Chapter 4
Configuring the Switch

The navigation tabs across the top of the user interface provide access to all of the submenu screens which allow you to manage your GS748T Smart Switch. The features under the following main headings:

- "Configuring Ports"
- "Configuring the Link Aggregation Group (LAG)"
- "Setting Up SNMP"
- "Configuring and Creating VLANs"
- "Enabling Spanning Tree Protocol"
- "Establishing Multicast Groups"
- "Enabling Jumbo Frames"
- "Setting Rate Limits"
- "Setting QoS Global Configuration"
- "Enabling Storm Control"
- "Configuring the IP Access List"
- "Controlling Switch Access by MAC Address and VLAN ID"
- "Setting up Mirroring or "Sniffer Ports""
- "Viewing Packet Statistics"

The description that follows in this chapter covers these features and tells you how to configure them in the GS748T switch.

Configuring Ports

The Port Configuration table displays the port status and contains fields for defining port parameters.

To configure port settings:

1. Select Switching > Ports from the main menu. The Port Configuration screen will display.

2. Select the row of the port that you want to configure. Then, at the top of screen, enter the following information for the selected port:
   - Type a description for the port in the **Port Description** field.
   - From the **Port Speed** pull-down menu, select the rate for the port:
     – 100M (100 Mbps)
     – 10M (10 Mbps)
     – Auto (Auto will set the speed to 1000Mbps)
     – Disable (disable the port)
3. From the **Duplex Mode** pull-down menu, select the duplex mode for the port (this field is available only when auto-negotiation is disabled and the port speed is set to 10M or 100M):
   - Full (Full duplex)
   - Half (Half duplex)
4. From the **Flow Control** pull-down menu, select whether or not to enable or disable Flow Control.
5. From the **Default Priority** pull-down menu, assign a default packet priority for packets without IEEE802.1P tagging. If the packet comes in with a priority tag, the priority is retrieved from priority field of the tag.
6. Click **Apply.**

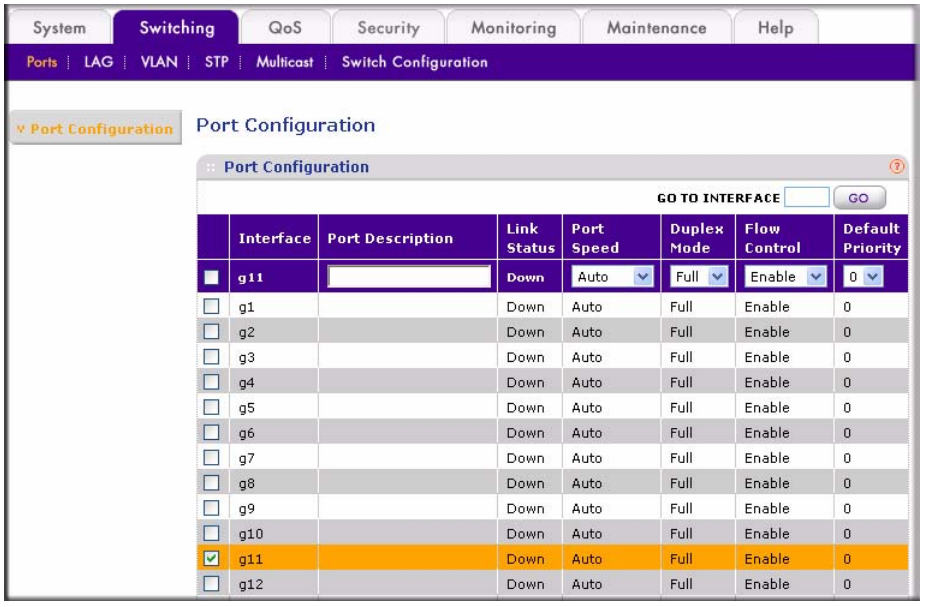

Figure 4-8

Configuring the Link Aggregation Group (LAG)

Link Aggregation Groups (otherwise known as Port Trunking) enables multiple links between switches to work as one virtual link (aggregate link) to provide greater bandwidth than would be available by confining the traffic to a single port. LAGs can be defined for similar port types only. For example, a 10/100 port cannot form a LAG with a gigabit port. Up to 10 LAGs can be operating at the same time.

The LAG table displays the status and administration settings for all the available LAGs, also known as trunks. The GS748T Smart Switch supports 10 static LAGs.

To enable or disable a LAG:

1. Select Switching > LAG > LAG Configuration from the main menu. The LAG Configuration screen will display.
2. Select the row of the LAG ID you want to enable or disable.
3. From the **Admin Mode** pull-down menu, select Enable or Disable.

4. Click **Apply**.

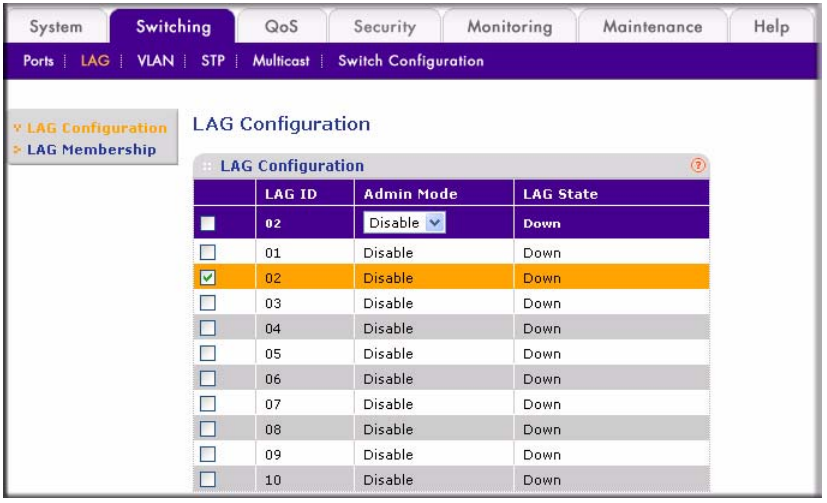

Figure 4-9

The LAG Membership table displays the port members in each LAG. You can also specify port members for LAGs. When specifying LAGs, the following policies apply:

- Each port can belong to only one LAG.
- Each LAG can have up to 8 ports.
- Ports in a LAG must have the same speed and be in the same VLAN group.

