GIGABIT WEB-SMART SWITCH USER MANUAL

MODELS 524063
& 524087

Shown: Model 524063, 24-Port

INTELLINET™
NETWORK SOLUTIONS

INT-524063/524087-UM-0112-03

Thank you for purchasing the INTELLINET NETWORK SOLUTIONS™ Gigabit Web-Smart Switch, Model 524063 (24-Port) or Model 524087 (16-Port).

This handy device lets you increase the speed of your network with 10/100/1000 Mbps auto-sensing ports that automatically detect optimal network speeds, and it lets you increase the speed of your own work through user-friendly Web-based management for uncomplicated administration.

Easy-to-follow instructions in this user manual help make installation of the switch quick and simple, so you'll also soon be enjoying the benefits of these additional features:

- All RJ45 ports with Auto-MDIX (auto uplink) support
- Supports NWay auto-negotiation
- Broadcast storm control with multicast packet rate settings
- Store and forward switching architecture
- Packet filtering/forwarding rates: 1,488,000 pps (1000 Mbps), 148,800 pps (100 Mbps), 14,880 pps (10 Mbps)
- Supports port controls (speed, flow control and maximum frame size)
- Supports VLAN (tag-based and port-based)
- Supports link aggregation (trunking)
- Provides IEEE 802.1x port-based security
- Supports port mirroring
- 19" rackmount
- LEDs for power, link/activity, connection speed
- Supports IEEE802.1D Spanning Tree Protocol
- Supports static priority, ToS, 802.1p Class of Service with 4-level priority queuing
- Three-Year Warranty

Some of the following screen images have been modified to fit the format of this user manual.

NOTE: For a quick install procedure, refer to the printed quick install guide enclosed with this product.

CONTENTS

SAFETY & COMPLIANCE STATEMENTS

FEDERAL COMMUNICATIONS COMMISSION (FCC) STATEMENT

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

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

CE STATEMENT

This equipment complies with the requirements relating to electromagnetic compatibility, EN 55022 class A for ITE, the essential protection requirement of Council Directive 89/336/EEC on the approximation of the laws of the member states relating to electromagnetic compatibility.

HARDWARE INSTALLATION

SELECTING A SITE FOR THE SWITCH

As with any electrical device, you should place the switch where it will not be subjected to extreme temperatures, humidity or electromagnetic interference. Specifically, the site you select should meet the following requirements:

- The ambient temperature should be between 32 and 104 degrees Fahrenheit (0 to 40 degrees Celsius).
- The relative humidity should be less than 90 percent, non-condensing.
- Surrounding electrical devices should not exceed the electromagnetic field (RFC) standards for IEC 801-3, Level 2 (3V/M) field stength.
- Make sure that the switch receives adequate ventilation. Do not block the fan exhaust port on the switch.
- The power outlet should be within 1.5 meters of the switch.
- Do not place objects on top of the unit.
- Always avoid dust and dirt.

CONNECTING TO POWER

1. Connect the AC power cord to the receptacle on the back of the switch, then plug it into a standard AC outlet with a voltage range from 180 to 260 V AC.
2. Disconnect the power cord if you want to shut down the switch.

CABLING

1. Ensure the power of the switch and end devices is turned off. ***NOTE:*** Always ensure that the power is off before any installation.
2. Prepare cable with corresponding connectors for each type of port in use.
3. Connect one end of the cable to the switch and the other end to a desired device.
4. Once the connections between two end devices are made successfully, turn on the power and the switch is operational.

WEB-BASED BROWSER MANAGEMENT

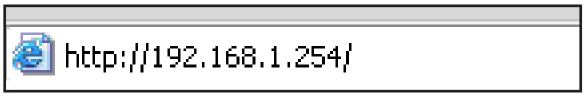
The Gigabit Web-Smart Switch switch provides an Administration Authority that lets you configure and manage the switch remotely. This section describes how to configure the switch using its Web-based browser management interface.

Switch Access

The advanced management capabilities of the switch can be accessed using a standard Internet browser. To access the Web-based management interface, configure the management station with an IP address and subnet mask that are compatible with your switch.

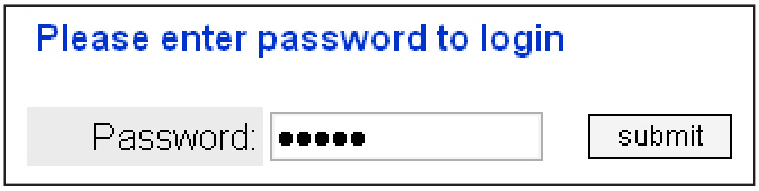
The factory defaults are 192.168.1.254 for the IP address; 255.255.255.0 for the subnet mask.

1. Activate your Web browser and enter the IP address (192.168.1.254) in the address field.



http://192.168.1.254/

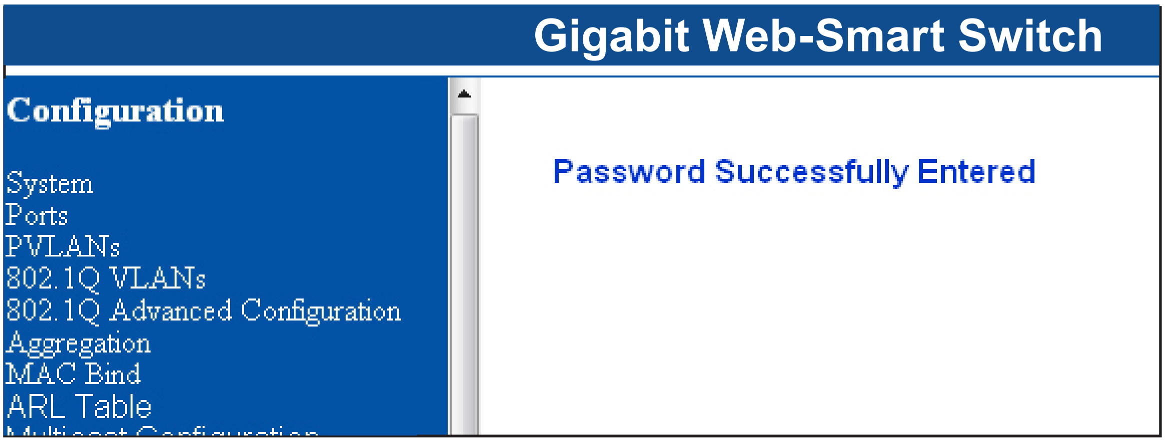
2. Select the Administration Authority and key in the password. The factory default for the password is “admin.”



Please enter password to login

Password: ●●●●●

After login, the initial menu screen displays. Click on the links on the left side of each screen to access the various management functions.



Gigabit Web-Smart Switch

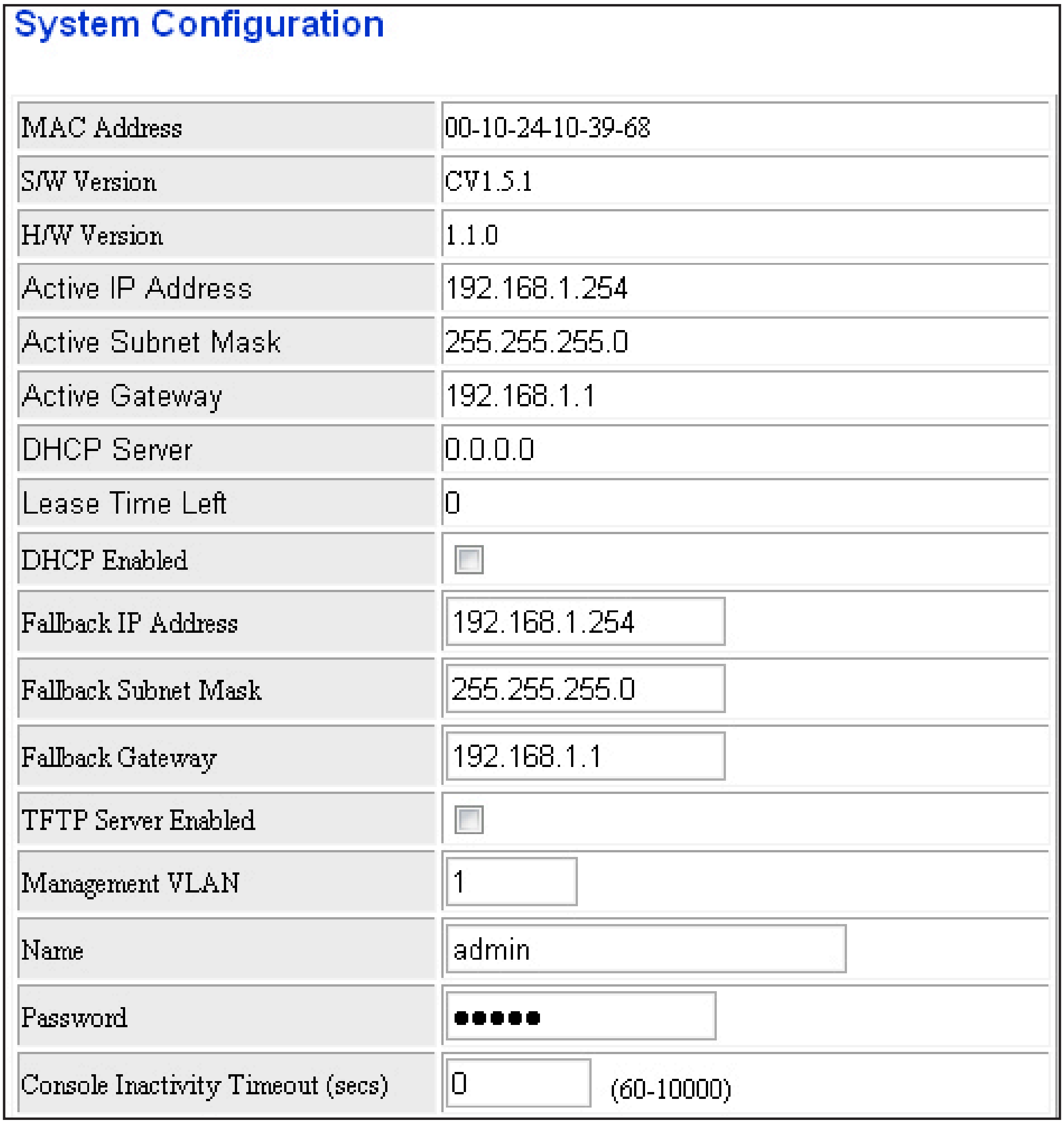
Password Successfully Entered

Configuration

The Configuration menu includes the following subsections: System, Ports, PVLANs, 802.1Q VLANs, Aggregation, MAC Binding, ARL Table, Multicast Configuration, RSTP, Mirroring, Quality of Service, Filter, Rate Limit and Storm Control.

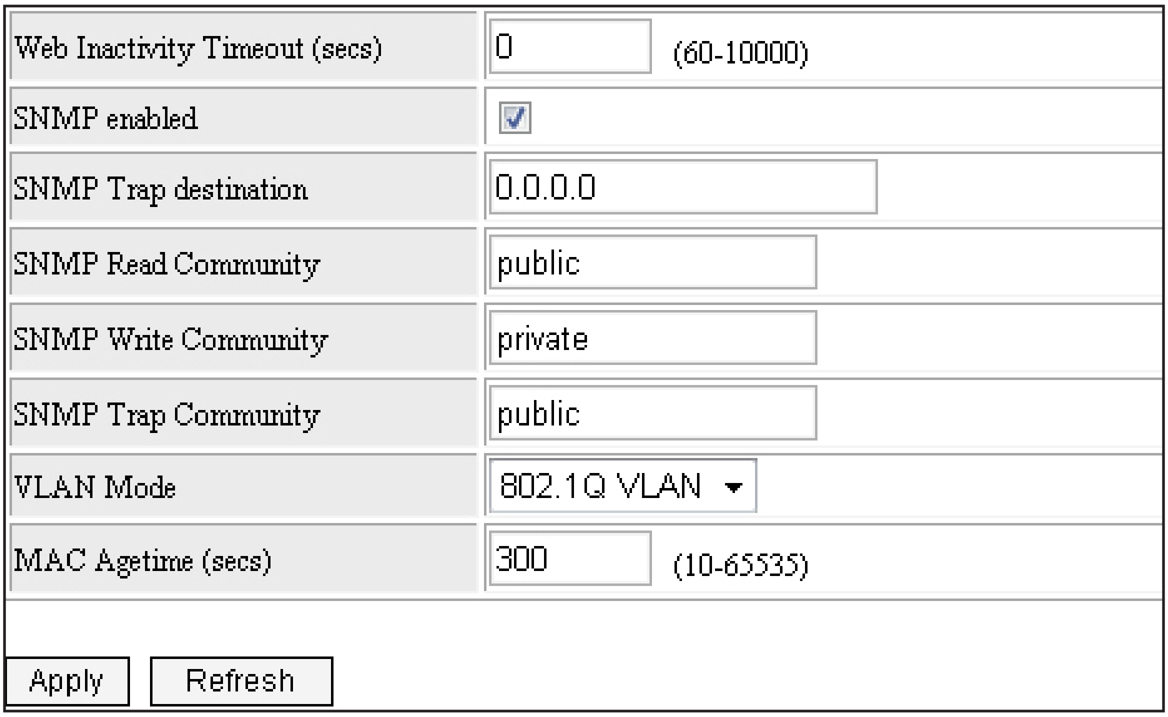
SYSTEM

This screen provides the current status of the device. Click “Apply” so any changes that are made will take effect.



System Configuration

MAC Address	00-10-24-10-39-68
S/W Version	CV1.5.1
H/W Version	1.1.0
Active IP Address	192.168.1.254
Active Subnet Mask	255.255.255.0
Active Gateway	192.168.1.1
DHCP Server	0.0.0.0
Lease Time Left	0
DHCP Enabled	□
Fallback IP Address	192.168.1.254
Fallback Subnet Mask	255.255.255.0
Fallback Gateway	192.168.1.1
TFTP Server Enabled	□
Management VLAN	1
Name	admin
Password	●●●●●
Console Inactivity Timeout (secs)	0 (60-10000)



Web Inactivity Timeout (secs)	0 (60-10000)
SNMP enabled	☑
SNMP Trap destination	0.0.0.0
SNMP Read Community	public
SNMP Write Community	private
SNMP Trap Community	public
VLAN Mode	802.1Q VLAN ▾
MAC Agetime (secs)	300 (10-65535)

S/W Version: This is the software version of this device.

H/W Version: This is the hardware version of this device.

Active IP Address: Displays the current effective IP address of the device.

Active Subnet Mask: Displays the current effective subnet mask of the device.

Active Gateway: Displays the current effective gateway of the device.

DHCP Server: If the device uses the DHCP server to connect to the network, the system will display the IP address of the DHCP server. The default value is 0.0.0.0, indicating the DHCP is disabled.

Lease Time Left: Displays the real remaining lease time to the DHCP server.

DHCP Enabled: Either “Enabled” or “Disabled” (default). Specifies whether the IP address is static or dynamically assigned via DHCP. “Enabled” is a special case of a dynamically assigned IP address. DHCP is widely used in LAN environments to dynamically assign IP addresses from a centralized server, which reduces the overhead of administrating IP addresses.

Fallback IP Address: XXX.XXX.XXX.XXX, where XXX ranges from 0 to 255. Default: 192.168.1.254. Specifies the IP address of this device. An IP address is a 32-bit number that is notated by using four segments of numbers, each from 0 through 255, separated by periods. Only a unicast IP address is allowed, which ranges from 1.0.0.0 to 233.255.255.255.

Fallback Subnet Mask: XXX.XXX.XXX.XXX, where XXX ranges from 0 to 255. Default: 255.255.255.0. Specifies the IP subnet mask of this device. An IP subnet mask is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods. Typically, subnet mask numbers use either 0 or 255 as values (e.g., 255.255.255.0), but other numbers can appear.

Fallback Gateway: XXX.XXX.XXX.XXX, where XXX ranges from 0 to 255. Default: 192.168.1.1. Specifies the default gateway IP address. It is only required if you intend to manage the device from another LAN connected via an IP router. The gateway address must be on the same IP subnet as this device.

NOTE: After applying a new IP address, a new login page will automatically appear. Log in again to proceed to other configurations.

TFTP Server Enabled: Either “Enabled” or “Disabled” (default). When you want to use the TFTP upgrade model from the console, enable this parameter.

Management VLAN: The number ranges from 1 to 4094. Default: 1. Modify this parameter with care! It specifies the VLAN through which the switch can be managed. By default, the switch is programmed to use VLAN 1 for management and every port on the switch is programmed to use VLAN 1. If you modify a switch port to use a VLAN other than the management VLAN, devices on that port will not be able to manage the switch. If you change the management VLAN without having at least one port that supports the new management VLAN number, you will lose the ability to contact the management package. The switch will immediately stop responding to any pings, TFTP, Telnet and Web sessions from the old management VLAN. For this reason, it’s suggested that modification of VLAN management information be made early in the switch-commissioning process, and via the console port.

Name: 16-character ASCII string. Default: admin. The system name can make it easier to identify the switches within your network provided that all switches are given a unique name.

Password: 16-character ASCII string. Default: admin. From here, you can modify the default management password.

Console Inactivity Timeout (secs): 0 or 60 to 10000. Default: 0. Specifies when the console will time out and display the login screen if there is no user activity. A value of zero disables timeouts for console users. For console users, the maximum timeout value is limited to 10,000 seconds.

Web Inactivity Timeout (secs): 0 or 60 to 10000. Default: 0. Specifies when the Web management interface will time out and display the login screen if there is no user activity. A value of zero disables timeouts for Web management users. For Web server users, the maximum timeout value is limited to 10,000 seconds.

SNMP Enabled: Either “Enabled” or “Disabled” (default). This parameter enables or disables SNMP access to the device. The device supports Simple Network Management Protocol Version 1 and Version 2 (SNMPv1 and SNMPv2), which provide access to devices over the network.

SNMP Trap Destination: XXX.XXX.XXX.XXX, where XXX ranges from 0 to 255.

Default: 0.0.0.0. This is the IP address of the user's SNMP management station if it is configured to receive traps and notifications.

SNMP Read Community: Any 20 characters. Default: public. This parameter identifies the MIB tree(s) to which this entry authorizes read access.

