MANAGED LAYER 3 ACCESS SWITCH USER MANUAL

MODEL 523868

INTELLINET™
NETWORK SOLUTIONS

INT-523868-UM-0807-01

INTRODUCTION

Thank you for purchasing the INTELLINET NETWORK SOLUTIONS™ Managed Layer 3 Access Switch, Model 523868.

This is a high-performance managed SNMP switch that provides users with 24 10/100 Mbps Ethernet and four Gigabit combo ports. The Web/SNMP management provides remote control capability that gives flexible network management and monitoring options. Whether managed through an “in-band” SNMP management station, an Internet Web browser or an “out-of-band” RS-232 console port, the Managed Layer 3 Access Switch facilitates network operational control and diagnosis.

For increased bandwidth application, it can accommodate up to 32 trunk groups with LACP link aggregation. Moreover, these trunk ports are set up with a fail-over function to provide redundant backup if one or more ports are malfunctioning. It also supports both 802.1Q VLAN and GVRP VLAN registration, thereby simplifying network traffic segmentation, broadcast domain extension and other associated benefits of constructing VLANs.

The abundance of popular features (highlighted below) translates into increased efficiency and performance in network administration, and the easy-to-follow instructions in this user manual help make setup and operation quick and simple.

- Integrated 10/100 Mbps LAN switch with Auto MDI/MDI-X support
- Supports virtual server, port forwarding and DMZ (demilitarized zone)
- Supports DDNS (dynamic DNS)
- Supports VPN pass-through (IPSec, PPTP, L2TP)
- 94 Mbps WAN to LAN throughput for wired networks
- WOL (Wake-On LAN) function sends a wakeup signal to any computer in the LAN
- Integrated scheduler to limit Internet access to client computers in the LAN
- Remote management function (enable/disable and management port)
- Easy installation through Web-based user interface
- Firmware updates via Web-based user interface
- Lifetime Warranty

Package Contents

- Managed Layer 3 Access Switch
- Power cable
- 19” rackmount brackets
- User manual

FCC Warning

This equipment has been tested and found to comply with the limits for a class A device, pursuant to part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. 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 the user’s own expense.

CE

This is a class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

TABLE OF CONTENTS

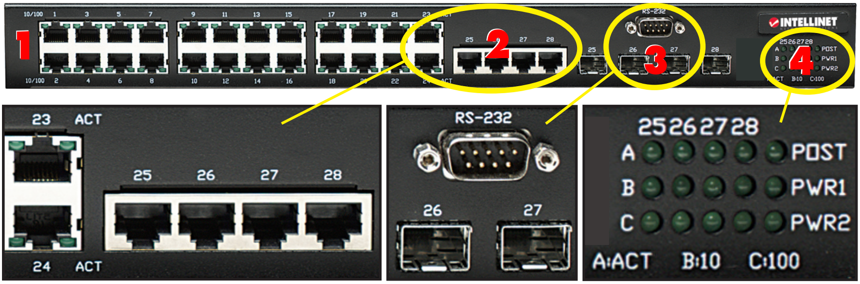
section page

NOTE: Some screen-shot images have been modified to fit the format of this user manual.

1 HARDWARE

1.1 Front Panel Connections & Indicators

The Managed Layer 3 Access Switch utilizes ports with copper and SFP fiber port connectors functioning under Ethernet/Fast Ethernet/Gigabit Ethernet standards.



1.1.1 10/100Base-TX Ports

The 10/100Base-TX ports (1 above) support network speeds of either 10 Mbps or 100 Mbps, and can operate in half- and full-duplex transfer modes. These ports also offer automatic MDI/MDI-X crossover detection that gives true Plug and Play capability — just plug the network cables into the ports and the ports will adjust according to the end-node devices. ***NOTE:*** Cat3 cables or better are recommended for 10 Mbps connections; Cat5 or better for 100 Mbps.

1.1.2 10/100/1000Base-T Ports

The switch has four Gigabit 10/100/1000Base-T ports (2 above)) for RJ-45 connectors that have the same features as the above-mentioned 10/100 ports. The only difference is that the Gigabit copper ports support network speeds of 10/100/1000 Mbps. These four ports are located next to the four SFP-type fiber slots, and each of these RJ-45 ports is interchangeable with a corresponding SFP slot. The Gigabit copper port will have the same number as its corresponding SFP slot. This means that once an SFP slot is connected, the corresponding RJ-45 port (25, 26, 27 or 28) won’t function.

1.1.3 SFP Slots for SFP Modules

The four SFP slots (3 above) are designed to house Gigabit SFP modules that support network speeds of 1000 Mbps. These slots are interchangeable with the four 1000Base-T ports to their left, and the slots have the same port numbers as their corresponding 1000Base-T ports. This means that once an SFP slot is connected via an SFP module the correspondingly numbered 1000Base-T port (25, 26, 27 or 28) won’t function.

1.1.4 LEDs

The switch is equipped with Unit LEDs (4 above), which indicate the status of the device, and Port LEDs, which display what is happening with all of the connections.

Unit LED	Condition	Status
POST	Flashing On	Indicating POST (Power On Self Test) function upon start-up POST function successfully performed
PWR1	On (Green) Off	Primary power normal Primary power off or failure
PWR2	On (Green) Off	Backup power normal Backup power off or failure

Port LED	Condition	Status
10/100	On (green)	Port operating at 100 Mbps
(copper)	Off	Port operating at below 100 Mbps
ACT	On (green)	Illuminated when connectors are attached
	Flashing (green)	Data traffic passing through port
	Off	No valid link established on port
A 25-28	On (green)	Illuminated when connectors are attached
Gigabit E’net	Flashing (green)	Data traffic passing through port
	Off	No valid link established on port
B 25-28 Gigabit E’net	On (green)	Port is operating at 10 Mbps. If LED C is also on, port is operating at 1000 Mbps
	Off	If LED C is on, port is operating at 100 Mbps or link is down
C 25-28 Gigabit E’net	On (green)	Port is operating at 100 Mbps. If LED B is also on, port is operating at 1000 Mbps
	Off	If LED B is on, port is operating at 10 Mbps or link is down

1.2 Installation

1.2.1 Location/Position

The location of the switch can greatly affect its performance. Consider these guidelines before placement, connection and operation.

- Choose a location that complies with the acceptable temperature and humidity ranges listed in the Specifications section.
- Avoid placing the switch in the vicinity of strong electromagnetic field generators (such as motors), vibration, dust and direct sunlight.
- Allow at least 10 cm of space at the front and rear of the unit for ventilation.
- As the switch is capable of connecting up to 28 network devices employing a combination of twisted-pair and fiber cabling paths, check that all cords/connectors can be safely secured.

You have three options for positioning the switch:

- For desktop use, choose a clean, flat surface with convenient access to an AC power outlet and affix the four included self-adhesive rubber pads to the bottom of the unit.
- For vertical mounting, use the underside of the switch as a template to measure and mark out the position of the holes on the vertical surface where the unit is to be installed. Then use the two screws provided to mount the switch firmly in place.
- For rack mounting, attach brackets to each side of the switch and place the brackets in the rack’s slots. Insert and tighten two screws to secure the bracket to the rack on each side.

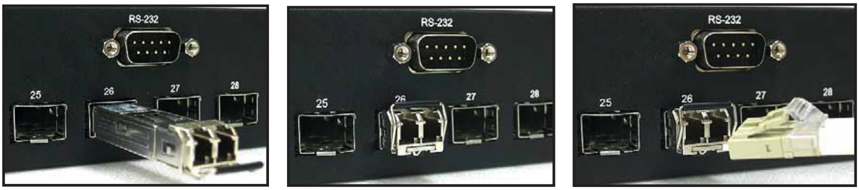
1.2.2 Powering On the Unit

The switch uses an AC power supply: 100–240 V AC / 50–60 Hz; or -48 V DC. The power on/off switch is located at the rear of the unit, adjacent to the AC power connector and the system fans. The switch’s power supply automatically self-adjusts to the local power source, and may be powered on without having any or all LAN segment cables connected.

1. Plug the power cable directly into the receptacle located at the back of the device.
2. Plug the power adapter into an available socket. ***NOTE:*** For international use, you may need to change the AC power adapter cord. Use only a power cord set that has been approved for the receptacle type and electrical current in the country you’re in.
3. Check the front-panel LEDs as the device is powered on to verify that the PWR LEDs are lit. If they’re not, check that the power cable is correctly and securely plugged in.