To configure port membership of a LAG:

1. Select Switching > LAG > LAG Membership. The LAG Membership screen will display.
2. From the **LAG ID** pull-down menu, select the LAG that you want to modify.
3. Click the **Unit** link next to the check box to display all available ports. (All ports are selected if the **Unit** checkbox is selected. If not selected, no ports are selected.)
4. Select or clear the check box for the ports you want to include or remove.
5. Click **Apply.**

Figure 4-10

Note: The selected LAG ID port must correspond to VLAN group IDs.

Setting Up SNMP

SNMP (Simple Network Management Protocol) is a transport protocol used for network management. The protocol is used in communication between a Manager—the management station—and an agent within the managed device, in this case your switch. The Manager polls the agent which responds by returning data from the Management Information Bases (MIBs) that it maintains on the managed device to indicate its status. An agent can return Traps to the Manager, Traps are messages that alert the manager to conditions that may need attention. Managers and Agents work within Communities which are defined to confine messaging within named groups. An agent only responds to requests from Managers within its community.

The SNMP screen allows you to limit the IP addresses from which the switch MIBs can be accessed and to which IPs the switch sends SNMP traps. The switch only responds to requests from management computers whose IP addresses are carried in the list. This list also holds Privilege information that controls which IPs have read-only or read-write access. You can also select the traps which the switch sends to the hosts from the following trap events. The **Status** field must be set to **Enable** to allow management host communication.

Trap Events are indicated by:

- T1: Authentication fail – The switch generates an SNMP trap when a host tries to gain access to the switch but the host's IP is not in the SNMP host table.
- T2: Device bootup – The switch generates an SNMP trap when it reboots.

- T3: Link Up/Down – The switch generates an SNMP trap when one of its ports changes its link status

You can specify the SNMP management station that can access the MIB of the switch and to which the switch will send the trap. When adding a management station, be aware that:

- You can specify up to four management station IP addresses.
- The switch will respond only to requests from a computer or management station with an IP address that is in the list.
- You can also select the traps that the switch will send to the hosts when the trap events you specify occur.

To add a management station:

1. Select System > SNMP. The SNMP V1/V2 screen will display.
2. In the **Management Station** field, enter the IP address of the management station.
3. In the **Community String** field, specify the community string. The switch processes requests from the management station only if the community string in the request packet matches the community string entered here.
4. From the **Access Mode** pull-down menu, select the access privilege for the management station:
    - Read Only (for GET and GETNEXT requests).
    - Read Write (for GET, GETNEXT, and SET requests).
5. From the **Trap(T2)** pull-down menu, select **Enable** if you want the switch to generate the SNMP cold Start trap when it reboots; otherwise select **Disable.**
6. From the **Trap(T3)** pull-down menu, select **Enable** if you want the switch to generate the SNMP linkUp and linkDown trap when one of its ports changes its link status.
7. From the **Status** pull-down menu, select **Enable** or **Disable** to specify the administration status. A managed station or host is not active until it is set to **Enable**.
8. Click **Add** to add a management station.

To delete a management station:

Select the entry you want to delete and click **Delete.**

To modify an entry:

1. Select the checkbox by the entry you want to modify. The fields available for modifying will appear at the top of the table.

2. Modify the settings in the top row and click **Apply.**

Configuring and Creating VLANs

A Virtual Local Area Network (VLAN) is a means of electronically separating ports on the same switch from a single broadcast domain into separate broadcast domains. By using VLANs, users can group nodes by logical function instead of physical location. For example, Engineering and Accounting department traffic can be separated from one another. VLAN memberships are manipulated by associating switch ports with VLAN IDs (VIDs).

You can choose from two types of VLAN to set up on the switch: IEEE 802.1Q VLAN (Tagged VLAN), or Port-based VLAN. You cannot mix the types on the same switch. In either case, any port can be a member of multiple VLANs.

- **IEEE 802.1Q VLAN**. The VLAN tagging option is a standard set by the IEEE to facilitate the spanning of VLANs across multiple switches (Reference: Appendix A and IEEE Std 802.1Q-1998 Virtual Bridged Local Area Networks). This switch supports the creation of 256 Static-Tag VLAN groups.

  This implementation separates traffic by adding a VLAN tag into the appropriate egress frames (packets) from selected switch ports. A receiving switch associates the tagged frame with the VLAN and forwards it, according to its own VLAN-to-port lookup table, to all ports on the VLAN except the ingress port. In this way, a VLAN structure may be built across a “tree” of switches. You have the option of setting egress frames to be:

  - **Tagged.** This setting adds an 802.1Q tag into the frame leaving the selected port.
  - **Untagged**. This option strips the 802.1Q tags from frame leaving the selected port. The port retains its association with the VLAN. This facility is used when these ports are connected to downstream equipment that does not recognize (and which consequently may be confused by) 802.1Q tags.
  - **Unchanged**. This option is the default and signifies that the port is not associated with a VLAN.

  Every port is a member of VLAN ID 1 by default. You can change the default assignment of any port adjusting the Primary VLAN ID Setting (PVID) table. Use this feature to ensure that untagged frames reach the VLAN that you require.

- **Port-based VLAN**. This implementation confines VLAN members to the ports on the particular switch (for example, the VLANs cannot span multiple switches). VLAN port membership is determined via a lookup table that you set up when you configure the switch. You can create up to 48 port-based VLANS. Every port belongs to VLAN ID 1 by default.

Adding and Configuring IEEE 802.1Q VLAN Groups

Depending on the VLAN type selected in the VLAN Type Configuration table, you can create 256 IEEE 802.1Q-based VLANs or 48 port-based VLANs.

