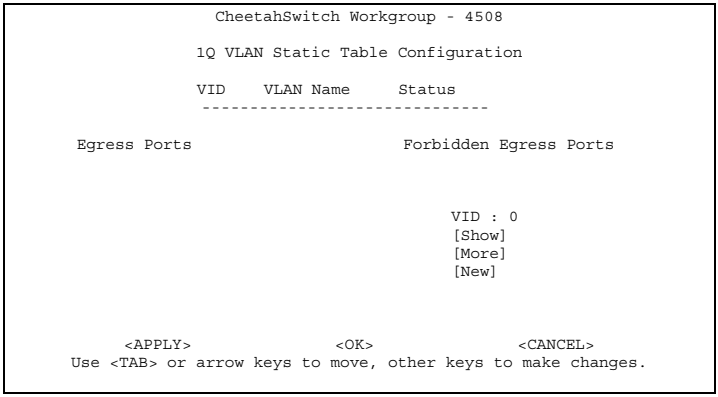
This screen shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can assign ports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



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 that this VLAN was added to the switch 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.
Sorted by VID	The VID number where the table display starts.
[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. 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.



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.
Unit	Stack unit.
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. Note that GVRP is not supported by this switch.
[Show]	Displays settings for the specified VLAN.
[More]	Displays consecutively numbered VLANs.
[New]	Sets up the screen for configuring a new VLAN.

For example, the following screen displays settings for VLAN 2, which includes tagged ports 1-6, and forbidden port 8.

```
                    CheetahSwitch Workgroup - 4508

                  1Q VLAN Static Table Configuration

                  VID    VLAN Name     Row Status
                   ------------------------------
                   2     RD            Active

          Egress Ports                 Forbidden Egress Ports
          11111100                     00000001

                                       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.

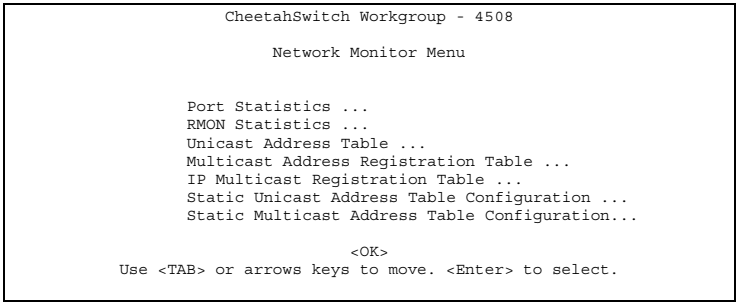
```
                    CheetahSwitch Workgroup - 4508

                802.1Q VLAN Port Configuration : Port 1 - 8


Port  PVID   Acceptable   Ingress    GVRP    GVRP Failed     GVRP Last
             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	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	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.

Note: This switch does not support GVRP. Therefore, the GVRP Status parameter is set to disabled and cannot be enabled. The other GVRP parameters will always display zeros.

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.



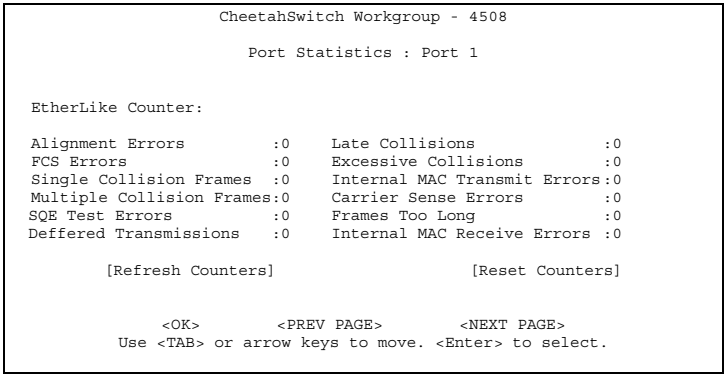
Menu	Description
Port Statistics	Displays statistics on network traffic passing through the selected port.
RMON Statistics	Displays detailed statistical information for the selected port such as packet type and frame size counters.
Unicast Address Table	Provides full listing of all unicast addresses 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. (Not implemented for this switch.)
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 for this switch.)

Note: This switch does not support GMRP. Therefore, both the Multicast Address Registration Table and the Static Multicast Address Table Configuration items are not accessible.

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.

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



Parameter	Description
Alignment Errors	For 10 Mbps ports, this counter records alignment errors (mis-synchronized data packets). For 100 Mbps ports, this counter records the sum of alignment errors and code errors (frames received with rxerror signal).
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[1]	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames[1]	A count of successfully transmitted frames for which transmission is inhibited by more that one collision.
SQE Test Errors[1]	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer.
Deferred Transmissions[1]	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[1]	The number of frames for which transmission failed due to excessive collisions.
Internal Mac Transmit Errors[1]	The number of frames for which transmission failed due to an internal MAC sublayer transmit error.

Parameter	Description
Carrier Sense Errors[1]	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[1]	The number of frames for which reception failed due to an internal MAC sublayer receive error.

1: 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 RMON Group 1 statistics for each port. (RMON groups 2, 3 and 9 can only be accessed using SNMP management software such as AccView.) The following screen displays overall statistics on traffic passing through each port. RMON statistics provides 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.

