Edge-corE

Powered by Accton

ES4324
24-Port Gigabit
Web-Smart Switch

Management Guide

www.edge-core.com

Management Guide

24-Port Gigabit Web-Smart Switch

with 24 1000BASE-T (RJ-45) Ports,
and 4 Combination (RJ-45/SFP) Ports

ES4324
E082007-AP-R02
149100031800A

Contents

Tables

Figures

Chapter 1: Introduction

This switch provides a broad range of features for Layer 2 switching. It includes a management agent that allows you to configure the features listed in this manual. The default configuration can be used for most of the features provided by this switch. However, there are many options that you should configure to maximize the switch's performance for your particular network environment.

Key Features

Table 1-1 Key Features

Feature	Description
Authentication	web – password SNMP – Community strings Port – IEEE 802.1X, MAC address filtering
Access Control Lists	Supports up to 8 IP ACLs
DHCP Client	Supported
Port Configuration	Speed, duplex mode and flow control
Rate Limiting	Input and output rate limiting per port
Port Mirroring	One port mirrored to a single analysis port
Port Trunking	Supports up to 8 trunks using static trunking
Broadcast Storm Control	Supported
Static Address	Up to 8K MAC addresses in the forwarding table
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames
Spanning Tree Protocol	Supports standard STP and Rapid Spanning Tree Protocol (RSTP)
Virtual LANs	Up to 255 using IEEE 802.1Q, port-based, or private VLANs
Traffic Prioritization	Default port priority, traffic class map, queue scheduling, IP Precedence or Differentiated Services Code Point (DSCP), and TCP/UDP Port
Multicast Filtering	Supports IGMP snooping and query

Description of Software Features

The switch is a managed Gigabit switch that delivers performance and control to your network. It provides 24 full-duplex 1000BASE-T ports that significantly improve network performance and boost throughput using features configured through a web-based management interface. With 48 Gigabits of throughput bandwidth, this switch provides an effective solution to meeting the growing demands on your network. Some of the management features are briefly described below.

Configuration Backup and Restore – You can save the current configuration settings to a file on the web management station, and later download this file to restore the switch configuration settings.

Authentication – The switch supports port-based user authentication via the IEEE 802.1X protocol. This protocol uses the Extensible Authentication Protocol over LANs (EAPOL) to request user credentials from the 802.1X client, and then verifies the client's right to access the network via an authentication server.

Access Control Lists – ACLs provide packet filtering for IP frames (based on IP address). ACLs can be used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols.

Port Configuration – You can manually configure the speed, duplex mode, and flow control used on specific ports, or use auto-negotiation to detect the connection settings used by the attached device. Use the full-duplex mode on ports whenever possible to double the throughput of switch connections. Flow control should also be enabled to control network traffic during periods of congestion and prevent the loss of packets when port buffer thresholds are exceeded. The switch supports flow control based on the IEEE 802.3x standard.

Rate Limiting – This feature controls the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Port Mirroring – The switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

Port Trunking – Ports can be combined into an aggregate connection. The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail. The switch supports up to eight trunks.

Broadcast Storm Control – Broadcast suppression prevents broadcast traffic from overwhelming the network. When enabled on a port, the level of broadcast traffic passing through the port is restricted. If broadcast traffic rises above a pre-defined threshold, it will be throttled until the level falls back beneath the threshold.

Static Addresses – A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table. Static addresses can be used to provide network security by restricting access for a known host to a specific port.

IEEE 802.1D Bridge – The switch supports IEEE 802.1D transparent bridging. The address table facilitates data switching by learning addresses, and then filtering or forwarding traffic based on this information. The address table supports up to 8K addresses.

Store-and-Forward Switching – The switch copies each frame into its memory before forwarding them to another port. This ensures that all frames are a standard Ethernet size and have been verified for accuracy with the cyclic redundancy check (CRC). This prevents bad frames from entering the network and wasting bandwidth.

To avoid dropping frames on congested ports, the switch provides 8 MB for frame buffering. This buffer can queue packets awaiting transmission on congested networks.

Spanning Tree Algorithm – The switch supports these spanning tree protocols:

Spanning Tree Protocol (STP, IEEE 802.1D) – This protocol provides loop detection and recovery by allowing two or more redundant connections to be created between a pair of LAN segments. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.

Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) – This protocol reduces the convergence time for network topology changes to 3 to 5 seconds, compared to 30 seconds or more for the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

Virtual LANs – The switch supports up to 255 VLANs. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Ports can be manually assigned to a specific set of VLANs. This allows the switch to restrict traffic to the VLAN groups to which a user has been assigned. By segmenting your network into VLANs, you can:

- Eliminate broadcast storms which severely degrade performance in a flat network.
- Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection.
- Provide data security by restricting all traffic to the originating VLAN.

Traffic Prioritization – This switch prioritizes each packet based on the required level of service, using four priority queues with strict or Weighted Round Robin Queuing. It uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application. These functions can be used to provide independent priorities for delay-sensitive data and best-effort data.

This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic can be prioritized based on the priority bits in the IP frame’s Type of Service (ToS) octet or the number of the TCP/UDP port. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Multicast Filtering – Specific multicast traffic can be assigned to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The switch uses IGMP Snooping and Query to manage multicast group registration.

System Defaults

To reset the switch defaults:

1. Remove the power cord from the back of the switch.
2. Remove all cables from the front-panel ports.
3. Use a standard network cable to connect port 1 to port 2 on the front panel.
4. Reconnect the power cord to the switch.
5. Wait at least 40 seconds before disconnecting port 1 from port 2.

The following table lists some of the basic system defaults.

Table 1-2 System Defaults

Function	Parameter	Default
Authentication	Web Management	Password “admin“
	802.1X Port Authentication	Disabled
	Port Security	Disabled
	IP Filtering	Disabled
SNMP	SNMP Agent	Enabled
	Community Strings	“public” (read only) “private” (read/write)
	Traps	Enabled
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Rate Limiting	Input and output limits	Disabled
Port Trunking	Static Trunks	None
Broadcast Storm Protection	Status	Disabled (all ports)
	Broadcast Limit Rate	1K frames per second
Spanning Tree Protocol	Status	Disabled (all ports) (Defaults: All values based on IEEE 802.1w)
	Fast Forwarding (Edge Port)	Enabled
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All

Table 1-2 System Defaults (Continued)

Function	Parameter	Default
Traffic Prioritization	Queue Mode	Strict
	QoS Mode	Disabled
IP Settings	IP Address	192.168.2.10
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	DHCP	Client: Enabled
Multicast Filtering	IGMP Snooping	Snooping: Enabled Querier: Disabled

Chapter 2: Initial Configuration

To make use of the management features of your switch, you must first configure it with an IP address that is compatible with the network it is being installed in. This should be done before you permanently install the switch in the network.

Follow this procedure:

1. Place your switch close to the PC that you intend to use for configuration. It helps if you can see the front panel of the switch while working on your PC.

2. Connect the Ethernet port of your PC to any port on the front panel of your switch. Connect power to the switch and verify that you have a link by checking the front-panel LEDs.

3. Check that your PC has an IP address on the same subnet as the switch. The default IP address of the switch is 192.168.2.10 and the subnet mask is 255.255.255.0, so the PC and switch are on the same subnet if they both have addresses that start 192.168.2.x. If the PC and switch are not on the same subnet, you must manually set the PC’s IP address to 192.168.2.x (where “x” is any number from 1 to 255, except 10). If you are unfamiliar with this process, see “Changing a PC’s IP Address” on page 2-2.

4. Open your web browser and enter the address http://192.168.2.10. If your PC is properly configured, you will see the login page of your switch. If you do not see the login page, repeat step 3.

5. Enter the default password “admin” and click on the Login button.

6. From the menu, click on SYSTEM, then click on LAN Settings. On the LAN Settings page, enter the new IP address, Subnet Mask and Gateway IP Address for the switch, then click on the APPLY button.

No other configuration changes are required at this stage, but it is recommended that you change the administrator’s password before logging out. To change the password, click SYSTEM, Password, and then fill in all the fields on the Password Settings page before clicking on the APPLY button.

Changing a PC’s IP Address

To change the IP address of a Windows 2000 PC:

1. Click Start, Settings, then Network and Dial-up Connections.
2. For the IP address you want to change, right-click the network connection icon, and then click Properties.
3. In the list of components used by this connection on General tab, select Internet Protocol (TCP/IP), and then click the Properties button.
4. In the Internet Protocol (TCP/IP) Properties dialog box, click to select Use the following IP address. Then type your intended IP address, Subnet mask, and Default gateway in the provided text boxes.
5. Click OK to save the changes.

To change the IP address of a Windows XP PC:

1. Click Start, Control Panel, then Network Connections.
2. For the IP address you want to change, right-click the network connection icon, and then click Properties.
3. In the list of components used by this connection on General tab, select Internet Protocol (TCP/IP), and then click the Properties button.
4. In the Internet Protocol (TCP/IP) Properties dialog box, click to select Use the following IP address. Then type your intended IP address, Subnet mask, and Default gateway in the provided text boxes
5. Click OK to save the changes.

For users of systems other than Windows 2000 or Windows XP, refer to your system documentation for information on changing the PC’s IP address.

Chapter 3: Configuring the Switch

Using the Web Interface

This switch provides an embedded HTTP Web agent. Using a Web browser you can configure the switch and view statistics to monitor network activity. The Web agent can be accessed by any computer on the network using a standard Web browser (Internet Explorer 5.0 or above, or Firefox v1.5 or above).

Prior to accessing the switch from a Web browser, be sure you have performed the tasks in the Initial Configuration chapter.

Notes: **1.** You are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

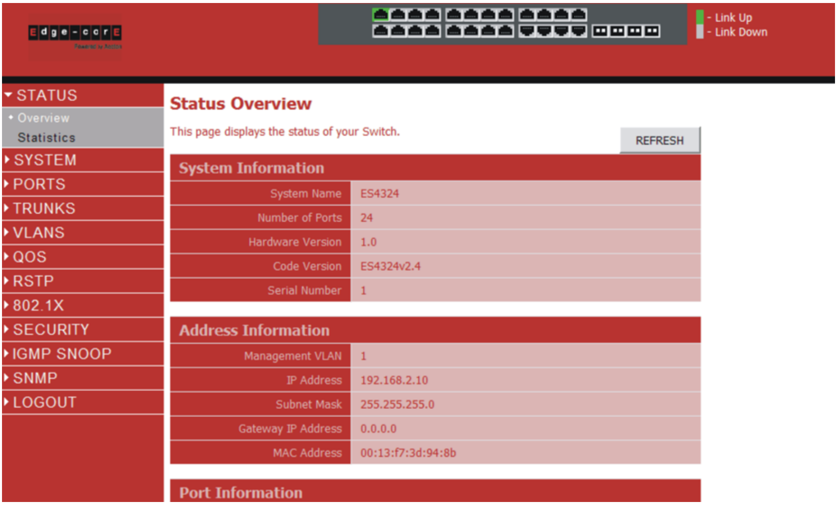
2. If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Algorithm, then you can set the switch port attached to your management station to fast forwarding (i.e., enable Edge Port) to improve the switch's response time to management commands issued through the web interface. See "RSTP Port Configuration" on page 3-33.

Navigating the Web Browser Interface

To access the web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name and password for the administrator is "admin."

Home Page

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



Status Overview

This page displays the status of your Switch.

System Information

System Name	ES4324
Number of Ports	24
Hardware Version	1.0
Code Version	ES4324v2.4
Serial Number	1

Address Information

Management VLAN	1
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
MAC Address	00:13:f7:3d:94:8b

Port Information

Figure 3-1 Home Page

Configuration Options

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

Table 3-1 Configuration Options

Button	Action.
Revert	Cancels specified values and restores current values prior to pressing Apply.
Apply	Sets specified values to the system.
Help	Links directly to webhelp.

Notes: **1.** To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu "Tools / Internet Options / General / Temporary Internet Files / Settings," the setting for item "Check for newer versions of stored pages" should be "Every visit to the page."

2. When using Internet Explorer 5.0, you may have to manually refresh the screen after making configuration changes by pressing the browser's refresh button.

Panel Display

The web agent displays an image of the switch's ports. The switch ports display green when they have a valid link to another device.

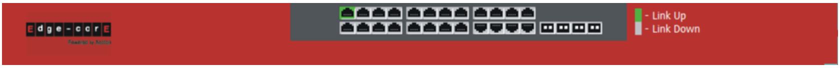


Figure 3-2 Panel Display

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions. The following table briefly describes the selections available from this program.