WARNING: Because invisible laser radiation may be emitted from the aperture of the ports when no cable is connected, avoid exposure to laser radiation and do not stare into open apertures.

1.2.3 Installing the SFP Modules and Fiber Cable



1. Slide the selected SFP module into one of the four Gigabit SFP slots below the RS-232 port, making sure the SFP module is aligned correctly with the inside of the slot.
2. Insert and slide the module into the SFP slot until it clicks into place, removing any rubber plugs that may be present in the SFP module's mouth.
3. Align the fiber cable's connector with the SFP module's mouth and slide the connector in until a click is heard. (To pull the connector out, first push down the release clip on top of the connector.) Check the corresponding port LED on the front panel to be sure the connection is valid (see subsection 1.1.4).

TIP: To properly connect fiber cabling, check that the fiber terminators are clean. You can clean the cable plugs by wiping them gently with a clean tissue or cotton ball moistened with a little ethanol. Dirty fiber terminators on fiber optic cables will impair the quality of the light transmitted through the cable and lead to degraded performance on the port.

1.2.4 Connecting Copper Cable

The 10/100Base-TX RJ-45 Ethernet port fully supports auto-sensing and auto negotiation.

1. Insert one end of a Category 3/4/5/5e twisted-pair cable into an available RJ-45 port on the switch and the other end into the port of the network node.
2. Check the corresponding port LED on the front panel to ensure the connection is valid (see subsection 1.1.4).

1.2.5 Connecting the Console Port Cable

The console port (DB-9) provides the out-of-band management facility.

1. Use null modem cable to connect the console port on the front panel of the switch to the computer COM port.
2. Configure the HyperTerminal settings as explained in the next section(s).

1.2.6 Connecting to Computers or a LAN

Use Ethernet cable (either crossover or straight-through) to connect computers (or hubs or other switches) directly to the Managed Layer 3 Access Switch ports. ***NOTE:*** Use a twisted-pair Category 5 Ethernet cable to connect the 1000Base-T port; otherwise, the link speed cannot reach 1 Gbps.

2 SWITCH MANAGEMENT/OPERATION

2.1 System Overview

This system can be managed three ways:

- Out-of-band through the console port on the front panel;
- In-band by using Telnet; or
- By using Web-based management — accessible through a Web browser— which allows you to configure the switch, monitor the LED panel and display statistics graphically after a successful installation.

2.1.1 Configuration Using the Console Port (RS-232)

Prior to accessing the switch's onboard agent (software that supports SNMP — see subsection 2.1.3 below) via a network connection, first configure the switch by giving it a valid IP address, subnet mask and default gateway using an out-of-band connection or the BOOTP protocol. After configuring the switch's IP parameters, you can access the onboard configuration program from anywhere in the attached network or via the Internet by using Telnet from any computer attached to the network or by using a Web browser (Internet Explorer 4.0 or above or Netscape Navigator 4.0 or above).

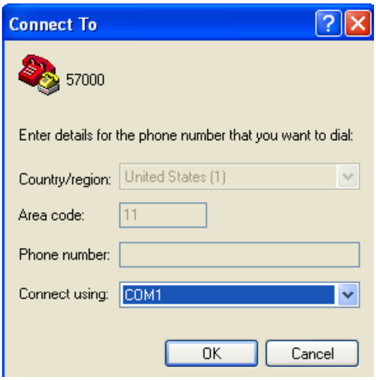
Access the switch via a terminal emulator (such as HyperTerminal) attached to the console port. The console port is set at the factory with the following default COM port properties:

- Baud rate: 38,400
- Data size: 8 bits
- Parity: None
- Stop bits: 1
- Flow Control: None

NOTE: Configure your own terminal to match these settings; otherwise, the connection will not work.

2.1.1.1 Using HyperTerminal to Set the IP Address

1. Verify that a console cable (RJ-45 to DB9 [for the RS-232]) connection between the switch and the workstation exists.
2. Launch the terminal emulation program on the remote workstation and power on the switch. Confirm that the correct COM port is selected.



Connect To

57000

Enter details for the phone number that you want to dial:

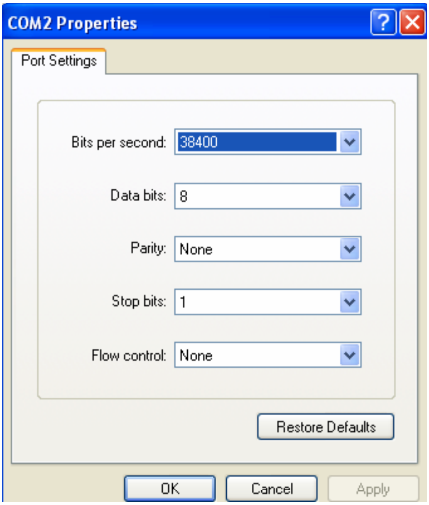
Country/region: United States (1)

Area code: 11

Phone number:

Connect using: COM1

3. Enter the correct parameters according to the defaults presented above. Click "OK."



COM2 Properties

Port Settings

Bits per second: 38400

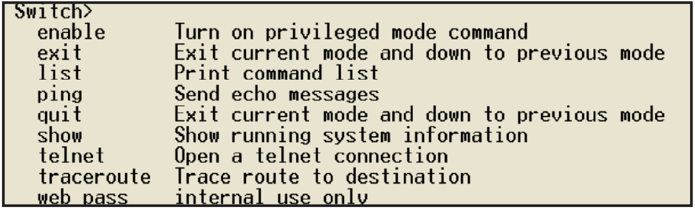
Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

3. The prompt screen will display. The default login is “admin,” with no preset password (just press the “Enter” key).
4. The prompt *Switch>* will display. For a list of main commands, type “?” and press “Enter.” For a list of subcommands, type a main command (such as “list”) and press “Enter.”

   ```
   Switch>
     enable       Turn on privileged mode command
     exit         Exit current mode and down to previous mode
     list         Print command list
     ping         Send echo messages
     quit         Exit current mode and down to previous mode
     show         Show running system information
     telnet       Open a telnet connection
     traceroute   Trace route to destination
     web pass     internal use only
   ```

   After a successful login, type the following command lines to change the device IP, network mask and gateway address. The “xxx” segments represent values between 0 and 255. Be sure to enter your IP address information in this form (including the periods separating the segments), as the configuration program will not accept any other format.
   - set eth0 ip xxx.xxx.xxx.xxx
   - set eth0 netmask xxx.xxx.xxx.xxx
   - set eth0 gateway xxx.xxx.xxx.xxx

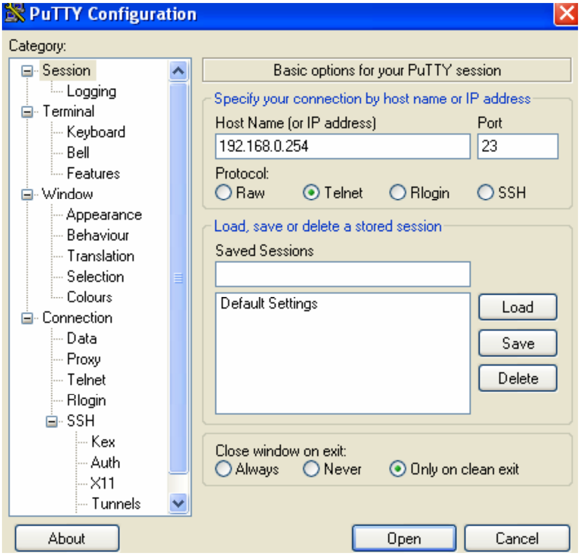
   Once the new information has been entered, the system will confirm whether the operation is successful and restart automatically. Record the new address information and store it in a secure location.

NOTE: With HyperTerminal, the command lines are the same as for Telnet: You can continue using HyperTerminal along with the instructions given in the following sections. Otherwise, log out by typing “exit” and pressing the “Enter” key. Then, you can configure the switch via an HTTP Web browser or by using Telnet with menu-driven or command line interfaces.

NOTE: Remember that IP addresses are unique. If an address isn’t available, contact your Internet service provider to obtain one.

2.1.2 Configuration Using Telnet and SSH

1. Activate your workstation’s command prompt program (such as PuTTY) and access your switch via the Internet by entering the correct IP address. ***NOTE:*** The factory default is 192.168.0.254: Connect directly via the console port to configure a unique IP address. A command prompt program such as PuTTY will provide you with the option of choosing either Telnet or SSH (Secure Shared). SSH is an encrypted protocol that’s ideal for ISP workers who need to be extra careful when managing their switches.