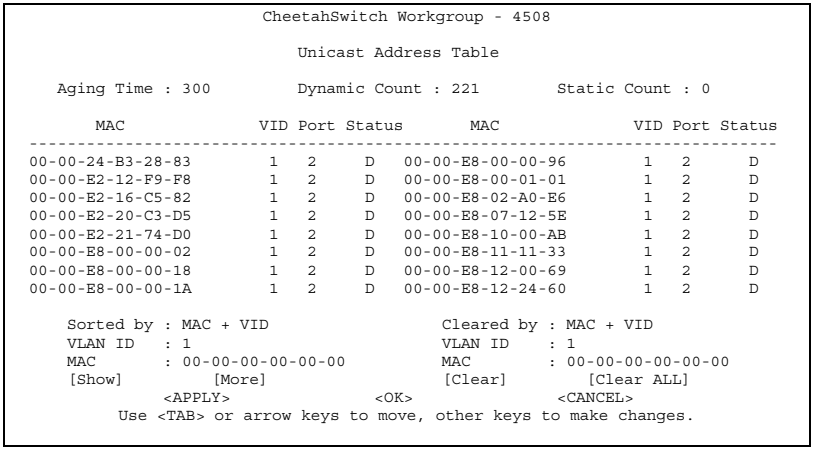
```
                    CheetahSwitch Workgroup - 4508

                        RMON Statistics : Port 1

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

          [Refresh Statistics]             [Reset Counters]

           <OK>             <PREV PAGE>           <NEXT PAGE>
           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.
Receive Bytes	Total number of data bytes 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	For 1000Mbps ports, the counter records the sum of CRC/alignment errors and code errors (frame received with rxerror signal).

Parameter	Description
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).
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).

Using the Address Table

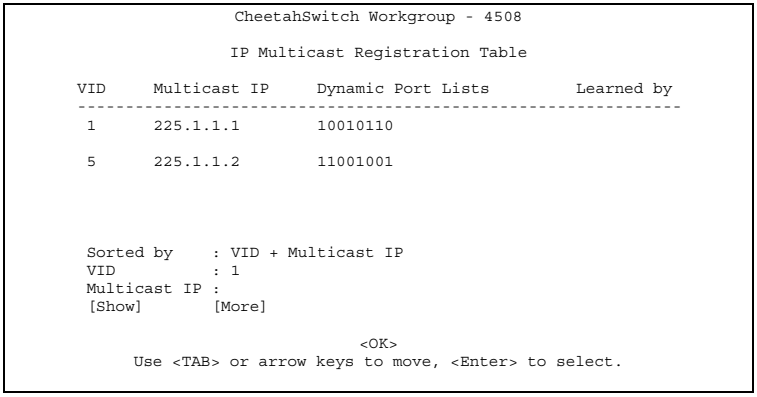
The Address Table contains the MAC addresses and VLAN identifiier associated with each port (that is, the source port associated with the address and VLAN). The address table provides search options for a specific port, address or VLAN identifier. You can also clear the entire address table, or information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



Parameter	Description
Aging Time	Time-out period in seconds for aging out dynamically learned forwarding information. Range: 10 - 458 seconds Default: 300 seconds
Dynamic Count	The number of dynamically learned addresses in the table.
Static Count	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.
[Clear]	Clears the specified MAC address.
[Clear All]	Clears all MAC addresses in the table.

Displaying the IP Multicast Registration Table

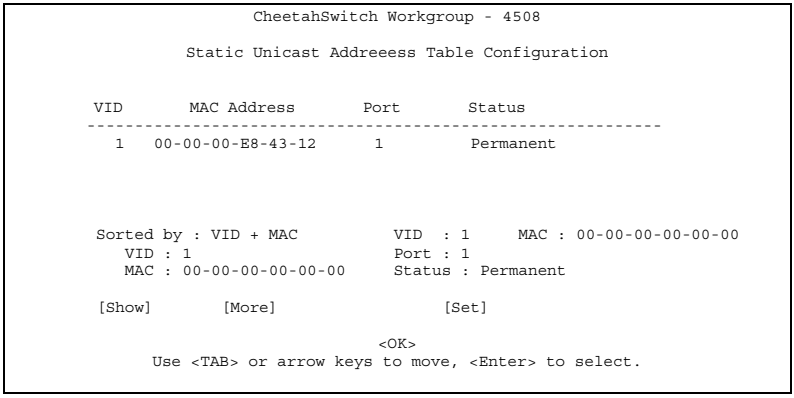
Use the IP Multicast Registration Table to display all the multicast groups active on this switch, including multicast IP addresses and the corresponding VLAN ID.



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 the manner in which this address was learned: Dynamic or 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.



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.) 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

Use the System Restart Menu under the Main Menu to reset the management agent. The reset screen also includes an option to return all configuration parameters to their factory defaults.

```
                    CheetahSwitch Workgroup - 4508


                          System Restart Menu


                  Restart Option :

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

                          [Restart]


                                  <OK>
        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.
[Restart]	Restarts the switch.

Logging Off the System

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

Chapter 3: Using the Web Agent

As well as the menu-driven system configuration program, the CheetahSwitch Workgroup-4508 provides an embedded HTTP Web agent. This 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).

Using the Web browser management interface you can configure the switch and view statistics to monitor network activity. The Web interface also provides access to a range of SNMP management functions with its MIB and RMON browser utilities.

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 the Administrator user name and password using an out-of-band serial connection. Access to the Web agent is controlled by the same Administrator user name and password as the on-board configuration program.

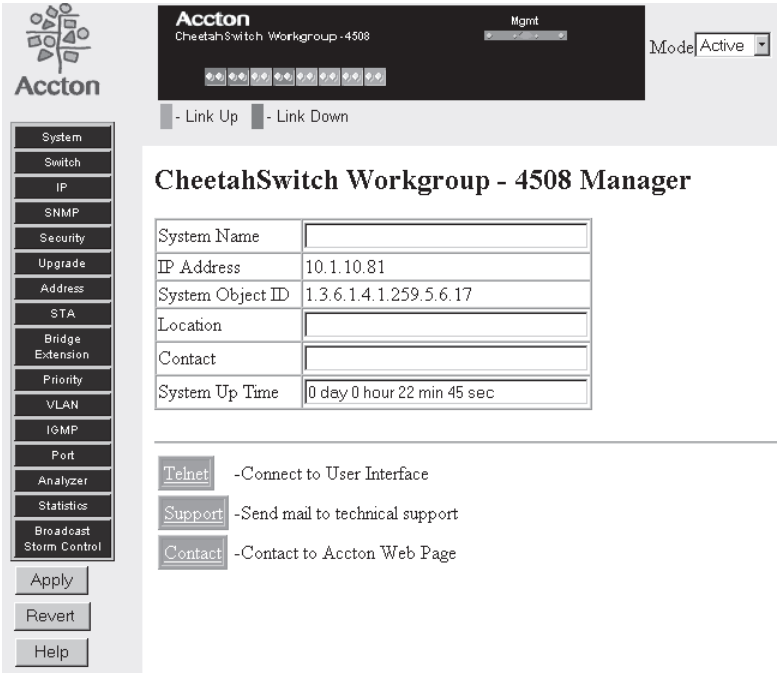
Navigating the Web Browser Interface

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

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 in Chapter 2.)

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-hand side of the screen and the System Information on the right-hand side. The Main Menu links are used to navigate to other menus and display configuration parameters and statistical data.

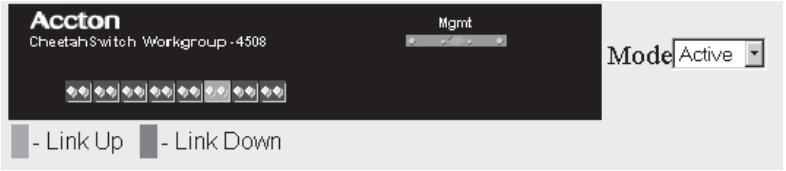


Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the "Apply" button at the bottom of the page to confirm the new setting. Alternatively, you can click on "Revert" to clear any changes prior to pressing "Apply."