Table 3-2 Main Menu

Menu	Description	Page
STATUS		3-6
Overview	Provides a basic system description, including system name, IP address, port, trunk, and VLAN information.	3-6
Statistics	Shows interface and RMON statistics for the selected port.	3-9
SYSTEM		3-12
Name	Shows the name of the switch.	3-12
LAN Settings	Sets the LAN IP address, subnet mask, and gateway IP address.	3-12
Password	Changes the password.	3-13
Tools		3-14
Restore to Factory Defaults	Force the switch to perform a power reset and restore the original factory settings.	3-14
Upgrade Firmware	Upgrade the switch system firmware using a file provided by Edgecore.	3-15
Upload/Download Configuration	Select to upload or download the switch system configuration file.	3-15
Set Boot Image	Select one of two software image files to run on the switch.	3-16
Restart	Restarts the switch.	3-16
Static MAC	Adds static MAC addresses to the switch MAC address table.	3-16
Counter Config	Selects traffic statistics you want to monitor.	3-17
PORTS		3-19
Settings	Configure the speed and duplex mode of ports.	3-19
Rate Limiting	Sets the rate limiting parameters for ports.	3-19
Storm Control	Sets the broadcast storm control parameters.	3-21
Port Mirroring	Sets up the port mirroring features of the switch to enable traffic monitoring.	3-22
Cable Diagnostic	Diagnoses cable faults.	3-23
TRUNKS		3-23
Membership	Selects ports to group into static trunks.	3-25
Settings	Configures trunk connection settings.	3-25
Rate Limiting	Sets the rate limiting parameters for trunks.	3-25
VLANS		3-26

Table 3-2 Main Menu (Continued)

Menu	Description	Page
VLAN Port Config	Configures VLAN behavior for individual ports and trunks.	3-26
VLAN Membership	Configure VLAN port groups.	3-28
QOS		3-29
Settings	Sets the priority of packets forwarded through the switch.	3-29
RSTP		3-32
Settings	Configures Spanning Tree parameters.	3-32
Status	Shows Spanning Tree bridge and port status.	3-34
802.1X		3-34
Settings	Sets up 802.1X port authentication.	3-35
Statistics	Displays the 802.1X statistics collected by the switch.	3-36
Security		3-37
IP Filter	Sets up port IP control filters.	3-37
Port Security	Sets security policy for port.	3-38
ACL	Sets up management access filter.	3-40
IGMP Snoop		3-41
Settings	Sets up IGMP Snooping configuration.	3-42
Status	Shows IGMP Snooping instances and port states.	3-42
SNMP		3-43
Settings	Enables and configures SNMP.	3-43
LOGOUT	Quits to the Login page.	

Basic Information

Displaying System Information

You can easily identify the system by displaying the device name, location and contact information.

Field Attributes

System Information

- **System Name** – Name assigned to the switch system.
- **Number of Ports** – Number of built-in ports.
- **Hardware Version** – Hardware version of the main board.
- **Code Version** – Version number of the code.
- **Serial Number** – The serial number of the switch.

Address Information

- **Management VLAN** – ID of the configured VLAN (this is set to 1 and cannot be changed) all ports on the unit are members of VLAN 1. The management station must always be attached to a port on VLAN 1.
- **IP Address** – Address of the VLAN to which the management station is attached. (Note that the management station must always be on VLAN 1. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods.
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.255.255.0)
- **Gateway IP Address** – IP address of the gateway router between the switch and management stations that exist on other network segments. (Default: 0.0.0.0)
- **MAC Address** – The physical layer address of the switch.

Port Information

- **Type** – Indicates the port type.
- **Link Status** – Indicates if the link is Up or Down.
- **Speed/Duplex Status** – Shows the current speed and duplex mode.
  - **10hdx**: 10 Mbps half duplex.
  - **10fdx**: 10 Mbps full duplex.
  - **100hdx**: 100 Mbps half duplex.
  - **100fdx**: 100 Mbps full duplex.
  - **1000fdx**: 1000 Mbps full duplex.
- **Flow Control Status** – Indicates whether flow control is enabled or disabled. (IEEE 802.3x, or Back-Pressure)
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Frame Type** – Either “Tagged” or “All.” “Tagged” means that the port will only receive VLAN-tagged packets. When set to “All,” the port will also receive untagged packets.

- **PVID** - The VLAN ID assigned to untagged frames received on the interface. Outgoing frames are tagged unless the frame’s VLAN ID is the same as the PVID. When the PVID is set to “None,” all outgoing frames are tagged. (Default: 1)

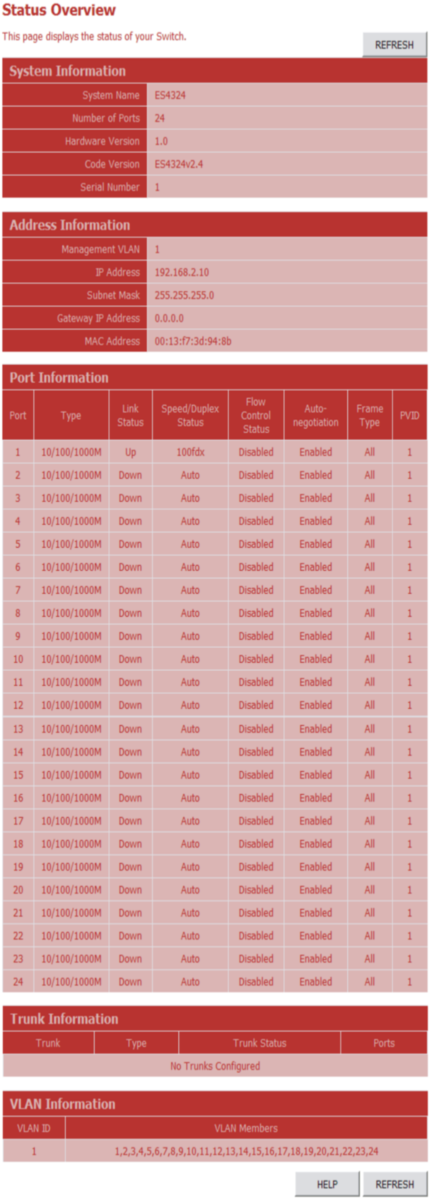
Trunk Information

- **Trunk** – The trunk label. “T1” through “T8” are used as trunk labels.
- **Type** – All trunks and ports on this switch are 10/100/1000Mbps
- **Trunk Status** – Indicates the speed and duplex setting of the trunk. This can be changed on the TRUNKS > Settings page.
  - **10hdx**: 10 Mbps half duplex.
  - **10fdx**: 10 Mbps full duplex.
  - **100hdx**: 100 Mbps half duplex.
  - **100fdx**: 100 Mbps full duplex.
  - **1000fdx**: 1000 Mbps full duplex.
- **Ports** – The ports that are members of the trunk.

VLAN Information

- **VLAN** ID – A number in the range 1 - 4094 which identifies the VLAN.
- **VLAN Member** – A list of the ports that are members of the VLAN. By default, all ports are members of VLAN 1.

Web – Click STATUS, Overview.



Status Overview

This page displays the status of your Switch.

System Information	
System Name	ES4324
Number of Ports	24
Hardware Version	1.0
Code Version	ES4324v2.4
Serial Number	1

Address Information	
Management VLAN	1
IP Address	192.168.2.10
Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
MAC Address	00:13:f7:3d:94:8b

Port Information

Port	Type	Link Status	Speed/Duplex Status	Flow Control Status	Auto-negotiation	Frame Type	PVID
1	10/100/1000M	Up	100fdx	Disabled	Enabled	All	1
2	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
3	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
4	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
5	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
6	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
7	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
8	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
9	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
10	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
11	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
12	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
13	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
14	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
15	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
16	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
17	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
18	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
19	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
20	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
21	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
22	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
23	10/100/1000M	Down	Auto	Disabled	Enabled	All	1
24	10/100/1000M	Down	Auto	Disabled	Enabled	All	1

Trunk Information

Trunk	Type	Trunk Status	Ports
No Trunks Configured			

VLAN Information

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

Figure 3-3 System Information

Showing Port Statistics

You can display statistics on network traffic from the ports. These statistics can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). All values displayed have been accumulated since the last system reboot, but can be reset to zero by clicking the CLEAR button. The current statistics are not displayed until you click the REFRESH button.

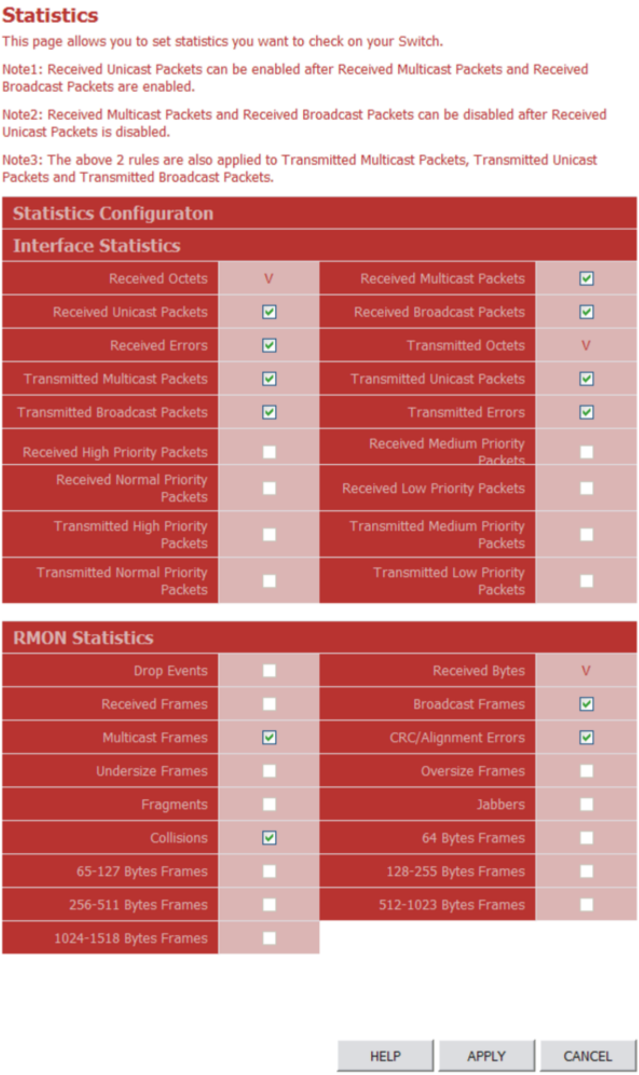
Table 3-3 Port Statistics

Parameter	Description
Interface Statistics	
Received Octets	The total number of octets received on the interface, including framing characters.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmitted Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Transmitted Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Received High Priority Packets	The total number of received packets that set as High Priority in the QoS settings.
Transmitted High Priority Packets	The total number of transmitted packets that set as High Priority in the QoS settings.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Transmitted Octets	The total number of octets transmitted out of the interface, including framing characters.
Transmitted Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Transmitted Errors	The number of outbound packets that could not be transmitted because of errors.
Received Normal Priority Packets	The total number of received packets that set as High Priority in the QoS settings.
Transmitted Normal Priority Packets	The total number of transmitted packets that set as High Priority in the QoS settings.

Table 3-3 Port Statistics

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

Web – Click STATUS, Statistics.



Statistics

This page allows you to set statistics you want to check on your Switch.

Note1: Received Unicast Packets can be enabled after Received Multicast Packets and Received Broadcast Packets are enabled.

Note2: Received Multicast Packets and Received Broadcast Packets can be disabled after Received Unicast Packets is disabled.

Note3: The above 2 rules are also applied to Transmitted Multicast Packets, Transmitted Unicast Packets and Transmitted Broadcast Packets.

Statistics Configuraton

Interface Statistics

Received Octets	V	Received Multicast Packets	☑
Received Unicast Packets	☑	Received Broadcast Packets	☑
Received Errors	☑	Transmitted Octets	V
Transmitted Multicast Packets	☑	Transmitted Unicast Packets	☑
Transmitted Broadcast Packets	☑	Transmitted Errors	☑
Received High Priority Packets	□	Received Medium Priority Packets	□
Received Normal Priority Packets	□	Received Low Priority Packets	□
Transmitted High Priority Packets	□	Transmitted Medium Priority Packets	□
Transmitted Normal Priority Packets	□	Transmitted Low Priority Packets	□

RMON Statistics

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

Figure 3-4 Port Statistics

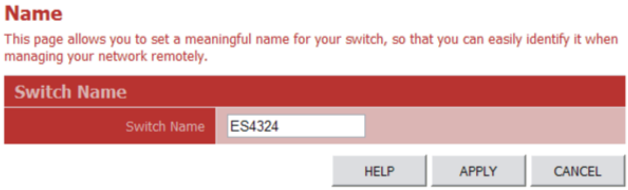
Displaying the System Name

You can identify the system by displaying the device name.

Field Attributes

- **Switch Name** – A name assigned to the switch system.

Web – Click System, Name.



Name

This page allows you to set a meaningful name for your switch, so that you can easily identify it when managing your network remotely.

Switch Name

Switch Name: ES4324

Figure 3-5 System Name

Setting the Switch’s IP Address

This section describes how to configure an IP interface for management access over the network. The IP address for this switch is 192.168.2.10 by default. To manually configure an address, you need to change the switch’s default settings (IP address 192.168.2.10 and netmask 255.255.255.0) to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment.

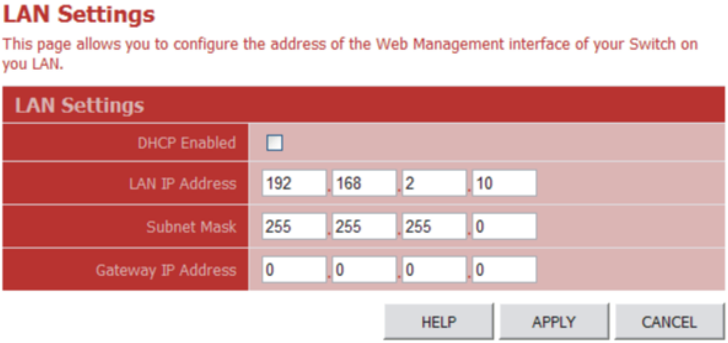
Field Attributes

- **DHCP Enabled** – Check the box to enable DHCP. (default: enabled)
- **LAN IP Address** – Address of the VLAN interface that is allowed management access. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default : 192.168.2.10)
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.255.255.0)
- **Gateway IP Address** – IP address of the gateway router between this device and management stations that exist on other network segments. (Default: 0.0.0.0)

Note: If you cannot remember the switch’s IP address, you can restore the original settings by following the procedure described in “System Defaults” on page 1-5.