PuTTY Configuration

Basic options for your PuTTY session

Specify your connection by host name or IP address

Host Name (or IP address): 192.168.0.254

Port: 23

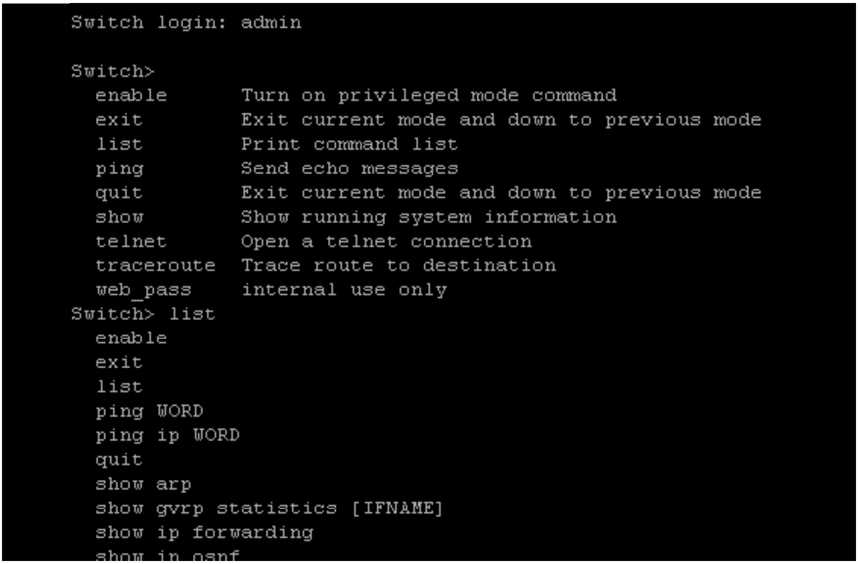
Protocol: ○ Raw ● Telnet ○ Rlogin ○ SSH

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

2. Click “Open” to display a command prompt screen.



```
Switch login: admin

Switch>
  enable       Turn on privileged mode command
  exit         Exit current mode and down to previous mode
  list         Print command list
  ping         Send echo messages
  quit         Exit current mode and down to previous mode
  show         Show running system information
  telnet       Open a telnet connection
  traceroute   Trace route to destination
  web_pass     internal use only
Switch> list
  enable
  exit
  list
  ping WORD
  ping ip WORD
  quit
  show arp
  show gvrp statistics [IFNAME]
  show ip forwarding
  show ip ospf
```

3. On the *Switch login:* line, type the pre-set password (the factory default is “admin”). Type “?” and press the “Enter” key for a list of the main commands. As shown above, the “list” command has been entered below the last main command listed.

2.1.3 SNMP-Based Management and Settings

You can manage the Managed Layer 3 Access Switch with SNMP Manager software (referred to as an agent) that runs locally on the device. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB (Management Information Base) objects that are defined and stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

The Simple Network Management Protocol (SNMP) is an application layer specifically designed for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches and other network devices. Use SNMP to configure system features for proper operation, to monitor performance and to detect potential problems in the switch, switch group or network.

In short, SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

2.1.3.1 MIB Objects

The Management Information Base (MIB) stores management and counter information. The switch uses the standard MIB-II Management Information Base module, so, consequently, values for MIB objects can be retrieved from any SNMP-based network management software. MIB values can be either read-only or read-and-write.

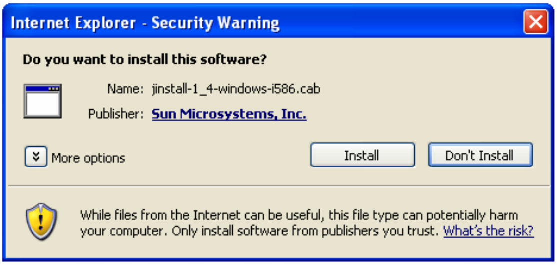
2.1.3.2 Traps

Traps are messages that notify network personnel of events that occur on the switch. The events can be as serious as a reboot (someone accidentally turns the switch off) or as minor as a port status change. The switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change and Broadcast/Multicast Storm.

2.1.4 Initial Connection to the Switch

The switch supports user-based security that allows you to prevent unauthorized users from accessing the switch or changing its settings. This feature requires Java Runtime Environment (JRE) 5.0 Update 5, which, if not already on your computer, can be easily installed in as little time as five minutes by following these steps.

1. Open your network browser (you must be connected to the Internet) and enter the factory default IP address of the switch (192.168.0.254) in the address bar. If a pop-up screen appears and advises you to click on it to install, do so.
2. If the security warning shown at right displays, click “Install.”
3. The initial Java Installer screen will display. Wait a few moments until the next screen (License Agreement) appears.
4. After reading the License Agreement, select *Typical setup* (the recommended option vs. *Custom setup*). Click “Accept.”



Internet Explorer - Security Warning

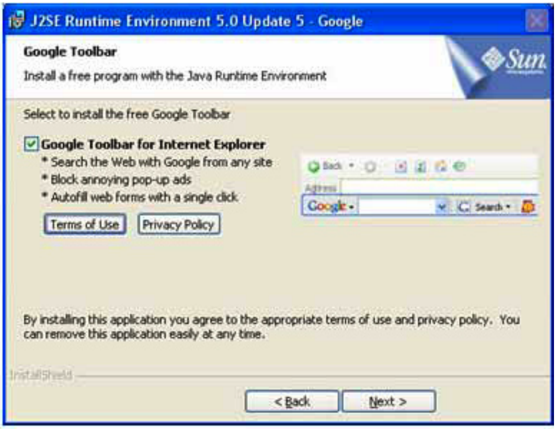
Do you want to install this software?

Name: jinstall-1_4-windows-i586.cab

Publisher: Sun Microsystems, Inc.

While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. What's the risk?

5. If Internet Explorer is set as the default browser on your system, then the Java Runtime Environment 5.0 Update 5 – Google Programs dialog box will appear. By default, *Google Toolbar for Internet Explorer* is selected. Click “Next” to begin installing selected program features, including the JRE, on your system.



J2SE Runtime Environment 5.0 Update 5 - Google

Google Toolbar

Install a free program with the Java Runtime Environment

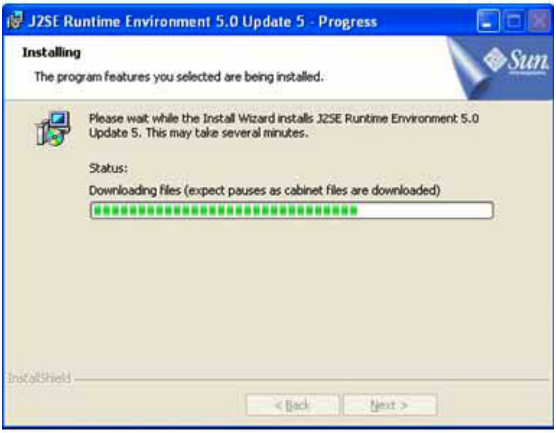
Select to install the free Google Toolbar

☑ Google Toolbar for Internet Explorer

- Search the Web with Google from any site
- Block annoying pop-up ads
- Autofill web forms with a single click

By installing this application you agree to the appropriate terms of use and privacy policy. You can remove this application easily at any time.

6. The Progress screen displays to indicate installation status once the process has begun. (Depending on connection speed, the process takes between five and 30 minutes.) A few brief dialog boxes will confirm the last steps of the installation process, then a concluding message will appear with the confirmation “Installation Completed OK.” Click “Finish.”



J2SE Runtime Environment 5.0 Update 5 - Progress

Installing

The program features you selected are being installed.

Please wait while the Install Wizard installs J2SE Runtime Environment 5.0 Update 5. This may take several minutes.

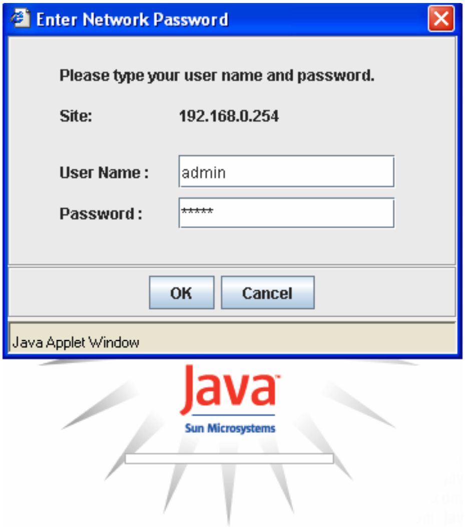
Status:

Downloading files (expect pauses as cabinet files are downloaded)

After completing the installation process, the program will display the screen at right every time you enter the IP address. The default username and password are both “admin.” Click “OK” to enter the switch’s management interface.