SNMP Write Community: Any 20 characters. Default: private. This parameter identifies the MIB tree(s) to which this entry authorizes write access.

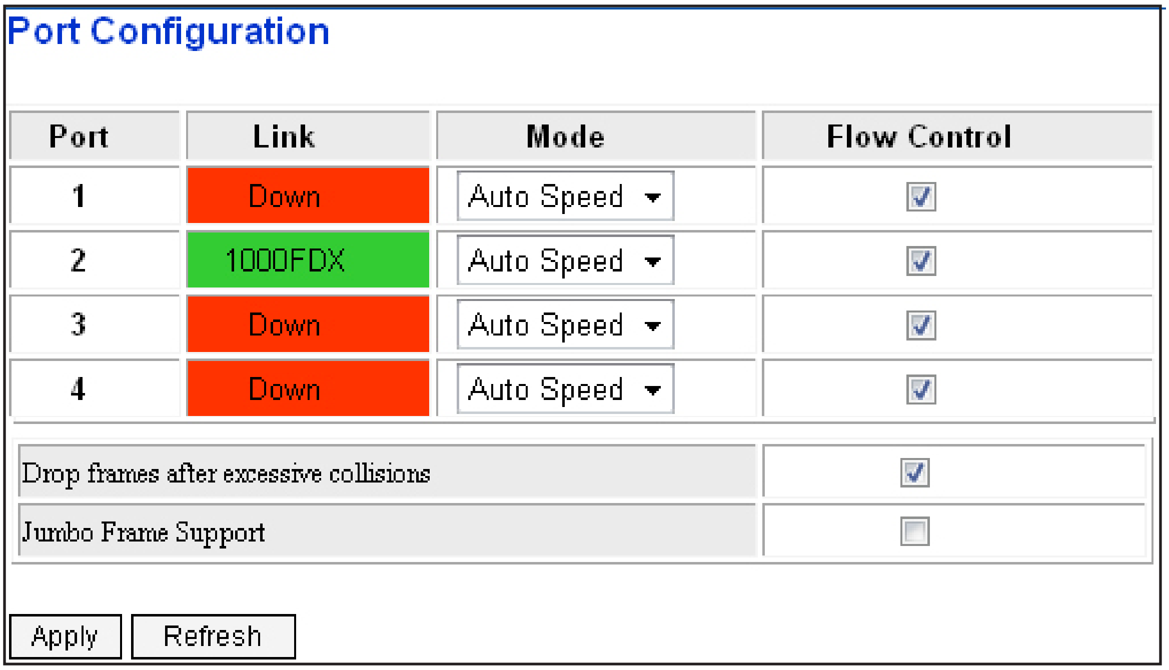
SNMP Trap Community: Any 20 characters. Default: public. This parameter identifies the MIB tree(s) to which this entry authorizes access for notifications.

VLAN Mode: Either "Port-based" or "802.1Q VLAN" (default). Specifies the VLAN mode to configure the 802.1Q-based VLAN or the port-based VLAN, or to close the function. This device supports Virtual VLAN, which means the network can be segmented into groups to reduce collisions caused by wide broadcasting. The device supports both port-based VLAN and 802.1Q tag-based VLAN: Port-based VLAN directs incoming packets to VLANs according to their ingress ports; 802.1Q tag-based VLAN adds a tag to the header of the packet to direct the packet to the right VLAN. ***NOTE:*** When you change the VLAN mode, the system will reboot.

MAC Agetime (secs): 10 to 65535. Default: 300 seconds. This configures the time a learned MAC address is held before being aged out.

PORTS

On this screen, you can configure the function of each port, including Mode and Flow Control settings. Select the port number and set its function, then click "Apply" to save the new settings to the device.



Port Configuration

Port	Link	Mode	Flow Control
1	Down	Auto Speed	☑
2	1000FDX	Auto Speed	☑
3	Down	Auto Speed	☑
4	Down	Auto Speed	☑

Drop frames after excessive collisions	☑
Jumbo Frame Support	□

Link: Displays the current link status of each port: "1000MFDX," "100MFDX," "100MHDX," "10MFDX," "10MHDX" or "Down." The field lights green and shows the link speed if there is a valid connection on the port.

Mode: Options are "Auto speed," "10M/Half," "10M/Full," "100M/Half," "100M/Full," "1000M/Full" and "Disabled." Default: Auto. Enabling auto-negotiation ("Auto") results in speed and duplex being negotiated upon link detection; both end devices must be auto-negotiation compliant for the best possible results. 10Mbps and 100Mbps fiber optic media don't support auto-negotiation, so these media must be explicitly configured to either half or full duplex. Full duplex operation requires that both ends be configured as such; otherwise, severe frame loss will occur during heavy network traffic. "Auto" supports all speed and duplex modes. Disabling a port (for troubleshooting or to secure it from unauthorized connections, perhaps) will prevent all frames from being sent and received on that port. Also, when disabled, link integrity pulses aren't sent, so the link/activity LED will never be lit.

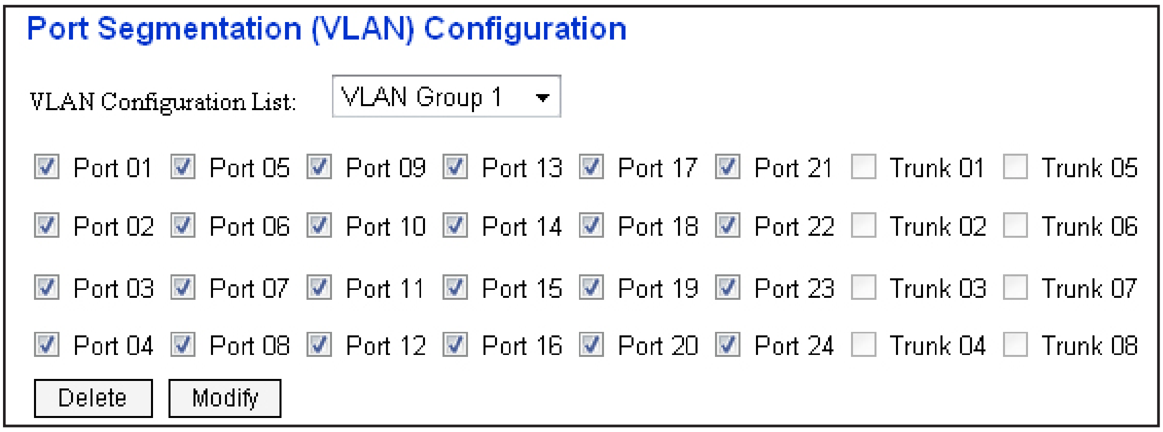
Flow Control: Either "Enabled" or "Disabled" (default). This is useful for preventing frame loss during times of severe network traffic. Examples of this include multiple source ports sending to a single destination port or a higher-speed port bursting to a lower-speed port. When the port is half duplex, it is accomplished using backpressure, in which the switch simulates collisions, causing the sending device to retry transmissions according to the Ethernet backoff algorithm. When the port is full duplex, it is accomplished using PAUSE frame, which causes the sending device to stop transmitting for a certain period of time.

Drop frames after excessive collisions: Either "Enabled" or "Disabled" (default). Enable to discard the frames after excessive collision.

Jumbo Frame Support: Either "Enabled" or "Disabled" (default, or 1518 bytes). Enable to adjust the size of Jumbo Frames to a maximum value of 9600 bytes.

PVLANS

Configure the port-based VLAN members on this screen. You need to configure the current VLAN mode on the System Configuration screen to be PVLAN.



Port Segmentation (VLAN) Configuration

VLAN Configuration List: VLAN Group 1 ▾

☑ Port 01	☑ Port 05	☑ Port 09	☑ Port 13	☑ Port 17	☑ Port 21	□ Trunk 01	□ Trunk 05
☑ Port 02	☑ Port 06	☑ Port 10	☑ Port 14	☑ Port 18	☑ Port 22	□ Trunk 02	□ Trunk 06
☑ Port 03	☑ Port 07	☑ Port 11	☑ Port 15	☑ Port 19	☑ Port 23	□ Trunk 03	□ Trunk 07
☑ Port 04	☑ Port 08	☑ Port 12	☑ Port 16	☑ Port 20	☑ Port 24	□ Trunk 04	□ Trunk 08

VLAN Configuration List: Options range from “VLAN Group 1” to ““VLAN Group 24” (default). Specifies the VLAN Group No. to configure its members.

VLAN Members: Options range from “Port 1” to “Port 24” and “Trunk 01” to “Trunk 08” (default: none selected). These are ports that are allowed to be members of the VLAN. A trunk can be selected as a VLAN member, but a trunk group needs to be configured first. ***NOTE:*** Model 524063 (24-Port) allows up to 12 member ports per trunk; Model 524087 (16-Port) allows up to 8 member ports per trunk.

Delete: Click to delete the current VLAN Group configuration.

Modify: Click to complete the current VLAN configuration.

802.1Q VLANS

A virtual LAN, or VLAN, is a group of devices on one or more LAN segments that communicate as if they were attached to the same physical LAN segment. VLANs are extremely flexible because they are based on logical instead of physical connections. When VLANs are introduced, all traffic in the network must belong to one or another VLAN. Traffic on one VLAN cannot pass to another, except through an intranetwork router or Layer 3 switch. A VLAN tag is the identification information that is present in frames in order to support VLAN operation.

Tagged vs. Untagged Frames

Tagged frames are frames with 802.1Q (VLAN) tags that specify a valid VLAN identifier (VID). Untagged frames are frames without tags or frames that carry 802.1p (Prioritization) tags only having prioritization information and a VID of 0. Frames with a VID of 0 are also called priority-tagged frames. When a switch receives a tagged frame, it extracts the VID and forwards the frame to other ports in the same VLAN.

Native VLAN

Each port is assigned a native VLAN number, the port VLAN ID (PVID). When an untagged frame ingresses a port, it is associated with the port’s native VLAN. By default, when the switch transmits a frame on the native VLAN, it sends the frame untagged, but can be configured to transmit frames on the native VLAN tagged.

VLAN Ingress and Egress Rules

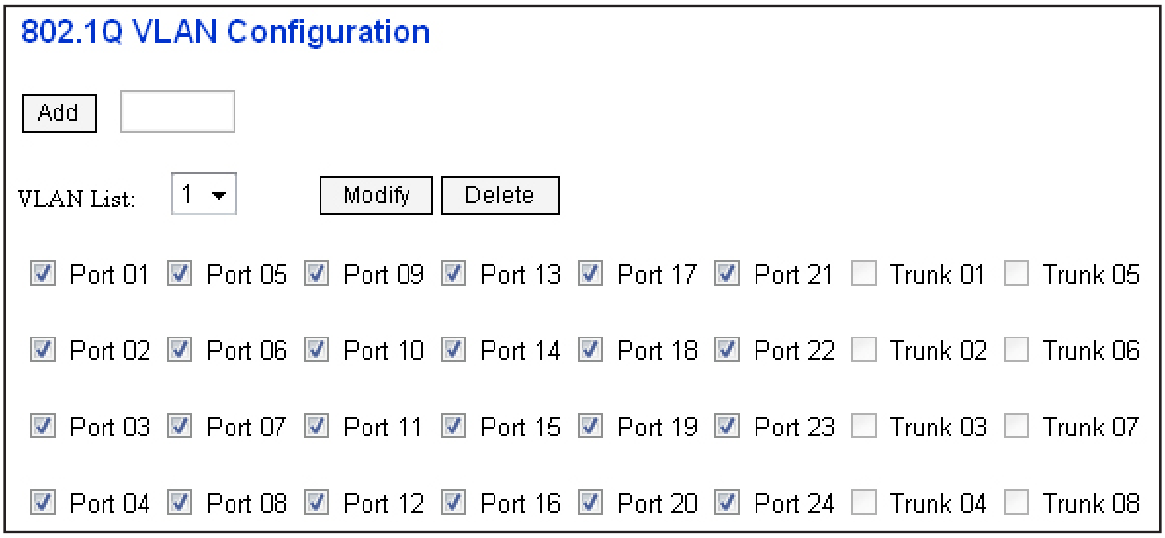
Ingress rules are the rules applied to all frames when they are *received* by the switch, as indicated below.

Frame received This doesn't depend on ingress port 's VLAN configuration parameters	Untagged	Priority Tagged (VID=0)	Tagged (valid VID)
VLAN the frame associated with	PVID	PVID	VID in the tag
Frame dropped due to its tagged/untagged format	No	No	No
Frame dropped, if associated with VLAN not configured (or learned) in the switch	N/A	N/A	Yes
Frame dropped, if ingress port is not a member of the VLAN the frame associated with	N/A	N/A	No

Egress rules are the rules applied to all frames when they are *transmitted* by the switch, as indicated below.

Frame sent Egress port type	On egress port's native VLAN	On other VLAN	
		Port is member of the VLAN	Port is NOT member of the VLAN
Edge	According to the egress port's "PVID Format" parameter	N/A (frame is dropped)	
Trunk		Tagged	dropped

From here, you can configure the IEEE 802.1Q tag-based VLAN members. You need to configure the current VLAN mode on the System Configuration screen to be 802.1Q VLAN.



802.1Q VLAN Configuration

Add

VLAN List: 1 Modify Delete

☑ Port 01 ☑ Port 05 ☑ Port 09 ☑ Port 13 ☑ Port 17 ☑ Port 21 □ Trunk 01 □ Trunk 05

☑ Port 02 ☑ Port 06 ☑ Port 10 ☑ Port 14 ☑ Port 18 ☑ Port 22 □ Trunk 02 □ Trunk 06

☑ Port 03 ☑ Port 07 ☑ Port 11 ☑ Port 15 ☑ Port 19 ☑ Port 23 □ Trunk 03 □ Trunk 07

☑ Port 04 ☑ Port 08 ☑ Port 12 ☑ Port 16 ☑ Port 20 ☑ Port 24 □ Trunk 04 □ Trunk 08

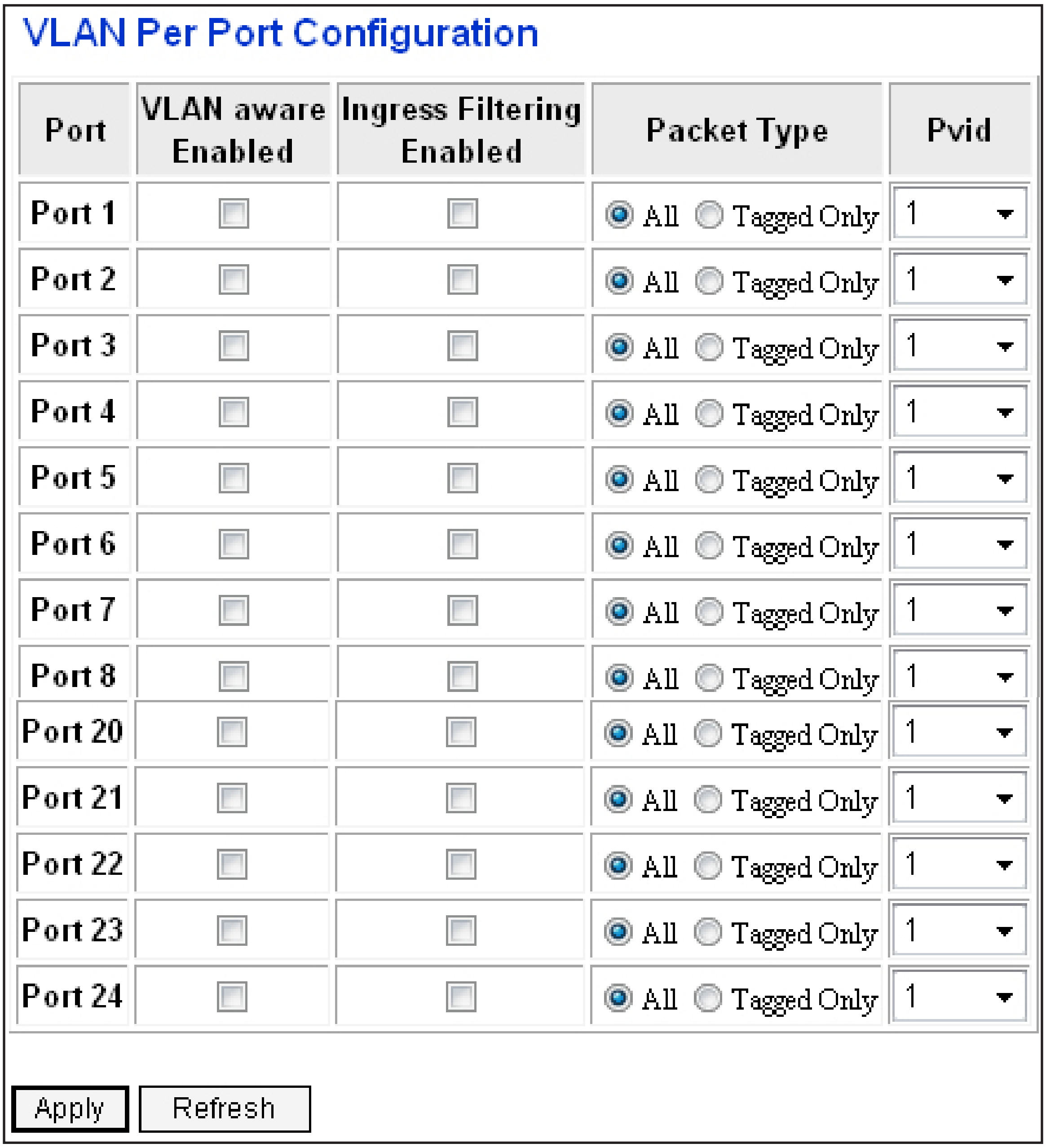
VLAN List: Options range from "1" (default) to "4094." Specifies the VLAN ID to configure its members. First you need to click "Add" to add your VLAN ID.

VLAN Members: Options range from "1" to "24" and "Trunk 01" to "Trunk 08" (default: none selected). These are ports that are allowed to be members of the VLAN. A trunk can be selected as a VLAN member, but a trunk group needs to be configured first.

Delete: Click to delete the current VLAN Group configuration.

Modify: Click to complete the current VLAN configuration.

When your VLAN Mode option is 802.1Q tag-based VLAN, you need to configure the VLAN member port's attribute.