Note: To ensure proper screen refresh after a command entry, 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."

Panel Display

The Web Agent displays an image of the switch's ports, showing port link 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 (labelled "Mgmt") displays the Console Configuration screen.



Console Configuration

Click on the serial port icon in the switch image to display and configure the out-of-band serial port connection, as shown in the following figure and table.

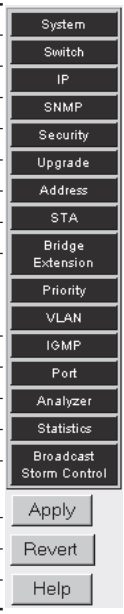
Baudrate	19200
Time-Out	0 minute(s)
Databits	8
Stopbits	1
Parity	None
Auto Refresh Time	5 second(s)

Parameter	Default	Description
Baudrate	19200	The rate at which data is sent between devices. (Options: 2400, 4800, 9600, 19200, 38400, 57600, 115200 bps, and Auto detection). Note that when AUTO is selected, you need to first press the Enter key once to set the data rate and initialize the connection.
Time Out	0 minutes	If no input is received from the attached device after this interval (in minutes), the current session is automatically closed. (Range: 0 -100 minutes; where 0 indicates disabled.)
Databits	8 bits	Sets the data bits of the RS-232 port. (Options: 7, 8)
Stopbits	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	0 sec.	Sets the interval before a console session will auto refresh the console information, including Spanning Tree Information, Port Configuration, Port Statistics, and RMON Statistics. (Range: 0, or 5 - 255 seconds; where 0 indicates disabled.)

Main Menu

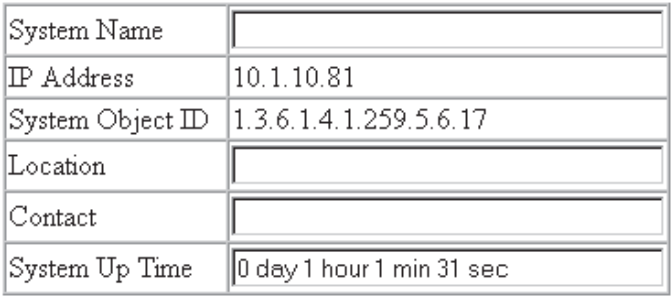
Using the on-board Web agent, you can define system parameters, manage and control the switch and all its ports, or monitor network conditions. The figure to the right of the Main Menu and the following table briefly describe the selections available from this program.

Item	Description
System	Provides basic system description, including contact information.
Switch	Shows hardware/firmware version numbers and power status.
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.
Address	Provides full address listing, sorted by address or port.
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.
Port	Enables any port and enables/disables flow control.
VLAN	Assigns switch ports to form up to 16 independent LAN groups.
Analyzer	Sets analysis and monitored port.
Statistics	Displays statistics on network traffic passing through the selected port.
Broadcast Storm Control	Enables/disables broadcast suppression on a per-port basis. Also sets the broadcast-rate threshold above which broadcast packets are discarded.
Apply	Implement the changes made to the current configuration menu.
Revert	Cancel changes made to current configuration menu (prior to pressing Apply).
Help	Help on using the Web management interface.



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.



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

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

2: The default value is null.

Switch Information

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

Main Board

Hardware Version	0
POST Version	V01.00.01
Firmware Version	V01.00.02
Port Number	8
Serial Number	
Internal Power Status	
Redundant Power Status	

Parameter	Description
Hardware Version	Hardware version of the main board.
POST Version	System POST version.
Firmware Version	Version number of the system firmware in ROM.
Port Number	Number of ports.
Serial Number[1]	Serial number of the main board.
Internal Power Status[1]	Power status for the switch.
Redundant Power Status[1]	Redundant power status for the switch.

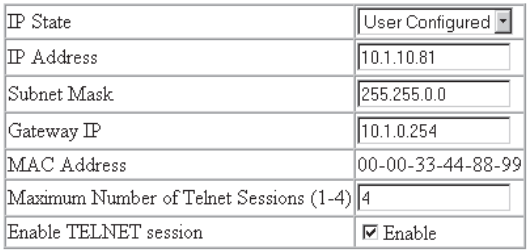
1: These parameters are not implemented in the current hardware version.

Network Configuration

Use the IP Configuration screen to set the bootup option, configure the Ethernet IP addresses for the agent module, or set the number or concurrent Telnet sessions allowed. The Access Host screen can be used to limit access to the Web management agent to specified subnet groups.

IP Configuration

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

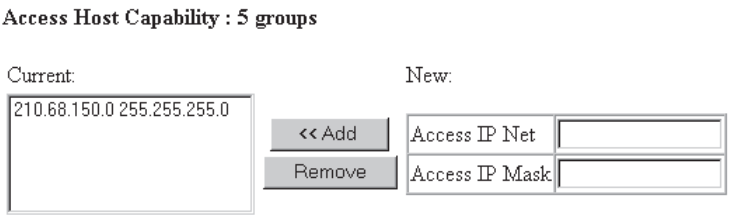


Parameter	Description
IP State	Specifies whether IP functionality is enabled via manual configuration, or set by Boot Protocol (BOOTP). Options include: USER-CONFIG - IP functionality is enabled based on the default or user specified IP Configuration. (This is the default setting.) BOOTP Get IP - IP is enabled but will not function until a BOOTP reply has been received. BOOTP requests will be periodically broadcast by the switch in an effort to learn its IP address. (BOOTP values include the IP address, default gateway, subnet mask, TFTP boot file name, and TFTP server IP.)
IP Address[1]	IP address of the SNMP agent. The management agent supports SNMP over UDP/IP transport protocol. In this environment, all systems on the Internet, such as network interconnection devices and any PC accessing the agent (or running AccView) are assigned an IP address. Valid IP addresses consist of four numbers, of 0 to 255, and separated by periods. Anything outside of this format will not be accepted by the configuration program.
Subnet Mask[1]	Subnet mask of the SNMP agent. This mask identifies the host address bits used for routing to specific subnets.
Gateway IP[1]	Gateway used to pass trap messages from the switch's agent to the management station. Note that the gateway must be defined if the management station is located in a different IP segment.
Telnet Session Number	Sets the number of concurrent Telnet sessions allowed to access the management agent. The default is four sessions.