Manual Configuration

Web – Click System, LAN Settings. Enter the IP address, subnet mask and gateway, then click APPLY. Note that if you change the switch IP address, you must close the web interface and start a new session using the new IP address.



LAN Settings

This page allows you to configure the address of the Web Management interface of your Switch on you LAN.

LAN Settings				
DHCP Enabled	□			
LAN IP Address	192	168	2	10
Subnet Mask	255	255	255	0
Gateway IP Address	0	0	0	0

Figure 3-6 LAN Settings

Configuring the Logon Password

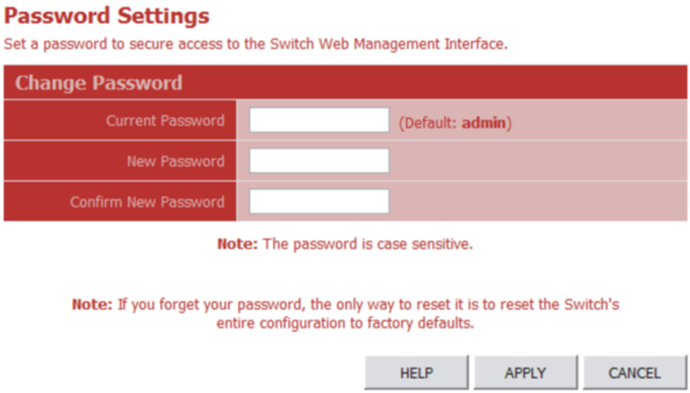
The administrator has write access for all parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place.

Field Attributes

- **Password** – Specifies the user password.
(Range: 1-16 characters plain text, case sensitive)

Note: If you cannot remember the password, you can restore the original settings by following the procedure described in “System Defaults” on page 1-5.

Web – Click System, Password. To change the password for the administrator, enter current password, the new password, confirm it by entering it again, then click APPLY.



Password Settings

Set a password to secure access to the Switch Web Management Interface.

Change Password	
Current Password	(Default: admin)
New Password	
Confirm New Password	

Note: The password is case sensitive.

Note: If you forget your password, the only way to reset it is to reset the Switch's entire configuration to factory defaults.

Figure 3-7 Password Settings

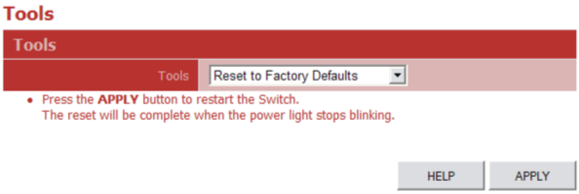
Tools

On the Tools page, you can restore the switch to default settings, upgrade the firmware of the switch, or restart the switch.

Restore to Factory Defaults

Forces the switch to restore the original factory settings. To reset the switch, select “Reset to Factory Defaults” from the drop-down list and click APPLY. The LAN IP Address, Subnet Mask and Gateway IP Address will not be reset.

Web – Click System, Tools, Reset to Factory Defaults.



Tools

Tools	
Tools	Reset to Factory Defaults

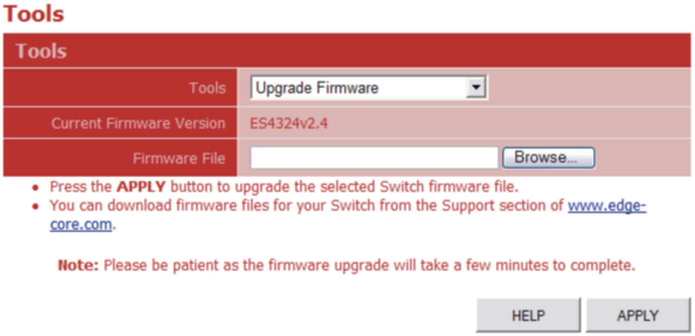
- Press the **APPLY** button to restart the Switch.
  The reset will be complete when the power light stops blinking.

Figure 3-8 Reset to Factory Defaults

Upgrade Firmware

Upgrades the switch system firmware using a file provided by Edgecore. Select “Upgrade Firmware” from the Tools drop-down list, then click on the “Browse” button to select the firmware file. Click the APPLY button to upgrade the selected switch firmware file. You can download firmware files for your switch from the Support section of the Edgecore web site at www.edge-core.com.

Web – Click System, Tools, Reset to Factory Defaults.



Tools

Tools	
Tools	Upgrade Firmware ▾
Current Firmware Version	ES4324v2.4
Firmware File	Browse...

- Press the **APPLY** button to upgrade the selected Switch firmware file.
- You can download firmware files for your Switch from the Support section of www.edge-core.com.

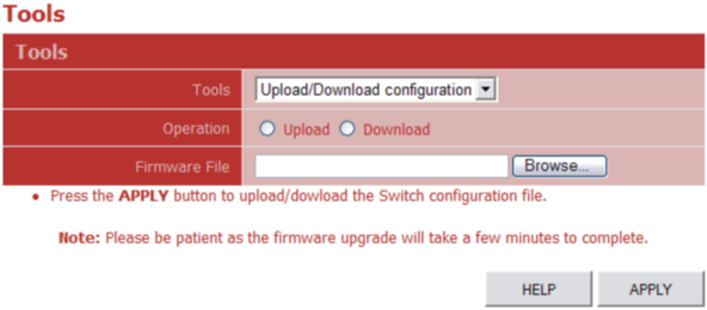
Note: Please be patient as the firmware upgrade will take a few minutes to complete.

Figure 3-9 Upgrade Firmware

Upload/Download Configuration

The Upload/Download Configuration feature allows you to save the switch’s current configuration or restore a previously saved configuration back to the device. Configuration files can be saved to any location on the web management station.

Web – Click SYSTEM, Tools, Upload/Download Configuration. To upload or download the configuration file, select “Upload/Download Configuration” from the Tools drop-down list, then select "Upload" to save a configuration or "Download" to restore a configuration. Use the Browse button to choose a file location on the web management station, or to find a saved configuration file.



Tools

Tools	
Tools	Upload/Download configuration ▾
Operation	○ Upload ○ Download
Firmware File	Browse...

- Press the **APPLY** button to upload/dowload the Switch configuration file.

Note: Please be patient as the firmware upgrade will take a few minutes to complete.

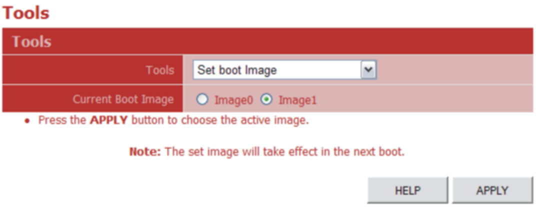
Figure 3-10 Upload/Download Configuration

Set Boot Image

Allows you to select one of two software image files to run on the switch. (Default: Image0)

When a new software image file is downloaded to the switch, it replaces the non-active file. For example, if the switch has booted from Image0, the new downloaded file replaces Image1. Also, the new software file is automatically set as the boot image.

Web – Click SYSTEM, Tools, Set Boot Image. Select the software image file to boot after the next switch reset. Click APPLY, then reset the switch.



Tools

Tools

Tools: Set boot Image

Current Boot Image: ○ Image0 ● Image1

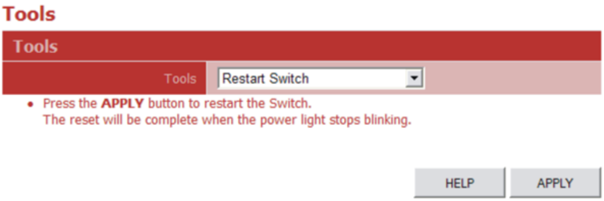
- Press the **APPLY** button to choose the active image.

Note: The set image will take effect in the next boot.

Figure 3-11 Set Boot Image

Restart Switch

Web – Click SYSTEM, Tools, Restart Switch. To restart the switch, select from the Tools drop-down list, and then click APPLY. The reset will be complete when the user interface displays the login page.



Tools

Tools

Tools: Restart Switch

- Press the **APPLY** button to restart the Switch.
  The reset will be complete when the power light stops blinking.

Figure 3-12 Restart Switch

Static MAC

Switches store the MAC addresses for all known devices in the attached network. This information is used to forward traffic directly between the inbound and outbound ports. All the MAC addresses learned by monitoring traffic are stored in a dynamic address table, which removes (ages out) any addresses that are not “seen” for a specified time period .

You can also manually configure static MAC addresses that are assigned to specific ports on the switch. A static MAC address is bound to a specific port and will not be moved or aged out. You can define up to 24 static MAC addresses on the switch.

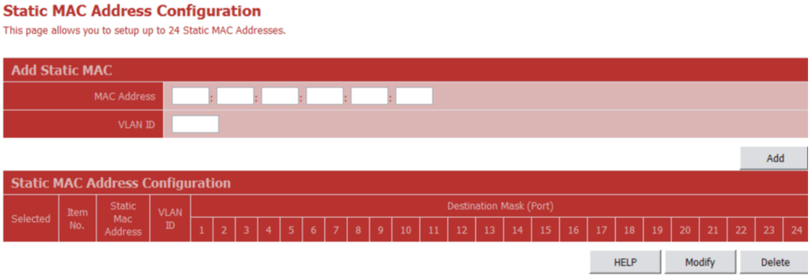
Add Static MAC

Type the static MAC address and associated VLAN ID (1-4095) into corresponding fields in the Add Static MAC table. After clicking the ADD button, a new page opens to configure the Destination Mask for this MAC entry. Only one static MAC address can be added at a time.

Static MAC Address Configuration

This table shows the stored static MAC entries in MAC table.

Web – Click System, Static MAC. Enter the MAC address, VLAN ID, then click ADD button to add a new static MAC address.



Static MAC Address Configuration

This page allows you to setup up to 24 Static MAC Addresses.

Add Static MAC	
MAC Address	__ : __ : __ : __ : __ : __
VLAN ID	__

Static MAC Address Configuration

Selected	Item No.	Static Mac Address	VLAN ID	Destination Mask (Port)																							
				1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

Figure 3-13 Static MAC Address Configuration

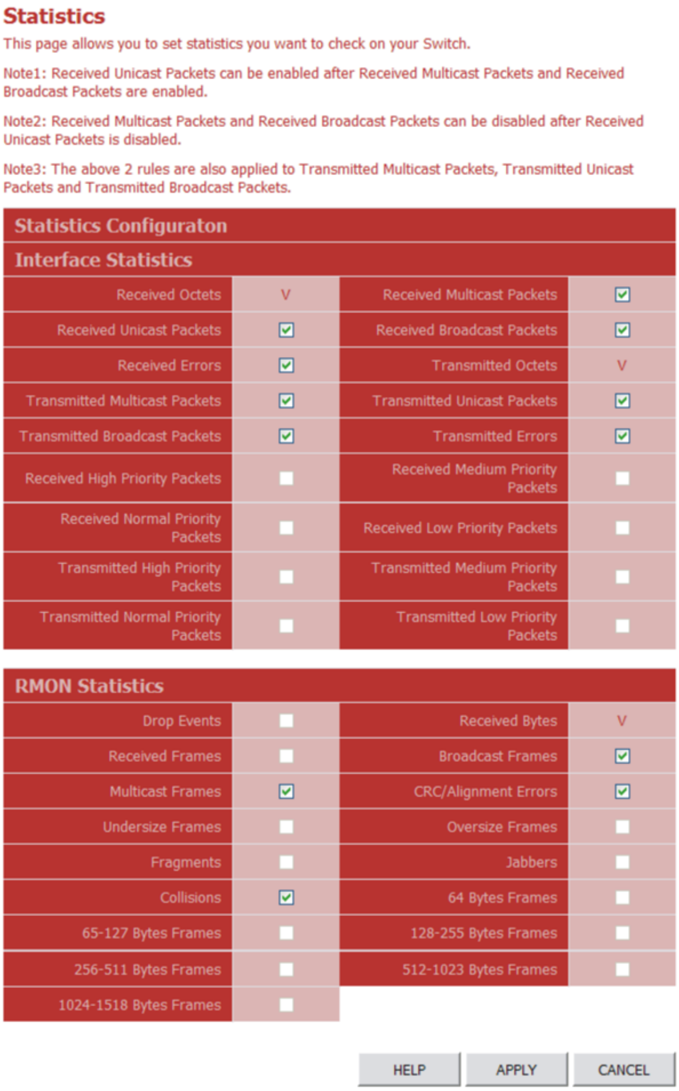
Counter Config

This page allows specific statistics to be selected for monitoring. It is possible to monitor up to five transmit counters and five receive counters, as well as 1 transmit byte counter and receive byte counter.

Please also note the following restrictions.

- Received Unicast Packets can be enabled after Received Multicast Packets and Received Broadcast Packets are enabled.
- Received Multicast Packets and Received Broadcast Packets can be disabled after Received Unicast Packets is disabled.
- The above 2 rules are also applied to Transmitted Multicast Packets, Transmitted Unicast Packets and Transmitted Broadcast Packets.

Web – Click SYSTEM, Counter Config.



Statistics

This page allows you to set statistics you want to check on your Switch.

Note1: Received Unicast Packets can be enabled after Received Multicast Packets and Received Broadcast Packets are enabled.

Note2: Received Multicast Packets and Received Broadcast Packets can be disabled after Received Unicast Packets is disabled.

Note3: The above 2 rules are also applied to Transmitted Multicast Packets, Transmitted Unicast Packets and Transmitted Broadcast Packets.