VLAN Per Port Configuration

Port	VLAN aware Enabled	Ingress Filtering Enabled	Packet Type	Pvid
Port 1	□	□	● All ○ Tagged Only	1
Port 2	□	□	● All ○ Tagged Only	1
Port 3	□	□	● All ○ Tagged Only	1
Port 4	□	□	● All ○ Tagged Only	1
Port 5	□	□	● All ○ Tagged Only	1
Port 6	□	□	● All ○ Tagged Only	1
Port 7	□	□	● All ○ Tagged Only	1
Port 8	□	□	● All ○ Tagged Only	1
Port 20	□	□	● All ○ Tagged Only	1
Port 21	□	□	● All ○ Tagged Only	1
Port 22	□	□	● All ○ Tagged Only	1
Port 23	□	□	● All ○ Tagged Only	1
Port 24	□	□	● All ○ Tagged Only	1

VLAN Aware: Either “Enabled” or “Disabled” (default). When enabled, the VLAN-aware attribute will be enabled; when disabled, the VLAN-unaware attribute will be enabled. The native operation mode for an IEEE 802.1Q-compliant switch is VLAN-aware. Even if a specific network architecture doesn’t use VLANs, the system default VLAN settings allow the switch to still operate in a VLAN-aware mode while providing functionality required for almost any network application. However, the IEEE 802.1Q standard defines a set of rules that must be followed by all VLAN-aware switches. For example:

- Valid VID range is 1 to 4094 (VID=0 and VID=4095 are invalid)
- Each frame ingressing a VLAN-aware switch is associated with a valid VID
- Each frame egressing a VLAN-aware switch is either untagged or tagged with a valid VID (which means priority-tagged frames with VID=0 are never sent out by a VLAN-aware switch)

It turns out that some applications have requirements conflicting with the IEEE 8202.1Q native mode of operation (e.g., some applications explicitly require priority-tagged frames to be received by end devices). To ensure the required operation in any possible application scenario and provide full compatibility with legacy (VLAN-unaware) devices, the switch can be configured to work in a VLAN-unaware mode. In that mode:

- Frames ingressing a VLAN-unaware switch are not associated with any VLAN
- Frames egressing a VLAN-unaware switch are sent out unmodified; i.e., in the same untagged, 802.1Q-tagged format as they were received.

Ingress Filtering Enabled: Either “Enabled” or “Disabled” (default). When enabled, checks whether the source port and this port are in the same VLAN, only allowing the same VLAN members to forward packets. When disabled, it allows the same PVID packets to receive.

Packet Type: Either “All” or “Tagged Only” (default: All). When selecting “Tagged Only,” the port will only be allowed to receive the tagged frames. “All” allows all packets to access this port.

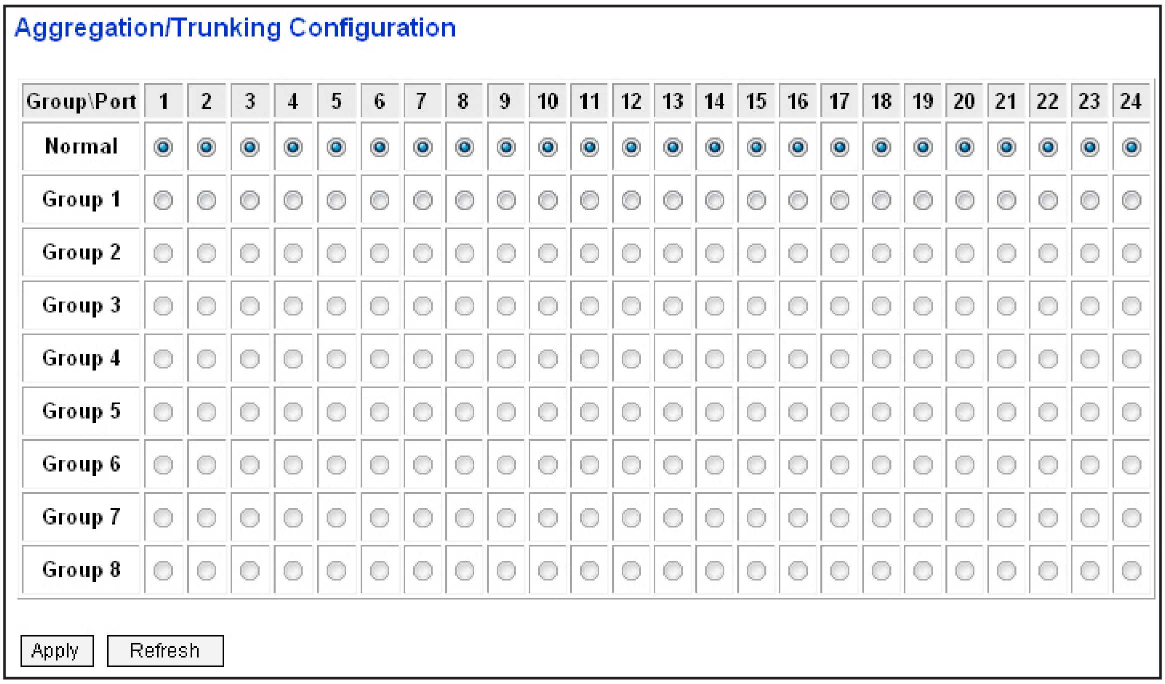
PVID: Default: 1. Specifies the VLAN ID associated with untagged frames received on this port. Frames tagged with a non-zero VLAN ID will always be associated with the VLAN ID retrieved from the frame tag.

AGGREGATION

This screen allows you to aggregate several Ethernet ports into one logical link (port trunk) with a higher bandwidth. Aggregation can be used for two purposes:

- To obtain increased, linearly incremental link bandwidth
- To improve network reliability by creating link redundancy. If one of the aggregated links fails, the switch will balance the traffic between the remaining links.

To set up port trunk groups, put the selected ports’ numbers into the same trunk group. You can configure up to eight groups. Click “Apply” to complete the configuration.



Aggregation/Trunking Configuration

Group\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
Normal	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Group 1	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 2	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 3	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 4	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 5	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 6	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 7	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Group 8	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

Group: Options range from “Group1” to “Group 8” or “Normal” (default). ***NOTE:*** The trunk group number doesn’t affect port trunk operation in any way and is only used for identification. The port of the normal group does not belong to any trunk groups.

Port: Select any combination of numbers valid for this parameter (default: none selected). This creates a list of ports aggregated in the trunk.

Procedure Recommendations and Limitations

Link aggregation is also known as port trunking or port bundling. The Gigabit Web-Smart Switch provides these related features:

- Support for up to eight port trunks. ***NOTE:*** At least two ports are required to compose a port trunk.
- Up to 12 ports can be aggregated in a port trunk for Model 524063 (24-Port); up to 8 ports for Model 524087 (16-Port).
- Highly randomized load balancing between the aggregated links based on trunk algorithm configuration.

Port trunks must be properly configured on both sides of the aggregated link. In switch-to-switch connections, if the configuration on both sides doesn’t match (e.g., some ports are mistakenly not included in the port trunk), it will result in a loop. To avoid this and ensure a successful configuration, the following procedure is strongly recommended.

1. Disconnect or disable all the ports involved in the configuration; i.e., either being added to or removed from the port trunk.
2. Configure the port trunk on *both* switches.

3. Double-check the port trunk configuration on *both* switches.
4. Reconnect or re-enable the ports.

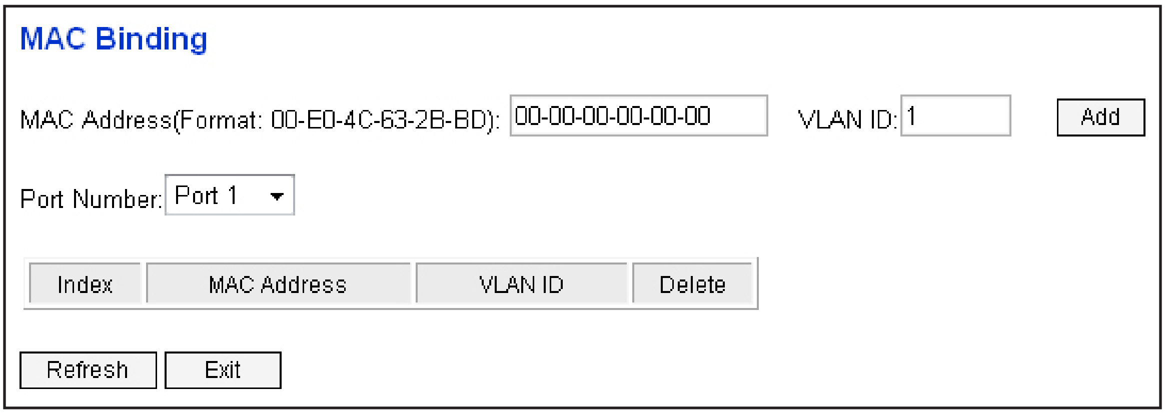
If the port trunk is being configured while the ports are still connected or enabled, the ports will be disabled for a few seconds automatically.

Also, consider these function limitations when configuring port trunks:

- A port mirroring target port can not be a member of a port trunk. However, a port mirroring source port *can* be.
- A DHCP relay agent client port can not be a member of a port trunk.
- Load balancing between the links of a bundle is randomized and may not be ideal. For instance, if three 1000Mbps links are aggreagted, the result bandwidth of the port trunk may not be precisely 3000 Mbps.
- A static MAC address should not be configured to reside on an aggregated port, as it may cause some frames destined to that address to be dropped.

MAC BINDING

This screen allows you to bind a MAC address to a specific port on the switch. Static MAC addresses are usually configured to enforce port security (if supported), and when a device can receive — but cannot transmit — frames.



MAC Binding

MAC Address(Format: 00-E0-4C-63-2B-BD): 00-00-00-00-00-00 VLAN ID: 1

Port Number: Port 1

Index	MAC Address	VLAN ID	Delete

Port Number: Options range from "Port 1" (default) to "Port 24." Specifies the port number to be bound with MAC addresses.

MAC Address: XX-XX-XX-XX-XX-XX, where XX ranges from 0 to FF. Default: 00-00-00-00-00-00. This is the MAC address that is to be statically configured.

VLAN ID: Options range from "1" (default) to "4094." This is the VLAN identifier of the VLAN upon which the MAC address operates.

Add: Click to add the item.

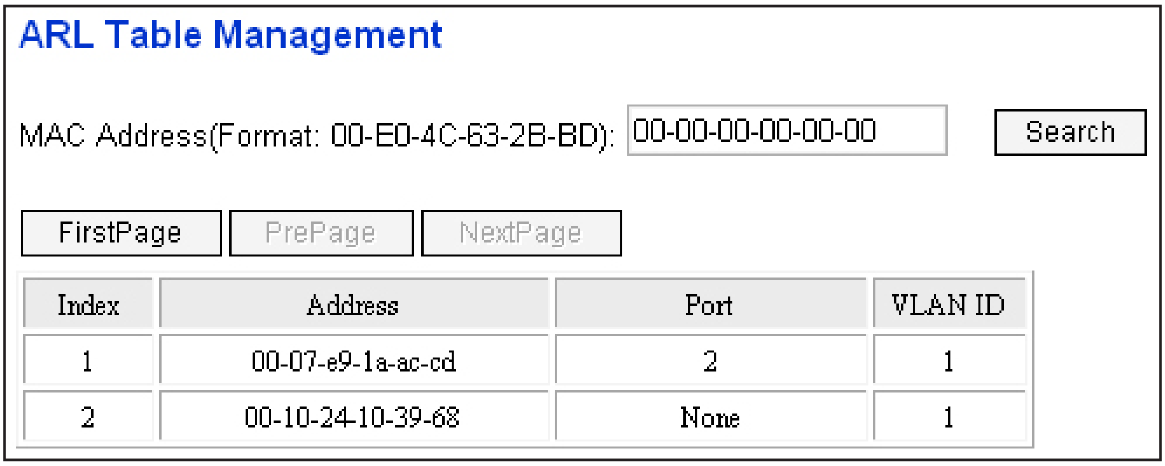
Delete: Click to delete the bound MAC address item.

Exit: Click to exit this configuration screen.

NOTE: When the current VLAN Mode option is *not* IEEE802.1Q tag-based VLAN, the VLAN ID parameter will be disabled.

ARL TABLE

This screen allows you to view MAC addresses of the MAC address table.



ARL Table Management

MAC Address(Format: 00-E0-4C-63-2B-BD): 00-00-00-00-00-00

Index	Address	Port	VLAN ID
1	00-07-e9-1a-ac-cd	2	1
2	00-10-24-10-39-68	None	1

MAC Address: XX-XX-XX-XX-XX-XX, where XX ranges 0 to FF. Default: 00-00-00-00-00-00. Specifies the MAC address to search for.

Search: Click to start searching for the specified MAC address.

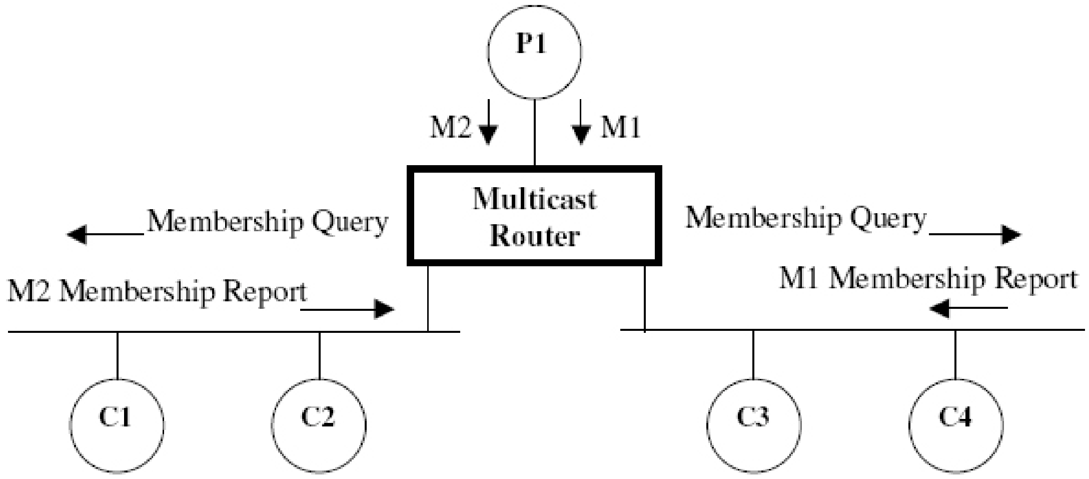
NOTE: The MAC address table consists of static addresses, dynamic addresses and the device address.

MULTICAST CONFIGURATION

IGMP (Internet Group Management Protocol) is used by IP hosts to report their host group memberships to multicast routers. As hosts join and leave specific multicast groups, streams of traffic are directed to or withheld from that host. The IGMP protocol operates between multicast routers and IP hosts. When an unmanaged switch is placed between multicast routers and their hosts, the multicast streams will be distributed to all ports. This may introduce significant traffic onto ports that do not require it and receive no benefit from it.

A device with IGMP Snooping enabled will act upon IGMP messages sent from the router and the host, restricting traffic streams to the appropriate LAN segments. The following figure provides a simple example of IGMP use. One “producer” IP host (P1) is generating two IP multicast streams, M1 and M2. There are four potential “consumers” of these streams, C1 through C4. The multicast router discovers which host wishes to subscribe to which stream by sending general membership queries to each of the segments.

In this example, the general membership query sent to the C1-C2 segment is answered by a membership report (also referred to as a “join”) indicating the desire to subscribe to stream M2. The router will forward the M2 stream onto the C1-C2 segment. In a similar fashion, the router discovers that it must forward M1 onto segment C3-C4.



A consumer may join any number of multicast groups, issuing a membership report for each group. Hosts on the segment note membership reports from other hosts and will suppress their own reports accordingly. In this way, the IGMP protocol guarantees the segment will issue only one join for each group.

The router periodically queries each of its segments in order to determine if at least one consumer still subscribes to a given stream. If no responses occur within a given timeout period (usually two query intervals), the router will prune the multicast stream from the given segment. A more usual method of pruning occurs when consumers wishing to unsubscribe issue an IGMP "leave group" message. The router will immediately issue a group-specific membership query to determine if there are any remaining subscribers of that group on the segment. After the last consumer of a group has un-subscribed, the router will prune the multicast stream from the given segment.

IGMP Snooping Rules

When a multicast source starts multicasting, the traffic stream will be immediately blocked on segments from which joins have not been received. The switch will always forward all multicast traffic to the ports where multicast routers are attached unless configured otherwise.

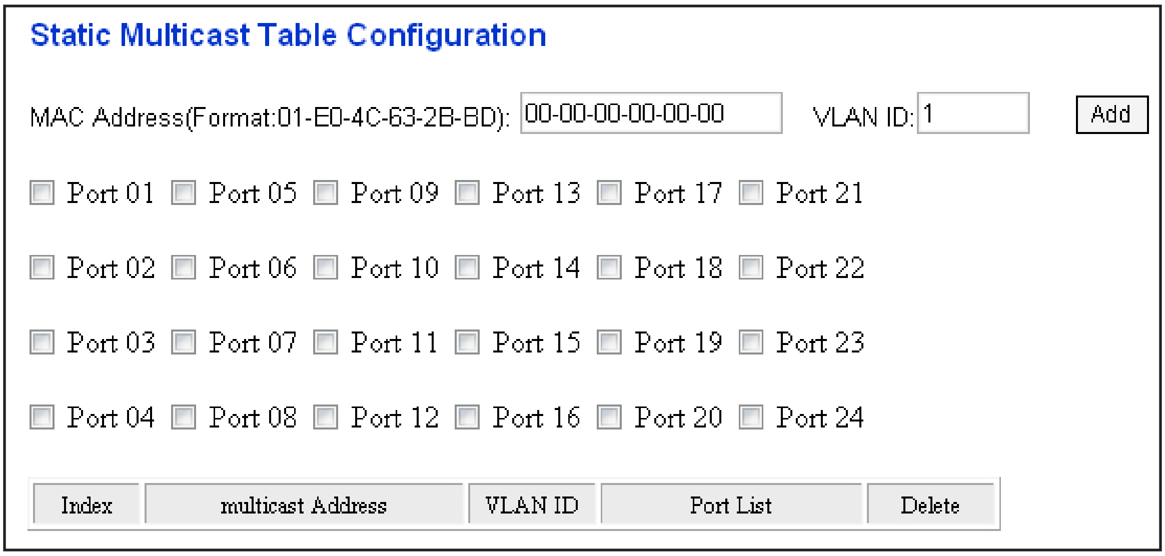
Packets with a destination IP multicast address in the 224.0.0.X range which are not IGMP are always forwarded to all ports. This behavior is based on the fact that many systems do not send joins for IP mulicast addresses in this range while still listening to such packets. The switch will only send IGMP membership reports out of those ports where multicast routers are attached because sending membership reports to hosts could result in unintentionally preventing a host from joining a specific group.