NOTE: If you still have problems accessing the hyperlink:

- Check the firewall in your PC or the firewall that your company uses. This firewall could be blocking access to the hyperlink.
- Make sure you have downloaded the latest version of Java Runtime Environment. This software will run on any of the normal Windows systems, as well as on Unix.



Enter Network Password

Please type your user name and password.

Site: 192.168.0.254

User Name : admin

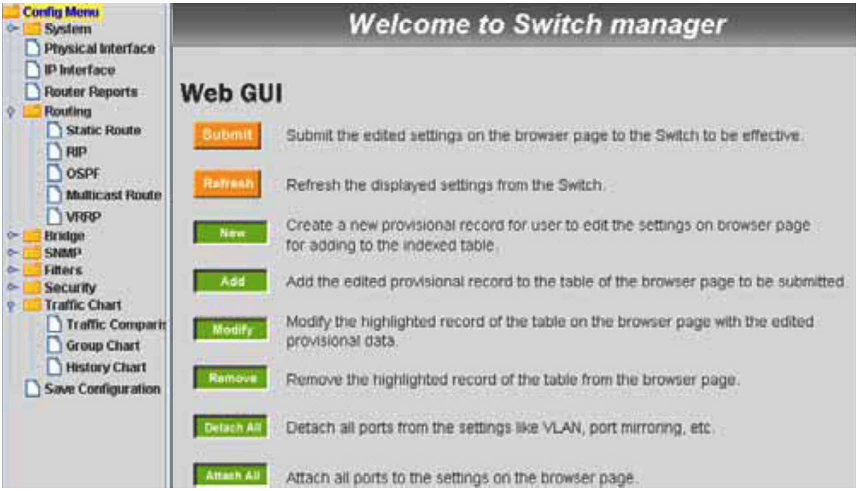
Password : *****

2.2 Web Management

The Managed Layer 3 Access Switch provides Web pages that allow equipment management through the Internet. The Java Runtime Environment (JRE) is required to run Java applet programs that are automatically downloaded from the switch during management functions. (See subsection 2.1.4 above.)

2.2.1 Login

1. Open your Web browser, enter the factory default IP address — http://192.168.0.254 — in the Web address (location) box, then press “Enter.” The login screen shown above (subsection 2.1.4) is displayed.
2. Enter the default username and password (“admin” for both) the first time you log in. These can subsequently be changed (recommended for security purposes) through the CLI interface. (See subsection 2.3.2.) Click “OK.”
3. The Welcome (home) screen will display each time you log in, presenting the Configuration Menu (on the left side of the screen) and the following Web GUI options.



Welcome to Switch manager

Web GUI

Submit — Submit the edited settings on the browser page to the Switch to be effective.

Refresh — Refresh the displayed settings from the Switch.

New — Create a new provisional record for user to edit the settings on browser page for adding to the indexed table.

Add — Add the edited provisional record to the table of the browser page to be submitted.

Modify — Modify the highlighted record of the table on the browser page with the edited provisional data.

Remove — Remove the highlighted record of the table from the browser page.

Detach All — Detach all ports from the settings like VLAN, port mirroring, etc.

Attach All — Attach all ports to the settings on the browser page.

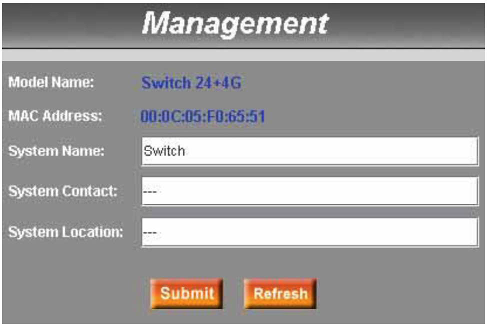
- Click “New” to create a new entry for editing to the table (temporary until “Submit” is clicked).
- Click “Add” to add the new entry to the table (temporary until “Submit” is clicked).
- Click “Modify” to save changes to an existing entry (temporary until “Submit” is clicked).
- Click “Remove” to remove a selected entry (temporary until “Submit” is clicked).
- Click “Attach All” to select all ports for a selected entry (temporary until “Submit” is clicked).
- Click “Detach All” to unselect all ports for a selected entry (temporary until “Submit” is clicked).
- Click “Submit” to save changes to the RAM memory of the switch.
- Click “Refresh” to display current settings of the switch for viewing the effect of changes.

WARNING: Clicking “Submit” only configures the switch hardware and saves the settings to RAM memory. Such changes will be lost if the switch is powered off. To save changes permanently in the switch’s Flash memory, click on “Save Configuration” (listed at the bottom of the Configuration Menu). Once the “Save Configuration” screen displays, click “Save” to store all configurations permanently in the Flash memory.

2.2.2 System

System on the Config Menu presents Management, IP Setup, Reboot and Firmware Upgrade.

2.2.2.1 Management



Model Name: Switch 24+4G

MAC Address: 00:0C:05:F0:65:51

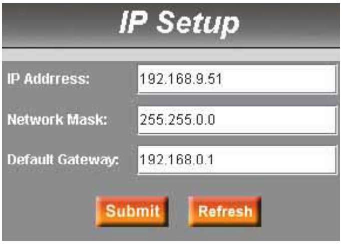
System Name: Switch

System Contact: ---

System Location: ---

Model Name: The product name is listed.
MAC Address: The switch’s MAC address is listed.
System Name: The user-assigned name to identify the system (editable).
System Contact: Enter info as desired.
System Location: Enter info as desired.
Click “Submit” to commit the settings. Click “Refresh” to display current switch settings. To eventually make all changes permanent in Flash memory, click on “Save Configuration” (listed at the bottom of the Configuration Menu) and click “Save.”

2.2.2.2 IP Setup



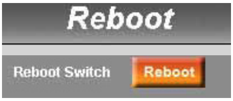
IP Addrress: 192.168.9.51

Network Mask: 255.255.0.0

Default Gateway: 192.168.0.1

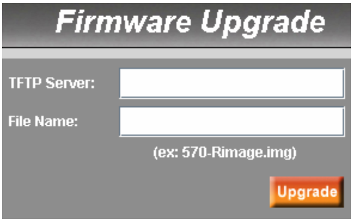
IP Address: This is the IP address for the switch.
Network Mask: This is the network mask for this network.
Default Gateway: This is the default gateway of the network.
Click “Submit” to commit the settings. Click “Refresh” to display current switch settings. To eventually make all changes permanent in Flash memory, click on “Save Configuration” (listed at the bottom of the Configuration Menu) and click “Save.”

2.2.2.3 Reboot



Clicking “Reboot” (rebooting the system) stops the network traffic and terminates the Web interface connection.

2.2.2.4 Firmware Upgrade



TFTP Server:

File Name:

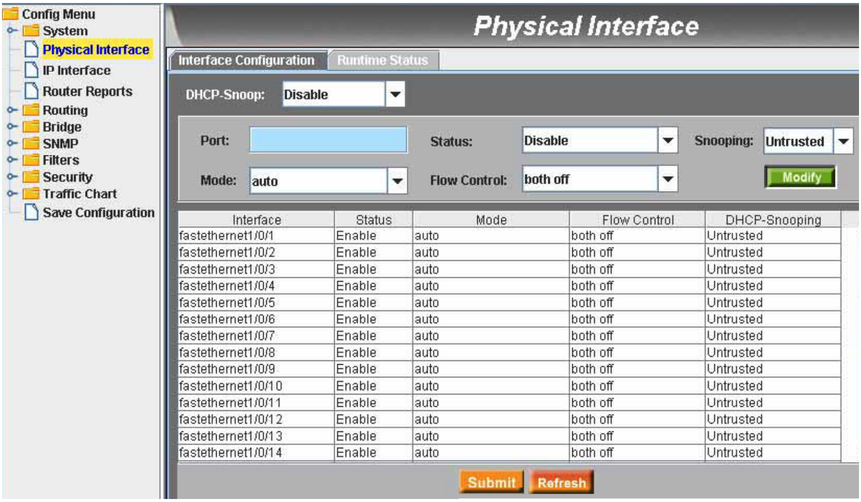
(ex: 570-Rimage.img)

Enter the TFTP server IP address and firmware filename (e.g., enter “192.168.1.155” and “3112Single-v10.img”). Click “Upgrade” to update the switch’s firmware from the TFTP server. Click “Upload” to load the assigned firmware to the switch, then reboot the system after a successful firmware update. You’ll need to log in to the Web interface again.