To create a VLAN:

1. Select Switching > VLAN > VLAN Configuration from the main menu. The VLAN Configuration screen will display.
2. Select the **IEEE.802.1Q** radio box and click **Apply.**

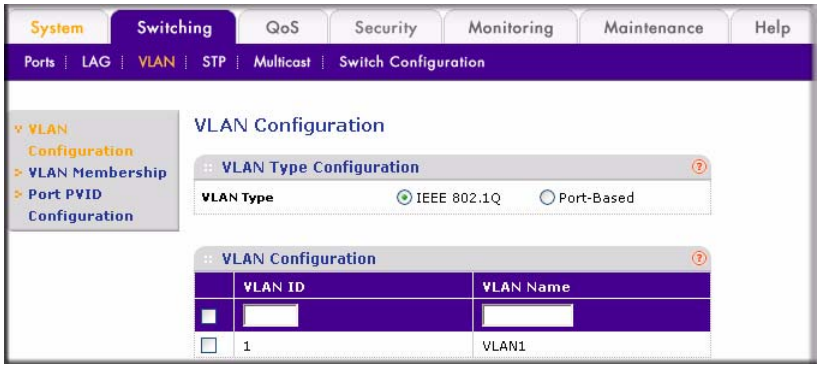

Figure 4-11

3. In the VLAN ID field, specify a VLAN ID from 1 to 4094. This field is available only when the 802.1Q VLAN type is selected. If you have not previously created a VLAN, this window shows VLAN ID 1 (default) with all ports set Untagged
4. In the VLAN Name field, assign a name to help you to identify this VLAN.
5. Click **Add.**

   Use the VLAN Membership table to manage each port's VLAN membership for transmitting packets. These settings determine if packets transmitted from each port are tagged with the VLAN ID and other information. By default, every port is a member of VLAN 1, which has a port VLAN ID (PVID) of 1.

To modify 802.1Q VLAN membership:

1. Select Switching > VLAN > VLAN Membership from the main menu. The VLAN Membership screen will display.
2. In the VLAN Identifier list, select the VLAN that you want to modify. The possible operations are:

   - Untag All: Add all the ports to this VLAN and remove tag on all egress packets)

- Tag All: Add all the ports to this VLAN and tag all egress packets.
- Remove All: Remove all the ports from this VLAN.

3. Click the **Unit** link to display all available ports.
4. Toggle the check box for each port to change its membership and tag setting:
   - An empty check box indicates that the port is not a member of this VLAN.
   - **T** indicates that the egress packet is tagged.
   - **U** indicates that the egress packet is untagged.
5. Click **Apply.**

Figure 4-12

Note: Every port has an initial default VID of 1 (PVID = 1). Whether a port has this VID or has been made a member of another default VID, you cannot remove any port from its prior default VLAN until you have reassigned its PVID to its new value. Use the PVID Setting menu option of VLAN Management to change its PVID before attempting to remove it from its prior default membership.

The PVID Configuration table contains parameters for assigning Port VLAN ID (PVID) values to interfaces. All ports must have a defined PVID. If no other value is specified, the default VLAN PVID is used. If you want to change the port's default PVID, you must first create a VLAN group that includes the port.

To modify a PVID:

1. Select the interface or port that you want to modify.
2. In the PVID field, enter a valid VLAN ID.

3. Click **Apply**.

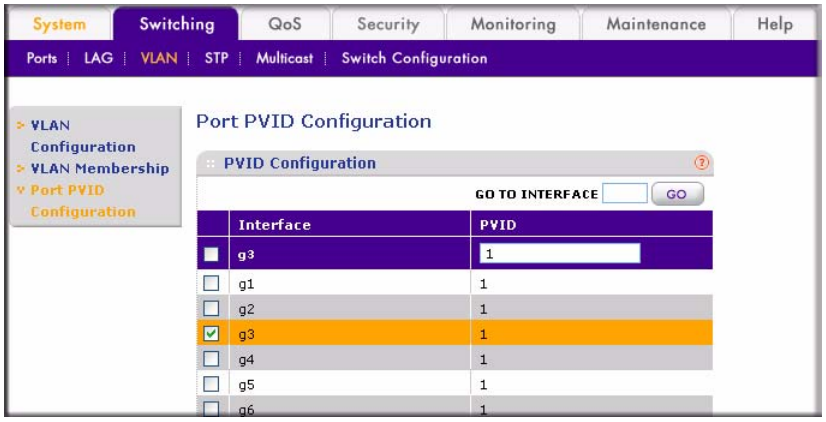

Figure 4-13

Configuring Port-Based VLANs

Unlike 802.1Q based VLAN, an ingress packet with an 802.1Q tag is ignored and preserved.

To modify port-based VLAN membership:

1. Select Switching > VLAN > VLAN Configuration from the main menu. The VLAN Configuration screen will display.

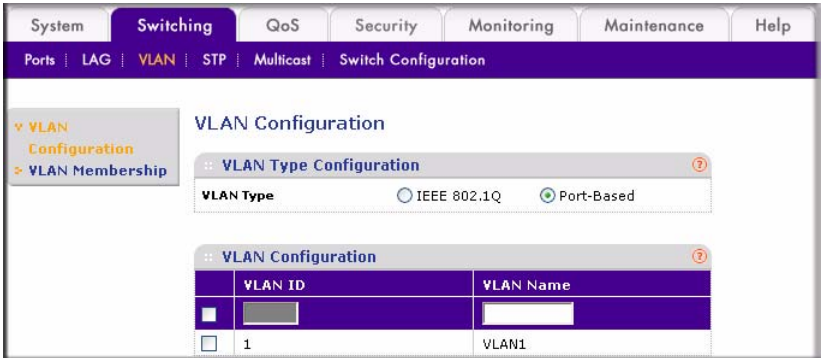

Figure 4-14

2. Ensure that the **Port-Based** radio box has been enabled for **VLAN Type.**
3. In the VLAN Name field, assign a name to help you to identify this VLAN.
4. Click **Add**.