Multicast routers use IGMP to elect a master router known as the querier: the one with the lowest IP address. All other routers become of non-queriers, participating only to forward multicast traffic. When the querier election process is complete, the switch simply relays IGMP queries received from the querier.

When sending IGMP packets, the switch uses its own IP address, if it has one, or an address of 0.0.0.0, if it doesn't have any assigned IP address (e.g., when sending packets on a non-management VLAN). ***NOTE:*** IGMP Snooping switches perform multicast pruning using a multicast frame's destination MAC multicast address, which depends on the group IP multicast address: IP address W.X.Y.Z corresponds to MAC address 01-00-5E-XX-YY-ZZ, where XX is the lower 7 bits of X and YY and ZZ are simply Y and Z coded in hexadecimal.

IP multicast addresses such as 224.1.1.1 and 225.1.1.1 will both map onto the same MAC address 01-00-5E-01-01-01. This is indeed a problem for which the IETF Network Working Group currently has offered no solution. Users are advised to be aware of and avoid this problem.

From here, you can configure your Static Multicast Groups.



Static Multicast Table Configuration

MAC Address(Format:01-E0-4C-63-2B-BD): 00-00-00-00-00-00 VLAN ID: 1

□ Port 01 □ Port 05 □ Port 09 □ Port 13 □ Port 17 □ Port 21

□ Port 02 □ Port 06 □ Port 10 □ Port 14 □ Port 18 □ Port 22

□ Port 03 □ Port 07 □ Port 11 □ Port 15 □ Port 19 □ Port 23

□ Port 04 □ Port 08 □ Port 12 □ Port 16 □ Port 20 □ Port 24

Index	multicast Address	VLAN ID	Port List	Delete

MAC Address: XX-XX-XX-XX-XX-XX, where XX ranges from 0 to FF. Default: 00-00-00-00-00-00. This is the multicast group MAC address.

VLAN ID: Options range from "1" (default) to "4094." This is the VLAN identifier of the VLAN upon which the multicast group operates.

Ports: Select any combination of numbers valid for this parameter (default: none selected). These are ports to which the multicast group traffic is forwarded.

Add: Click to add a new static multicast group.

Delete: Click to delete the item.

Static Multicast Group Table: From the static multicast table, you can view all of the current static multicast groups' information.

RSTP

The Gigabit Web-Smart Switch provides these RSTP-related features:

- Industry-standard support of the Rapid Spanning Tree Protocol, which features a compatibility mode with legacy STP.
- Superior performance, as RSTP will recognize a link failure and put an alternate port into forwarding mode within milliseconds.
- RSTP may be enabled on a per-port basis.
- Ports may be configured as edge ports, which allows rapid transitioning to the forwarding state for non-STP hosts.
- Path costs may be hard-configured or determined by port speed negotiation, in either the STP or RSTP style.
- Full bridge (historically, a device implementing STP on its ports has been referred to as a bridge, and the device uses the terms *bridge* and *switch* synonymously) and port status provide a rich set of tools for performance monitoring and debugging.

RSTP Operation

The 802.1D Spanning Tree Protocol was developed to allow the construction of robust networks that incorporate redundancy while pruning the active topology of the network to prevent loops. While STP is effective, it requires that frame transfer must halt after a link outage until all bridges in the network are sure to be aware of the new topology. Using 802.1D-recommended values, this period lasts 30 seconds.

Rapid Spanning Tree Protocol (IEEE 802.1w) was a further evolution of the 802.1D Spanning Tree Protocol. It replaced the settling period with an active handshake between bridges that guarantees topology information to be rapidly progagated through the network. RSTP also offers a number of other significant innovations:

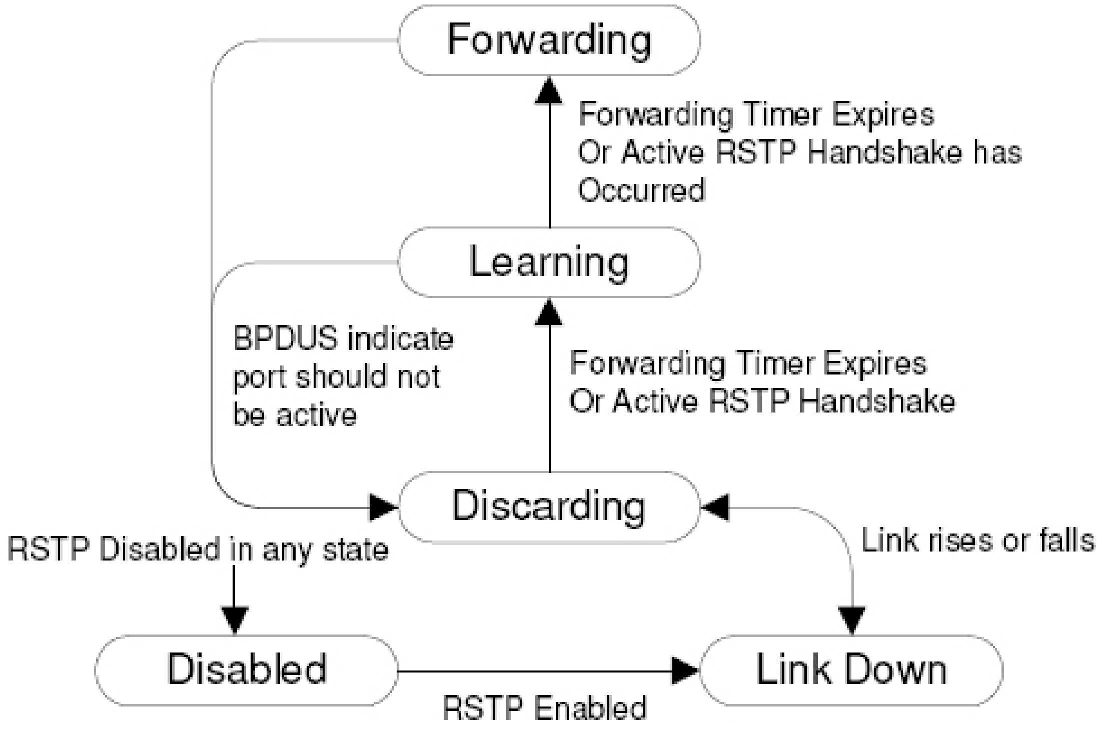
- Topology changes in RSTP can be originated from and acted upon by any designated bridges, leading to more rapid propagation of address information; unlike topology changes in STP, which must be passed to the root bridge before they can be propagated to the network.
- RSTP explicitly recognizes two blocking roles — alternate and backup port roles — including them in computations of when to learn and forward; while STP recognizes one state — blocking — for ports that should not forward.
- RSTP bridges generate their own configuration messages, even if they fail to receive one from the root bridge. This leads to quicker failure detection, but STP relays configuration messages received on the root port out its designated ports. If an STP bridge fails to receive a message from its neighbor, it cannot be sure where along the path to the root a failure occurred.
- RSTP offers edge port recognition, allowing ports at the edge of the network to forward frames immediately after activation while at the same time protecting them against loops.

- While providing a much better performance than STP, IEEE 802.1w RSTP still . required up to a few seconds to restore network connectivity when a topology change occurred. A revised and highly optimized RSTP version (which this switch supports) was defined in the IEEE standard 802.1D-2004 edition and now reduces network recovery times to just milliseconds.

RSTP States and Roles

RSTP bridges have roles to play, being either root or designated. One bridge, the root bridge, is the logical center of the network. All other bridges in the network are designated bridges. RSTP also assigns each port of the bridge a state and a role. The RSTP state describes what is happening at the port in relation to address learning and frame forwarding. The RSTP role basically describes whether the port is facing the center or edges of the network and whether it can currently be used or not.

There are three RSTP states: discarding, learning and forwarding.

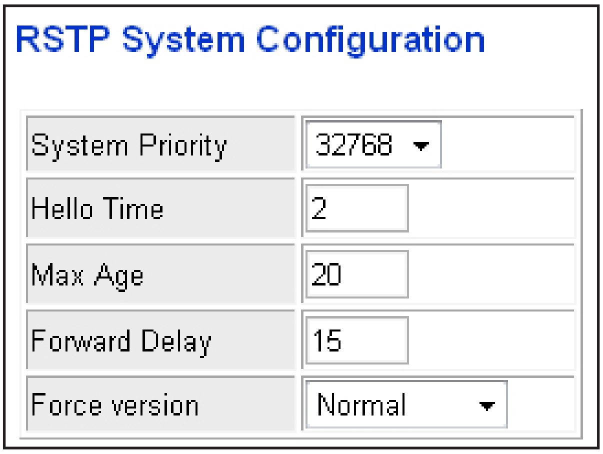

Forwarding
Forwarding Timer Expires Or Active RSTP Handshake has Occurred
Learning
BPDUS indicate port should not be active
Forwarding Timer Expires Or Active RSTP Handshake
Discarding
RSTP Disabled in any state
Link rises or falls
Disabled
Link Down
RSTP Enabled

The discarding state is entered when the port is first taken into service. The port does not learn addresses in this state and does not participate in frame transfer. The port looks for RSTP traffic in order to determine its role in the network. When it is determined that the port will play an active part in the network, the state will change to learning.

The learning state is entered when the port is preparing to act as an active member of the network. The port learns addresses in this state but does not participate in frame transfer. In a network of RSTP bridges, the time spent in this state is usually quite short. RSTP bridges operating in STP compatibility mode will spend 6 to 40 seconds in this state.

After learning, the bridge will place the port in the forwarding state. The port both learns addresses and participates in frame transfer while in this state.

From here, you can configure the RSTP.



RSTP System Configuration

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

System Priority: Options range from "0" to "61440." Default: 32768. This setting provides a way to control the topology of the STP-connected network. The desired root and designated bridges can be configured for a particular topology. The bridge with the lowest priority will become root. In the event of a failure of the root bridge, the bridge with the next-lowest priority will then become root. Designated bridges that (for redundancy purposes) service a common LAN also use priority to determine which bridge is active. In this way, careful selection of System Priorities can establish the path of traffic flows in normal and abnormal conditions.

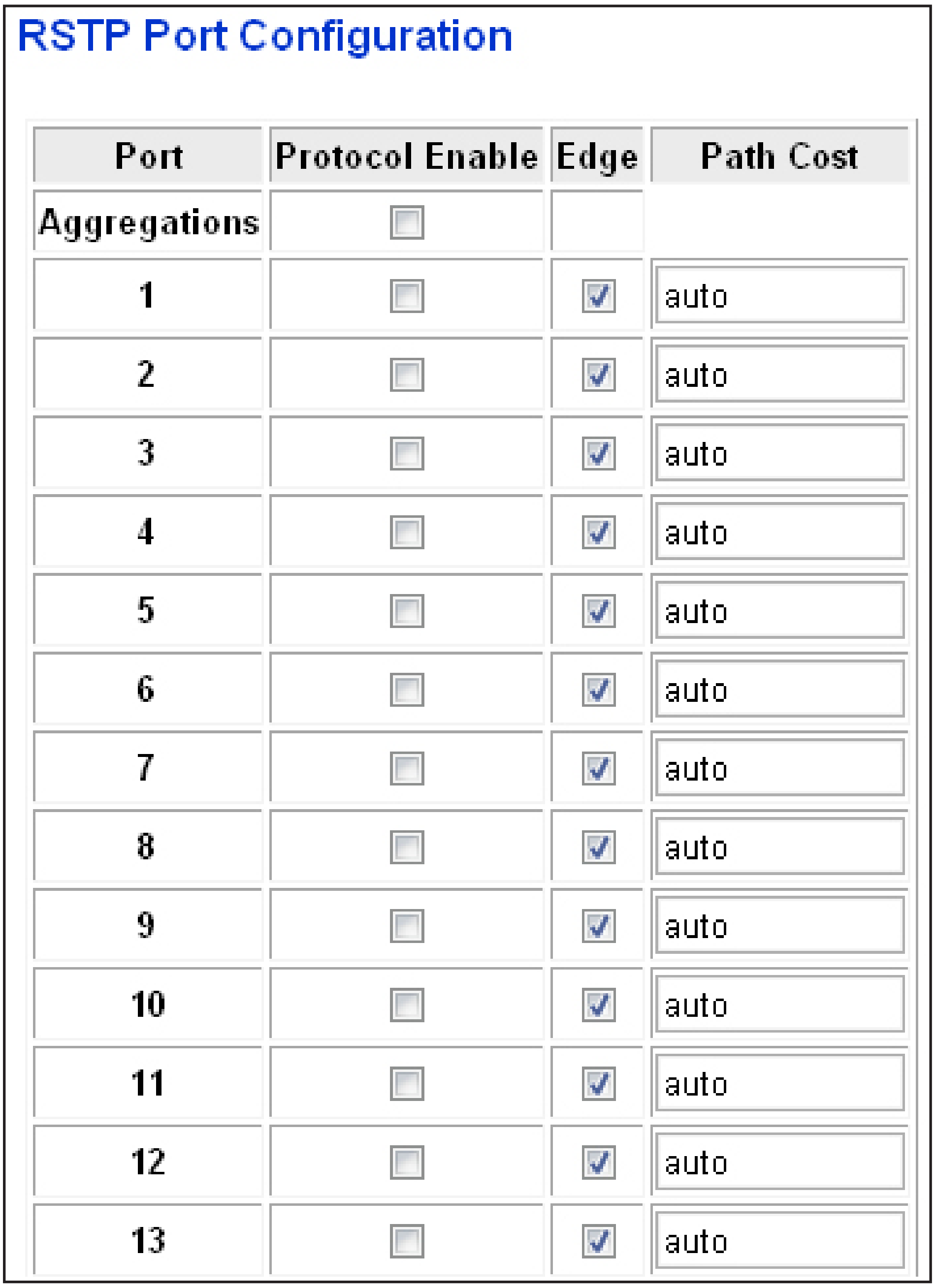
Hello Time: Enter a value from 1 to 10. Default: 2. This is the time between configuration messages issued by the root bridge. Shorter hello times result in faster detection of topology changes at the expense of moderate increases in STP traffic.

Max Age: Enter a value from 6 to 40. Default: 20. This is the time for which a configuration message remains valid after being issued by the root bridge. Configure this parameter with care when many tiers of bridges exist or when slow speed links (such as those used in WANs) are part of the network.

Forward Delay: Enter a value from 4 to 30. Default: 15. This is the amount of time a bridge spends learning MAC addresses on a rising port before beginning to forward traffic. Lower values allow the port to reach the forwarding state more quickly, but at the expense of flooding unlearned addresses to all ports.

Force Version: Either "Normal" (default) or "Compatible." Select the version of

Spanning Tree Protocol to support: Normal only supports Rapid Spanning Tree Protocol; Compatible supports both STP (802.1d) and RSTP.



RSTP Port Configuration

Port	Protocol Enable	Edge	Path Cost
Aggregations	□		
1	□	☑	auto
2	□	☑	auto
3	□	☑	auto
4	□	☑	auto
5	□	☑	auto
6	□	☑	auto
7	□	☑	auto
8	□	☑	auto
9	□	☑	auto
10	□	☑	auto
11	□	☑	auto
12	□	☑	auto
13	□	☑	auto

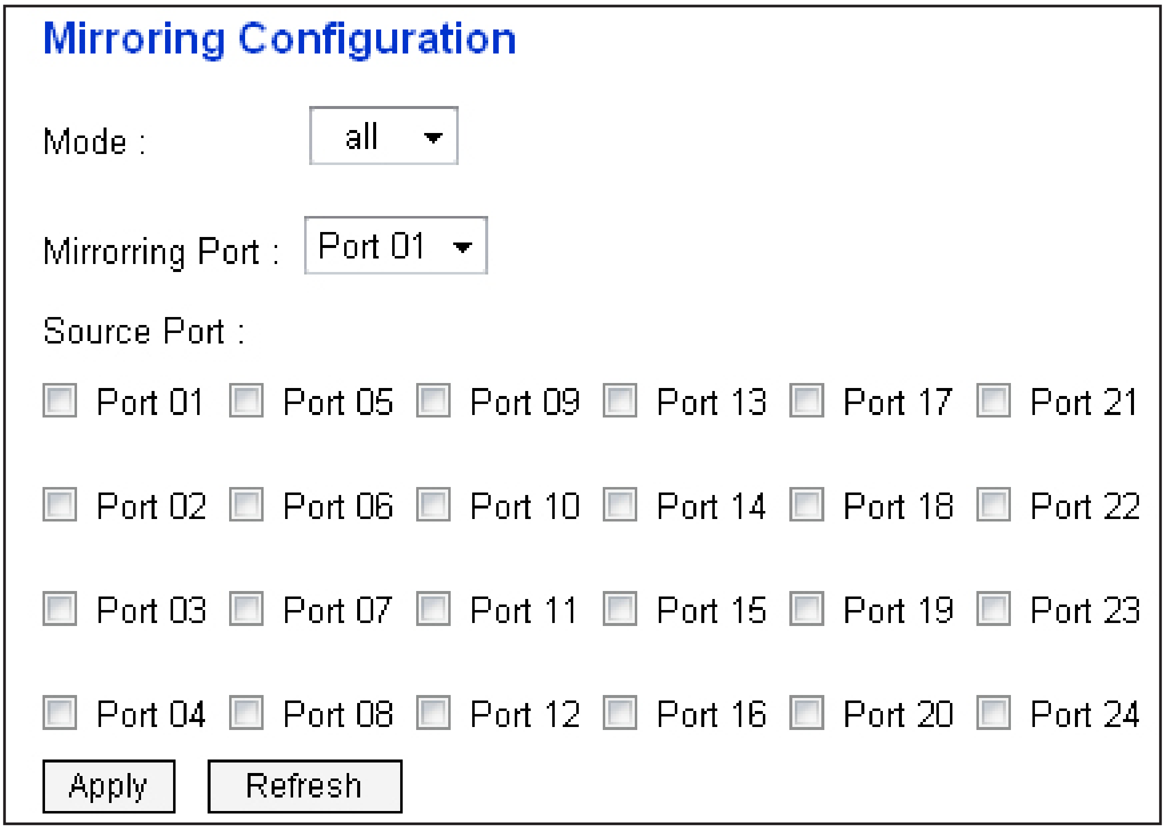
Protocol Enabled: Either “Enabled” or “Disabled” (default). Enabled means you’re enabling RSTP for this port as per the configuration in the RSTP Port Configuration menu. STP may be disabled for the port *only* if the port does not attach to an STP-enabled bridge in any way. Failure to meet this requirement will result in an undetectable traffic loop in the network. A more desirable alternative to disabling the port is to leave STP enabled but to configure the port as an edge port. A good candidate for disabling STP would be a port that services a single host computer. You can enable RSTP of all aggregations.