2.2.3 Physical Interface

Physical Interface on the Config Menu displays Ethernet port status in real time. Two options are available: Configure the port in the fields in the Interface Configuration window; and check the results in the Runtime Status window.

2.2.3.1 Interface Configuration



DHCP-Snoop: Disable

Port:

Status: Disable

Snooping: Untrusted

Mode: auto

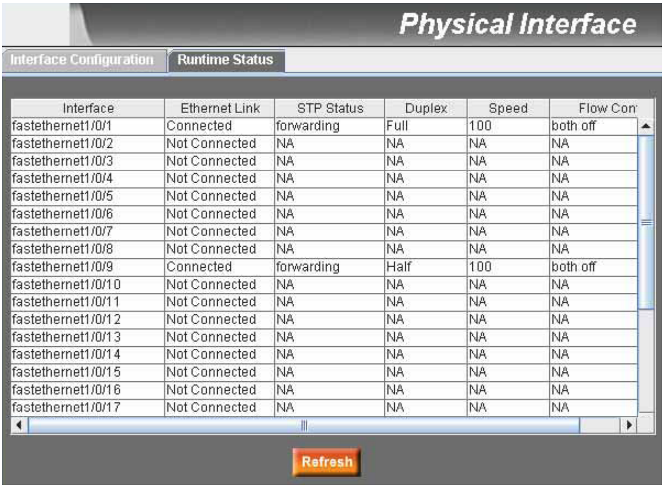
Flow Control: both off

Interface	Status	Mode	Flow Control	DHCP-Snooping
fastethernet1/0/1	Enable	auto	both off	Untrusted
fastethernet1/0/2	Enable	auto	both off	Untrusted
fastethernet1/0/3	Enable	auto	both off	Untrusted
fastethernet1/0/4	Enable	auto	both off	Untrusted
fastethernet1/0/5	Enable	auto	both off	Untrusted
fastethernet1/0/6	Enable	auto	both off	Untrusted
fastethernet1/0/7	Enable	auto	both off	Untrusted
fastethernet1/0/8	Enable	auto	both off	Untrusted
fastethernet1/0/9	Enable	auto	both off	Untrusted
fastethernet1/0/10	Enable	auto	both off	Untrusted
fastethernet1/0/11	Enable	auto	both off	Untrusted
fastethernet1/0/12	Enable	auto	both off	Untrusted
fastethernet1/0/13	Enable	auto	both off	Untrusted
fastethernet1/0/14	Enable	auto	both off	Untrusted

Port: Select the port to configure.
Status: Enable/disable the port.
Mode: Set the speed and duplex mode.
Flow Control: Enable/disable the 802.3x flow control mechanism.
DHCP-Snoop: Enable/disable the DHCP snooping function.
Snooping: Assign the selected port to be an untrusted or trusted port.
Select the corresponding port number and configure the port setting, then click “Modify.” The field you change will update the content of the display window. However, the new settings do not take effect until “Submit” is clicked.

2.2.3.2 Runtime Status

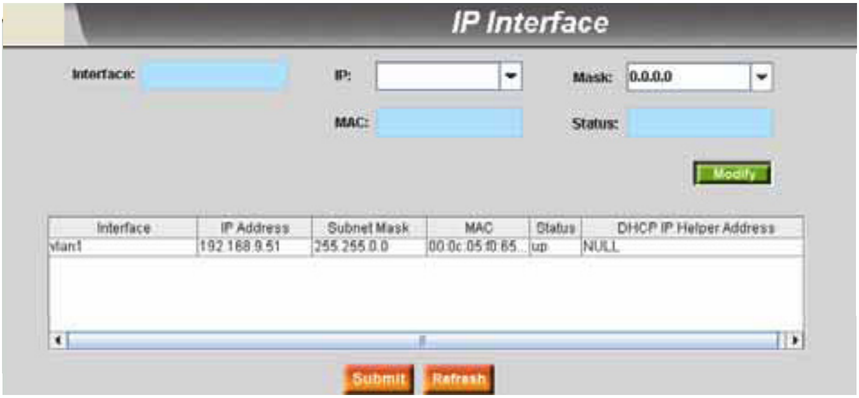
Ethernet Link: The link is connected or not connected.
STP Status: STP is enabled or disabled on the port.
Duplex: Full duplex, half duplex or NA.
Speed: This is the link speed.
Flow Control: The setting of the 802.3x flow control mechanism on both directions of the port.



Interface	Ethernet Link	STP Status	Duplex	Speed	Flow Con
fastethernet1/0/1	Connected	forwarding	Full	100	both off
fastethernet1/0/2	Not Connected	NA	NA	NA	NA
fastethernet1/0/3	Not Connected	NA	NA	NA	NA
fastethernet1/0/4	Not Connected	NA	NA	NA	NA
fastethernet1/0/5	Not Connected	NA	NA	NA	NA
fastethernet1/0/6	Not Connected	NA	NA	NA	NA
fastethernet1/0/7	Not Connected	NA	NA	NA	NA
fastethernet1/0/8	Not Connected	NA	NA	NA	NA
fastethernet1/0/9	Connected	forwarding	Half	100	both off
fastethernet1/0/10	Not Connected	NA	NA	NA	NA
fastethernet1/0/11	Not Connected	NA	NA	NA	NA
fastethernet1/0/12	Not Connected	NA	NA	NA	NA
fastethernet1/0/13	Not Connected	NA	NA	NA	NA
fastethernet1/0/14	Not Connected	NA	NA	NA	NA
fastethernet1/0/15	Not Connected	NA	NA	NA	NA
fastethernet1/0/16	Not Connected	NA	NA	NA	NA
fastethernet1/0/17	Not Connected	NA	NA	NA	NA

2.2.4 IP Interface

IP Interface on the Config Menu allows users to see the Layer 3 interface status in real time and configure the interface in the following fields.



Interface:

IP:

Mask: 0.0.0.0

MAC:

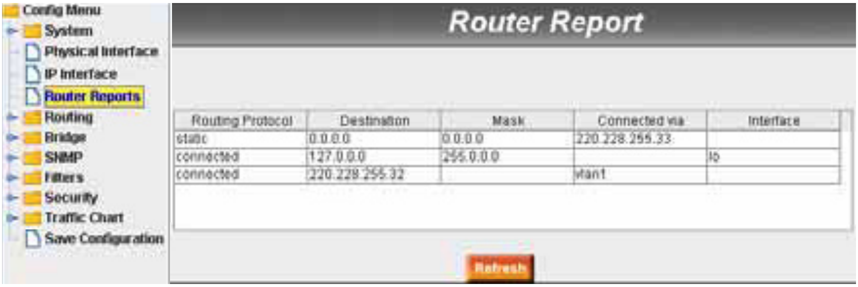
Status:

Interface	IP Address	Subnet Mask	MAC	Status	DHCP IP Helper Address
vlan1	192.168.9.51	255.255.0.0	00:0c:05:f0:65...	up	NULL

Interface: Select the interface to be configured (vlan1 is used by the system).
IP: This is the interface IP address
Mask: This is the interface subnet mask.
MAC: This is the MAC address of this interface.
Status: This is the up/down status of this interface.
DHCP IP Helper Address: This is the IP address of your DHCP server.
Select the corresponding interface and configure the interface parameters, then click “Modify.” The field you changed will update the associated content in the display window. To save any changes and make them effective immediately, click “Submit.” Click “Refresh” to refresh the display.
NOTE: There is one important thing to remember regarding DHCP and VLANs: Because each VLAN is a separate IP subnet, you must configure your DHCP server to deliver IP addresses that are appropriate for each subnet. With Windows 2000’s DHCP server, you do this by setting up a separate DHCP realm for each VLAN. Not all DHCP servers have this capability. If your existing DHCP server works only with flat LANs, you’ll probably have to upgrade to a more sophisticated package.
SPECIAL NOTE: It is strongly recommended that each interface have its own VLAN; i.e, one VLAN should not be assigned for two interfaces. Otherwise, it will create confusion while RIP is enabled. It is also recommended that only one physical port be assigned to the VLAN used for the L3 interface. When assigning multiple ports to one L3 interface, the L3 traffic will always go through the the port with lowest ID. The traffic load sharing is not supported in this case.

2.2.5 Router Reports

Router Reports on the Config Menu displays the routing table of the switch.