To modify a Port-Based VLAN membership:

1. Select VLAN Membership. The VLAN Membership screen will display all port-based VLAN members.
2. From the **VLAN Identifier** pull-down menu, select the VLAN that you want to modify. You can also click the **Unit** link to display all available ports.
3. Select or clear the check box for the port for the VLAN.
4. Click **Apply**.

To delete a VLAN:

Select the VLAN you want to remove and click **Delete**. all port associations are separated from the VLAN and it is removed.

Selecting a Management VLAN

The Management VLAN allows you to establish an IP connection to the switch from a PC connected to a port in that VLAN. This increases security by allowing only PCs in the management VLAN to configure the switch. Any VLAN can be designated as the management VLAN.

To configure the management VLAN:

1. Select System > Management > IP Configuration. The IP Configuration screen will display.
2. In the **Management VLAN ID** field, enter the ID of the VLAN that you want to use for managing the switch. A zero value means that any PC in any of the VLANs can establish an IP connection to the switch.
3. Click **Apply** to save your settings.

Enabling Spanning Tree Protocol

To achieve reliability in a network, some path redundancy must be provided. However, multiple paths between network nodes can cause loops to exist and result in switching confusion and duplication of traffic. Spanning Tree Protocol (defined by IEE 802.1D) controls the duplicate paths by accounting for statistical weights in the available paths. It blocks the least efficient alternate paths and causes traffic only to be carried over the optimal paths between nodes.

The GS748T switch supports Rapid Spanning Tree Protocol (defined by IEEE 802.1w), which is an improvement (over the 802.1D STP) that shortens connection latency between nodes. The

resultant path between nodes determined by RSTP is the same as that eventually determined by STP. Use the Bridge Settings table to manage attributes related to the Spanning Tree Protocol.

- **Bridge Priority**. The priority value of this switch. After exchanging BPDUs with other STP-enabled devices, the device with the lowest priority value becomes the root bridge.
- **Bridge Max Age.** The maximum age of the current bridge. This is the maximum age of the Spanning Tree Protocol information learned from the network before it is discarded (in seconds).
- **Bridge Hello Time**. Indicates the amount of time (in seconds) that the switch waits before sending configuration PDUs when it is the root of the spanning tree or trying to become the root.
- **Bridge Forward Delay.** Indicates the amount of time, measured in seconds, that the port stays in each of the listening and learning states that precedes the forward state. This value is also used to age all dynamic entries in the forwarding databases when a topology change has been detected and is underway.

The IEE 802.1W RSTP Setting page of the GS748T switch contains a set of default values which are optimal for most applications. Adjust these values if you must provide for special conditions.

To set up RSTP:

1. Select Switching > STP > Advanced > RSTP Configuration from the main menu. The RSTP Configuration screen will display.
2. Select the **Enable** radio box for **RSTP Configuration** and click **Apply.**
3. Then select the **Advanced** link to display the Bridge Settings. You can accept the default settings or modify the default settings and click **Apply.**

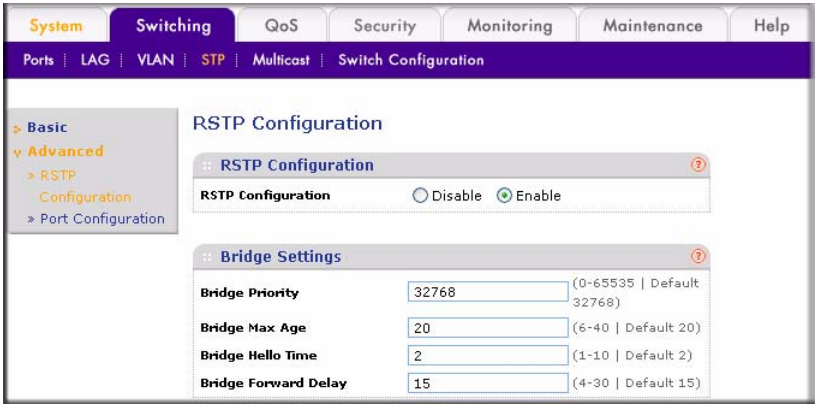

Figure 4-15

The Port Configuration table displays the current status of individual ports. You can also configure ports from this table.

To modify port settings:

1. Select the **Port Configuration** link. The RSTP Port Configuration screen will display.
2. Select the interface or port you want to modify.
3. Modify the settings in the top row:
   - **Path Cos**t. Displays the cost of this port. Cost means the contribution of this port to the cost of paths toward the spanning tree root that include this port. The switch uses this value to determine which port is the forwarding port. If all other factors are equal, the path with the lowest cost to the root bridge is the active path.
   - **Priority**. Displays the priority of this port. This is the value of the priority field contained in the first octet of the port ID. The port with the lowest number has the highest priority.
   - **Edge**. Indicates if this port is the edge port. Once configured as an edge port, the port immediately transitions to the forwarding state.
   - **P2P Forc**e. Indicates if this port is a point-to-point link. If you connect a port to another port though a point-to-point link and the local port becomes a designated port, it negotiates a rapid transition with the other port to ensure a loop-free topology.
4. Click **Apply**.

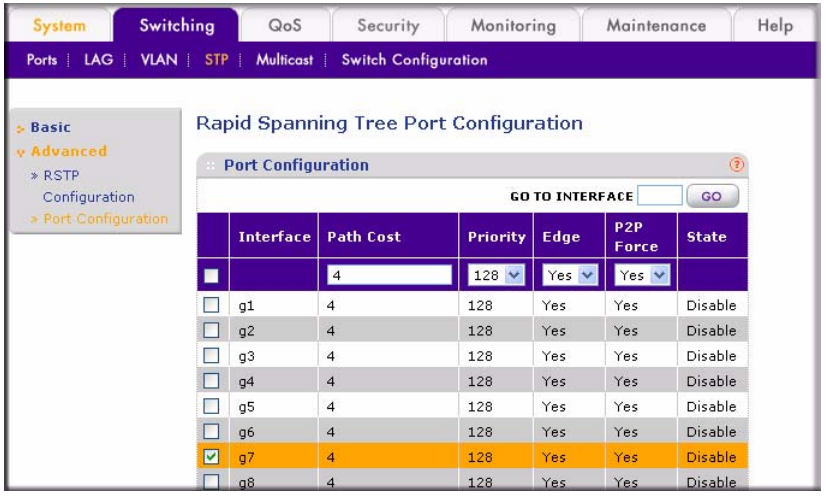

Figure 4-16

Establishing Multicast Groups

You can specify specific ports and VLANs for receiving Multicast packets with specific MAC addresses. The MAC addresses are IPv4 Multicast Addresses (RFC 1112A) formatted as: 01:00:5E-XX-XX-XX. A maximum of 64 groups is supported.