Edge Port: Either “Enabled” (default) or “Disabled.” Edge ports are ports that do not participate in the Spanning Tree, but still send configuration messages. Edge ports transition directly to frame forwarding without any listening and learning delays. The MAC tables of edge ports do not need to be flushed when topology changes occur in the STP network. Unlike an STP-disabled port, accidentally connecting an edge port to another port in the spanning tree will result in a detectable loop.

Path Cost: Enter a value from 0 to 2147483647, or “Auto” (default). Setting the cost manually provides the ability to preferentially select specific ports to carry traffic over others. Leave this field set to Auto to use the standard RSTP port costs as negotiated (20,000 for 1Gbps links, 200,000 for 100Mbps links and 2,000,000 for 10Mbps links); or the standard STP port costs as negotiated (4 for 1Gbps links, 19 for 100Mbps links and 100 for 10Mbps links).

MIRRORING

Port mirroring is a troubleshooting tool in which all traffic on a designated port is copied, or mirrored, to a target port. If a protocol analyzer is attached to the target



Mirroring Configuration

Mode : all

Mirroring Port : Port 01

Source Port :

□ Port 01
□ Port 02
□ Port 03
□ Port 04
□ Port 05
□ Port 06
□ Port 07
□ Port 08
□ Port 09
□ Port 10
□ Port 11
□ Port 12
□ Port 13
□ Port 14
□ Port 15
□ Port 16
□ Port 17
□ Port 18
□ Port 19
□ Port 20
□ Port 21
□ Port 22
□ Port 23
□ Port 24

port, the traffic stream of valid frames on any source port is made available for analysis.

Select a target port that has a higher speed than the source port. Mirroring a 1000Mbps port onto a 100Mbps port may result in an improperly mirrored stream. Frames will be dropped if the full duplex rate of frames on the source port exceeds the transmission speed of the target port. Since both transmitted and received frames on the source port are mirrored to the target port, frames will be discarded if the sum traffic exceeds the target port's transmission rate. This problem reaches its extreme in the case where traffic on a 1000Mbps full duplex port is mirrored onto a 100Mbps half duplex port. ***NOTE:*** Invalid frames received on the source port will not be mirrored. These include CRC errors, oversize and undersize packets, fragments, jabbers, collisions, late collisions and drop events.

Mode: Either "Tx" (default) or "All." The All mode causes all frames received and transmitted by the mirrored port to be transmitted out of the sniffer port; Tx mode causes all frames transmitted by the mirrored port to be transmitted out of the sniffer port.

Source Port: Options range from "Port 01" to "Port 24." The selected port is the port being monitored.

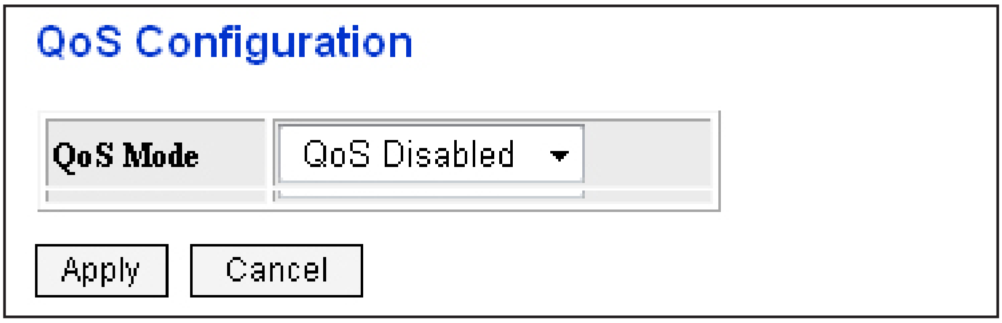
Mirroring Port: Options range from "Port 01" to "Port 24." The selected port is the port where a monitoring device should be connected.

QUALITY OF SERVICE

QoS (Quality of Service) enhances communication quality by giving precedence to certain classes of packets. This device provides Disabled, 802.1p, DSCP and Port QoS modes. The inspection phase results in the QoS of individual frames being determined. When these frames are forwarded to the egress port, they're collected into one of the priority queues according to the QoS assigned to each frame.

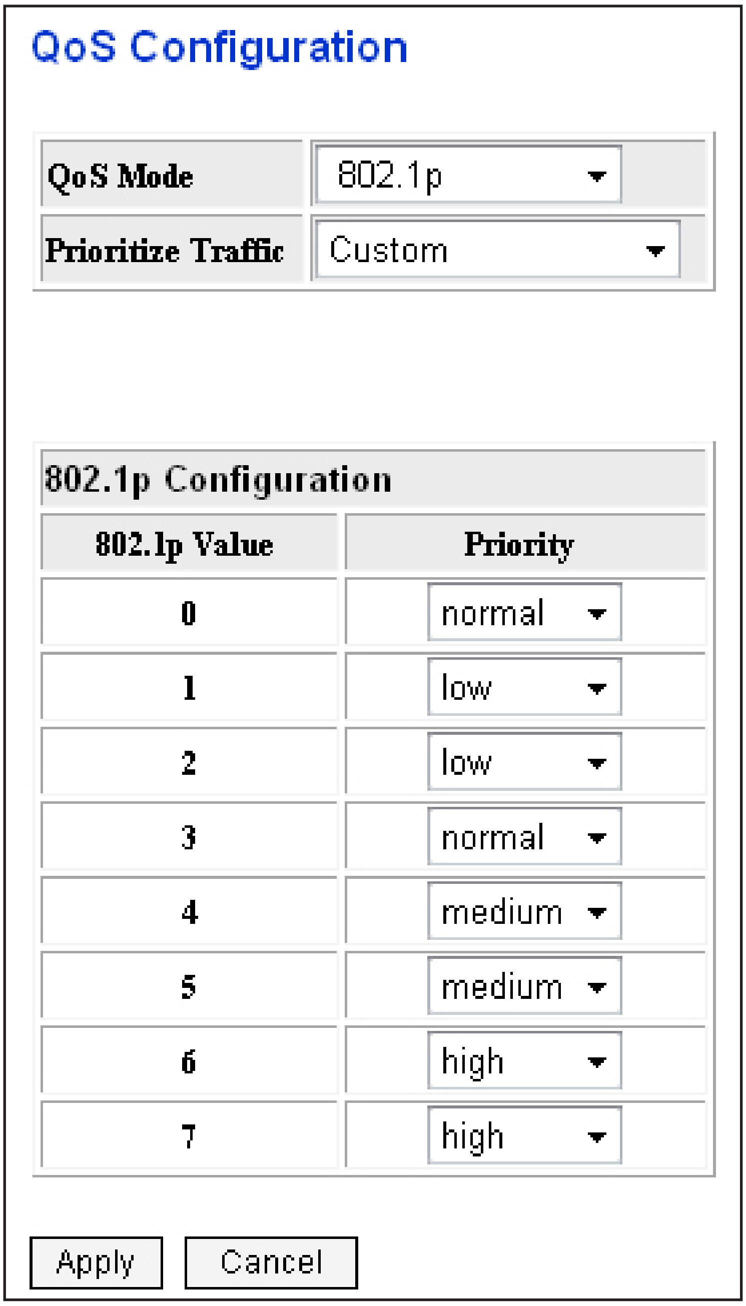
QoS weighting selects the degree of preferential treatment attached to different priority queues. The ratio of the number of higher QoS to lower QoS frames transmitted can be programmed. If desired, the user can program that lower QoS frames are transmitted only after all higher QoS frames have been serviced.

From here, select a QoS mode and click "Apply" to put settings into effect.



QoS Configuration

QoS Mode: QoS Disabled



QoS Configuration

QoS Mode	802.1p
Prioritize Traffic	Custom

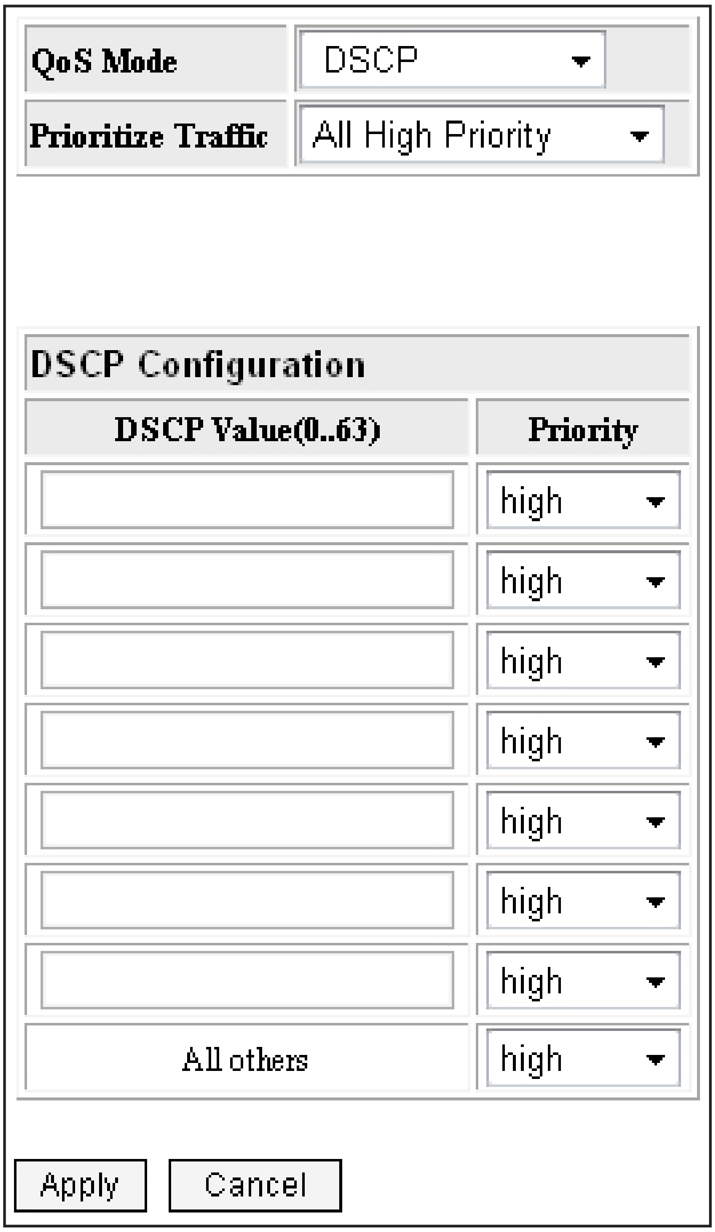
802.1p Configuration

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

Prioritize Traffic: Options are “Custom” (default), “All Low Priority,” “All Normal Priority,” “All Medium Priority” and “All High Priority.” This screen allows you to quickly configure the 802.1p priorities.

802.1p Value: Ranging from 0 to 7, these are the values of the IEEE 802.1p priority.

Priority: Options are “low,” “normal,” “medium” and “high.” Default: according to the Priority Traffic option. This is a QoS assigned to received tagged frames with the specified IEEE 802.1p priority value.



QoS Mode	DSCP
Prioritize Traffic	All High Priority

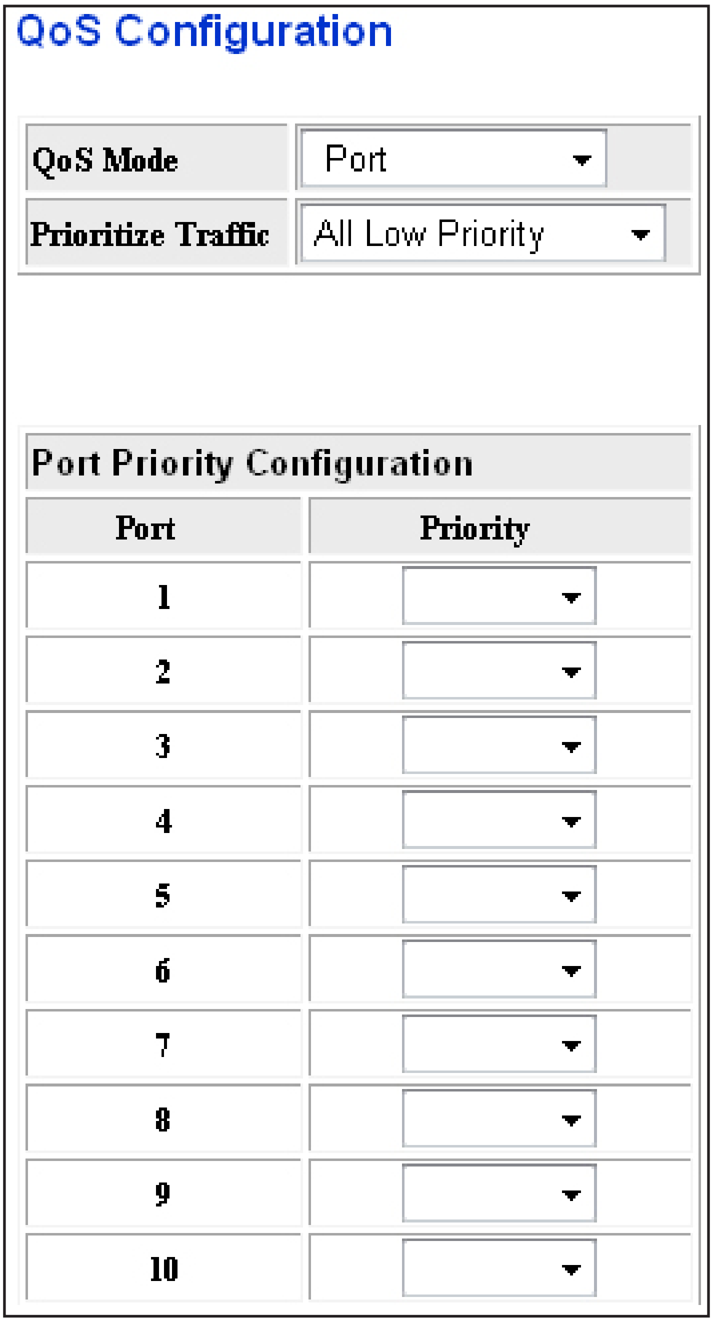
DSCP Configuration

DSCP Value(0..63)	Priority
	high
	high
	high
	high
	high
	high
	high
All others	high

Prioritize Traffic: Options are “Custom,” “All Low Priority,” “All Normal Priority,” “All Medium Priority” and “All High Priority” (default). This screen allows you to quickly configure the DSCP priorities.

DSCP Value: Enter a value from 0 to 63. This is a Differentiated Services Code Point (DSCP) – a value of the 6-bit DiffServ field in the Type-of-Service (ToS) field of the IP header.

Priority: Options are “low,” “normal,” “medium” and “high.” Default: according to the Priority Traffic option. This is a QoS assigned to received tagged frames with the specified DSCP.



QoS Configuration

QoS Mode	Port
Prioritize Traffic	All Low Priority

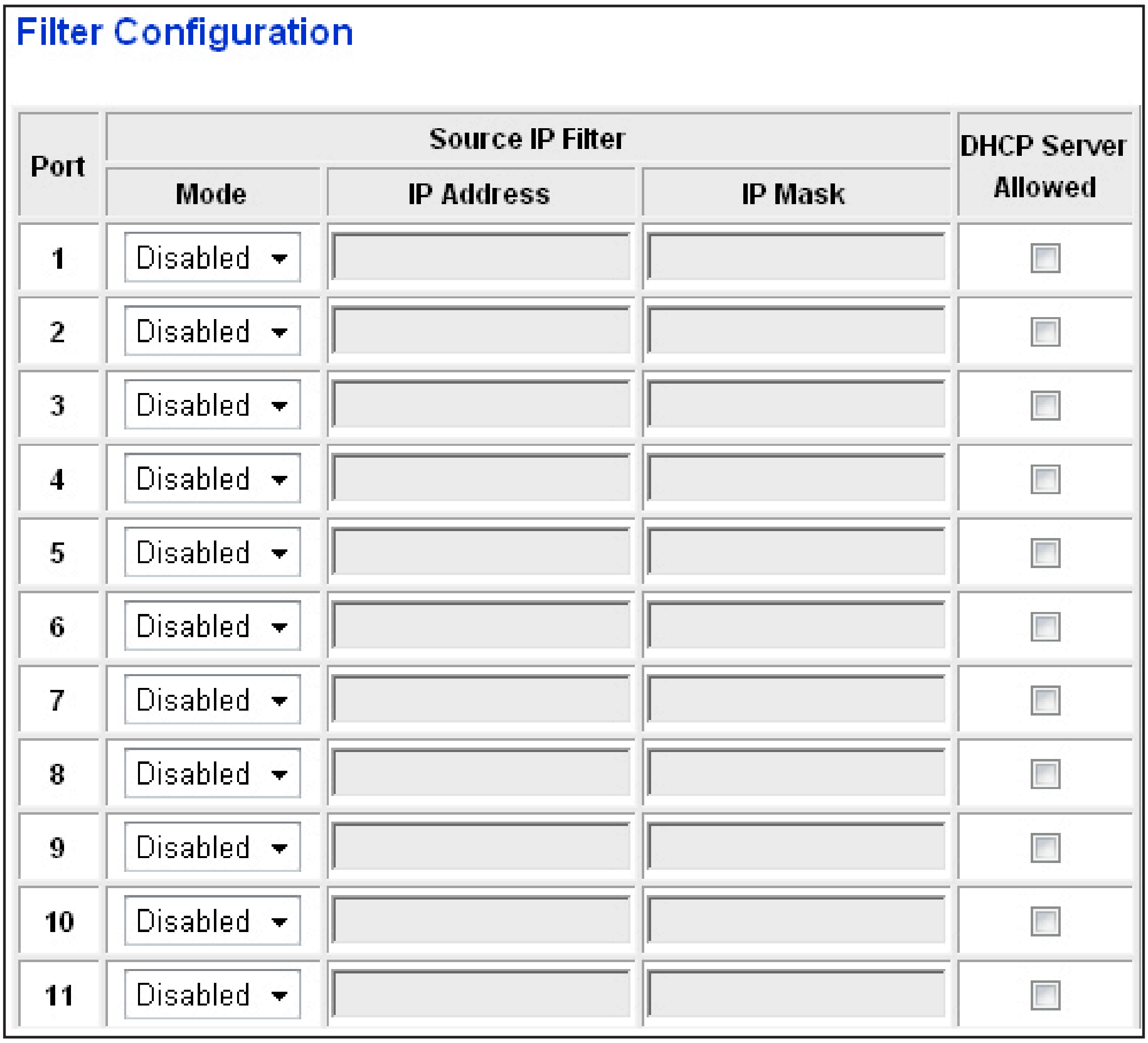
Port Priority Configuration

Port	Priority
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

Prioritize Traffic: Options are “Custom,” “All Low Priority” (default), “All Normal Priority,” “All Medium Priority” and “All High Priority.” This screen allows you to quickly configure the Port priorities.