Routing Protocol	Destination	Mask	Connected via	Interface
static	0.0.0.0	0.0.0.0	220.228.255.33	
connected	127.0.0.0	255.0.0.0		lo
connected	220.228.255.32		vlan1	

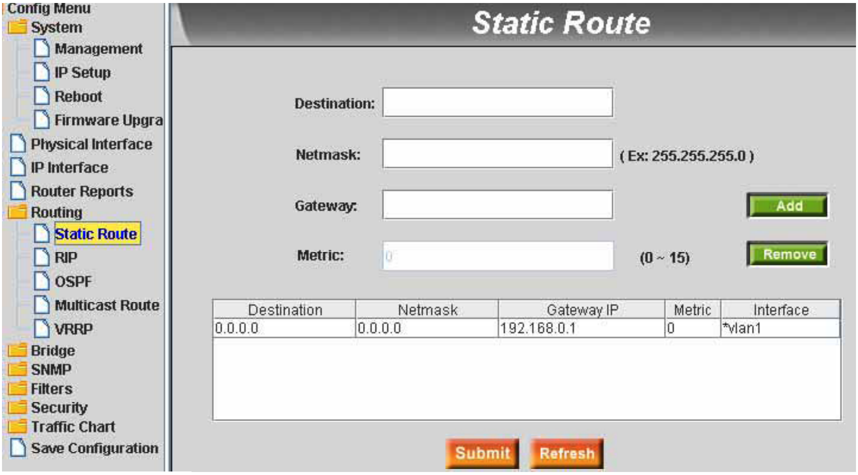
Routing Protocol: This is the routing protocol type of the route. If it's "connected," the destination is on the local LAN segment connected to the interface.
Destination: The destination IP address will be masked to generate an IP range as the objective IP addresses of packets to be routed.
Mask: This is the mask for generating a range of IP addresses.
Connected via: This is the IP address of the next router for routing to another network.
Interface: This is the interface or VLAN ID from which the packets are routed outside.

2.2.6 Routing

Routing on the Config Menu presents Static Route, RIP, OSPF, Multicast Route and VRRP.

2.2.6.1 Static Route

This section is used to add a routing entry into the switch routing table. A routing entry added this way will never be deleted by the system, hence the designation as "static." The parameters below must be input in order to configure a static route.



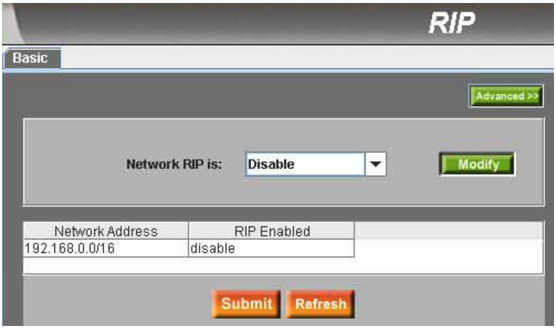
Destination:
Netmask: (Ex: 255.255.255.0)
Gateway:
Metric: 0 (0 ~ 15)

Destination	Netmask	Gateway IP	Metric	Interface
0.0.0.0	0.0.0.0	192.168.0.1	0	*vlan1

Destination: Enter the destination of the IP address.
Netmask: Enter the subnet mask of the destination for generating the IP range to be routed.
Gateway IP: Enter the gateway IP address of the next router the packets are to be sent to.
Metric: Enter a metric value (1-15). The lower the metric value, the more preferred the route.
Click "Add" after entering a new static route. The newly added entry displays in the list window. Delete the selected route by clicking "Remove." Routes that are added or removed will be stored in the configuration file immediately.

2.2.6.2 RIP

This section is used to activate the RIP routing protocol. When RIP is turned on, the switch will exchange routing information with neighbor switches that are also running RIP. Three subsections present additional options: Basic, Passive Interfaces and RIP Version, the latter two being accessible from the Basic screen, as explained below.



Network RIP is: Disable

Network Address	RIP Enabled
192.168.0.0/16	disable

2.2.6.2.1 Basic

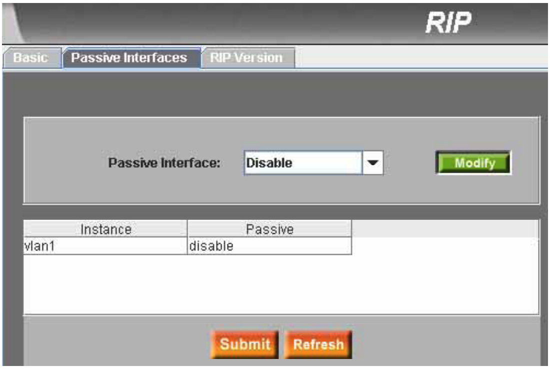
Network RIP is: Enable/Disable the RIP function for all Layer 3 interfaces. All active L3 interfaces will be shown on the screen, and you can then enable/disable the RIP function for each.

NOTE: Click “Advanced>>” to display the other two RIP screens.

2.2.6.2.2 Passive Interfaces

If an interface doesn’t need to receive and forward routing updates, disable the sending of the updates through it. The particular subnet will continue to advertise other interfaces of routing updates, and routing updates from other routers on that interface will continue to be received and processed.

Passive Interface: Enable/disable the passive interface function for a specific L3 interface. If an interface is enabled as passive, the RIP update messages will not be sent out through it except to RIP neighbors.



Passive Interface: Disable

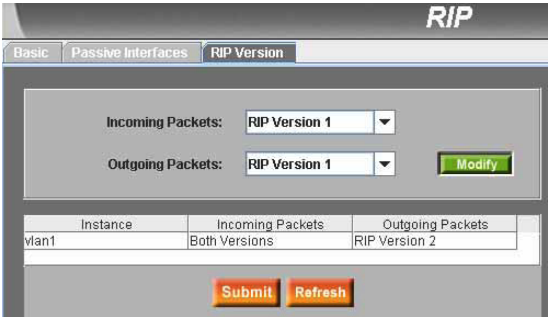
Instance	Passive
vlan1	disable

2.2.6.2.3 RIP Version

The Managed Layer 3 Access Switch can support RIPv1, RIPv2 or both.

Incoming Packets: Used to specify the RIP version for the interpretation of incoming RIP packets.

Outgoing Packet: Used to specify the RIP version for sending RIP packets to a neighboring router.



Incoming Packets: RIP Version 1

Outgoing Packets: RIP Version 1

Instance	Incoming Packets	Outgoing Packets
vlan1	Both Versions	RIP Version 2

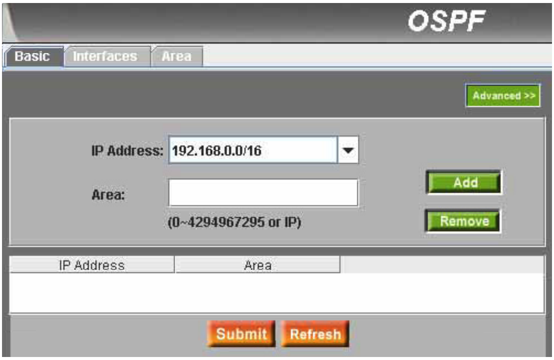
2.2.6.3 OSPF

This section is used to configure the Open Shortest Path First (OSPF) routing protocol. Three subsections present additional options: Basic, Interfaces and Area.

2.2.6.3.1 Basic

You can use this page to add L3 interfaces to specific OSPF areas.

IP Address: All active L3 interfaces are displayed — you can select any one of them to configure as an OSPF interface.



IP Address: 192.168.0.0/16

Area:

(0~4294967295 or IP)

IP Address	Area

Area: Specify the area ID for a specific L3 interface.

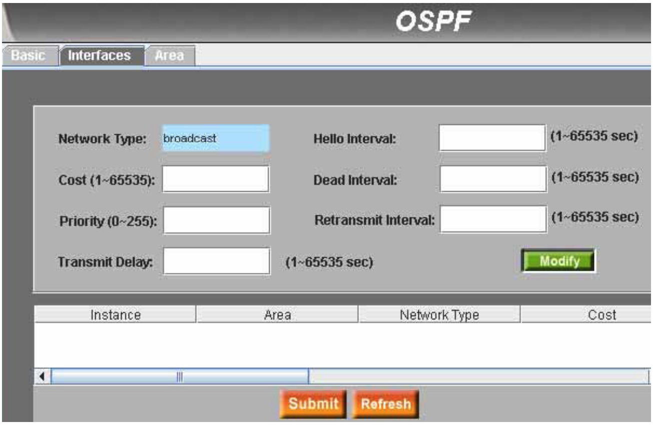
NOTE: Click “Advanced>>” to display the other two OSPF screens.