IGMP Snooping

IGMP (Internet Group Management Protocol) specifies how to register a host to a router in order to receive specific multicast traffic. It allows your switch to examine IGMP packets and forward them in ways based on their content.To receive messages, the switch must be configured to use IGMP snooping in subnets that receive IGMP queries from either IGMP groups or the IGMP snooping querier. IGMP snooping constrains multicast traffic at Layer 2 by dynamically configuring Layer 2 LAN ports to forward multicast traffic only to those ports that want to receive the messages. IGMP is a standard defined in RFC 1112 for IGMPv1 and in RFC 2236 for IGMPv2.

Both IGMP Snooping and blocking of unknown multicast addresses (flooding) are disabled by default.

To enable IGMP snooping:

1. Select Switching > Multicast > Basic from the main menu. The IGMP Snooping screen will display.
2. Select the **Enable** radio box to enable the **IGMP Snooping Status** feature.
3. Select the **Enable** radio box for **Block Unknown Multicast Addresses** to allow unknown multicast flooding.
4. Click **Apply**.

Multicast Group Configuration

The Static Multicast table allows you to add and delete static multicast groups. Up to 256 static multicast groups can be supported.

To add a static multicast entry:

1. 1. Select Switching > Multicast > Advanced > Multicast group Configuration. The Multicast Group Configuration screen will display.
2. Enter the following parameters for each field in the top row:

- **VLAN ID**. Specifies the VLAN ID. This field is only applicable if 802.1Q VLAN mode is used.
- **Multicast Entry**. Specifies the multicast group MAC address associated with the VLAN.

3. Click **Add**.

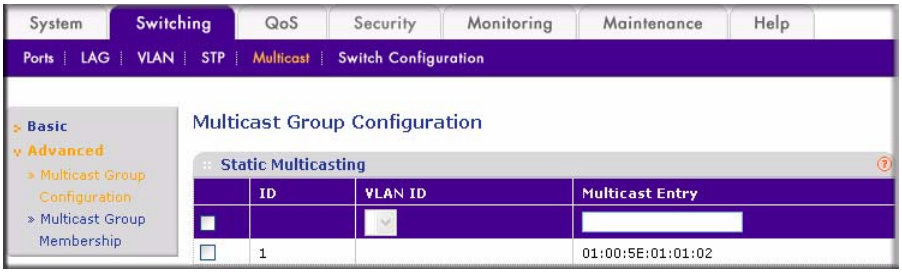

Figure 4-17

To delete a static multicast entry:

1. Select the checkbox adjacent to the multicast group you want to delete.
2. Click **Delete.**

Multicast Group Membership

The Multicast Group Membership table displays the ports associated with each multicast group.

To configure the multicast group membership:

1. Select Switching > Multicast > Advanced > Multicast Group Membership. The Multicast Group Membership screen will display
2. From the ID pull-down menu, select a multicast group that you created in the Multicast Group Configuration screen.
3. Click the **Unit 1** link. All the available ports will display. Select the ports for the Multicast Group (Select the Unit 1 checkbox to select all ports.)
4. Click **Apply.**

Figure 4-18

To remove a multicast group:

1. In the line of the table that specifies the group, check the **Delete** box.
2. Click **Apply** to remove the group.

Enabling Jumbo Frames

Jumbo Frames are not an approved standard Ethernet frame size, so you must ensure that all of your networking equipment can support these nonstandard jumbo frames to prevent them from being dropped. The Jumbo Frame screen allows you to enable or disable jumbo frame support. The maximum default frame size is 1,518 bytes. When jumbo frame support is enabled, the frame size can vary from 64 bytes to 9,216 bytes. Jumbo frames is disabled by default.

To configure a jumbo frame:

1. Select Switching > Switch Configuration from the main menu. The Jumbo Frame Configuration will display.
2. In the **Jumbo** Frame radio box, select **Enable**.
3. Click **Apply.**

Setting Rate Limits

Rate Limiting determines the bandwidth of ingress and egress traffic for a specific port.[1] There are 11 data rate options in the range 512K bps to 1000M bps, including a disable option that applies no limit to the data rate. Ingress and egress rates are separately configurable.

To configure the rate limit for a specific port:

1. Select QoS > Basic > Rate Limit. The Rate Limit | Rate Control Setting screen will display.
2. Select the checkbox adjacent to the port you want to configure.
3. In the top row, select the rate limitations from the pull-down menus:
   - In the **Ingress Rate** list, select the rate limitation of incoming traffic in this port.
   - In the **Egress Rate** list, select the rate limitation of outgoing traffic in this port.
4. Click **Apply**.

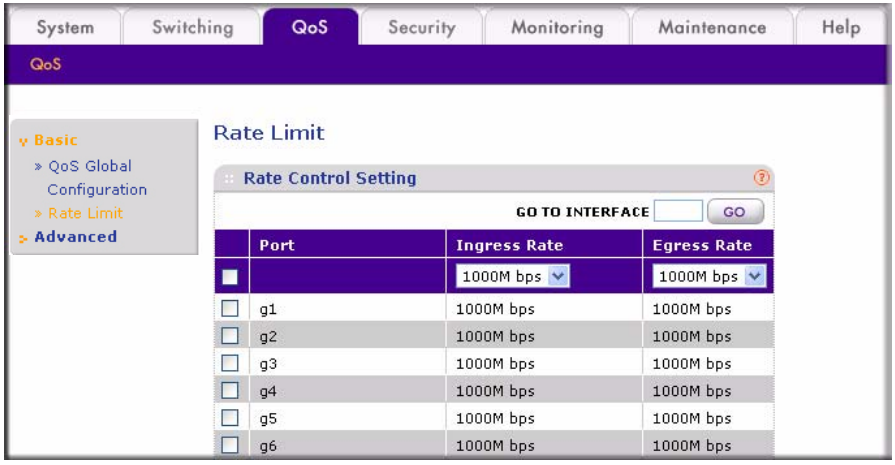

Figure 4-19

Setting QoS Global Configuration

Quality of Service (QoS) is used to manage traffic in a network by treating different types of traffic with different levels of priority. Higher priority traffic receives preferential treatment during times of switch congestion.