1: The default value is null.

Access Host

Use the Access Host screen to specify subnet groups from which the switch's management agent can be accessed. The screen shown below is described in the following table.



Parameter	Description
Access IP Net	An IP address of a subnet authorized for management access.
Access IP Mask	A subnet mask that identifies the host address bits of the subnet.
Add/Remove	Add/remove strings from the active list.

SNMP Configuration

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

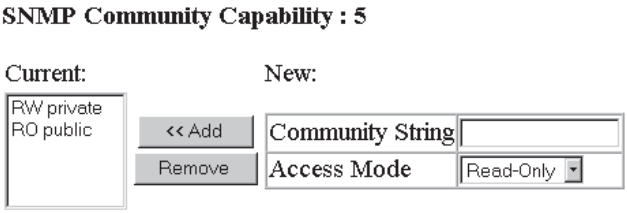
SNMP Administration Enable

Access to the management agent from SNMP-based network management software can be enabled/disabled from this screen.

Clearing the checkbox disables the SNMP protocol in the agent so that the switch can only be managed through the Web-based interface or a direct connection to the serial port. Note that even when SNMP Administration is disabled, the agent will continue to issue SNMP trap messages.

SNMP Community

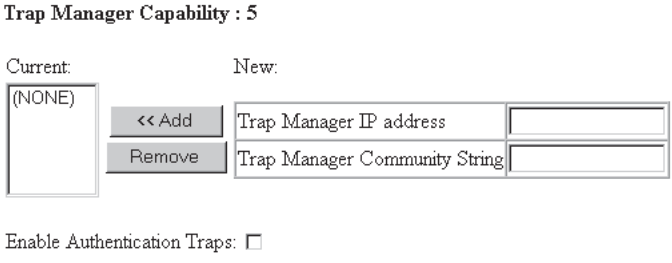
The following figure and table describe how to configure the community strings authorized for trap management access. All community strings used for IP Trap Managers must be listed in this table. Up to 5 community names may be entered.



Parameter	Description
Community String	A community entry authorized for trap management access. (The maximum string length is 20 characters).
Access Mode	Management access is restricted to Read Only or Read/Write.
Add/Remove	Add/remove strings from the active list.

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. Note that all community strings used for IP Trap Managers must be listed in the SNMP Communities table. Up to 5 trap managers may be entered.

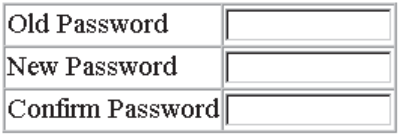


Parameter	Description
Trap Manager IP Address	IP address of the trap manager.
Trap Manager Community String	A community specified in the SNMP Communities table.
Add/Remove	Add/remove strings from the active list.
Enable Authentication Traps	Issues a trap message to specified IP trap managers whenever authentication of an SNMP request fails. (The default is enabled.)

Security Configuration

Use the Security Configuration screen to restrict management access based on Administrator user name and password. Only the Administrator has write access for parameters governing the SNMP agent. 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 can not gain access to the system's configuration program, contact your Accton distributor for assistance.) The parameters shown on this screen are indicated in the following figure and table.

Change Password



Parameter	Description
Old Password	Current Administrator password for read/write access (Default password is null).
New Password	Enter a new password for the Administrator.
Confirm Password	Re-enter the new password for the Administrator.

Note: Passwords can consist of up to 15 alphanumeric characters and are not case sensitive.

Firmware Upgrade Options

Web Upload Management

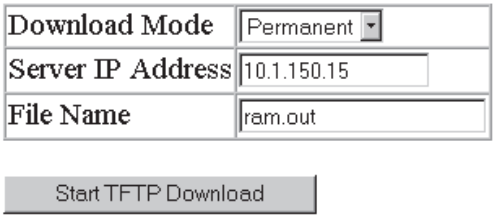
Use the Web Upload Management menu to load software updates into the switch. The upload file should be an ES4508 binary file from Accton; otherwise the agent will not accept it. The success of the upload operation depends on the quality of the network connection. After downloading the new software, the agent will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table.

Parameter	Description
Upload Mode	You can upload to permanent flash ROM or temporary storage in RAM (for test purposes). Note that if you download to temporary memory, this firmware will be lost upon power off.

Parameter	Description
File Name	The ES4508 binary file to download. Use the Browse button to locate the firmware file.
Start Web Upload	Issues request to TFTP server to download the specified file.

TFTP Download Management

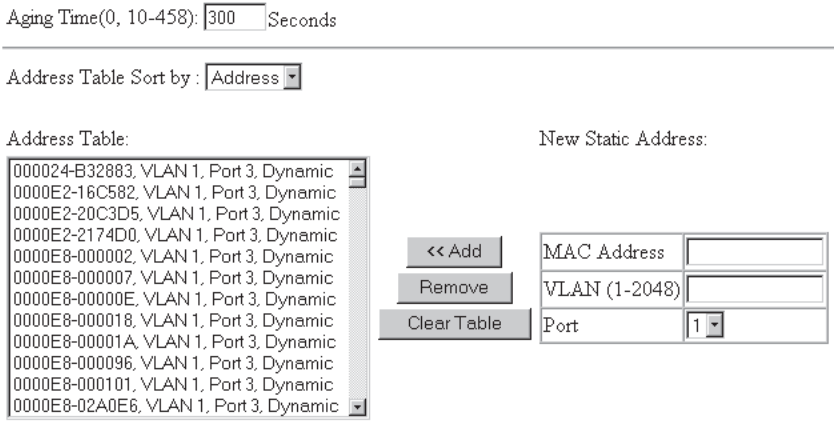
Use the TFTP Download Management menu to load software updates into the switch. The download file should be an ES4508 binary file from Accton; otherwise the agent will not accept it. The success of the download operation depends on the accessibility of the TFTP server and the quality of the network connection. After downloading the new software, the agent will automatically restart itself. Parameters shown on this screen are indicated in the following figure and table.



Parameter	Description
Download Mode	You can download to permanent flash ROM or temporary storage in RAM (for test purposes). Note that if you download to temporary memory, this firmware will be lost upon power off.
Server IP Address	IP address of a TFTP server.
File Name	The ES4508 binary file to download.
Start TFTP Download	Issues request to TFTP server to download the specified file.

Address Table Configuration

The Address Table contains the MAC addresses associated with each port (that is, the source port associated with the address). The address table provides search options for a specific port or address. You can also clear the entire address table, or information associated with a specific port or 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.