Priority: Options are “low,” “normal,” “medium” and “high.” Default: according to the Priority Traffic option. Specifies the default QoS priority for each port.

FILTER



Filter Configuration

Port	Source IP Filter			DHCP Server Allowed
	Mode	IP Address	IP Mask	
1	Disabled ▾			□
2	Disabled ▾			□
3	Disabled ▾			□
4	Disabled ▾			□
5	Disabled ▾			□
6	Disabled ▾			□
7	Disabled ▾			□
8	Disabled ▾			□
9	Disabled ▾			□
10	Disabled ▾			□
11	Disabled ▾			□

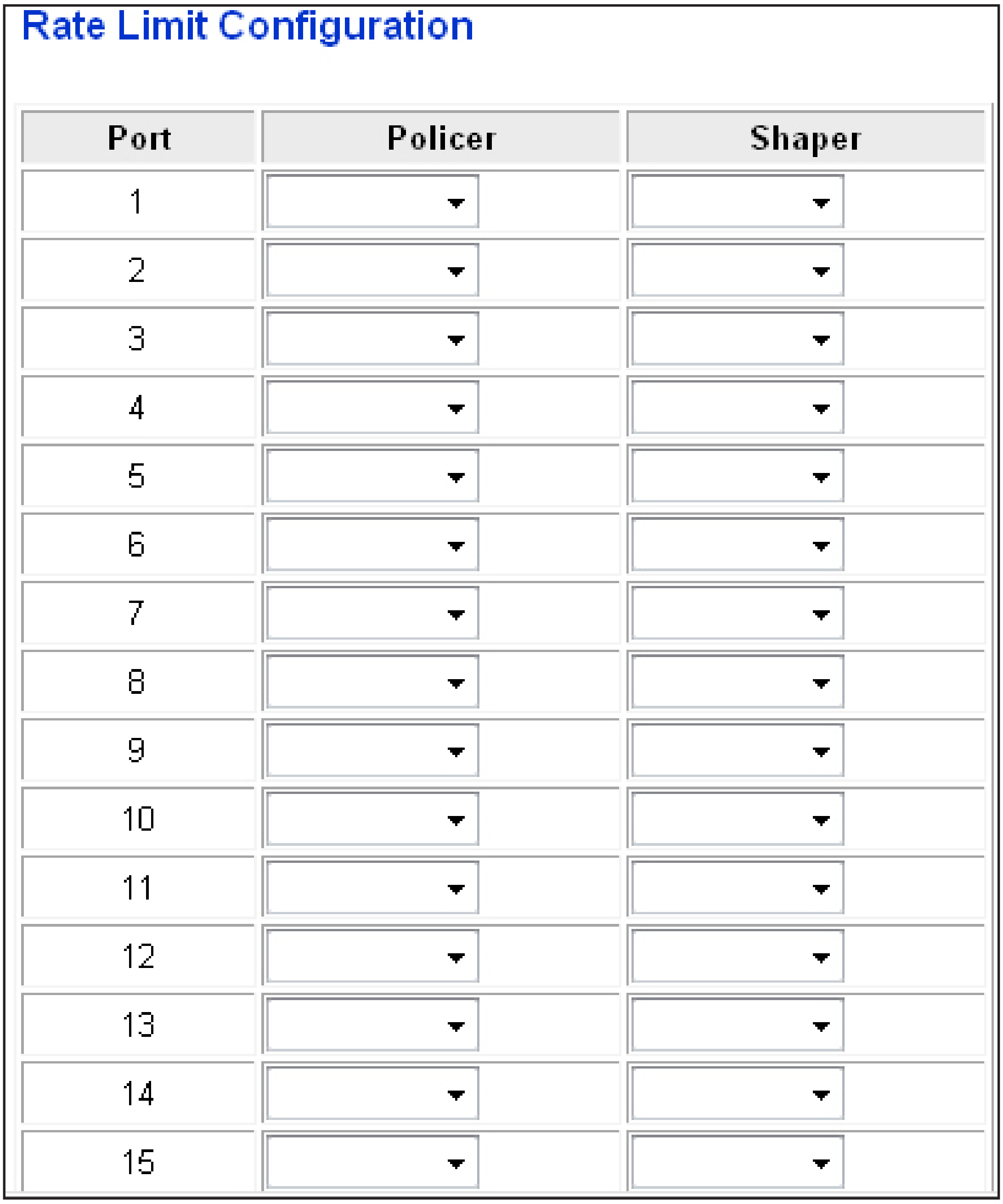
Mode: Options are “Disabled” (default), “Static” and “DHCP.” Specifies the source IP address filter model. Disabled allows all packets to be forwarded; Static allows packets with the specified source IP address to be forwarded while other packets are discarded; DHCP allows packets with a DHCP server assigned as the source IP address to be forwarded.

IP Address: XXX.XXX.XXX.XXX where XXX ranges from 0 to 255. Default: 0.0.0.0. Specifies the packets’ source IP address to be allowed forwarding. An IP address is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods. Only a unicast IP address is allowed that ranges from 1.0.0.0 to 233.255.255.255.

IP Mask: XXX.XXX.XXX.XXX where XXX ranges from 0 to 255. Default: 0.0.0.0, Specifies the packets’ source IP address range to be allowed forwarding. An IP subnet mask is a 32-bit number that is notated by using four numbers from 0 through 255, separated by periods. Typically, subnet mask numbers use either 0 or 255 as values (e.g., 255.255.255.0), but other numbers can appear.

DHCP Server Allowed: Either “Enabled” or “Disabled” (default). When the DHCP option is configured, enable these parameters; otherwise, the DHCP packets will be discarded and the port will discard all packets.

RATE LIMIT



Rate Limit Configuration

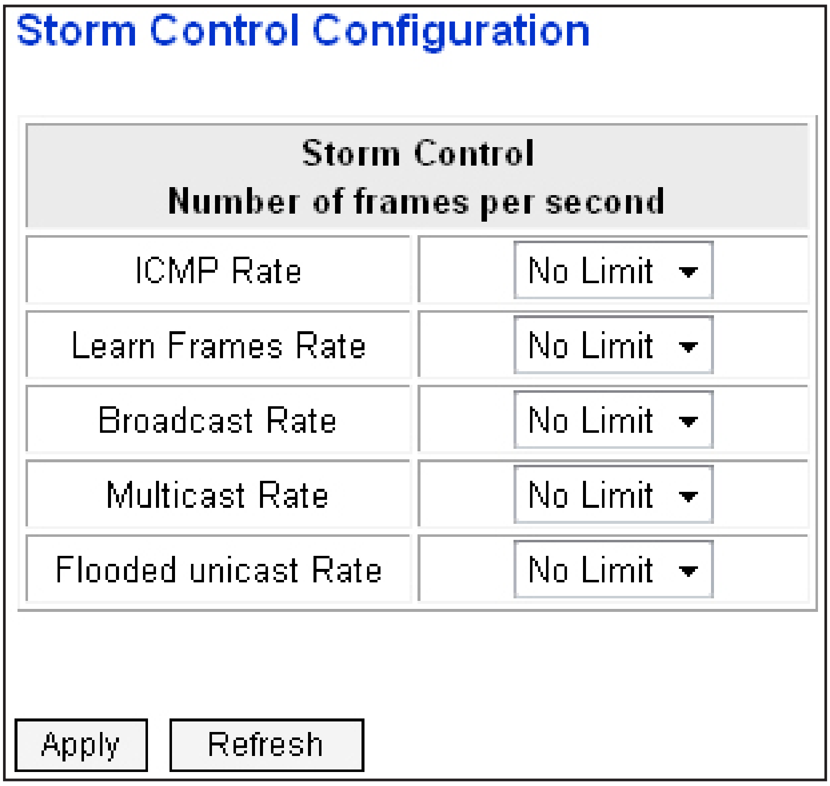
Port	Policer	Shaper
1	▾	▾
2	▾	▾
3	▾	▾
4	▾	▾
5	▾	▾
6	▾	▾
7	▾	▾
8	▾	▾
9	▾	▾
10	▾	▾
11	▾	▾
12	▾	▾
13	▾	▾
14	▾	▾
15	▾	▾

Policer: Options range from “128” to “3698 Kbps” or “None” (default). This is the rate at which received frames will start to be discarded by the switch.

Shaper: Options range from “128” to “3698 Kbps” or “None” (default). This is the maximum rate at which the switch will transmit frames on this port. The switch will discard frames in order to meet this rate, if required.

STORM CONTROL

This screen allows you to configure the rules for Storm Control, which limits ICMP Rate, Learn Frames Rate, Broadcast Rate, Multicast Rate, Multicast Rate and Flooded Unicast Rate.



Storm Control Configuration

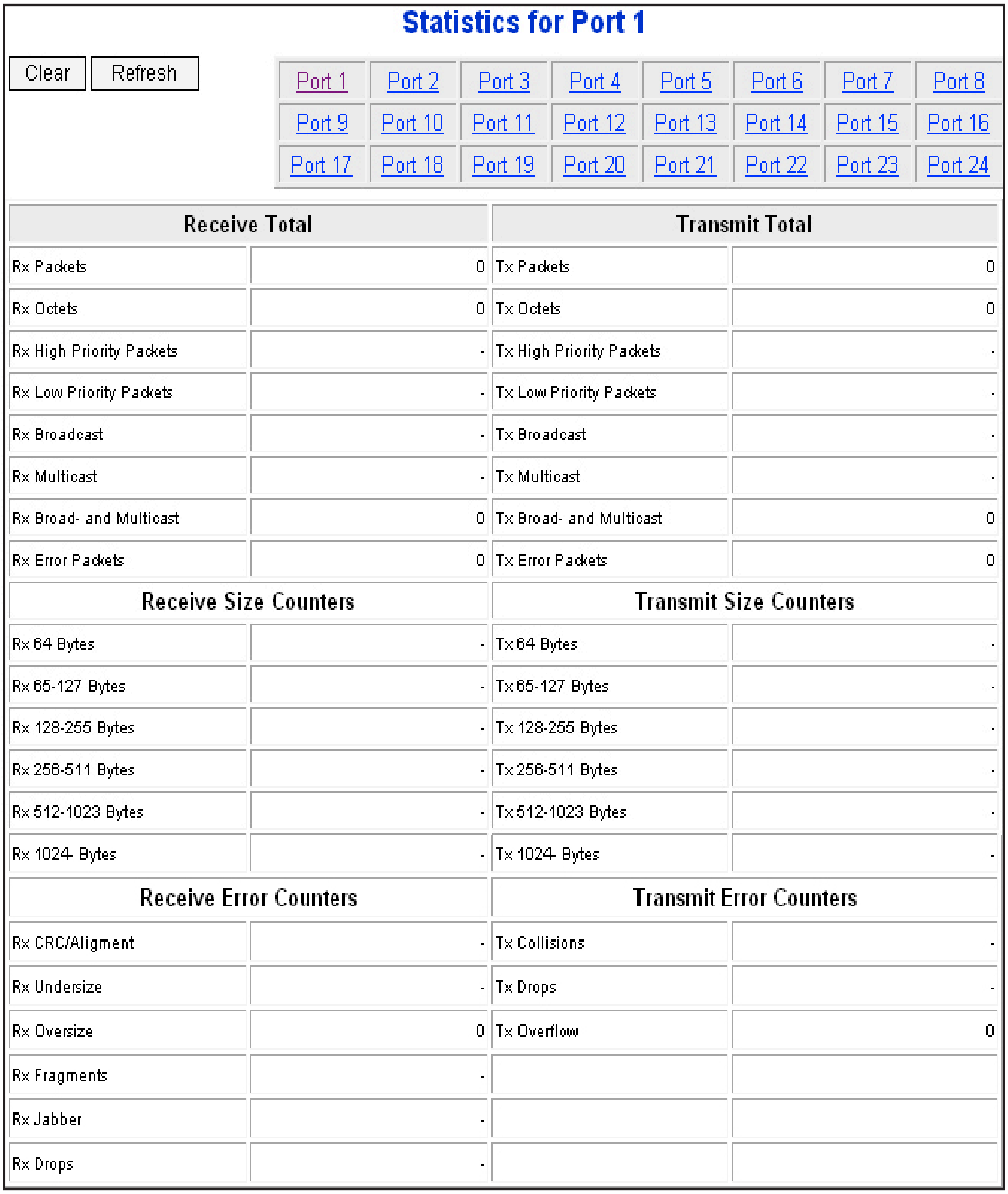
Storm Control Number of frames per second	
ICMP Rate	No Limit ▾
Learn Frames Rate	No Limit ▾
Broadcast Rate	No Limit ▾
Multicast Rate	No Limit ▾
Flooded unicast Rate	No Limit ▾

ICMP Rate: Options range from “No Limit” (default) to “1K” to “32768K.”
Learn Frames Rate: Options range from “No Limit” (default) to “1K” to “32768K.”
Broadcast Rate: Options range from “No Limit” (default) to “1K” to “32768K.”
Multicast Rate: Options range from “No Limit” (default) to “1K” to “32768K.”
Flooded Unicast Rate: Options range from “No Limit” (default) to “1K” to “32768K.”
NOTE: No Limit means all frames will not be limited. Specify the appropriate limit rate of the frame type.

Monitoring

DETAILED STATISTICS

View the detailed transmitting and receiving status of each port by clicking the port's hyperlink. Click "Clear" to clear all statistics; click "Refresh" to renew them.



Statistics for Port 1

Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx High Priority Packets	-	Tx High Priority Packets	-
Rx Low Priority Packets	-	Tx Low Priority Packets	-
Rx Broadcast	-	Tx Broadcast	-
Rx Multicast	-	Tx Multicast	-
Rx Broad- and Multicast	0	Tx Broad- and Multicast	0
Rx Error Packets	0	Tx Error Packets	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	-	Tx 64 Bytes	-
Rx 65-127 Bytes	-	Tx 65-127 Bytes	-
Rx 128-255 Bytes	-	Tx 128-255 Bytes	-
Rx 256-511 Bytes	-	Tx 256-511 Bytes	-
Rx 512-1023 Bytes	-	Tx 512-1023 Bytes	-
Rx 1024- Bytes	-	Tx 1024- Bytes	-
Receive Error Counters		**Transmit Error Counters**	
Rx CRC/Aligment	-	Tx Collisions	-
Rx Undersize	-	Tx Drops	-
Rx Oversize	0	Tx Overflow	0
Rx Fragments	-		
Rx Jabber	-		
Rx Drops	-		

Receive Total Panel

Rx Packets: The number of received good packets (Unicast+Multicast+Broadcast) and dropped packets.

Rx Octets: The number of octets in received good packets (Unicast+Multicast+ Broadcast) and dropped packets.

Rx High Priority Packets: The number of received High Priority good packets and dropped packets.

Rx Low Priority Packets: The number of received Low Priority good packets and dropped packets.

Rx Broadcast: The number of good Broadcast packets received.

Rx Broad- and Multicast: The number of good Broadcast and Multicast Packets received.

Rx Error Packets: The number of any type of erroneous packets.

Transmit Total Panel

Tx Packets: The number of transmitted good packets.

Tx Octets: The number of octets on a transmitted good packets.

Tx High Priority Packets: The number of transmitted High Priority good packets.

Tx Low Priority Packets: The number of transmitted Low Priority good packets.

Tx Broadcast: The number of transmitted Broadcast packets.

Tx Broad- and Multicast: The number of transmitted Broadcast and Multicast packets.

Tx Error Packets: The number of any type of erroneous packets.

Receive Size Counters Panel

Rx 64 Bytes: The number of received packets with size of 64 octets.

Rx 65-127 Bytes: The number of received packets with size of 65 to 127 octets.

Rx 128-255 Bytes: The number of received packets with size of 128 to 255 octets.

Rx 256-511 Bytes: The number of received packets with size of 256 to 511 octets.

Rx 512-1023 Bytes: The number of received packets with size of 512 to 1023 octets.

Rx 1024- Bytes: The number of received packets with size of 1024 to maximum octets.

Transmit Size Counters Panel

Tx 64 Bytes: The number of transmitted packets with size of 64 octets.

Tx 65-127 Bytes: The number of transmitted packets with size of 65 to 127 octets.

Tx 128-255 Bytes: The number of transmitted packets with size of 128 to 255 octets.

Tx 256-511 Bytes: The number of transmitted packets with size of 256 to 511 octets.

Tx 512-1023 Bytes: The number of transmitted packets with size of 512 to 1023 octets.