1. Egress rate limiting is available only with v3 hardware.

Two possible system mode implementations of QoS are supported:

- **IEEE 802.1p-based QoS.**
- **DSCP-based (Differentiated Services Code Point) QoS.**

To specify the QoS Global system mode:

1. Select QoS > Basic > QoS Global Configuration from the main menu. The QoS Global Configuration screen will display.
2. Select either the **802.1p Based** radio box or the **DSCP Based** radio box.
3. Click **Apply.**

IEEE 802.1p-Based QoS

IEEE 802.1p-based QoS enables the user to map each of the eight priority levels specified in IEEE 802.1p (p0 to p7) to one of four internal hardware priority queues: **High**, **Normal**, **Low**, and **Lowest**. The eight priority levels specified in IEEE 802.1p (p0 to p7) are implemented by a three-bit priority field in the VLAN tag. The switch empties the four hardware priority queues in order, from High to Lowest. Packets are transferred to empty the buffers of each higher hardware priority queue in turn before the next lower hardware priority queue can begin to transfer its received packets through the switch.

The 802.1p to Queue Mapping table contains fields for mapping 802.1p priority values to the four hardware traffic queues

To map 802.1p priorities to queues:

1. Select QoS > Advanced > 802.1p Queue Mapping. The 802.1p to Queue Mapping screen will display.

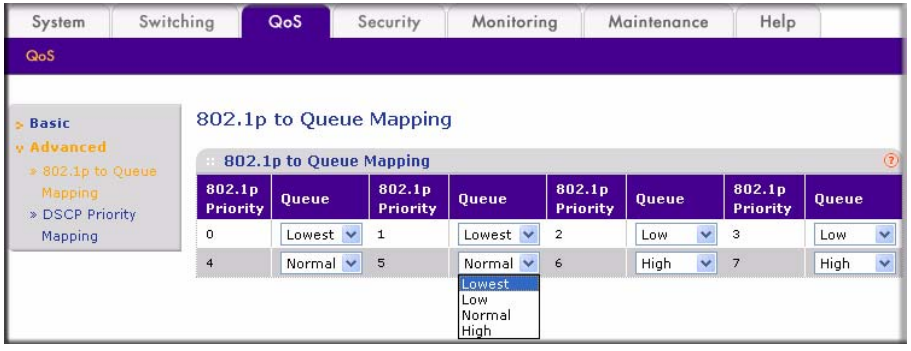

Figure 4-20

2. From each 802.1p priority value pull-down menu, select one of the four hardware priority queues.
3. Click **Apply.**

Differentiated Services Code Point (DSCP)-based QoS

The DSCP 6-bit field in an IP packet header enables levels of service to be assigned to network traffic according to the field's binary value. This 6-bit field comprises three IP Precedence MSBs with a least-significant 3-bit expansion field as defined in RFC 2474. The IP Precedence bits in the DSCP field are compatible with routers that only support IP Precedence. DSCPs specifically tailored to be backward compatible with routers that only support IP precedence lack the 3-bit expansion field and are called Class-selector DSCPs.

The DSCP to Priority Mapping table contains fields for mapping DSCP values to the eight 802.1p priority values. For the DSCP QoS to work properly, make sure that the priority values are correctly mapped to the appropriate hardware queues.

To map DSCP values to 802.1p priorities:

1. Select QoS > Advanced > DSCP Priority Mapping from the main menu. The DSCP to Priority Mapping screen will display.
2. Select one of the eight priority values for each DSCP value.
   - Match these DHCP values to set "Per Hop Behavior" (PHB) priorities by selecting a QoS service-class value of between 0 and 7. Packets within these service classes are treated with equal priority.
   - RFC 2597 defines the assured forwarding (AF) PHB. It guarantees a certain amount of bandwidth to an AF class.
   - The Expedited Forwarding (EF) PHB is defined in RFC 2598 and uses Codepoint 101110. The EF PHB is used to build a low loss, low latency, low jitter, assured bandwidth service. This premium service can appear to the user be a point to point connection.
3. Click **Apply**.