Statistics Configuraton

Interface Statistics

Received Octets	V	Received Multicast Packets	☑
Received Unicast Packets	☑	Received Broadcast Packets	☑
Received Errors	☑	Transmitted Octets	V
Transmitted Multicast Packets	☑	Transmitted Unicast Packets	☑
Transmitted Broadcast Packets	☑	Transmitted Errors	☑
Received High Priority Packets	□	Received Medium Priority Packets	□
Received Normal Priority Packets	□	Received Low Priority Packets	□
Transmitted High Priority Packets	□	Transmitted Medium Priority Packets	□
Transmitted Normal Priority Packets	□	Transmitted Low Priority Packets	□

RMON Statistics

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

Figure 3-14 Counter Configuration

Ports Configuration

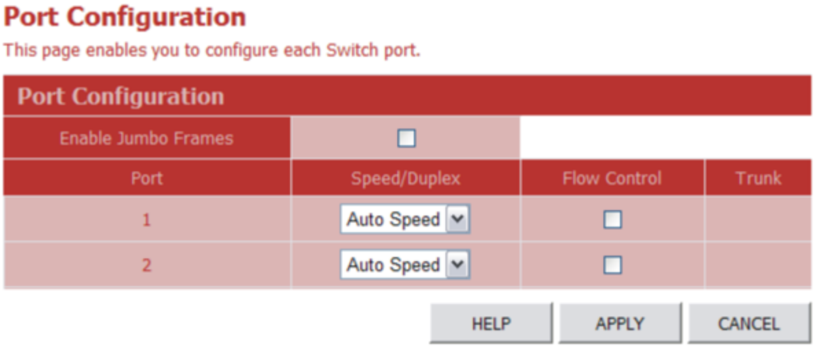
Ports Settings

You can use the Port Configuration page to manually set the speed, duplex mode, and flow control.

Field Attributes

- **Speed/Duplex** – Allows you to manually set the port speed and duplex mode.
- **Flow Control** – Allows flow control to be enabled or disabled. When the box is checked, flow control is enabled.
- **Trunk** – Indicates if a port is a member of a trunk.

Web – Click PORTS, Settings.



Port Configuration

This page enables you to configure each Switch port.

Port Configuration			
Enable Jumbo Frames	□		
Port	Speed/Duplex	Flow Control	Trunk
1	Auto Speed ▾	□	
2	Auto Speed ▾	□	

Figure 3-15 Port Configuration

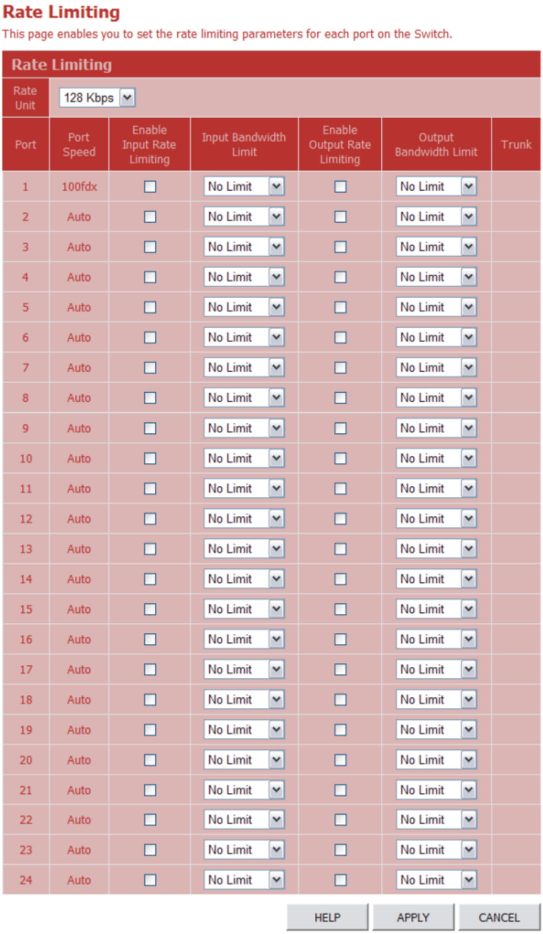
Configuring Rate Limits

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the switch. Traffic that falls within the rate limit is transmitted or received, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

The Input/Output Bandwidth Limit field is a type-in box which accepts an integer number in the range 1 to 100. The number specifies the percentage of the total bandwidth of the port that can be used before packets are dropped or flow-control starts.

Web – Click PORTS, Rate Limiting. This page enables you to set the rate limiting parameters for each port on the switch.



Rate Limiting

This page enables you to set the rate limiting parameters for each port on the Switch.

Rate Limiting

Rate Unit: 128 Kbps

Port	Port Speed	Enable Input Rate Limiting	Input Bandwidth Limit	Enable Output Rate Limiting	Output Bandwidth Limit	Trunk
1	100fdx	☐	No Limit	☐	No Limit	
2	Auto	☐	No Limit	☐	No Limit	
3	Auto	☐	No Limit	☐	No Limit	
4	Auto	☐	No Limit	☐	No Limit	
5	Auto	☐	No Limit	☐	No Limit	
6	Auto	☐	No Limit	☐	No Limit	
7	Auto	☐	No Limit	☐	No Limit	
8	Auto	☐	No Limit	☐	No Limit	
9	Auto	☐	No Limit	☐	No Limit	
10	Auto	☐	No Limit	☐	No Limit	
11	Auto	☐	No Limit	☐	No Limit	
12	Auto	☐	No Limit	☐	No Limit	
13	Auto	☐	No Limit	☐	No Limit	
14	Auto	☐	No Limit	☐	No Limit	
15	Auto	☐	No Limit	☐	No Limit	
16	Auto	☐	No Limit	☐	No Limit	
17	Auto	☐	No Limit	☐	No Limit	
18	Auto	☐	No Limit	☐	No Limit	
19	Auto	☐	No Limit	☐	No Limit	
20	Auto	☐	No Limit	☐	No Limit	
21	Auto	☐	No Limit	☐	No Limit	
22	Auto	☐	No Limit	☐	No Limit	
23	Auto	☐	No Limit	☐	No Limit	
24	Auto	☐	No Limit	☐	No Limit	

Figure 3-16 Rate Limiting

Storm Control

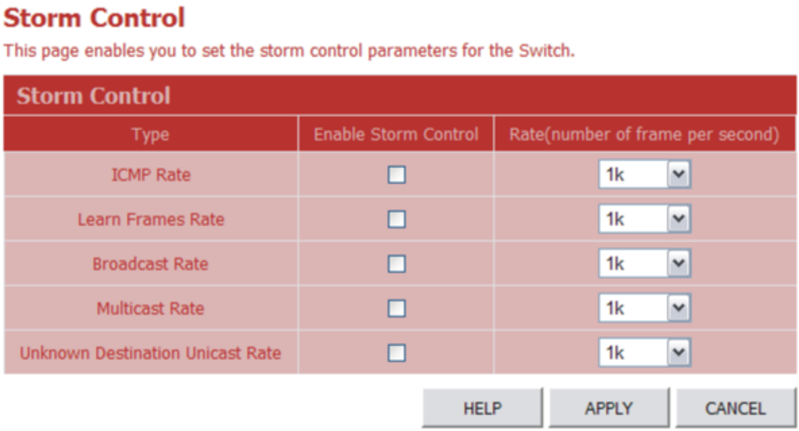
Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then be dropped.

Field Attributes

- **Type** – List the type of traffic which can be rate limited, including ICMP, learn frames, broadcast, multicast and flooded unicast frames.
- **Enable Storm Control** – Click the check box to enable storm control for the specific frame type.
- **Rate(number of frames per second)** – The Rate field is set by a single drop-down list. The same threshold is applied to every port on the switch. When the threshold is exceeded, packets are dropped, irrespective of the flow-control settings.

Web – Click PORTS, Storm Control. This page enables you to set the broadcast storm control parameters for every port on the switch.



Storm Control

This page enables you to set the storm control parameters for the Switch.

Storm Control

Type	Enable Storm Control	Rate(number of frame per second)
ICMP Rate	□	1k
Learn Frames Rate	□	1k
Broadcast Rate	□	1k
Multicast Rate	□	1k
Unknown Destination Unicast Rate	□	1k

Figure 3-17 Port Broadcast Control

Port Mirroring

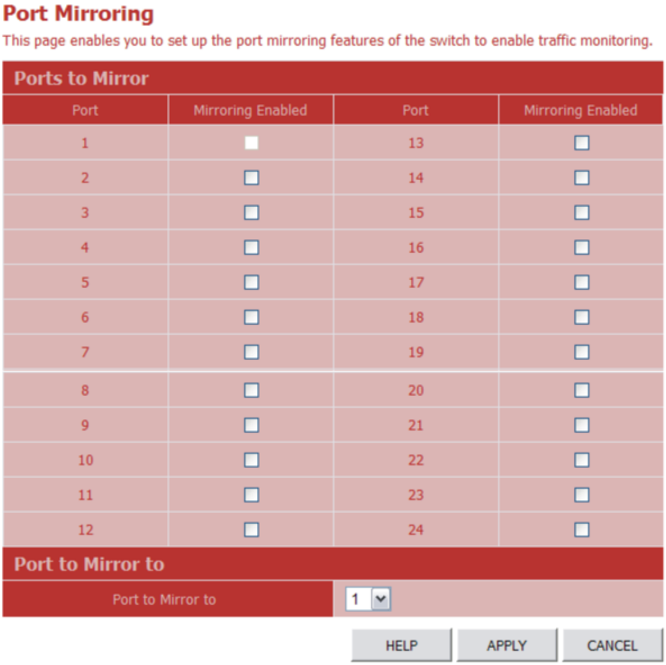
You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.

Field Attributes

- **Ports to Mirror** - Select the ports that you want to mirror from this section of the page. A port will be mirrored when the “Mirroring Enabled” check-box is checked.
- **Port to Mirror to** – The port that will “duplicate” or “mirror” the traffic on the source port. Only incoming packets can be mirrored. Packets will be dropped when the available egress bandwidth is less than ingress bandwidth.

Note: If the total ingress bandwidth exceeds the mirror port’s egress bandwidth, packets will eventually be dropped on ingress to the switch, which means they will not reach the mirror port or their intended destination port. Input rate-limiting in conjunction with port flow-control should be used to ensure that the total ingress bandwidth never exceeds the egress bandwidth.

Web – Click PORTS, Port Mirroring.



Port Mirroring

This page enables you to set up the port mirroring features of the switch to enable traffic monitoring.

Ports to Mirror

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

Port to Mirror to

Port to Mirror to: 1

Figure 3-18 Port Mirroring

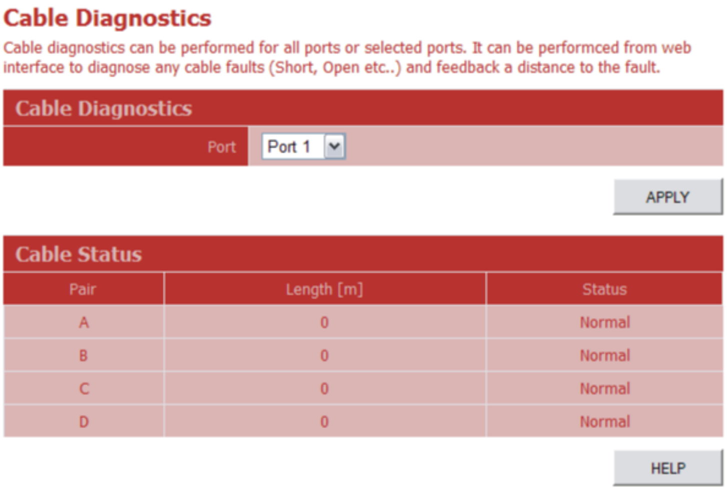
Cable Diagnostic

You can perform cable diagnostics for all ports or selected ports to diagnose any cable faults (short, open etc..) and feedback a distance to the fault.

Field Attributes

- **Cable Diagnostics** – Cable diagnostics is performed on a per-port basis. Select the port number from the drop-down list.
- **Cable Status** – Shows the cable length, operating conditions and isolates a variety of common faults that can occur on Category 5 twisted pair cabling.

Web – Click PORTS, Port Mirroring.



Cable Diagnostics

Cable diagnostics can be performed for all ports or selected ports. It can be performced from web interface to diagnose any cable faults (Short, Open etc..) and feedback a distance to the fault.