Parameter	Description
Aging Time	Time-out period in seconds for aging out dynamically learned forwarding information. Range: 0 or 10 - 458 secs; 0=disable, default: 300 secs.
Address Table Sort by	Entries can be sorted by MAC address or VLAN ID.
Address Table	The system displays the MAC address of each node, the 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 the “MAC Address,” “VLAN” and “Port” fields to add a static entry to the address table.
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” in Chapter 4.

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 screen.

Spanning Tree

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

Stanning Tree State	Enabled	Designated Root	128.0000E800E800
Bridge ID	32768.000033448899	Root Port	2
Max Age	20 seconds	Root Path Cost	4
Hello Time	2 seconds	Configuration Changes	9
Forward Delay	5 seconds	Last Topology Change	0 day 0 hour 1 min 58 sec

Parameter	Description
Spanning Tree State	Shows if 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 (the MAC address of the switch unit).
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).
Designated Root	The priority and MAC address of the device in the spanning tree that this switch has accepted as 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.
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.

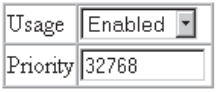
Port	Port Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port
1	Disabled	0	0	32768.000033448899	128.1
2	Forwarding	1	0	128.0000E800E800	128.4
3	Disabled	0	0	32768.000033448899	128.3
4	Disabled	0	0	32768.000033448899	128.4
5	Disabled	0	0	32768.000033448899	128.5
6	Disabled	0	0	32768.000033448899	128.6
7	Disabled	0	0	32768.000033448899	128.7
8	Disabled	0	0	32768.000033448899	128.8

Parameter	Description
Port Status	Displays the current state of this port within the spanning tree: Disabled — Port has been disabled by the user or has failed diagnostics. Blocked — Port receives STA configuration messages, but does not forward packets. Listening — Port will leave blocking state due to topology change, starts transmitting configuration messages, but does not yet forward packets. 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. Forwarding — The port forwards packets, and continues learning addresses. The rules defining port status are: • A port on a network segment with no other STA compliant bridging device is always forwarding. • 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. • All ports are blocked when the switch is booted, then some of them change state to listening, to learning, and then to forwarding.
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 port on the designated bridging device through which this switch must communicate with the root of the spanning tree.

Spanning Tree Configuration

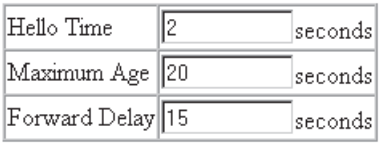
The following figures and tables describe Bridge STA configuration.

Switch



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. 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.

When the Switch Becomes Root

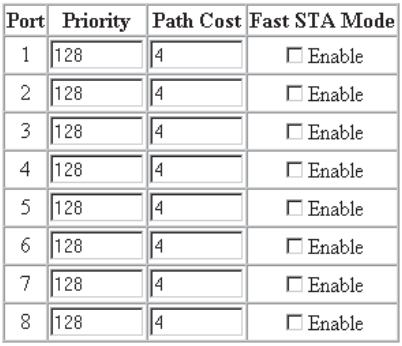


Parameter	Default	Description
Hello Time	2	The time interval (in seconds) at which the root device transmits a configuration message. The minimum value is 1. The maximum value is the lower of 10 or [(Max. Message Age / 2) -1].
Max (Message) Age	20	The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. The minimum value is the higher of 6 or [2 x (Hello Time + 1)]. The maximum value is the lower of 40 or [2 x (Forward Delay - 1)].

Parameter	Default	Description
Forward Delay	15	The maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The maximum value is 30. The minimum value is the higher of 4 or [(Max. Message Age / 2) + 1].

STA Port Configuration

The following figure and table describe STA configuration for ports.



Port	Priority	Path Cost	Fast STA Mode
1	128	4	☐ Enable
2	128	4	☐ Enable
3	128	4	☐ Enable
4	128	4	☐ Enable
5	128	4	☐ Enable
6	128	4	☐ Enable
7	128	4	☐ Enable
8	128	4	☐ Enable

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

Parameter	Default	Description
Fast STA Mode	Disabled	This enables/disables the Fast STA Mode for the port. In this mode, ports skip the Blocked, Listening and Learning states and proceed straight to Forwarding. The Fast STA Mode enables end-node workstations and servers to overcome time-out problems when the Spanning Tree Algorithm is implemented in a network. Therefore, the Fast STA Mode should only be enabled for ports that are connected to an end-node device.

Configuring Bridge MIB Extensions

The Bridge MIB includes extensions for managed devices that support Traffic Classes and Virtual LANs. To display the switch's support for 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	The switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
Traffic Classes	The switch provides mapping of user priorities to multiple traffic classes. (Refer to the Priority menu.)
Static Entry Individual Port	The switch provides static filtering for unicast and multicast addresses. (Refer to the Address Table.)
VLAN Learning	This switch uses Independent VLAN Learning (IVL), whereby each port maintains its own VLAN filtering database.
Configurable PVID Tagging	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 / VLAN Port Configuration.)
Local VLAN Capable	This switch does not support multiple local bridges (that is, multiple Spanning Trees).

Bridge Settings

Traffic Classes	☐ Enable
GMRP	☐ Enable
GVRP	☐ Enable

Parameter	Description
Traffic Class	Multiple traffic classes are supported by this switch as indicated under Bridge Capabilities. However, the switch supports just two priority queues and only the default port priority can be configured. The switch does not support the configuration of traffic class mapping. Therefore, this parameter under Bridge Settings is set to disabled and cannot be enabled.

Note: This switch does not support GMRP or GVRP. Therefore, the GMRP and GVRP functions cannot be enabled from this screen.

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 VLANs

Use the VLAN menu to create LAN groups and assign switch ports to any of up to 16 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 traffic. By using IEEE 802.1Q compliant VLANs, you can organize any group of network nodes into separate broadcast domains, confining broadcast traffic to the originating group, and provide a more secure and much cleaner network environment. For a more detailed description of how to use VLANs, see “Using Virtual LANs” in Chapter 4.

VLAN Basic Information

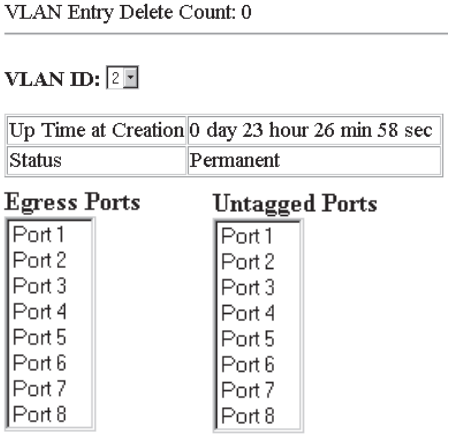
The VLAN Basic Information screen displays basic information on the VLAN type supported by this switch.