Tx 1024- Bytes: The number of transmitted packets with size of 1024 to maximum octets.

Receive Error Counters Panel

Rx CRC/Aligment: The number of packets received which meet all the following conditions:

- Packet data length is between 64 and 1518 octets inclusive.
- Packet has invalid CRC.
- Collision Event has not been detected.
- Late Collision Event has been detected.

Rx Undersize: The number of received packets that meet all the following conditions:

- Packet data length is less than 64 octets.
- Collision Event has not been detected.
- Late Collision Event has not been detected.
- Packet has valid CRC

Rx Oversize: The number of packets received with data length greater than 1518 octets and valid CRC.

Rx Fragments: The number of packets received which meet all the following conditions:

- Packet data length is less than 64 octets, or packet without SFD and is less than 64 octets in length.
- Collision Event has not been detected.
- Late Collision Event has not been detected.
- Packet has invalid CRC.

Rx Jabber: The number of packets which meet all the following conditions:

- Packet data length is greater that 1518 octets.
- Packet has invalid CRC.

Rx Drops: The number of received packets that are dropped.

Transmit Error Counters Panel

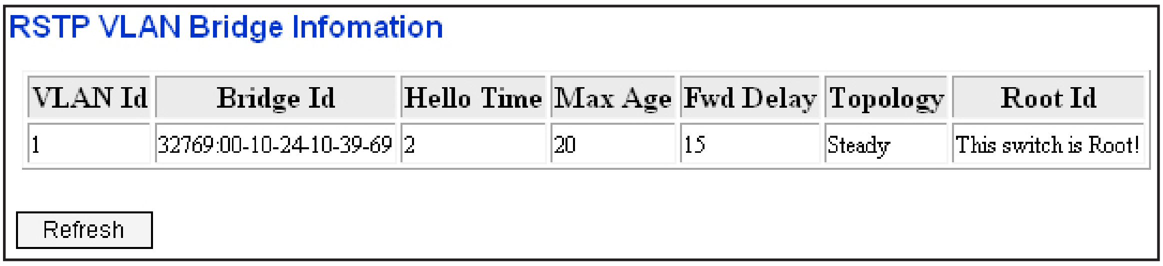
Tx Collisions: The number of transmitted packets for which Collision Event has been detected.

Tx Drops: The number of transmitted packets that are dropped.

Tx Overflow: The number of packets transmitted with data length greater than 1518 octets and valid CRC.

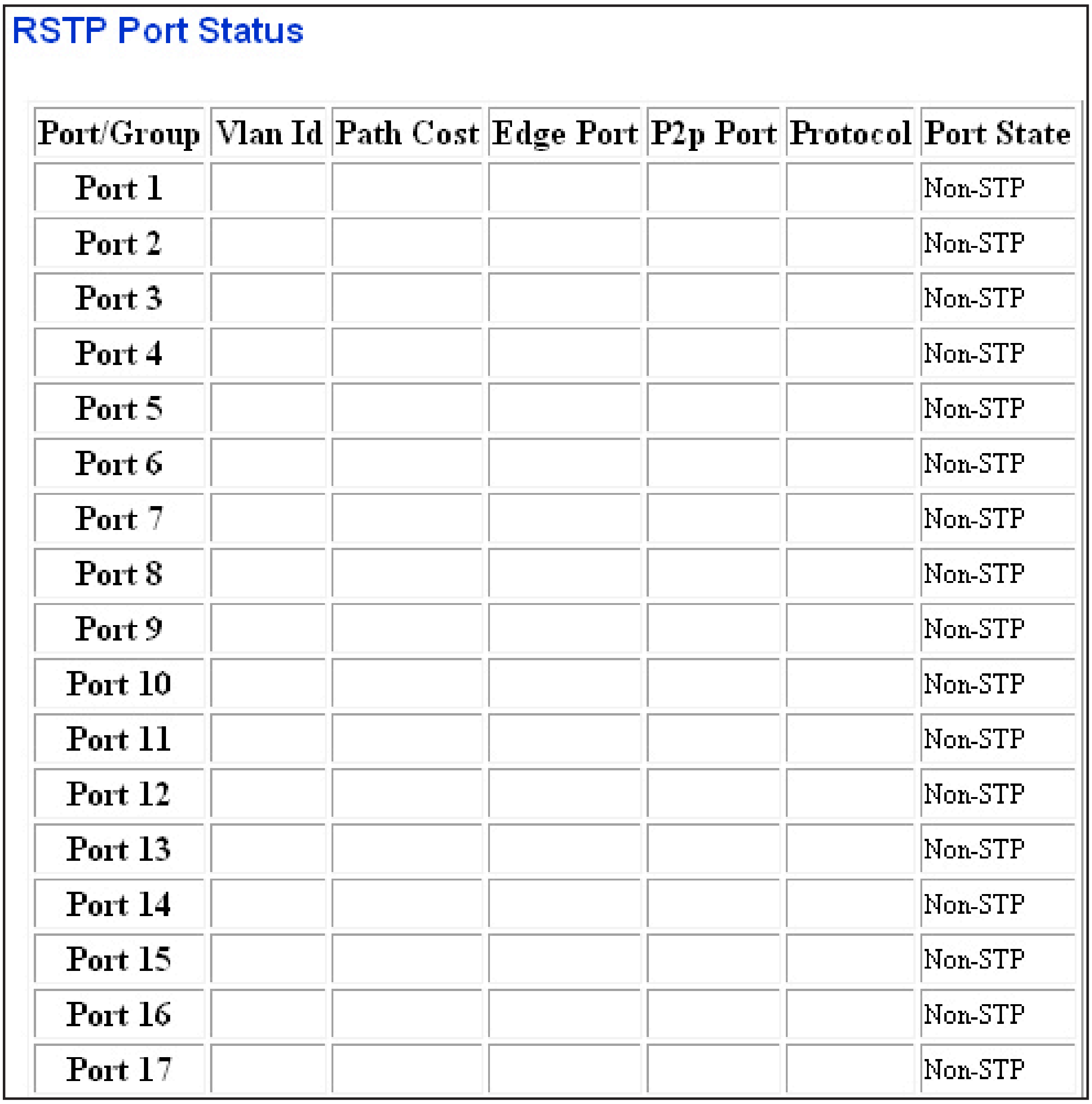
RSTP STATUS

This displays the switch's RSTP parameters. Click "Refresh" to renew the status.



RSTP VLAN Bridge Infomation

VLAN Id	Bridge Id	Hello Time	Max Age	Fwd Delay	Topology	Root Id
1	32769:00-10-24-10-39-69	2	20	15	Steady	This switch is Root!



RSTP Port Status

Port/Group	Vlan Id	Path Cost	Edge Port	P2p Port	Protocol	Port State
Port 1						Non-STP
Port 2						Non-STP
Port 3						Non-STP
Port 4						Non-STP
Port 5						Non-STP
Port 6						Non-STP
Port 7						Non-STP
Port 8						Non-STP
Port 9						Non-STP
Port 10						Non-STP
Port 11						Non-STP
Port 12						Non-STP
Port 13						Non-STP
Port 14						Non-STP
Port 15						Non-STP
Port 16						Non-STP
Port 17						Non-STP

Port: Any combination of numbers — corresponding to port numbers as seen on the switch's front panel — valid for this parameter.

VLAN ID: Displays a value from 1 to 4094 or "None" (default).

Path Cost: Displays a value from 0 to 2147483647 or "None" (default). This is the cost offered by this port. If the Bridge RSTP cost style is STP, 1Gbps ports will contribute 4, 100Mbps ports will contribute 19 and 10Mbps contribute a cost of 100. If the cost style is RSTP, 1Gbps ports will contribute 20,000, 100Mbps ports will contribute a cost of 200,000 and 10Mbps ports contribute a cost of 2,000,000.

Edge Port: Displays either yes or no.

P2P Port: Displays either yes or no. Default: None. RSTP uses a peer-to-peer protocol that provides for rapid transitioning on point-to-point links. This protocol is automatically turned off in situations where multiple STP brdges communicate over a shared (non-point-to-point) LAN. The bridge will automatically take point-to-point to be true when the link is found to be operating full duplex. The point-to-point parameter allows this behavior or operates a point-to-point link, but cannot run the link full duplex. It will force the parameter false when the port operates the link full duplex, but is still not point-to-point (e.g., a full duplex link to an unmanaged bridge that concentrates two other STP bridges).

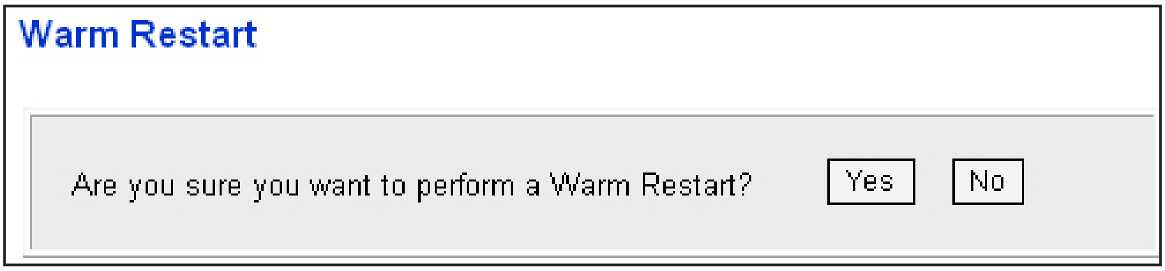
Protocol: Displays either RSTP or STP.

Port State: Displays Non-STP, Disabled, Learning, Forwarding, Blocking or Discarding to indicate the STP status of the port.

- Non-STP: STP is disabled on this port.
- Disabled: STP is enabled on this port, but the link is down.
- Learning: The port is learning MAC addresses in order to prevent flooding when it begins forwarding traffic.
- Forwarding: The port is forwarding traffic.
- Blocking: The port is used in the STP topology, but isn't forwarding traffic.
- Discarding: The link is not used in the STP topology, but is standing by.

Maintenance

WARM RESTART

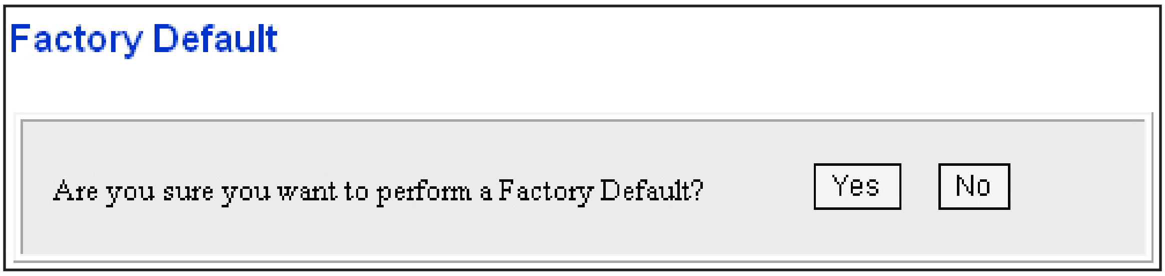


Warm Restart

Are you sure you want to perform a Warm Restart?

Yes: Click to reboot the device in software reset.

FACTORY DEFAULT

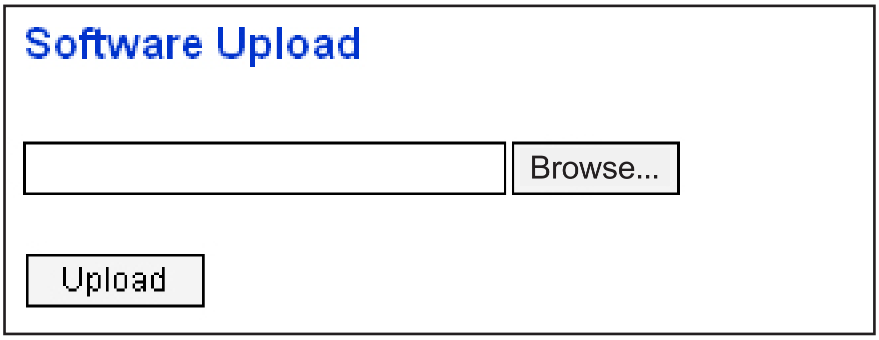


Factory Default

Are you sure you want to perform a Factory Default?

Yes: Click to reset the switch to the default configuration.

SOFTWARE UPLOAD



Browse...: Click to find the new firmware file you want, then click "Upload" to upgrade the firmware and reboot the switch system. ***IMPORTANT:*** During the upgrade process, don't turn off the power or any function on the Web page.

LOGOUT

Click to exit the Web management interface.

CONSOLE MANAGEMENT

The Gigabit Web-Smart Switch switch provides a console interface for local configuration through its RS232 port. This is an internal, character-oriented user interface for system administration, such as resetting factory configuration or changing some settings.

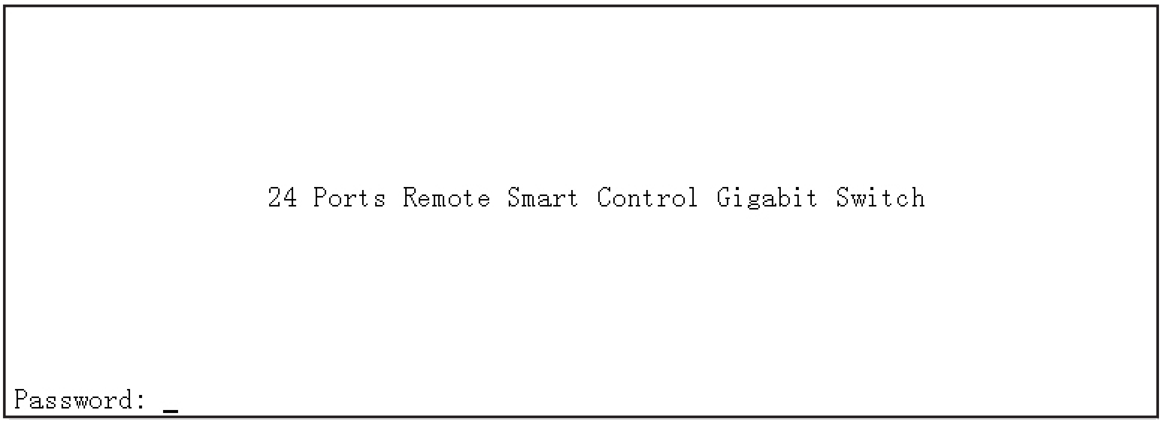
Direct Access

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as HyperTerminal) to the switch console port. When using the management method, configure the terminal-emulation program to use the following default parameters:

- 115200bps
- 8 data bits
- No parity
- 1 stop bit

Logging On

Enter the factory default password. The user default password is "admin"; the super password is "superword." Or enter a user-defined password if you change the factory default password later.

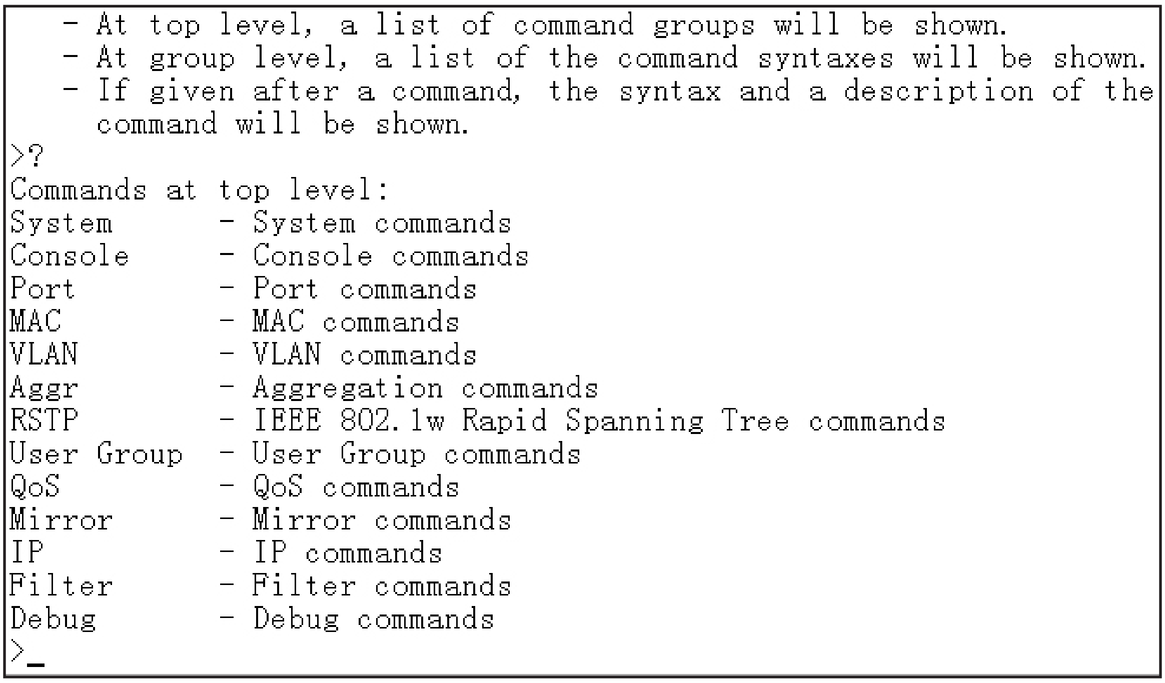


```
                24 Ports Remote Smart Control Gigabit Switch






Password: _
```

NOTE: The super password can’t be modified; and only one console user can log on to the switch at a time.