Cable Diagnostics

Port: Port 1

Cable Status

Pair	Length [m]	Status
A	0	Normal
B	0	Normal
C	0	Normal
D	0	Normal

Figure 3-19 Cable Diagnostics

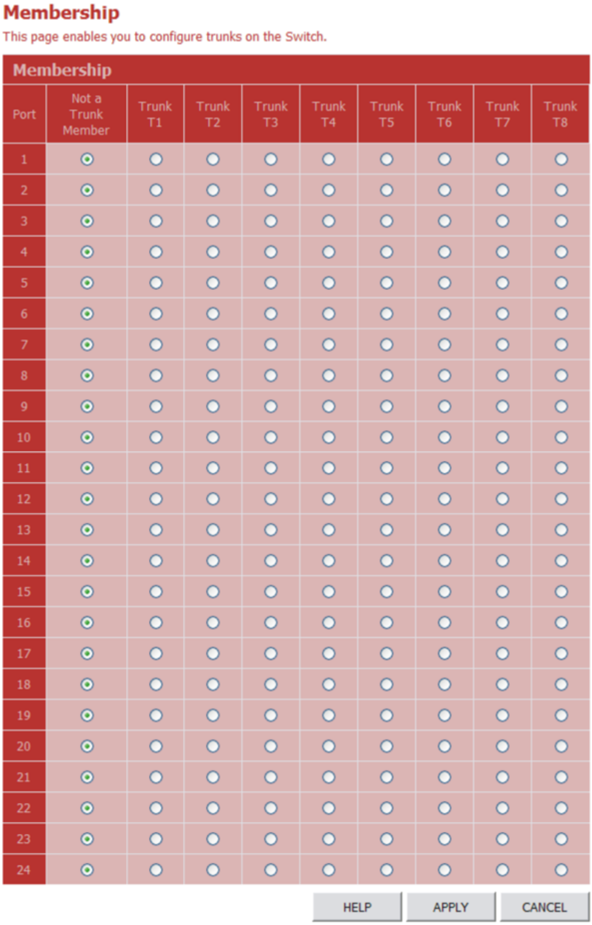
Trunk Membership

This page allows you to create a maximum of eight trunks of up to eight ports each. The Membership Table has one row for each port and ten columns. Each row contains nine radio buttons which are used to indicate which trunk (if any) the port belongs to.

Field Attributes

- **Port** – The front panel port number.
- **Not a Trunk Member** – If the radio button in this column is selected, the port is not a member of any trunks. This is the default state.
- **Trunk T1-T8** – These columns correspond to the eight trunks that are supported by the switch. To assign a port to a trunk, click on the radio button in the corresponding column, then click APPLY.

Web – Click TRUNKS, Membership. To assign a port to a trunk, click the required trunk number, then click APPLY.



Membership

This page enables you to configure trunks on the Switch.

Membership

Port	Not a Trunk Member	Trunk T1	Trunk T2	Trunk T3	Trunk T4	Trunk T5	Trunk T6	Trunk T7	Trunk T8
1	●	○	○	○	○	○	○	○	○
2	●	○	○	○	○	○	○	○	○
3	●	○	○	○	○	○	○	○	○
4	●	○	○	○	○	○	○	○	○
5	●	○	○	○	○	○	○	○	○
6	●	○	○	○	○	○	○	○	○
7	●	○	○	○	○	○	○	○	○
8	●	○	○	○	○	○	○	○	○
9	●	○	○	○	○	○	○	○	○
10	●	○	○	○	○	○	○	○	○
11	●	○	○	○	○	○	○	○	○
12	●	○	○	○	○	○	○	○	○
13	●	○	○	○	○	○	○	○	○
14	●	○	○	○	○	○	○	○	○
15	●	○	○	○	○	○	○	○	○
16	●	○	○	○	○	○	○	○	○
17	●	○	○	○	○	○	○	○	○
18	●	○	○	○	○	○	○	○	○
19	●	○	○	○	○	○	○	○	○
20	●	○	○	○	○	○	○	○	○
21	●	○	○	○	○	○	○	○	○
22	●	○	○	○	○	○	○	○	○
23	●	○	○	○	○	○	○	○	○
24	●	○	○	○	○	○	○	○	○

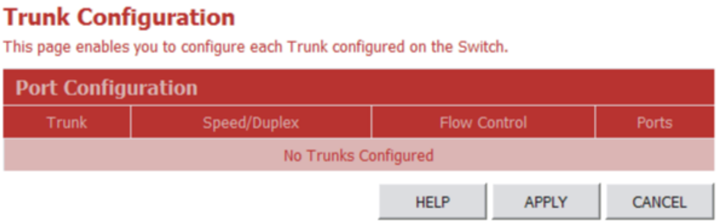
Figure 3-20 Trunk Membership

Trunk Configuration

Field Attributes

- **Trunk** – Indicates trunk identification.
- **Speed/Duplex** – Allows you to manually set the port speed and duplex mode for all ports in the trunk. (Default: Auto speed)
- **Flow Control** – Allows flow control to be enabled or disabled. When the box is checked, flow control is enabled.
- **Ports** – Indicates which ports belong to the trunk.

Web – Click TRUNKS, Settings.



Trunk Configuration

This page enables you to configure each Trunk configured on the Switch.

Port Configuration			
Trunk	Speed/Duplex	Flow Control	Ports
No Trunks Configured			

Figure 3-21 Trunk Configuration

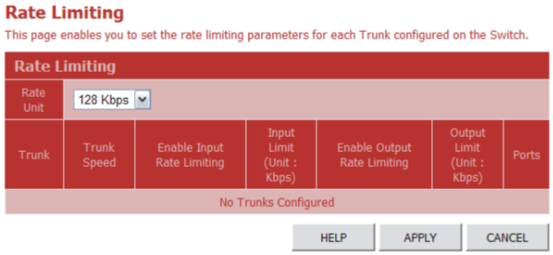
Trunk Rate Limit

This page allows you to change the maximum input and output data rate for each each trunk on the switch.

Field Attributes

- **Trunk** – Indicates trunk identification.
- **Trunk Speed** – Indicates the trunk speed.
- **Enable Input Rate Limiting** - Click to select the box to enable the Input Rate Limiting function.
- **Input Limit** – Enter the desired limit. (percentage of port speed)
- **Enable Output Rate Limiting** – Click to select the box to enable the Output Rate Limiting function.
- **Output Limit** – Enter the desired limit. (percentage of port speed)
- **Ports** – Indicates which ports belong to the trunk.

Web – Click TRUNKS, Settings.



Rate Limiting

This page enables you to set the rate limiting parameters for each Trunk configured on the Switch.

Rate Limiting

Rate Unit: 128 Kbps

Trunk	Trunk Speed	Enable Input Rate Limiting	Input Limit (Unit : Kbps)	Enable Output Rate Limiting	Output Limit (Unit : Kbps)	Ports
No Trunks Configured						

Figure 3-22 Trunk Rate Limiting

VLAN Settings

This page allows you to create and delete VLANs (Virtual LANs) and to change the VLAN membership and behaviour of individual ports. VLANs are powerful, but can be difficult to set up properly. Each row of the table corresponds to one port or trunk; trunked ports cannot be configured individually.

Introduction to VLANs

VLANs are logical partitions of the physical LAN. You can use VLANs to increase network performance or improve internal network security.

If the network has adequate performance and security for your current needs, it is recommended that you leave the VLAN settings in the default configuration. The default configuration is as follows:

- All ports are members of VLAN 1
- The switch management interface is on VLAN 1 (this cannot be changed)
- All ports have a Port VLAN ID (PVID) of 1
- All ports can send and receive both VLAN-tagged and untagged packets (that is, they are hybrid ports)

In the default configuration, any port is able to send traffic to any other port and a PC connected to any port will be able to access the management interface. Broadcast traffic, for example, will be flooded to all ports on the switch.

There are three different parameters that can be configured for each port on the switch; VLAN ID (VLAN membership), PVID's and Packet Type. Note that the ports within a trunk cannot be configured individually; configure the trunk instead (trunks are labelled T1 to T8).

IEEE 802.1Q Tunneling (QinQ) is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network. QinQ tunneling expands VLAN space by using this VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding SPVLAN tags to each frame (also called double tagging). Ports on the switch can be set to support QinQ when providing a direct link to a service provider's network.

Field Attributes

- **Port/Trunk** – The port-number of the port or the ID of a trunk. This cannot be changed.
- **VLAN Aware Enabled** – VLAN aware ports will strip the VLAN tag from received frames and insert the tag in transmitted frames (except PVID). VLAN unaware ports will not strip the tag from received frames or insert the tag in transmitted frames. For QinQ operation, a customer port should be set to VLAN unaware and a provider port (trunk port) should be set to VLAN aware.
- **QinQ** – A QinQ enabled port will accept packets up to 1526 bytes in length, which means double tag header frames can be accepted. QinQ should be enabled for provider ports but not for customer ports.

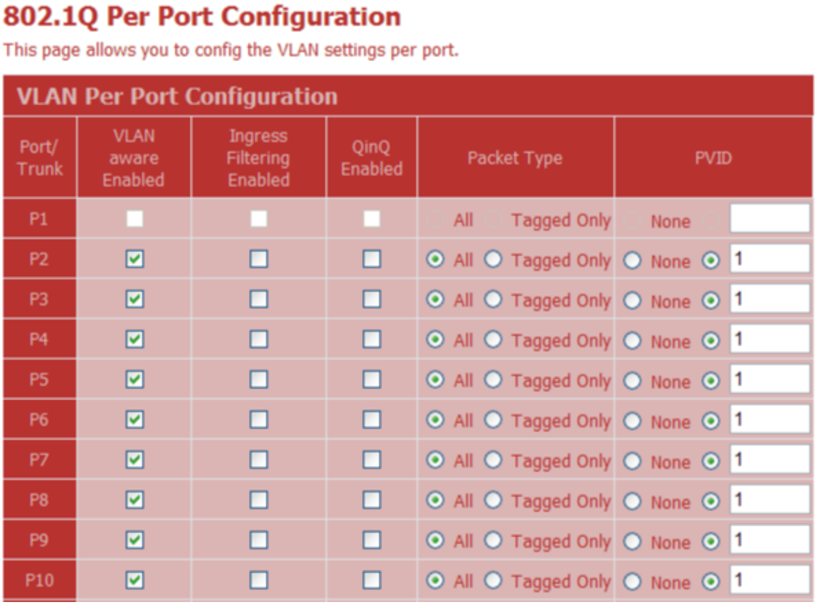
Note: QinQ "customer" ports are those ports that are connected to normal VLAN aware switches in the customer's network. QinQ "network" ports are those which are connected to the service provider's network. To tunnel packets through a service provider's metro network, QinQ needs to be enabled on the network port.

- **Packet Type** – Sets the interface to accept all frame types, or only tagged frames. If the Packet Type is set to "All," the port can accept incoming tagged and untagged packets. Untagged packets will be associated with the VLAN identified by the PVID. Tagged packets will be dropped unless the port is a member of the VLAN identified by the VLAN tag in the packet.

  If the Packet Type is set to "Tagged Only," the port will drop untagged packets and will only receive tagged packets. Tagged packets will be dropped unless the port is a member of the VLAN identified by the VLAN tag in the packet. (Default: All)
- **PVID** – The port VLAN ID (PVID) assigned to untagged frames received on the interface. Specify the VLAN ID that will be assigned to untagged frames received on the port. You cannot remove a port from VLAN 1 unless its PVID has been changed to something other than 1. You can only choose "None" for the VLAN ID when the packet type is set to "Tagged Only." Outgoing packets are tagged unless the packet's VLAN ID is the same as the PVID. When the PVID is set to "None," all outgoing packets are tagged. (Default: 1)

Note: If you select "Tagged Only" mode for a port, it is recommended to set the PVID to "None" as the standard configuration.

Web – Click VLANS, VLAN Settings. Fill in the required settings for each interface, click Apply.



802.1Q Per Port Configuration

This page allows you to config the VLAN settings per port.

VLAN Per Port Configuration

Port/ Trunk	VLAN aware Enabled	Ingress Filtering Enabled	QinQ Enabled	Packet Type	PVID
P1	□	□	□	○ All ○ Tagged Only	○ None ○
P2	☑	□	□	● All ○ Tagged Only	○ None ● 1
P3	☑	□	□	● All ○ Tagged Only	○ None ● 1
P4	☑	□	□	● All ○ Tagged Only	○ None ● 1
P5	☑	□	□	● All ○ Tagged Only	○ None ● 1
P6	☑	□	□	● All ○ Tagged Only	○ None ● 1
P7	☑	□	□	● All ○ Tagged Only	○ None ● 1
P8	☑	□	□	● All ○ Tagged Only	○ None ● 1
P9	☑	□	□	● All ○ Tagged Only	○ None ● 1
P10	☑	□	□	● All ○ Tagged Only	○ None ● 1

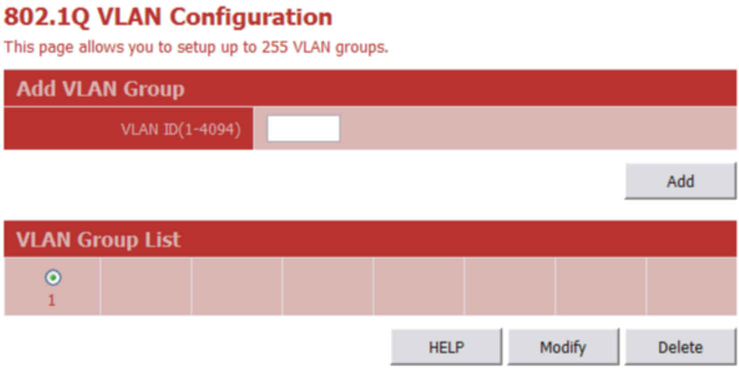
Figure 3-23 VLAN Settings

VLAN Memembership

The switch supports up to 255 VLANs based on 802.1Q standard. From the VLAN Membership page you can create and delete VLANs, and change the VLAN port membership.

Note: For QinQ application, the number of VLAN groups that would be setup is equal to the number of customer ports. Each VLAN group consists of two ports, customer port and network port. The VID equals to PVID of the customer port. Network port is member of the VLAN of customer port.

Web – Click VLANS, VLAN Membership. To add a new , type into the VLAN ID (1-4095) of the VLAN group you want the new group to be, then click Add to open up the 802.1Q VLAN Group window, on which you can configure VLAN membership.



802.1Q VLAN Configuration

This page allows you to setup up to 255 VLAN groups.