VLAN Version Number	1
Maximum VLAN ID	2048
Maximum Number of Supported VLANs	16
Current Number of 802.1Q VLANs Configured	2

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.

VLAN Current Table

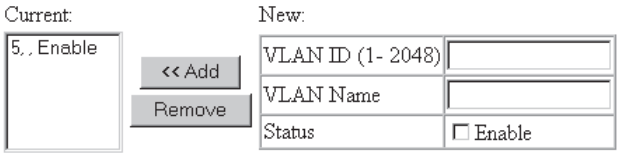
This screen shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can assign ports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



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 that this VLAN was added to the switch 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

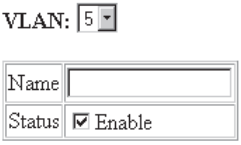
Use this screen to create or remove VLAN groups.



Parameter	Description
Current	Lists all the current VLAN groups created for this system. Up to 16 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.

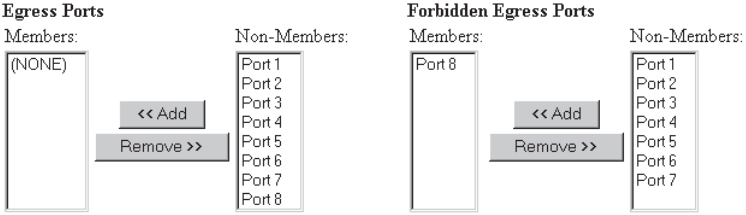
VLAN Static Table

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



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.

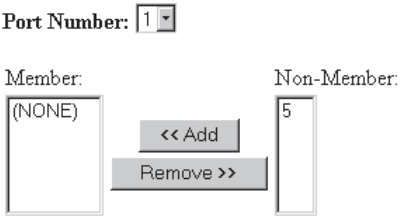
Use the screens shown below to assign ports to the specified VLAN group as an IEEE 802.1Q tagged port. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices. If the port is connected to VLAN-unaware devices, frames will passed to the untagged VLAN group this port has been assigned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



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. Note that GVRP is not supported by this switch.

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.



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	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
2	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
3	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
4	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
5	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
6	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
7	1	All	☐ Enable	☐ Enable	0	00-00-00-00-00-00
8	3	All	☐ Enable	☐ 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	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	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.

Note: This switch does not support GVRP. Therefore, the GVRP Status parameter is set to disabled and cannot be enabled. The other GVRP parameters will always display zeros.

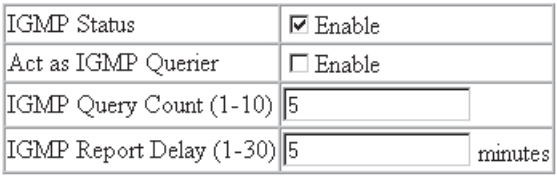
IGMP Multicast Filtering

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 and IP Multicast Filtering” in Chapter 4.)

Configuring IGMP

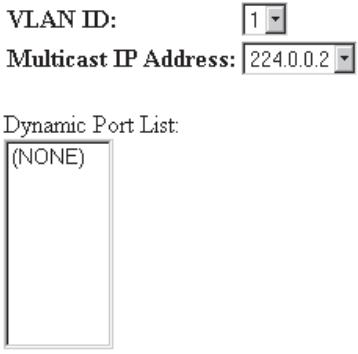
This protocol allows a host to inform its local switch/router that it wants to receive transmissions addressed to a specific multicast address group. Use the IGMP Configuration screen to set key parameters for multicast filtering as shown below.



Parameter	Description
IGMP Status	If enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.
Act as IGMP Querier	If enabled, the switch can serve as the “querier,” which is responsible for asking hosts is they want to receive multicast traffic. (Not available for the current firmware release.)
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 minutes) 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.

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.



Parameter	Description
VLAN ID	VLAN ID assigned to this multicast group.
Multicast IP Address	IP address for specific multicast services.
Dynamic Port List	The switch ports registered for the indicated multicast service.

Port Menus

Port Information

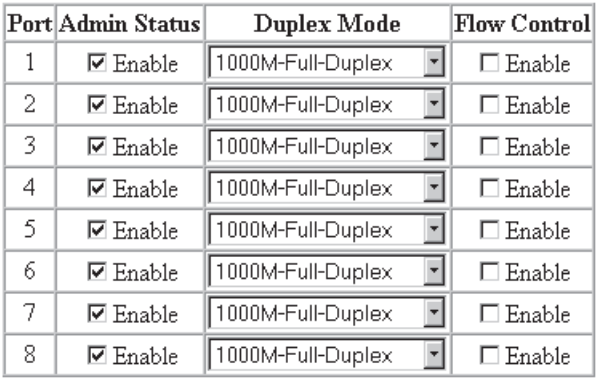
The Port Information screen displays the port status and link state, as well as the flow control in use. To change any of the port settings, use the Port Configuration menu. The parameters are shown in the following figure and table.

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

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	Indicates that the port is connected at 1000 Mbps..
Duplex Status	Indicates that the port is connected at full duplex.
Flow Control Status	Shows if flow control is in use. Flow control can eliminate frame loss by "blocking" traffic from end stations connected directly to the switch. Standard IEEE 802.3x full-duplex flow control is used.

Port Configuration

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

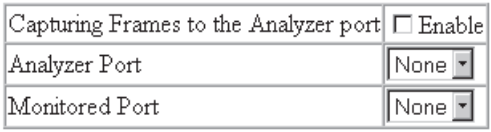


Parameter	Default	Description
Admin Status	Enable	Allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable a port for security reasons.
Duplex Mode	1000M-Full-Duplex	Used to set the duplex mode to full duplex or auto-negotiation. The default for all ports is to force full-duplex.
Flow Control	Enable	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. Standard IEEE 802.3x full-duplex flow control is used.

Port Mirroring Configuration

You can mirror the traffic from a target port to an analysis port for real-time analysis. You can then attach a logic analyzer or RMON probe to the analysis port and study the traffic crossing target port in a completely unobtrusive manner. When mirroring a port, note that the analysis port must be included in the same VLAN as the monitored port.