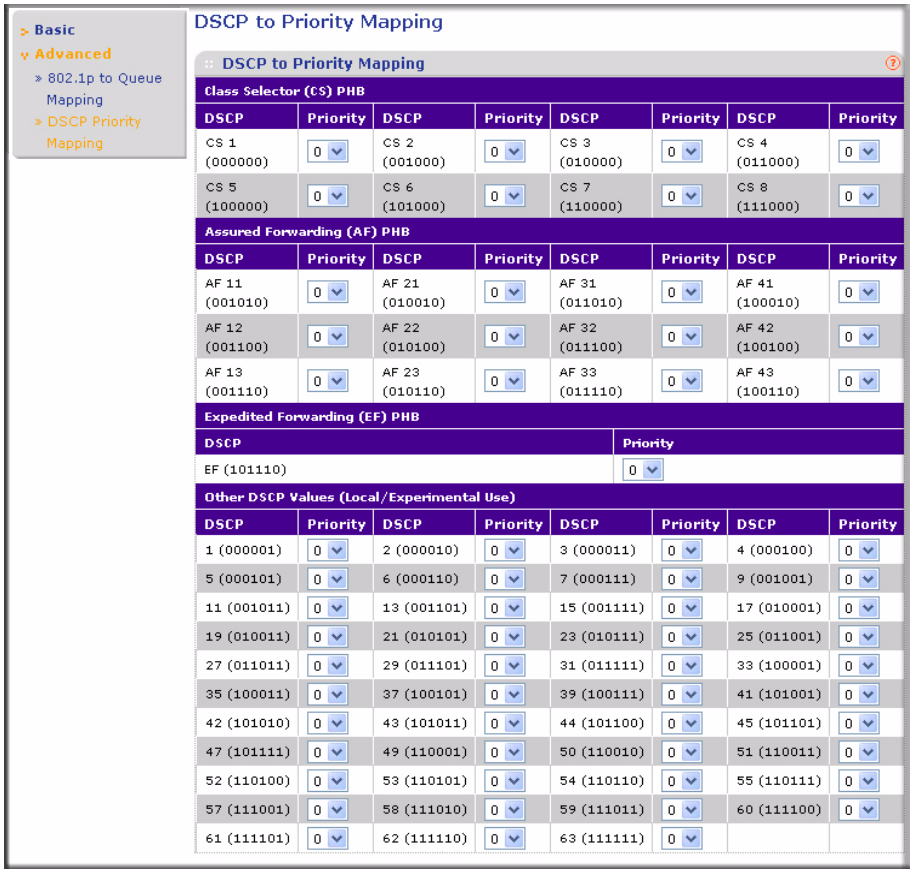

Figure 4-21

Enabling Storm Control

The Storm Control feature enables you to prevent network performance from being disrupted by specifying the threshold of ingress broadcast or multicast and broadcast packets on each port. The traffic source may be Multicast and Broadcast; Broadcast only; or Unknown Unicast, Multicast or Broadcast—or it may be disabled. A selected received threshold rate of between 1000 and 65535 packets per second may be specified in each case. If Multicast and Broadcast is selected as the source of the traffic, then the threshold value is the combined rate of both types of packet. If the incoming traffic rate of the specified packet types is above the specified value, the packets are discarded.

The Storm Control Settings table contains system-wide configuration parameters for storm control.

To configure storm control:

1. Select Security > Traffic Control. The Storm Control screen will display.

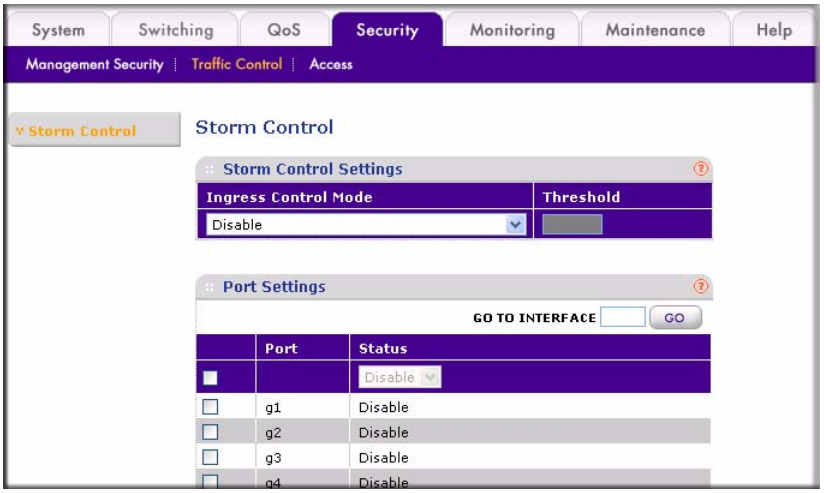

Figure 4-22

2. From the **Ingress Control Mode** pull-down menu, select the type of the packet storm:
   - Disable (to turn off storm control)
   - Unknown Unicast, Multicast and Broadcast
   - Multicast and Broadcast
   - Broadcast Only
3. In the Threshold field, specify the threshold rate limit (packets per seconds) for storm control. The valid range is from 1000 to 65535.
4. Click **Apply**.

You must enable the Storm Control feature on each port individually from the Port Settings table. Storm Control is disabled on every port by default.

To enable Storm Control:

1. Select Security > Traffic Control. The Storm Control screen will display.
2. Select the checkbox adjacent to the port that you want to change.

3. In the top row, from the **Status** pull-down menu, select either **Enable** or **Disable**.
4. Click **Apply**.

Configuring the IP Access List

The IP Access List table allows you to limit and specify the IP addresses that can access the management portion of the switch. An empty list means that all IP addresses are allowed to access the switch. Otherwise, the switch will respond only to requests from computers with an IP address in the list. So make sure that you include the IP address of your PC if you are setting this feature. The list can have a maximum of 10 IP addresses.

To add an entry to the IP Access list:

1. Select Security > Access > IP Access List from the main menu. The IP Access List will display.
2. In the IP Address field of the configuration row, enter the IP address of the PC that you want to manage the switch from.
3. Click **Add.**

To delete an entry from the IP Access list:

1. Select the checkbox adjacent to the entry of the IP address you want to remove.
2. Click **Delete**.

Controlling Switch Access by MAC Address and VLAN ID

The Trusted MAC table shows all the Trusted MAC addresses that you can specify to allow forwarded traffic to the switch. The maximum number of trusted MAC addresses is 256 per system. All source MACs are trusted when the Trusted MAC list is empty. If the list includes MAC addresses, any incoming traffic with a source MAC address that is not included in the trusted MAC table is dropped.

If the VLAN mode for the switch is set up as Port-based, you enter a MAC address and port number that you want to permit access this switch. If the VLAN is set up in 802.1Q mode, you enter a MAC address and VLAN ID to permit access

To add a trusted MAC address:

1. Select Security > Access > Trusted MAC. The Trusted MAC screen will display.

2. Specify the trusted MAC address parameters in the configuration row:
   - **Interface**. From the **Interface** pull-down menu, select the interface or port that you want to have this feature.
   - **MAC Address**. Specify the trusted source MAC address.
   - **VLAN ID.** Enter a VLAN ID that the interface belongs to if the 802.1Q VLAN mode is enabled.
3. Click **Add**.