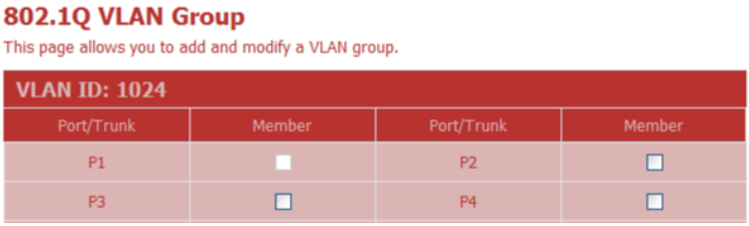
Add VLAN Group

VLAN ID(1-4094)

VLAN Group List

● 1

Figure 3-24 802.1Q VLAN Configuration



802.1Q VLAN Group

This page allows you to add and modify a VLAN group.

VLAN ID: 1024

Port/Trunk	Member	Port/Trunk	Member
P1	□	P2	□
P3	□	P4	□

Figure 3-25 802.1Q VLAN Group

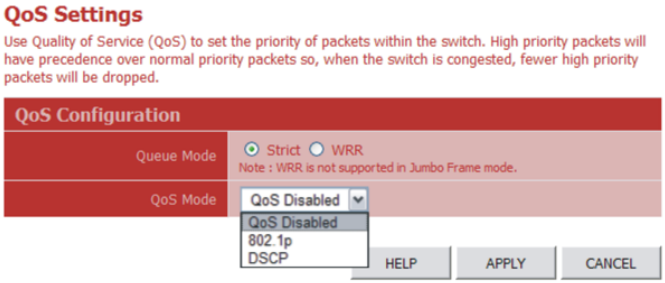
QoS Settings

QoS (Quality of Service) is a mechanism which is used to prioritize certain traffic as it is moves through the switch. Traffic can be classified as High, Medium, Normal or Low priority. This switch features both strict priority-based and weighted round-robin (WRR) forwarding, with guaranteed bandwidth allocation for the different QOS classes.

The queueing method can be selected using the **Queue Mode** drop-down list:

- **Strict priority** - Higher priority frames take precedence over lower priority frames during forwarding. In case of congestion, the lowest priority traffic is dropped before higher priority frames. Head-of-queue blocking may be encountered by using this mode.

Web – Click QOS, Settings. In Queue Mode, select Strict.



QoS Settings

Use Quality of Service (QoS) to set the priority of packets within the switch. High priority packets will have precedence over normal priority packets so, when the switch is congested, fewer high priority packets will be dropped.

QoS Configuration

Queue Mode: ● Strict ○ WRR

Note : WRR is not supported in Jumbo Frame mode.

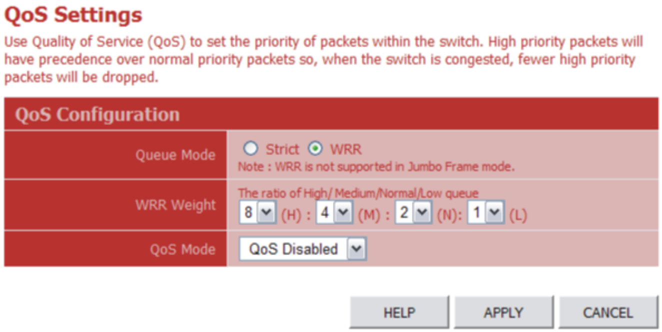
QoS Mode: QoS Disabled

Figure 3-26 QoS Settings - Queue Mode Strict

WRR - In this mode, all priorities can be guaranteed a share of the bandwidth when the system is overloaded. The bandwidth sharing percentage can be adjusted by specifying the four QOS class with different ratio in WRR Weight, which appears after WRR is enabled in Queue Mode.

Note: WRR is selectable when **Jumbo Frame** is disabled in Ports > Settings.

Web – Click QOS, Settings. In Queue Mode, select WRR. Adjust the WRR queue weights as required.



QoS Settings

Use Quality of Service (QoS) to set the priority of packets within the switch. High priority packets will have precedence over normal priority packets so, when the switch is congested, fewer high priority packets will be dropped.

QoS Configuration

Queue Mode: ○ Strict ● WRR

Note : WRR is not supported in Jumbo Frame mode.

WRR Weight: The ratio of High/ Medium/Normal/Low queue

8 (H) : 4 (M) : 2 (N): 1 (L)

QoS Mode: QoS Disabled

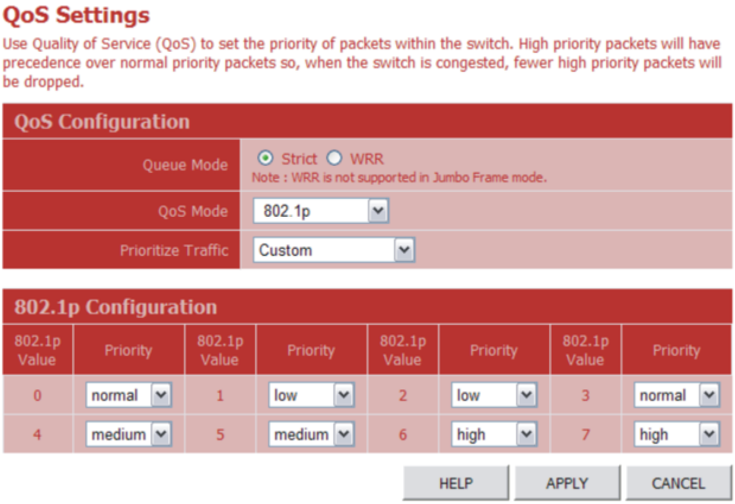
Figure 3-27 QoS Settings - Queue Mode WRR

802.1p Priority Mapping

Packets are prioritzed using the content of the VLAN-tag. The 802.1p field is held within the VLAN tag of a packet. The field is three bits long so can hold eight values; 0 - 7 inclusive. When the QoS Mode is set to 802.1p, the 802.1p Configuration table displays, which allows each of the eight values to be mapped to one of the four priority queues.

You can use the Prioritize Traffic drop-down list to quickly set the values in the 802.1p Configuration table. Select All Normal Priority to set all values to normal priority or select All High Priority to set all values to high priority. Use Custom if you want to set each value individually.

Note: End stations, such as PCs, are not usually VLAN aware and do not create VLAN-tagged frames. As a result, this method of prioritization is not ideal when there are a lot of PCs connected to the switch.



QoS Settings

Use Quality of Service (QoS) to set the priority of packets within the switch. High priority packets will have precedence over normal priority packets so, when the switch is congested, fewer high priority packets will be dropped.

QoS Configuration

Queue Mode	● Strict ○ WRR Note : WRR is not supported in Jumbo Frame mode.
QoS Mode	802.1p
Prioritize Traffic	Custom

802.1p Configuration

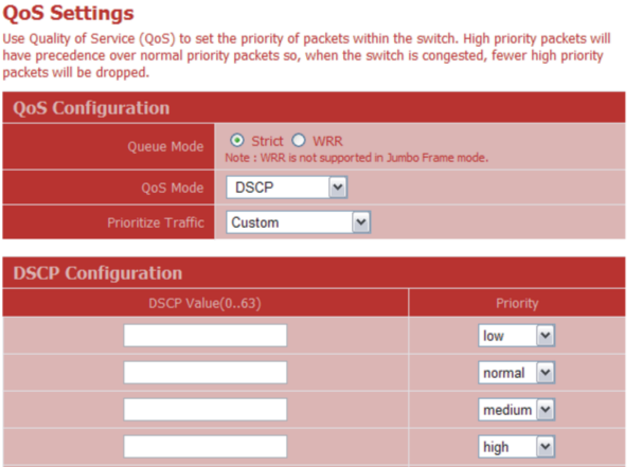
802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority	802.1p Value	Priority
0	normal	1	low	2	low	3	normal
4	medium	5	medium	6	high	7	high

Figure 3-28 QoS Settings - 802.1p Mode Priority Mapping

DSCP Priority Mapping

Packets are prioritized using the DSCP (Differentiated Services Code Point) value.The Differentiated Services Code Point (DSCP) is a six-bit field that is contained within an IP (TCP or UDP) header. The six bits allow the DSCP field to take any value in the range 0 - 63 inclusive. When QoS Mode is set to DSCP, the DSCP Configuration table is displayed, which allows DSCP values to be mapped to one of the four priority queues.

You can use the Prioritize Traffic drop-down list to quickly set the values in the DSCP Configuration table. Select All Normal Priority to set all values to normal priority or select All High Priority to set all values to high priority. Use Custom if you want to set each value individually.



QoS Settings

Use Quality of Service (QoS) to set the priority of packets within the switch. High priority packets will have precedence over normal priority packets so, when the switch is congested, fewer high priority packets will be dropped.

QoS Configuration

Queue Mode	● Strict ○ WRR Note : WRR is not supported in Jumbo Frame mode.
QoS Mode	DSCP
Prioritize Traffic	Custom

DSCP Configuration

DSCP Value(0..63)	Priority
	low
	normal
	medium
	high

Figure 3-29 QoS Settings - DSCP Mode Priority Mapping

RSTP

The Rapid Spanning Tree Protocol (RSTP) is a protocol that prevents loops in the network and dynamically reconfigures which physical links in a switch should forward frames.

Spanning Tree Protocol Introduction

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down. The spanning tree algorithms supported by this switch are STP, Spanning Tree Protocol (IEEE 802.1D), and RSTP, Rapid Spanning Tree Protocol (IEEE 802.1w).

RSTP System Configuration

Field Attributes

- **System Priority** – This parameter configures the spanning tree priority globally for this switch. The device with the highest priority becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Number between 0 - 61440 in increments of 4096. Therefore, there are 16 distinct values.

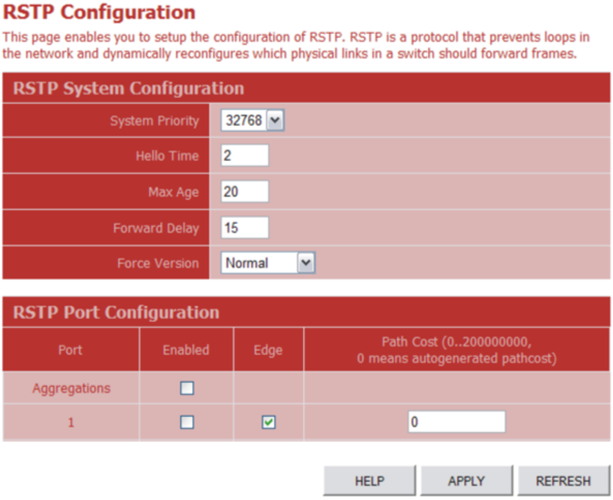
- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message (BPDU frame). Number between 1 - 10 (default is 2).
- **Max Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. That also means the maximum life time for a BPDU frame. Number between 6 - 40 (default is 20).
- **Forward Delay** – The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). Number between 4 - 30 (default is 15).
- **Force Version** – Set and show the RSTP protocol to use. Normal - use RSTP, Compatible - compatible with STP.

RSTP Port Configuration

Field Attributes

- **Port** - The port ID. It can not be changed. Aggregations means any configured trunk group.
- **Enabled** - Click on the tick-box to enable/disable the RSTP prototocl for the port.
- **Edge** - Expect the port to be an edge port (linking to an end station) or a link to another STP device.
- **Path Cost** - This parameter is used by the STP 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. Set the RSTP pathcost on the port. Number between 0 - 200000000. 0 means autogenerated pathcost.

Web – Click RSTP, Settings.



RSTP Configuration

This page enables you to setup the configuration of RSTP. RSTP is a protocol that prevents loops in the network and dynamically reconfigures which physical links in a switch should forward frames.

RSTP System Configuration

System Priority	32768
Hello Time	2
Max Age	20
Forward Delay	15
Force Version	Normal

RSTP Port Configuration

Port	Enabled	Edge	Path Cost (0..200000000, 0 means autogenerated pathcost)
Aggregations	□		
1	□	☑	0

Figure 3-30 RSTP Configuration

RSTP Status Overview

The RSTP Bridge Overview table has one row to display settings for the whole switch. Hello Time, Maximum Age and Forward Delay are displayed. Topology shows the switch current state. Root ID indicates the root port ID for the switch.

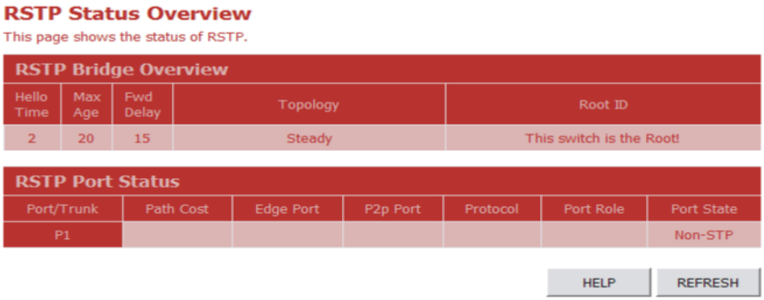
RSTP Port Status

Shows the detailed RSTP information for each port.

Field Attributes

- **Port/Trunk** - Port or trunk ID number.
- **VLAN ID** - VLAN IDs of the port.
- **Path Cost** - Show the path cost on this port.
- **Edge Port** -Displays “Yes” when the port is an edge port that connects to an end station.
- **P2p Port** - Displays “Yes” when the port link is connected to another STP device.
- **Protocol** - Show the running protocol, RSTP or STP.
- **Port State** - Show the current port state, blocking, forwarding, or learning.

Web – Click RSTP, Status.



RSTP Status Overview

This page shows the status of RSTP.