Use Port Monitoring Configuration to set up analysis ports as shown below:



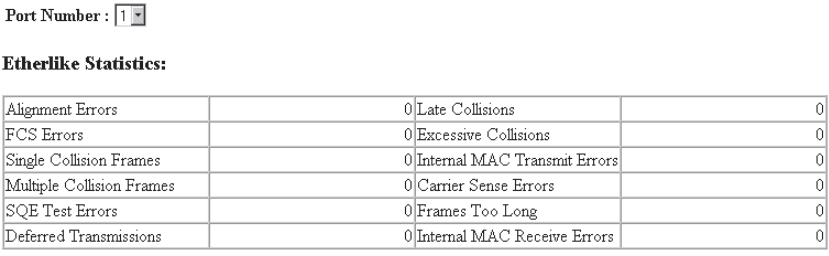
Parameter	Description
Capturing State	Enables or disables the mirror function.
Analyzer Port	The port that will "duplicate" or "mirror" all the traffic happening on the monitored port.
Analyzed Port	The port whose traffic will be monitored.

Port Statistics

Use the Port Statistics menu to display Etherlike or RMON statistics for any port on the switch. 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.



Parameter	Description
Alignment Errors	For 10 Mbps ports, this counter records alignment errors (mis-synchronized data packets). For 100 Mbps ports, this counter records the sum of alignment errors and code errors (frames received with rxerror signal).
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[1]	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Multiple Collision Frames[1]	A count of successfully transmitted frames for which transmission is inhibited by more that one collision.
SQE Test Errors[1]	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer.
Deferred Transmissions[1]	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[1]	The number of frames for which transmission failed due to excessive collisions.
Internal Mac Transmit Errors[1]	The number of frames for which transmission failed due to an internal MAC sublayer transmit error.
Carrier Sense Errors[1]	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[1]	The number of frames for which reception failed due to an internal MAC sublayer receive error.

1: The 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 or media module from RMON group 1. (RMON groups 2, 3 and 9 can only be accessed using SNMP management software such as AccView.) 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.

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	0
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	For 10Mbps ports, the counter records CRC/alignment errors (FCS or alignment errors). For 100Mbps ports, the counter records the sum of CRC/alignment errors and code errors (frame received with rxerror signal).
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.

Parameter	Description
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).
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).

Broadcast Storm Control

Use the Broadcast Storm Control page to enable/disable broadcast suppression on a per-port basis. You can also set the broadcast-rate threshold above which broadcast packets will be discarded. The parameters are shown in the following figure and table.

Port	Filtering Status	Filtering Threshold(1024-353422)
1	☐ Enable	10240
2	☐ Enable	10240
3	☐ Enable	10240
4	☐ Enable	10240
5	☐ Enable	10240
6	☐ Enable	10240
7	☐ Enable	10240
8	☐ Enable	10240

Parameter	Description
Filtering Status	Enables/disables Broadcast Storm Control for the port. When enabled, broadcast packets are discarded if the packets-per-second threshold rate is exceeded. (The default is disabled.)
Filtering Threshold	The broadcast-rate threshold above which broadcast packets are discarded. The default is 10240 packets per second. (Range is 1024 - 353,422 pps.)

Chapter 4: Advanced Topics

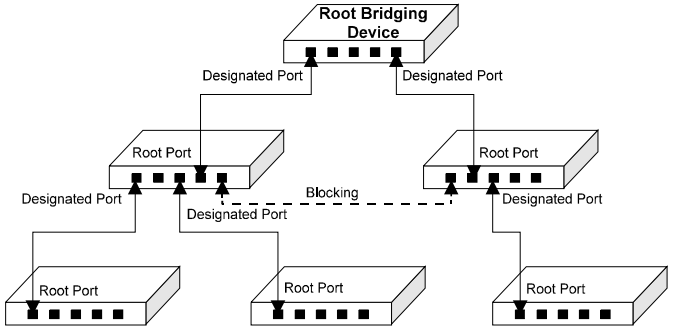
Spanning Tree Algorithm

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 re-establish 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 re-establish 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 separate domains to confine broadcast traffic to the originating group and provide a much cleaner network environment. By supporting VLANs, this switch allows you to create segregated broadcast domains. However, note that if you need to support intra-VLAN communications, you must use 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 16 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging
- 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
- Two-level priority queue

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.

VLAN Classification

When the switch receives a frame, it classifies the frame in one of two ways:

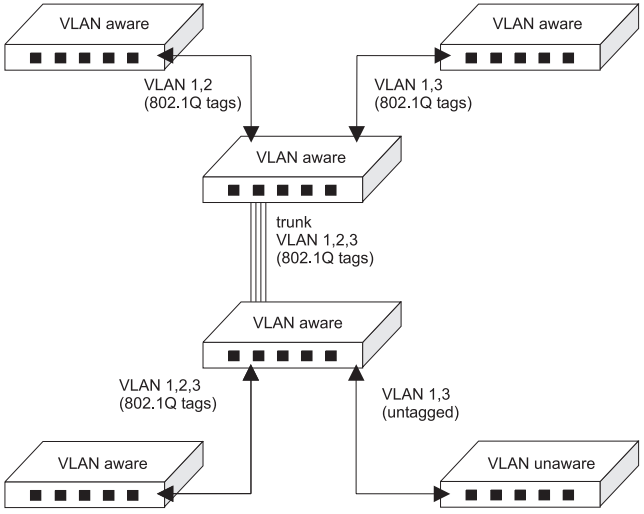
- If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the PVID of the receiving port).
- If the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

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 must connect them using a router or Layer 3 switch.

Forwarding Tagged/Untagged Frames

Ports can be assigned to one untagged VLAN and multiple tagged 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, but this can be changed (see page 2-32 or 3-24).



Forwarding Traffic with Unknown VLAN Tags

Up to 2048 VLANs are supported by the IEEE 802.1Q protocol, but this switch only supports 16 VLANs. Therefore, if this switch is attached to any device that forwards frames with unknown VLAN tags, or to endstations which issue VLAN registration requests for unknown VLANs, this traffic will be dropped.

Class-of-Service (CoS) Support

The CheetahSwitch Workgroup-4508 provides two transmit queues on each port, with a weighted round-robin 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 CheetahSwitch is accomplished through explicit assignment 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.

IGMP Snooping and IP Multicast Filtering

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

A router, or multicast-enabled switch, can periodically ask their hosts is 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, to support IP multicasting across the Internet.

IGMP provides the final step in an IP multicast packet delivery service since it is only concerned with forwarding multicast traffic from the local router/switch to group members on directly attached subnetwork or LAN segment.