To delete a trusted MAC address:

1. Select the checkbox adjacent to the trusted MAC entry that you want to delete from the list.
2. Click **Apply**.

Setting up Mirroring or "Sniffer Ports"

Port Mirroring allows you to configure traffic from any number of ports to be copied (mirrored) to your selected "sniffer" port, which may be any port that is not a source port. This traffic may be selected from transmitted or outgoing (egress) frames, received or incoming (ingress) frames or all frames. A port cannot be both a mirrored and a destination port at the same time. Sniffing may be disabled globally.

To configure port mirroring:

1. Select Monitoring > Mirroring. The Port Mirroring screen will display.
2. From the Destination Port pull-down menu, select a port to be the destination port. All mirrored traffic will be routed to this port.
3. From the **Mirroring** pull-down menu, select the mirroring mode. The possible settings are:
   - **Tx and Rx**. Mirrors both incoming and outgoing traffic on the designated source ports.
   - **Rx Only**. Mirrors only the incoming traffic to the designated source ports.
   - **Tx Only**. Mirrors only the outgoing traffic to the designated source ports.
   - **Disable**. Disables port mirroring globally.
4. Select the Source Port check boxes for the ports to be mirrored. Clear the check boxes for the ports you do not want to be mirrored.
5. Click **Add**.

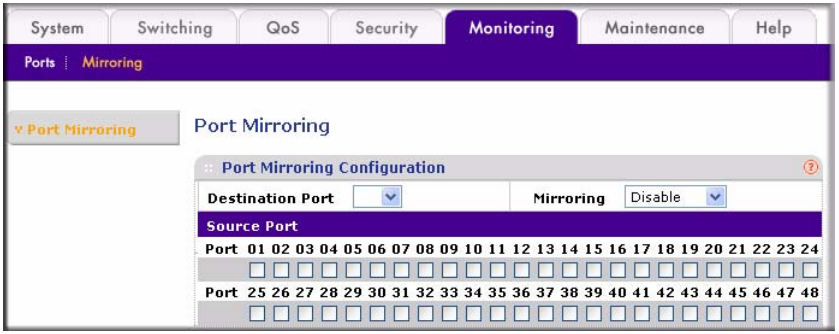

Figure 4-23

Viewing Packet Statistics

The Port Statistics screen shows reports of packet traffic and packet errors formatted as follows:

- **Port Selection**: The port number on the switch—selected from the Port pull-down menu.
- **Statistics**: Detailed Tx and Rx statistical information, by port.
- **Summary Statistics**: All ports Tx and Rx statistics summarized. Presents the information from each port's internal counters.

To view statistics for a single port:

1. From the **Port** pull-down menu, select the port number.
2. Click **Apply.**

To retrieve summary statistics.

1. Click **Refresh** to retrieve the current count from the device and update the tables.
2. Click **Clear Counters** to reset all counters to zero.

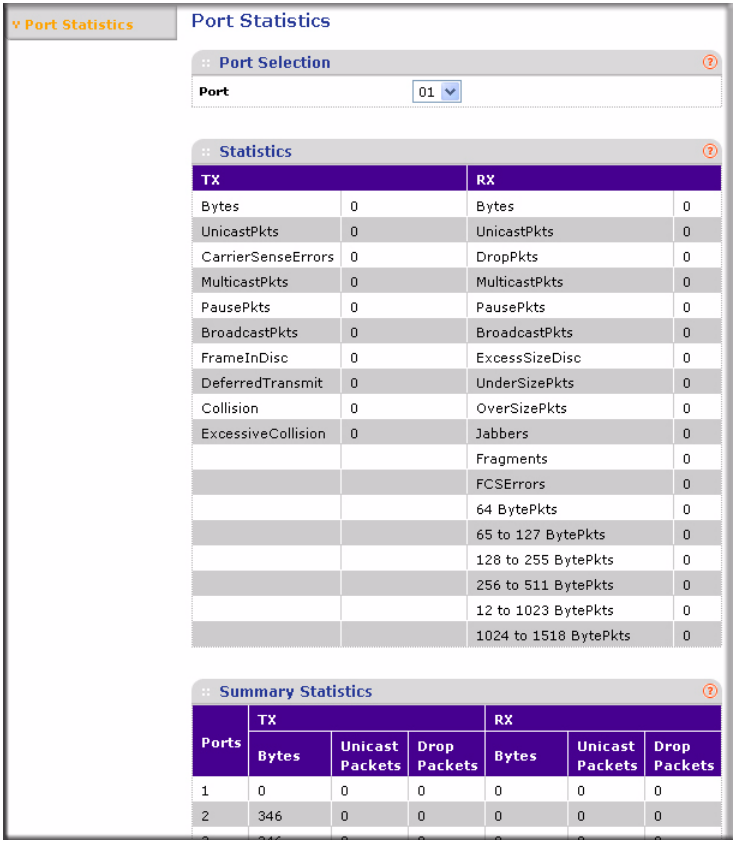
Port Statistics
Port Statistics
Port Selection
Port
01
Statistics
TX
Bytes 0
UnicastPkts 0
CarrierSenseErrors 0
MulticastPkts 0
PausePkts 0
BroadcastPkts 0
FrameInDisc 0
DeferredTransmit 0
Collision 0
ExcessiveCollision 0
RX
Bytes 0
UnicastPkts 0
DropPkts 0
MulticastPkts 0
PausePkts 0
BroadcastPkts 0
ExcessSizeDisc 0
UnderSizePkts 0
OverSizePkts 0
Jabbers 0
Fragments 0
FCSErrors 0
64 BytePkts 0
65 to 127 BytePkts 0
128 to 255 BytePkts 0
256 to 511 BytePkts 0
12 to 1023 BytePkts 0
1024 to 1518 BytePkts 0
Summary Statistics
Ports
TX
Bytes
Unicast Packets
Drop Packets
RX
Bytes
Unicast Packets
Drop Packets
1 0 0 0 0 0 0
2 346 0 0 0 0 0

Figure 4-24