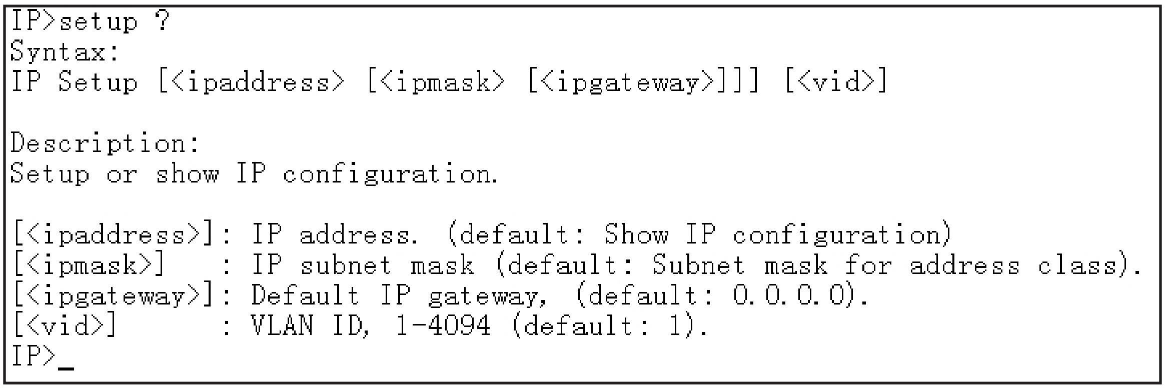
Command-Line Interface (CLI) Commands

The console management interface is based on command lines. After you log in to the system, the root directory displays. Enter “?” to show all commands.



```
   - At top level, a list of command groups will be shown.
   - At group level, a list of the command syntaxes will be shown.
   - If given after a command, the syntax and a description of the
     command will be shown.
>?
Commands at top level:
System      - System commands
Console     - Console commands
Port        - Port commands
MAC         - MAC commands
VLAN        - VLAN commands
Aggr        - Aggregation commands
RSTP        - IEEE 802.1w Rapid Spanning Tree commands
User Group  - User Group commands
QoS         - QoS commands
Mirror      - Mirror commands
IP          - IP commands
Filter      - Filter commands
Debug       - Debug commands
>_
```

If you’re not sure about the correctness of a command entry, enter “?” or a space and the system will list possible commands and descriptions, as shown on the screen below. Common commands and their resultant screens with options follow.

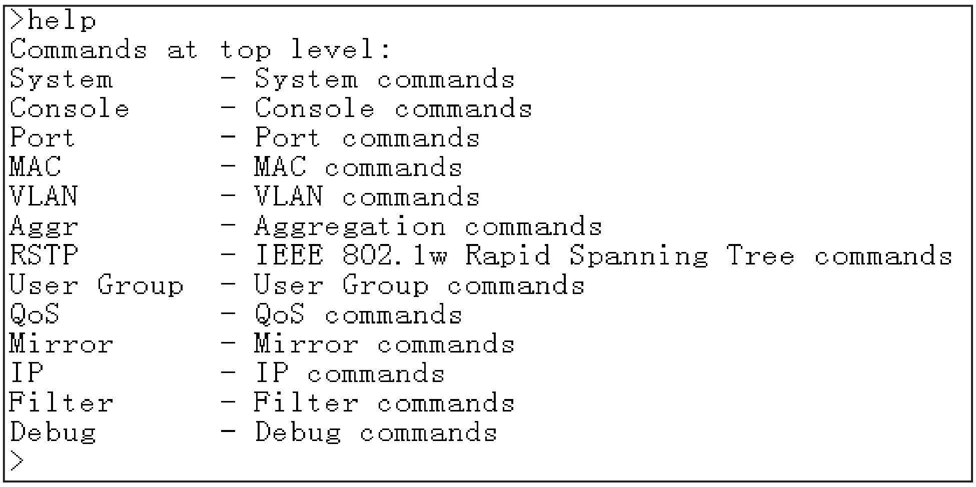


```
IP>setup ?
Syntax:
IP Setup [<ipaddress> [<ipmask> [<ipgateway>]]] [<vid>]

Description:
Setup or show IP configuration.

[<ipaddress>]: IP address.  (default: Show IP configuration)
[<ipmask>]    : IP subnet mask (default: Subnet mask for address class).
[<ipgateway>]: Default IP gateway, (default: 0.0.0.0).
[<vid>]       : VLAN ID, 1-4094 (default: 1).
IP>_
```

Enter the IP address, IP mask, IP gateway or VID according to the above format.

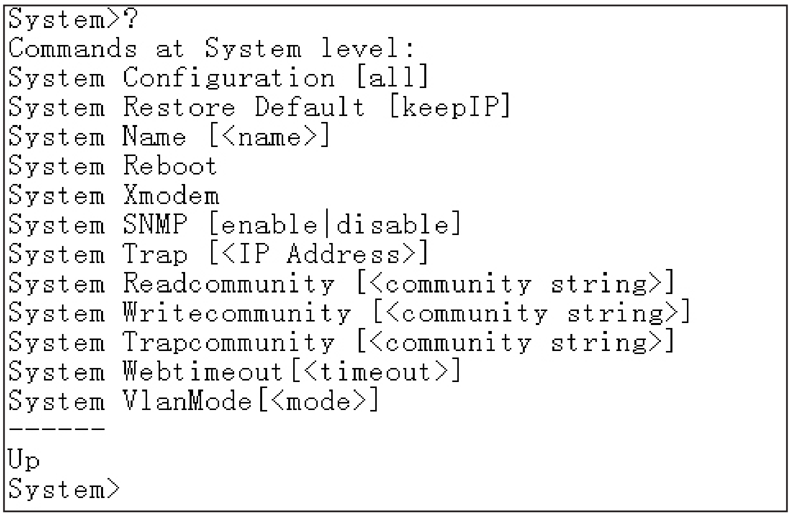
HELP

This displays command syntax information.



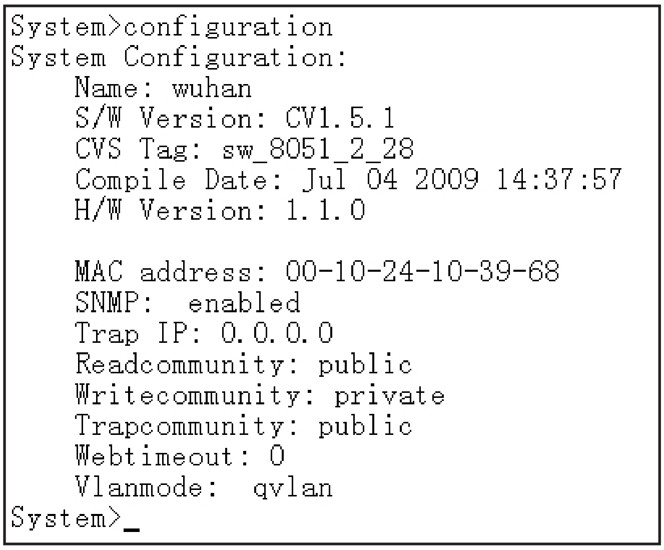
```
>help
Commands at top level:
System       - System commands
Console      - Console commands
Port         - Port commands
MAC          - MAC commands
VLAN         - VLAN commands
Aggr         - Aggregation commands
RSTP         - IEEE 802.1w Rapid Spanning Tree commands
User Group   - User Group commands
QoS          - QoS commands
Mirror       - Mirror commands
IP           - IP commands
Filter       - Filter commands
Debug        - Debug commands
>
```

SYSTEM



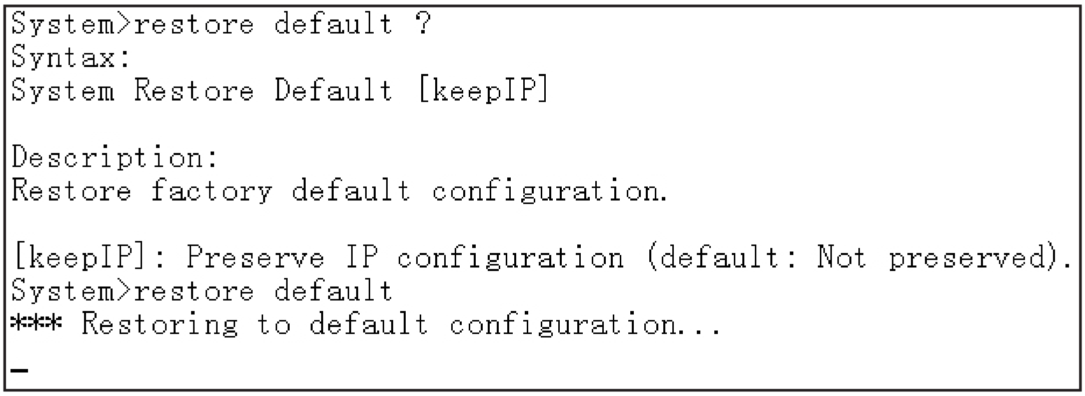
```
System>?
Commands at System level:
System Configuration [all]
System Restore Default [keepIP]
System Name [<name>]
System Reboot
System Xmodem
System SNMP [enable|disable]
System Trap [<IP Address>]
System Readcommunity [<community string>]
System Writecommunity [<community string>]
System Trapcommunity [<community string>]
System Webtimeout[<timeout>]
System VlanMode[<mode>]
------
Up
System>
```

SYSTEM CONFIGURATION



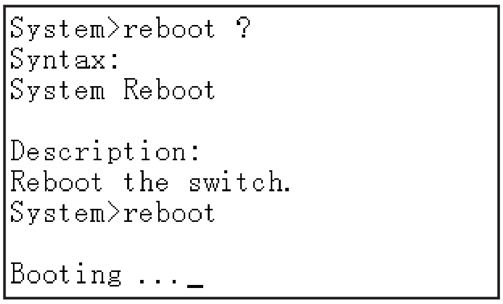
```
System>configuration
System Configuration:
    Name: wuhan
    S/W Version: CV1.5.1
    CVS Tag: sw_8051_2_28
    Compile Date: Jul 04 2009 14:37:57
    H/W Version: 1.1.0

    MAC address: 00-10-24-10-39-68
    SNMP:  enabled
    Trap IP: 0.0.0.0
    Readcommunity: public
    Writecommunity: private
    Trapcommunity: public
    Webtimeout: 0
    Vlanmode:  qvlan
System>_
```

SYSTEM RESTORE DEFAULT



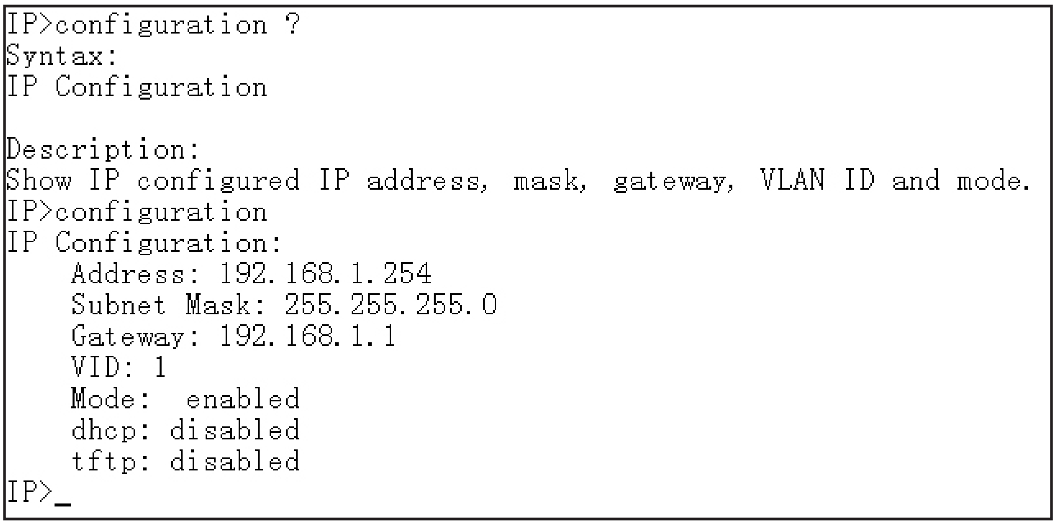
```
System>restore default ?
Syntax:
System Restore Default [keepIP]

Description:
Restore factory default configuration.

[keepIP]: Preserve IP configuration (default: Not preserved).
System>restore default
*** Restoring to default configuration...
_
```

SYSTEM REBOOT



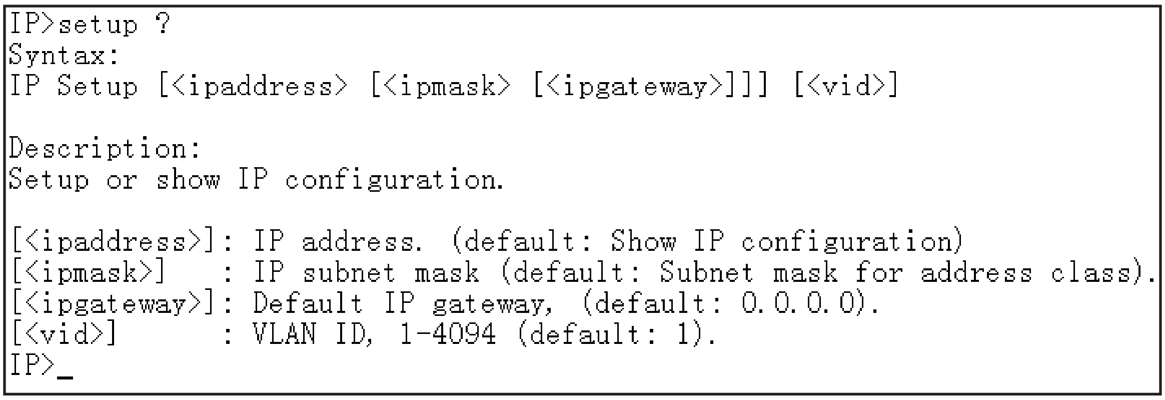
```
System>reboot ?
Syntax:
System Reboot

Description:
Reboot the switch.
System>reboot

Booting ..._
```

IP CONFIGURATION



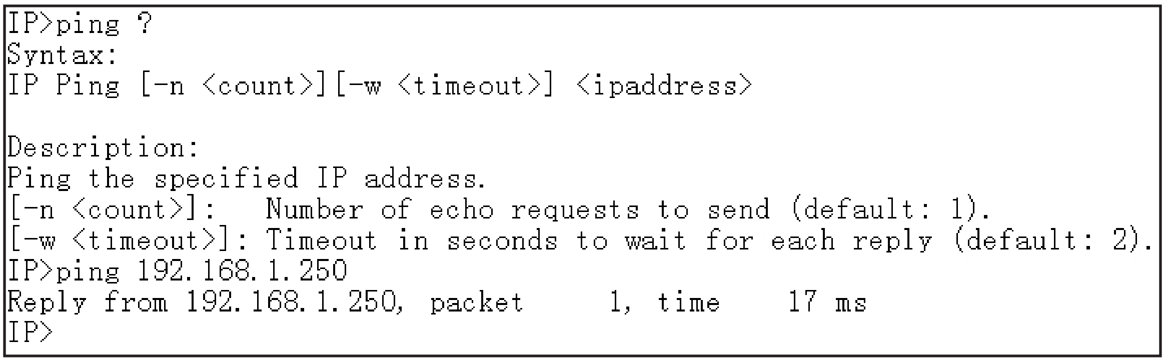
```
IP>configuration ?
Syntax:
IP Configuration

Description:
Show IP configured IP address, mask, gateway, VLAN ID and mode.
IP>configuration
IP Configuration:
    Address: 192.168.1.254
    Subnet Mask: 255.255.255.0
    Gateway: 192.168.1.1
    VID: 1
    Mode:  enabled
    dhcp: disabled
    tftp: disabled
IP>_
```

IP SETUP



```
IP>setup ?
Syntax:
IP Setup [<ipaddress> [<ipmask> [<ipgateway>]]] [<vid>]

Description:
Setup or show IP configuration.

[<ipaddress>]: IP address. (default: Show IP configuration)
[<ipmask>]   : IP subnet mask (default: Subnet mask for address class).
[<ipgateway>]: Default IP gateway, (default: 0.0.0.0).
[<vid>]      : VLAN ID, 1-4094 (default: 1).
IP>_
```

IP PING



```
IP>ping ?
Syntax:
IP Ping [-n <count>][-w <timeout>] <ipaddress>

Description:
Ping the specified IP address.
[-n <count>]:   Number of echo requests to send (default: 1).
[-w <timeout>]: Timeout in seconds to wait for each reply (default: 2).
IP>ping 192.168.1.250
Reply from 192.168.1.250, packet     1, time    17 ms
IP>
```

SPECIFICATIONS

Standards

- IEEE 802.1d (Spanning Tree Protocol)
- IEEE 802.1p (Traffic Prioritization)
- IEEE 802.1q (VLAN Tagging)
- IEEE 802.3 (10Base-T Ethernet)
- IEEE 802.3u (100Base-TX Fast Ethernet)
- IEEE 802.3ab (Twisted Pair Gigabit Ethernet)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3x (flow control for full duplex mode)

General

- Media support:
  - 10Base-T Cat3, 4, 5 UTP/STP RJ45
  - 100Base-TX Cat5 UTP/STP RJ45
  - 1000Base-T Cat5e UTP/STP RJ45
- Packet filter/forwarding rate:
  - 1,488,000 pps (1000 Mbps)
  - 148,800 pps (100 Mbps)
  - 14,880 pps (10 Mbps)
- MAC address table: 8192 entries
- Backplane speed:
  - Model 524063: 48 Gbps
  - Model 524087: 32 Gbps
- Switch architecture: store and forward
- Certifications: FCC Class A, CE

Configuration Options

- Port link speed: 10 Mbps, 100 Mbps, 1000 Mbps or auto-negotiation
- Flow control on/off per port
- VLAN
- Port Mirroring
- Port Aggregation/Trunking:
  - Model 524063: 8 groups, with up to 12 member ports per trunk
  - Model 524087: 8 groups, with up to 8 member ports per trunk
- Broadcast Storm configuration with ICMP rate, broadcast rate, multicast rate, flooded unicast rate
- Port Filter configuration

LEDs

- Power
- Link/Act

Power

- Internal power supply: 100 – 240 V AC, 50/60 Hz
- Power consumption: 30 Watts (max.)

Environmental

- Metal housing, 19” rackmount, 1U
- Dimensions: 440 (L) x 205 (W) x 44 (H) mm (17.3 x 8 x 1.7 in.)
- Weight: 3.7 kg (8.0 lbs.)
- Operating temperature: 0 – 40°C (32 – 104°F)
- Operating humidity: 10 – 90% RH, non-condensing
- Storage temperature: -40 – 70°C (-4 – 158°F)

Package Contents

- Gigabit Web-Smart Switch
- Quick installation guide
- Setup CD with user manual

INTELLINET™

NETWORK SOLUTIONS

INTELLINET NETWORK SOLUTIONS™ offers a complete line
of active and passive networking products.
Ask your local computer dealer for more information or visit
www.intellinet-network.com.