2.2.6.3.2 Interfaces

This screen is used to specify some protocol parameters for a specific OSPF interface.

Network Type: Support broadcast only.

Cost: Specify the cost for sending packets of this interface.



Network Type: broadcast

Instance	Area	Network Type	Cost

Priority: Set a priority to help determine the OSPF DR and BDR for a network.

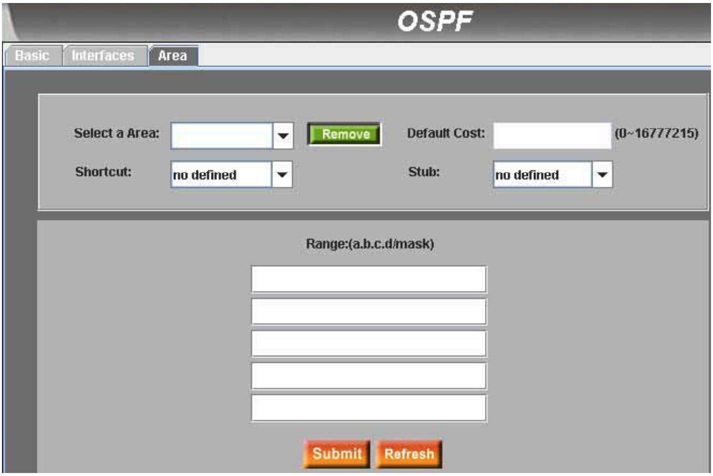
Transmit Delay: Set the estimated number of seconds to wait before sending a link update packet

Hello Interval: Set the number of seconds between two hello packets. Default is set at 10 seconds.

Dead Interval: Set the number of seconds after the last hello packet was received before notifying its neighbor that the OSPF router is down. Default is set at 40 seconds.

Retransmit Interval: Specify the number of seconds between transmitting link state advertisements.

2.2.6.3.3 Area



Shortcut: no defined

Stub: no defined

This screen is for configuring OSPF areas.

Select an Area: Input the area ID to be configured.

Default Cost: Default cost for a stub area sending a packet to the outside world.

Stub: A stub area is not a transit area since there is only one connection to the stub area. Selecting from the pull-down menu, use this attribute to specify characteristics of this area:

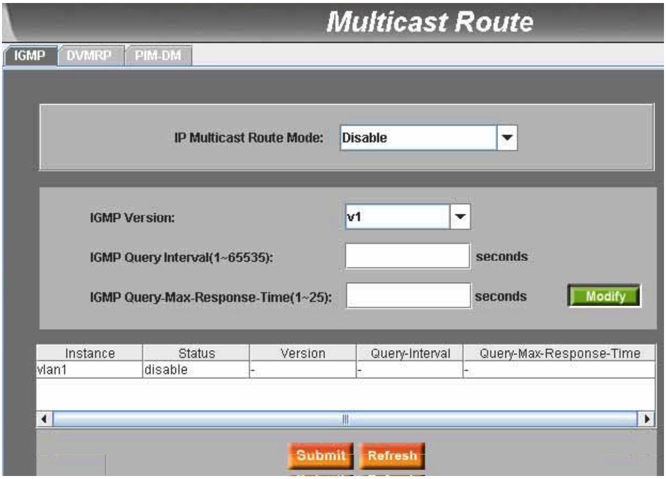
- “no defined” — not a stub area
- “no-summary” — do not inject inter-area routes into the stub
- “summary” — allow injecting inter-area routes into the stub

Shortcut: Enable/Disable the shortcut of the OSPF area (“no defined,” “disable” or “enable”).

2.2.6.4 Multicast Route

This section is used to configure the Multicast Route feature. It offers two different methods — DVMRP and PIM-DM — to establish a multicast route, and also includes IGMP (Internet Group Management Protocol), which is automatically enabled/disabled with the Multicast Route Protocol, allowing hosts to communicate in order to track data destined to a specific multicast group. The Multicast Route function uses this information to build and maintain a multicast distributed tree.

2.2.6.4.1 IGMP



IP Multicast Route Mode: Disable

IGMP Version: v1

IGMP Query Interval(1~65535): seconds

IGMP Query-Max-Response-Time(1~25): seconds

Instance	Status	Version	Query-Interval	Query-Max-Response-Time
vlan1	disable	-	-	-

This screen is for configuring the IP multicast route mode and IGMP (Internet Group Management Protocol) parameters.

IP Multicast Route Mode: Configure a multicast route protocol to run or disable.

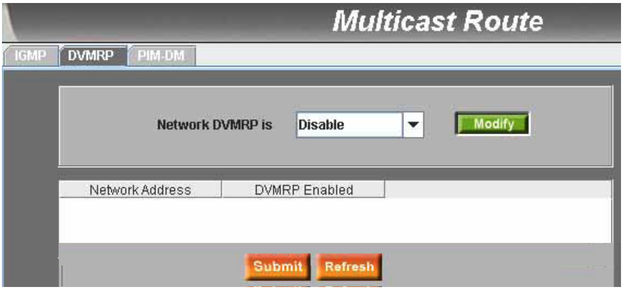
IGMP Version: Select which version to run. Default is "V2."

IGMP Query Interval: Set the number of seconds between two query packets. Default is set at 125 seconds.

IGMP Query-Max-Response: Set the response time when the host reports to its multicast group. Default is set at 10 seconds.

NOTE: When setting IGMP, select the corresponding interface to configure parameters, then click "Modify." Changes will be updated in the display window. To save any changes and make them effective immediately, click "Submit." Click "Refresh" to refresh the settings.

2.2.6.4.2 DVMRP



Network DVMRP is Disable

Network Address	DVMRP Enabled

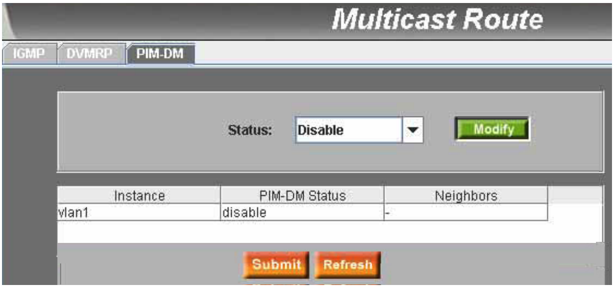
This function is used for configuring DVMRP (Distance Vector Multicast Routing Protocol).

Network DVMRP is: Enable or disable DVMRP for a specific network.

Select the corresponding network address to configure parameters, then click "Modify." Changes will be updated in the display window. To save any changes and make them effective immediately, click "Submit." Click "Refresh" to refresh the settings.

NOTE: Before setting this page, make sure that *IP Multicast Route Mode* on the IGMP screen is set to "DVMRP."

2.2.6.4.3 PIM-DM



Status: Disable

Instance	PIM-DM Status	Neighbors
vlan1	disable	-

This screen for configuring PIM-DM (Protocol-Independent Multicast – Dense Mode).

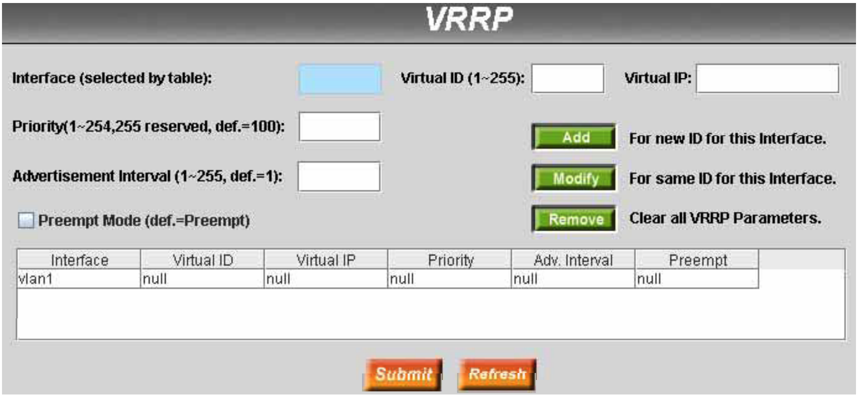
Status: Enable or disable PIM-DM for a specific interface.

Select the corresponding interface to configure parameters, then click

"Modify." Changes will be updated in the display window. To save any changes and make them effective immediately, click "Submit." Click "Refresh" to refresh the settings.
NOTE: The system only supports PIM-DM version 2.
NOTE: Before enabling, *IP Multicast Route Mode* on the IGMP screen must be set to "PIM-DM."