RSTP Bridge Overview

Hello Time	Max Age	Fwd Delay	Topology	Root ID
2	20	15	Steady	This switch is the Root!

RSTP Port Status

Port/Trunk	Path Cost	Edge Port	P2p Port	Protocol	Port Role	Port State
P1						Non-STP

Figure 3-31 RSTP Status Overview

802.1X

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data. With IEEE 802.1X (802.1X), access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

802.1X Setting

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication.

Field Attributes

System Setting

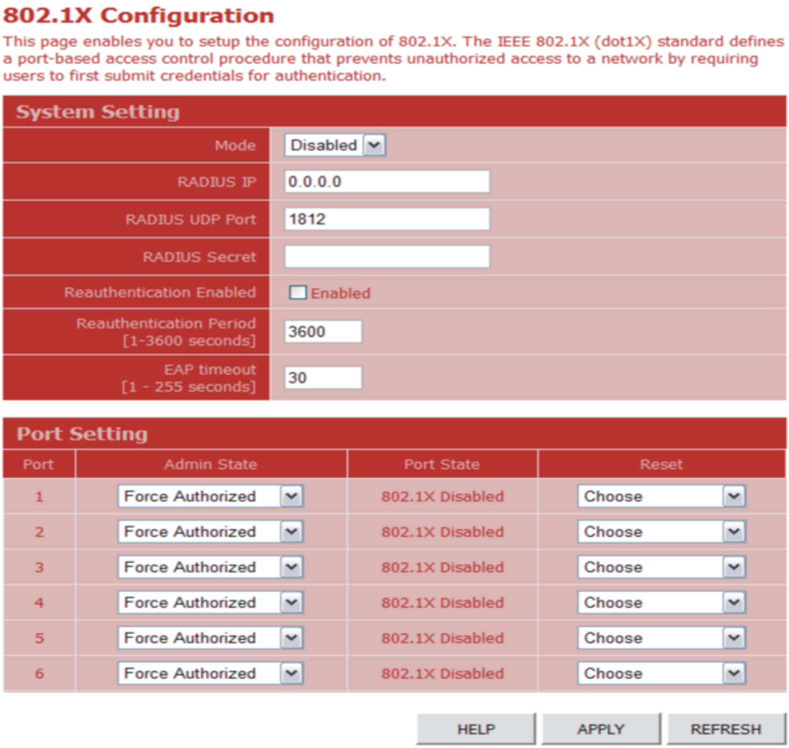
- **Mode** - Indicates if 802.1X protocol is globally enabled or disabled on the switch.
- **RADIUS IP** - Sets the RADIUS server IP address.
- **RADIUS UDP Port** - Sets the UDP port to the use for the external RADIUS server.
- **RADIUS Secret** - Sets the text string used for encryption between the switch and the RADIUS server.
- **Reauthentication Enabled** - Sets the client to be re-authenticated after the interval specified by the Re-authentication Period. Re-authentication can be used to detect if a new device is plugged into a switch port.
- **Reauthentication Period** - Sets the time period after which a connected client must be re-authenticated.
- **EAP timeout** - The time the switch shall wait for the supplicant response before re-transmitting a packet.

Port Setting

- **Port** - The port number.
- **Admin State** - Sets the authentication mode to one of the following options:
  - **Auto** - Requires a 802.1X-aware client to be authorized by the authentication server. Clients that are not 802.1X-aware will be denied access.
  - **Force-Authorized** - Forces the port to grant access to all clients, either 802.1X-aware or otherwise.
  - **Force-Unauthorized** - Forces the port to deny access to all clients, either 802.1X-aware or otherwise.
- **Port State** - The state of the port.
- **Reset** - Two options available:
  - **Re-Authenticate** - Schedules a reauthentication to whenever the quiet-period of the port runs out.
  - **Force-Reinitialize** - Bypasses the quiet-period of the port and enables immediate reauthentication regardless of the status for the quiet-period.

Note: The reason for a “quiet-period” follows: If a re-authentication fails, the IEEE802.1X standard enforces a so-called “quiet-period” in which the authenticator (switch) shall be quiet and not re-try another authentication–also packets from supplicant are discarded in this quiet period–this way “brute-force” attacks are prevented.

Web – Click 802.1X, Settings.



802.1X Configuration

This page enables you to setup the configuration of 802.1X. The IEEE 802.1X (dot1X) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication.

System Setting

Mode	Disabled
RADIUS IP	0.0.0.0
RADIUS UDP Port	1812
RADIUS Secret	
Reauthentication Enabled	□ Enabled
Reauthentication Period [1-3600 seconds]	3600
EAP timeout [1 - 255 seconds]	30

Port Setting

Port	Admin State	Port State	Reset
1	Force Authorized	802.1X Disabled	Choose
2	Force Authorized	802.1X Disabled	Choose
3	Force Authorized	802.1X Disabled	Choose
4	Force Authorized	802.1X Disabled	Choose
5	Force Authorized	802.1X Disabled	Choose
6	Force Authorized	802.1X Disabled	Choose

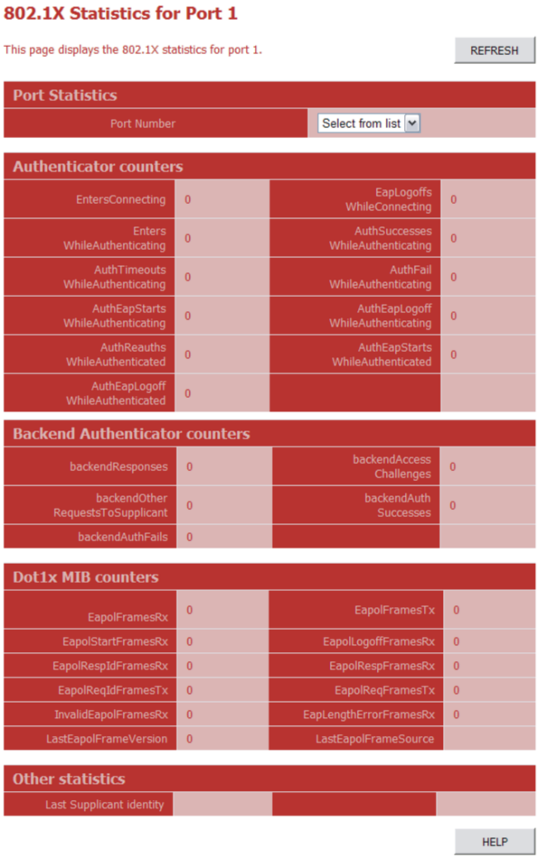
Figure 3-32 802.1X Configuration

802.1X Statistics

Field Attributes

- **Port Statistics** - Statistics can be viewed on a per-port basis. Select the port that you want to view here.
- **Authenticator counters** - General statistics for authenticator.
- **Backend Authenticator counters** - General statistics for RADIUS server.
- **802.1X MIB counters** - MIB module defined for 802.1X.

Web – Click 802.1X, Statistics.



802.1X Statistics for Port 1

This page displays the 802.1X statistics for port 1.

Port Statistics	
Port Number	Select from list

Authenticator counters			
EntersConnecting	0	EapLogoffs WhileConnecting	0
Enters WhileAuthenticating	0	AuthSuccesses WhileAuthenticating	0
AuthTimeouts WhileAuthenticating	0	AuthFail WhileAuthenticating	0
AuthEapStarts WhileAuthenticating	0	AuthEapLogoff WhileAuthenticating	0
AuthReauths WhileAuthenticated	0	AuthEapStarts WhileAuthenticated	0
AuthEapLogoff WhileAuthenticated	0		

Backend Authenticator counters			
backendResponses	0	backendAccess Challenges	0
backendOther RequestsToSupplicant	0	backendAuth Successes	0
backendAuthFails	0		

Dot1x MIB counters			
EapolFramesRx	0	EapolFramesTx	0
EapolStartFramesRx	0	EapolLogoffFramesRx	0
EapolRespIdFramesRx	0	EapolRespFramesRx	0
EapolReqIdFramesTx	0	EapolReqFramesTx	0
InvalidEapolFramesRx	0	EapLengthErrorFramesRx	0
LastEapolFrameVersion	0	LastEapolFrameSource	

Other statistics			
Last Supplicant identity			

Figure 3-33 802.1X Statistics

Security

IP Filter

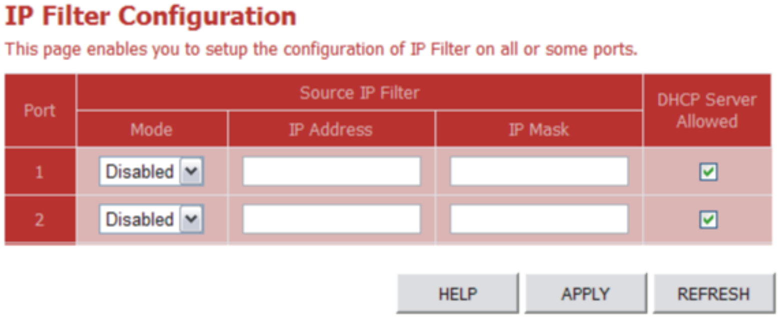
On this page, you can set up a source IP Filter on all or some ports. It is used to block unwanted access and provide access to the network for either a specific source IP address or a specific subnet. The IP Filter Configuration table has one row for each port and five columns.

Field Attributes

- **Port** - The front-panel port-number of the port. This cannot be changed.

- **Mode** - Select the IP filter mode for this port.
  - **Disabled** - Disable the source IP filter.
  - **Static** - Enable the IP filter with configured values in the Address and IP Mask fields.
  - **DHCP** - The IP address for the device connected to this port will be automatically assigned by DHCP server and only frames with the assigned IP address are allowed to access the network. The IP Address and IP Mask fields will be filled with the assigned IP address and 255.255.255.255 individually by software.
- **IP Address** - Set up IP addresses to allow access. Frames with IP address outside the allowed range will be dropped.
- **IP Mask** - Sets an IP mask to allow access for a specific subnet. To allow frames with a specific IP address, set the mask to 255.255.255.255.
- **DHCP Sever Allowed** - Enables or disables access to a DHCP server on a port. When DHCP Server Allowed is selected on a port, the port is allowed to be linked to a DHCP server. This can prevent the access of unwanted or unsolicited DHCP servers.

Web – Click Security, IP Filter.



IP Filter Configuration

This page enables you to setup the configuration of IP Filter on all or some ports.

Port	Source IP Filter			DHCP Server Allowed
	Mode	IP Address	IP Mask	
1	Disabled			☑
2	Disabled			☑

Figure 3-34 IP Filter Configuration

Port Security

Port security is a feature that allows you to configure a port with one or more MAC addresses that are authorized to access the network through that port. The Port Security table has one row for each port and five columns.

When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted as authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action as specified by Intrusion Action.

Field Attributes

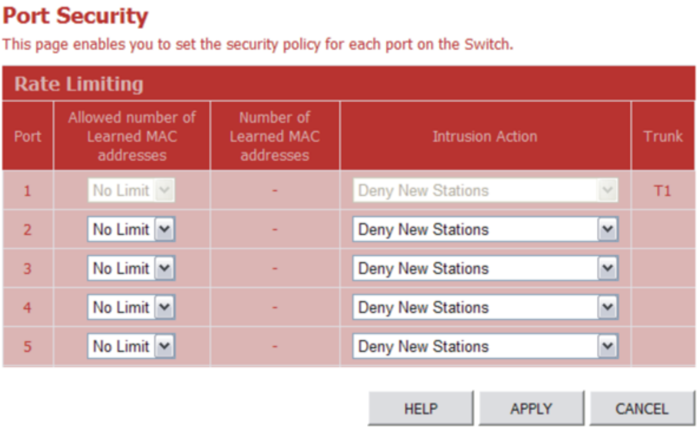
- **Port** - The front-panel port-number of the port. This cannot be changed.
- **Allowed number of Learned MAC addresses** - Set the maximum of MAC addresses that can be learned by this port. The Mode settings for the port are set by a single drop-down list.
  - **No Limit** - No limitation on the number of dynamcally learned MAC address. This means port security is disabled.
  - **8/7/6/5/4/3/2/1** - The maximum number of dynamically learned MAC address.
  - **0** - No dynamically learned MAC address is allowed on this port. This does not affect any static MAC addresses that are configured for the port.

Note: Port security only handles dynamically learned MAC addresses and has no limitations on static MAC addresses. On this switch, 24 static MAC address can be configured by System > Static MAC.

Note: The MAC addresses already in the address table will be retained and will not age out. Any other device that attempts to use the port will be prevented from accessing the switch.

- **Number of Learned MAC addresses** - Displays the number of currently learned MAC addresses. The string ‘-’ is displayed if a port is set with “No Limit” mode in the Allowed number of Learned MAC addresses field.
- **Intrusion Action** - Action to be carried out if unauthorized MAC addresses are detected.
  - **Deny New Stations** - The station with unauthorized MAC address will be denied to access the port.
  - **Send Trap and Deny New Stations** - Besides denying the new station, a trap message is sent by the switch to report an intrusion action.
- **Trunk** - Display the trunk ID if the port is member of a trunk group.

Web – Click Security, Port Security.



Port Security

This page enables you to set the security policy for each port on the Switch.