This switch supports IP Multicast Filtering by:

- Passively snooping on the IGMP Query and IGMP Report packets transferred between IP multicast routers and IP multicast host groups to learn IP Multicast group members, and
- Actively sending IGMP Query messages to solicit IP Multicast group members (see page 2-23 or 3-25).

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches instead of flooding to all ports in the subnet (VLAN).

The CheetahSwitch Workgroup-4508, with IP multicast filtering capability, not only passively monitors IGMP Query and Report messages; it can also actively send IGMP Query messages to learn locations of multicast routers/switches and member hosts in multicast groups within each VLAN.

However, note that IGMP neither alters nor routes any IP multicast packets. Since IGMP is not concerned with the delivery of IP multicast packets across subnetworks, an external IP multicast router is needed if IP multicast packets have to be routed across different subnetworks.

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.

Accton provides AccView/Open network management software for free with all of its manageable products. AccView/Open contains a complete management platform, including network discovery, mapping, event manager, log manager, MIB browser, RMON analysis tools, and device management modules. Accton can also provide optional plug-in device management modules for HP OpenView software.

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). Accton's AccView network management software can access the probes embedded in recent Accton network products to perform traffic analysis, troubleshoot network problems, evaluate historical trends, or implement pro-active 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 pro-active policies that can keep your network running based on real-time access to key statistical information.

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

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

History: Can be used to create a record of network utilization, packet types, errors and collisions. You need a historical record of activity to be able to track down intermittent 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

Refer to the Quick Installation Guide for a more detailed listing of troubleshooting procedures. However, if you have trouble making a connection to the agent module, then please refer to the following section.

Console Connection

If you cannot access the on-board configuration program via a serial port, be sure to have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity and 19200 bps. Also check that the null-modem serial cable conforms to the pin-out connections provided in Appendix B. If you forgot or lost the password, contact Accton Technical Support for help.

In-Band Connection

You can access the management agent on the switch from anywhere within the attached network using Telnet, a Web browser, or other network management software such as AccView. However, you must first configure the switch with a valid IP address, subnet mask, and default gateway. If you have trouble establishing a link to the management agent, check to see if you have a valid network connection. Then verify that you entered the correct IP address. Also, be sure the port through which you are connecting to the switch has not been disabled. If it has not been disabled, then check the network cabling that runs between your remote location and the switch.

Note: Up to four Telnet connections are supported.

Upgrading Firmware via the Serial Port

You can upgrade system firmware by connecting your computer to the serial port on the agent module, and using a console interface package that supports the XModem protocol. (See Making Connections for System Configuration on page 1-2.)

1. Restart the system by using the Restart System command.
2. When the system initialization screen appears as shown below, press “Ctrl+G” to download system firmware, and then indicate the code type (1: Runtime, 2: POST, 3: Mainboard).

```
(c)Copyright 2000, Accton Inc.
CheetahSwitch Workgroup-4508
LOADER Version V01.00.01
POST   Version V01.00.01

------ Performing the Power-On Self Test (POST) ------
EPROM Checksum Test ..................... PASS
Testing the System SDRAM ................ PASS
CPU Self Test ........................... PASS
EEPROM Checksum Test .................... PASS
SEEPROM Checksum Test ................... PASS
MAC Address ..............00-e0-29-52-28-00
------------ Power-On Self Test Completed ------------

(D)ownload System Image or (S)tart Application: [S]
Select the Firmware Type to Download (1)Runtime (2)POST (3)Mainboard
[1]:
```

For example, if you select 1 (for downloading agent firmware), the system will display the following message:

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

Select the Firmware Type to Download (1)Runtime (2)POST
(3)Mainboard [1]: 1
Your Selection: Runtime Code
Download code to FlashROM address 0x02880000
Change Baud Rate to 115200 and Press <ENTER> to Download.
```

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

   Notes: If you use Windows HyperTerminal, disconnect  and reconnect  to enable the new baud rate.

   The download file should be an ES4508 binary file from Accton; otherwise the agent will not accept it. The file naming convention is:

   Runtime program: Agent-Vx.yz,
   POST program: Boot-Vx.yx, and
   Mainboard program: 8051-Vx.yz

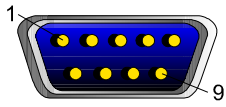
4. After the file has been downloaded, the console screen will display information similar to that shown below. Press “s” to start the management interface, change the baudrate back to 19200, and press Enter. The Logon screen will then appear

```
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] s
Change Baud Rate to 19200 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

DB9 Serial Port Pin Description



The DB9 serial port on the switch's rear panel is used to connect the switch to a management device. The on-board menu-driven configuration program can be accessed from a terminal, a PC running a terminal emulation program, or from a remote location via a modem connection. You can use the management port to configure port settings (e.g., enabled or disabled), or to update device firmware. The pin assignments used to connect various device types to the switch's management port are provided in the following tables.

DB9 Port Pin Assignments

EIA Circuit	CCITT Signal	Description	Switch's DB9 DTE Pin #	PC DB9 DTE Pin #	Modem DB25 DCE Pin #	Signal Direction DTE-DCE
CF	109	**DCD** (Data Carrier Detected)	1	1	8	<---------
BB	104	**RxD** (Received Data)	2	2	3	<---------
BA	103	**TxD** (Transmitted Data)	3	3	2	--------->
CD	108.2	**DTR** (Data Terminal Ready)	4	4	20	--------->
AB	102	**SG** (Signal Ground)	5	5	7	---------
CC	107	**DSR** (Data Set Ready)	6	6	6	<---------
CA	105	**RTS** (Request-to-Send)	7	7	4	--------->
CB	106	**CTS** (Clear-to-Send)	8	8	5	<---------
CE	125	**RI** (Ring Indicator)	9	9	22	<---------

Connection from Switch's Serial Port to PC's 9-Pin COM Port

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

Connection from Switch's Serial Port to Modem's 25-Pin DCE Port

Switch's 9-Pin Serial Port	CCITT Signal	Modem's 25-Pin COM Port
1	<------ DCD -------	8
2	<------ RXD -------	3
3	-------- TXD ------>	2
4	-------- DTR ------>	20
5	-------- SGND -----	7
6	<------ DSR -------	6
7	-------- RTS ------>	4
8	<------ CTS -------	5
9	<------ RI -------	22

Connection from Switch's Serial Port to PC's 25-Pin DTE Port

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

ES4508
E022000-R01
150065-102