Rate Limiting

Port	Allowed number of Learned MAC addresses	Number of Learned MAC addresses	Intrusion Action	Trunk
1	No Limit	-	Deny New Stations	T1
2	No Limit	-	Deny New Stations	
3	No Limit	-	Deny New Stations	
4	No Limit	-	Deny New Stations	
5	No Limit	-	Deny New Stations	

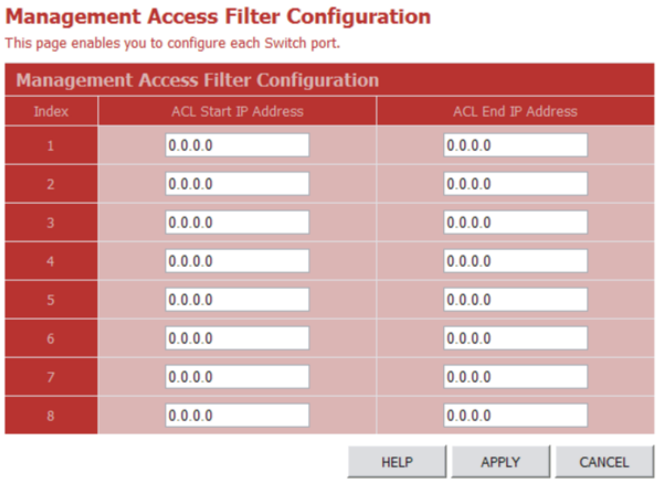
Figure 3-35 Port Security

ACL

This page enables you to set up a management access filter on the switch. With the Management Access Filter Configuration table, you can create a list of up to 8 IP addresses or IP address groups that are allowed management access to the switch through the web interface or SNMP. The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses. If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection.

Note: Invalid frames will not be able to access management interface, but normal forwarding is not impacted.

Web – Click Security, ACL.



Management Access Filter Configuration

This page enables you to configure each Switch port.

Management Access Filter Configuration

Index	ACL Start IP Address	ACL End IP Address
1	0.0.0.0	0.0.0.0
2	0.0.0.0	0.0.0.0
3	0.0.0.0	0.0.0.0
4	0.0.0.0	0.0.0.0
5	0.0.0.0	0.0.0.0
6	0.0.0.0	0.0.0.0
7	0.0.0.0	0.0.0.0
8	0.0.0.0	0.0.0.0

Figure 3-36 Management Access Filter Configuration

IGMP Snoop

The switch can use Internet Group Management Protocol (IGMP) to filter multicast traffic. IGMP Snooping monitors IGMP service requests passing between multicast clients and servers, and dynamically configures the ports which need to recieve the mulitcast traffic.

Note: For IGMPV3, the switch incudes basic support for reports only, Source Multicast is not supported.

IGMP Snooping Configurations

Field Attributes

IGMP Snooping Configuration

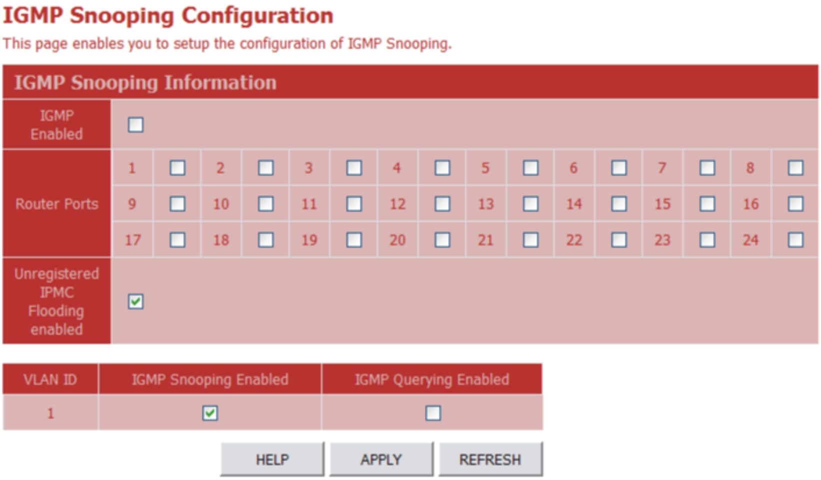
- **IGMP Enabled** - When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.
- **Router Ports** - Set if ports are conneting to the IGMP administrative routers.
- **Unregistered IPMC Flooding enabled** - Set the forwarding mode for unregistered (not-joined) IP multicast traffic. The traffic will flood when enabled, and forward to router-ports only when disabled.

IGMP Snooping VLAN Configuration

- **VLAN ID** - The VLAN ID. This cannot be changed.

- **IGMP Snooping Enabled** -When enabled, the port will monitor network traffic to determine which hosts want to receive the multicast traffic.
- **IGMP Querying Enabled** - When enabled, the port can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic.

Web – Click IGMP Snoop, Settings.



IGMP Snooping Configuration

This page enables you to setup the configuration of IGMP Snooping.

IGMP Snooping Information																
IGMP Enabled	□															
Router Ports	1	□	2	□	3	□	4	□	5	□	6	□	7	□	8	□
	9	□	10	□	11	□	12	□	13	□	14	□	15	□	16	□
	17	□	18	□	19	□	20	□	21	□	22	□	23	□	24	□
Unregistered IPMC Flooding enabled	☑															

VLAN ID	IGMP Snooping Enabled	IGMP Querying Enabled
1	☑	□

Figure 3-37 IGMP Snooping Configuration

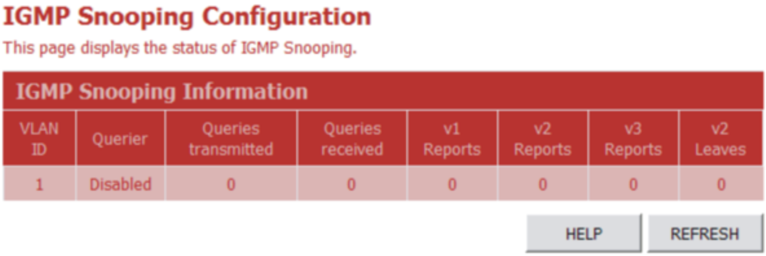
IGMP Status

Show the IGMP Snooping statistics for the whole switch.

Field Attributes

- **VLAN ID** - VLAN ID number.
- **Querier** - Show whether Querying is enabled.
- **Queries transmitted** - Show the number of transmitted Query packets.
- **Queries received** - Show the number of received Query packets.
- **v1 Reports** - Show the number of received v1 Report packets.
- **v2 Reports** - Show the number of received v2 Report packets.
- **v3 Reports** - Show the number of received v2 Report packets.
- **v3 Leave** - Show the number of v3 leave packets received.

Web – Click IGMP Snoop, Status.



IGMP Snooping Configuration

This page displays the status of IGMP Snooping.

IGMP Snooping Information

VLAN ID	Querier	Queries transmitted	Queries received	v1 Reports	v2 Reports	v3 Reports	v2 Leaves
1	Disabled	0	0	0	0	0	0

Figure 3-38 IGMP Snoop Status

SNMP

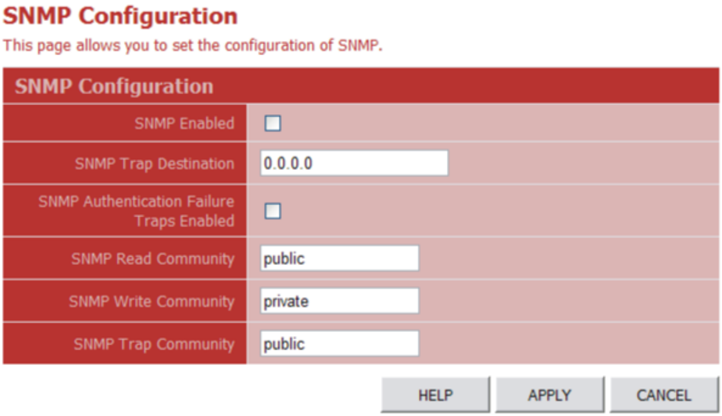
Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems. The switch includes an onboard SNMP agent that continuously monitors the status of its hardware, as well as the traffic passing through its ports. A network management station can access this information using network management software. Access rights to the onboard agent are controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication.

SNMP Configuration

Field Attributes

- **SNMP Enabled** -Activate or deactivate SNMP.
- **SNMP Trap Destination** - IP address of the trap manager.
  Traps indicating status changes are issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station. SNMP trap destination specifies the IP address of the trap manager.
- **SNMP Read Community** - A community string that acts like a password and permits access to the SNMP protocol. The read community string specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **SNMP Write Community** - Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.
- **SNMP Trap Community** - Community string sent with the notification operation.

Web – Click SNMP, Settings.



SNMP Configuration

This page allows you to set the configuration of SNMP.

SNMP Configuration	
SNMP Enabled	□
SNMP Trap Destination	0.0.0.0
SNMP Authentication Failure Traps Enabled	□
SNMP Read Community	public
SNMP Write Community	private
SNMP Trap Community	public

Figure 3-39 SNMP Configuration

Appendix A: Software Specifications

Software Features

Authentication
Port (802.1X), Port Security

Access Control Lists
IP filter for management access

DHCP Client

Port Configuration
100BASE-TX: 10/100 Mbps, half/full duplex
1000BASE-T: 10/100 Mbps at half/full duplex, 1000 Mbps at full duplex

Flow Control
Full Duplex: IEEE 802.3-2005
Half Duplex: Back pressure

Broadcast Storm Control
Traffic throttled above a critical threshold

Port Mirroring
One source port, one destination port

Rate Limits
Input Limit
Output limit
Range (configured per port)

Port Trunking
Static trunks (Cisco EtherChannel compliant)
Dynamic trunks (Link Aggregation Control Protocol)

Spanning Tree Algorithm
Spanning Tree Protocol (STP, IEEE 802.1D)
Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w)

VLAN Support
Up to 255 groups; port-based or tagged (802.1Q),

Class of Service
Supports four levels of priority and Weighted Round Robin Queueing (which can be configured by VLAN tag or port),
Layer 3/4 priority mapping: IP DSCP

Multicast Filtering
IGMP Snooping (Layer 2)

Additional Features
SNMP (Simple Network Management Protocol)

Management Features

In-Band Management
Web, SNMP manager

Software Loading
HTTP in-band

SNMP
Management access via MIB database
Trap management to specified hosts

Standards

IEEE 802.1D Spanning Tree Protocol and traffic priorities
IEEE 802.1p Priority tags
IEEE 802.1Q VLAN
IEEE 802.1w Rapid Spanning Tree Protocol
IEEE 802.1X Port Authentication
IEEE 802.3-2005
Ethernet, Fast Ethernet, Gigabit Ethernet
Full-duplex flow control
Link Aggregation Control Protocol
IEEE 802.3ac VLAN tagging
DHCP Client (RFC 1541)
IGMP (RFC 1112)
IGMPv2 (RFC 2236)
RADIUS+ (RFC 2618)
SNMP (RFC 1157)
SNMPv2 (RFC 2571)

Management Information Bases

Bridge MIB (RFC 1493)
Entity MIB (RFC 2737)
Ether-like MIB (RFC 2665)
Extended Bridge MIB (RFC 2674)
Extensible SNMP Agents MIB (RFC 2742)
Forwarding Table MIB (RFC 2096)
IGMP MIB (RFC 2933)
Interface Group MIB (RFC 2233)
Interfaces Evolution MIB (RFC 2863)
IP Multicasting related MIBs

MAU MIB (RFC 2668)
MIB II (RFC 1213)
Port Access Entity MIB (IEEE 802.1X)
Port Access Entity Equipment MIB
Private MIB
RADIUS Authentication Client MIB (RFC 2621)
SNMP Community MIB (RFC 2576)
SNMPv2 IP MIB (RFC 2011)
TCP MIB (RFC 2013)
Trap (RFC 1215)
UDP MIB (RFC 2012)

Appendix B: Troubleshooting

Problems Accessing the Management Interface

Table B-1 Troubleshooting Chart

Symptom	Action
Cannot connect using web browser, or SNMP software	• Be sure the switch is powered up. • Check network cabling between the management station and the switch. • Check that you have a valid network connection to the switch and that the port you are using has not been disabled. • Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask and default gateway. • Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected. • If you are trying to connect to the switch via the IP address for a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag.
Forgot or lost the password	• See "System Defaults" on page 1-5 for how to return the switch to its factory settings.

Glossary

Access Control List (ACL)

ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

Boot Protocol (BOOTP)

BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

Class of Service (CoS)

CoS is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

Differentiated Services Code Point Service (DSCP)

DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

Domain Name Service (DNS)

A system used for translating host names for network nodes into IP addresses.

Dynamic Host Control Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Extensible Authentication Protocol over LAN (EAPOL)

EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

IEEE 802.1D

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

IEEE 802.1Q

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

IEEE 802.1p

An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1X

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3ac

Defines frame extensions for VLAN tagging.

IEEE 802.3x

Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links.

IGMP Snooping

Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IGMP Query

On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

Internet Group Management Protocol (IGMP)

A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the “querier” and assumes responsibility for keeping track of group membership.

In-Band Management

Management of the network from a station attached directly to the network.

IP Multicast Filtering

A process whereby this switch can pass multicast traffic along to participating hosts.

IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

Layer 2

Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Link Aggregation

See Port Trunk.

Link Aggregation Control Protocol (LACP)

Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

Management Information Base (MIB)

An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MD5 Message-Digest Algorithm

An algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

Multicast Switching

A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

Port Mirroring

A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk

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

Remote Authentication Dial-in User Service (RADIUS)

RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

Remote Monitoring (RMON)

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

Rapid Spanning Tree Protocol (RSTP)

RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Spanning Tree Algorithm (STA)

A technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

User Datagram Protocol (UDP)

UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

Virtual LAN (VLAN)

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

ES4324
E082007-AP-R02
149100031800A