2.2.6.5 VRRP

The Virtual Router Redundancy Protocol (VRRP) is designed to eliminate the weak point inherent in the static default routed environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the "master," and forwards packets sent to these IP addresses. The election process provides dynamic fail-over in the forwarding responsibility, should the master become unavailable. Any of the virtual router's IP addresses on a LAN can then be used as the default first-hop router by end-hosts. The advantage gained from using VRRP is a higher-availability default path without requiring any configuration of dynamic routing or router discovery protocols on every end-host.


VRRP
Interface (selected by table):
Virtual ID (1~255):
Virtual IP:
Priority(1~254,255 reserved, def.=100):
Advertisement Interval (1~255, def.=1):
□ Preempt Mode (def.=Preempt)
Add
For new ID for this Interface.
Modify
For same ID for this Interface.
Remove
Clear all VRRP Parameters.
Submit
Refresh

Interface	Virtual ID	Virtual IP	Priority	Adv. Interval	Preempt
vlan1	null	null	null	null	null

Virtual ID: One virtual router ID can be used as the default gateway for one or several VLANs. The range is 1 – 255.
Virtual IP: This can be any IP address that belongs to the VLAN to be managed. In general, it can be the same as the interface IP address, acting as the master router.
Priority: This is the virtual router priority, used by this VRRP router in selecting the master for this virtual router. The range is 1 – 254 (default is 100), with higher values meaning higher priority. The value of 255 (decimal) is reserved for the router that owns the IP addresses associated with the virtual router. Zero is reserved for the master router to indicate that it is releasing responsibility for the virtual router. The range 1 – 254 (decimal) is available for VRRP routers backing up the virtual router.
Advertisement Interval: This is the time interval between advertisements (in seconds). Default is 1 second.
Preempt Mode: Controls whether a higher-priority backup router preempts a lower-priority master. Values are True to allow preemption and False to prohibit preemption. Default is True.

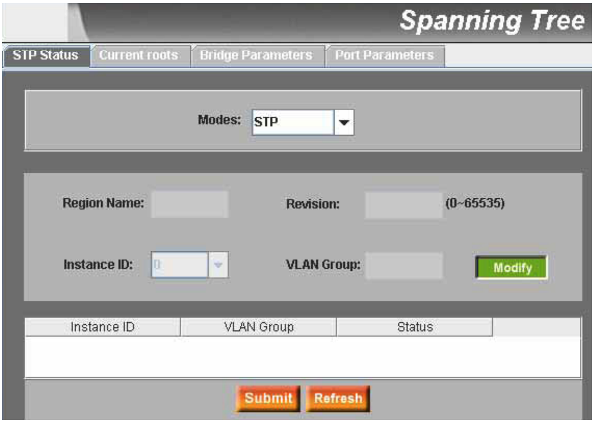
2.2.7 Bridge

The Bridge page group contains Layer 2 configurations. The 12 subsections are Spanning Tree, Link Aggregation Static, LACP, Mirroring, Static Multicast, IGMP Snooping, Traffic Control, Dynamic Addresses, Static Addresses, VLAN Configuration, GVRP and QoS/CoS.

2.2.7.1 Spanning Tree

This section is for configuring the Spanning Tree Protocol. Four subsections present additional options: STP Status, Current Roots, Bridge Parameters and Port Parameters.

2.2.7.1.1 STP Status



Modes: STP

Instance ID: 0

Instance ID	VLAN Group	Status

This screen lets you enable or disable STP.

Modes: Three modes are available in the drop-down menu: “STP,” “RSTP” (Rapid STP) and “MSTP” (Multiple STP).

If MSTP is enabled, the following four attributes are enabled at the same time.

Region Name: This is an alphanumeric configuration name.

Revision: This is a configuration revision number to identify the region along with Region Name.

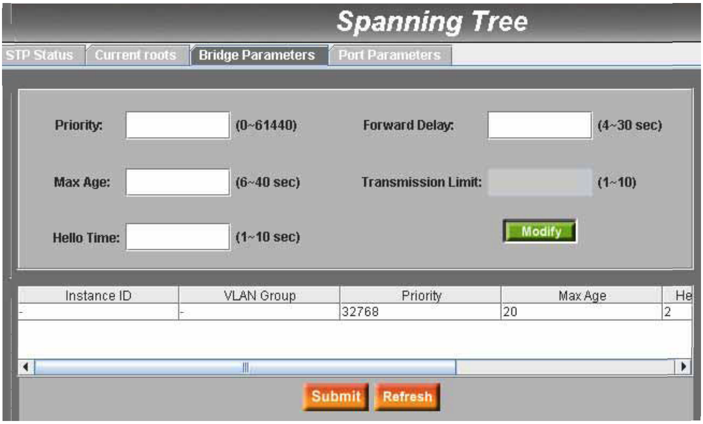
Instance ID: You can configure MSTP on your switch to map multiple VLANs into a single STP instance.

VLAN Group: A group associates each of the potential 4094 VLANs to the given instance.

2.2.7.1.2 Current Roots

This screen (not shown) displays information about the current root bridge: MAC address, priority, maximum age, hello timer, forwarding delay timer and path cost.

2.2.7.1.3 Bridge Parameters



Instance ID	VLAN Group	Priority	Max Age	He
-	-	32768	20	2

The spanning-tree parameters of BPDU (bridge protocol data unit) transmission can be configured on this screen.

Hello Time: This is the interval between the generation of configuration BPDUs.

Max Age: This is a timeout value to be used by all bridges in the LAN.

Forward Delay: This is a timeout value to be used by all bridges in the LAN.

Bridge Priority: This is the switch priority in the LAN.

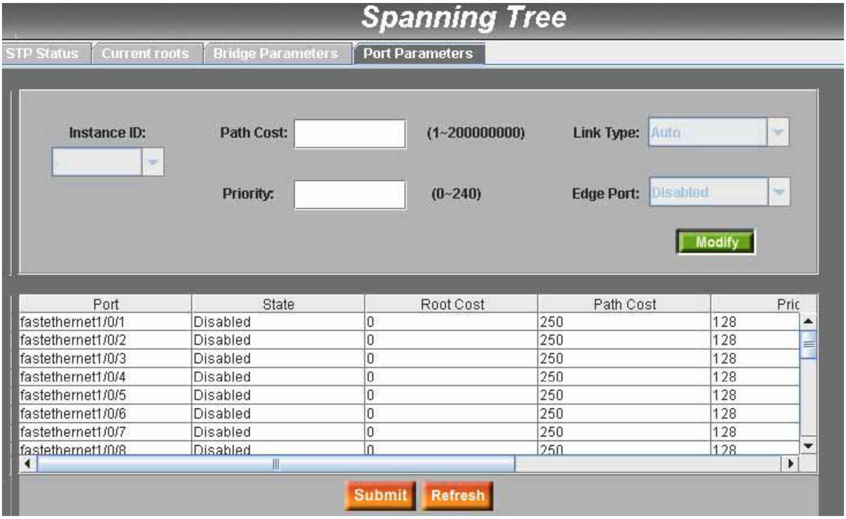
Transmission Limit: The root switch of the instance always sends a BPDU (or Mrecord) with a cost of 0 and the transmission limit set to the maximum value.

2.2.7.1.4 Port Parameters

This screen contains a display window to see and edit the current configurations for each port: Select a port, edit it, then click “Modify” to change the port setting for spanning-tree.

Instance ID: For MSTP (multiple STP) only, configure MSTP on your switch to map multiple VLANs into a single STP instance.

Path Cost: The valid range is 1 – 65535. The higher cost is more likely to be blocked by STP if a network loop is detected.



Instance ID:

Path Cost: (1~200000000)

Link Type: Auto

Priority: (0~240)

Edge Port: Disabled

Port	State	Root Cost	Path Cost	Pric
fastethernet1/0/1	Disabled	0	250	128
fastethernet1/0/2	Disabled	0	250	128
fastethernet1/0/3	Disabled	0	250	128
fastethernet1/0/4	Disabled	0	250	128
fastethernet1/0/5	Disabled	0	250	128
fastethernet1/0/6	Disabled	0	250	128
fastethernet1/0/7	Disabled	0	250	128
fastethernet1/0/8	Disabled	0	250	128

Priority: This is to set the port priority in the switch. Here, a low value indicates a high priority. The port with the lower priority is more likely to be blocked by STP if a network loop is detected. The valid range is 0 – 255.

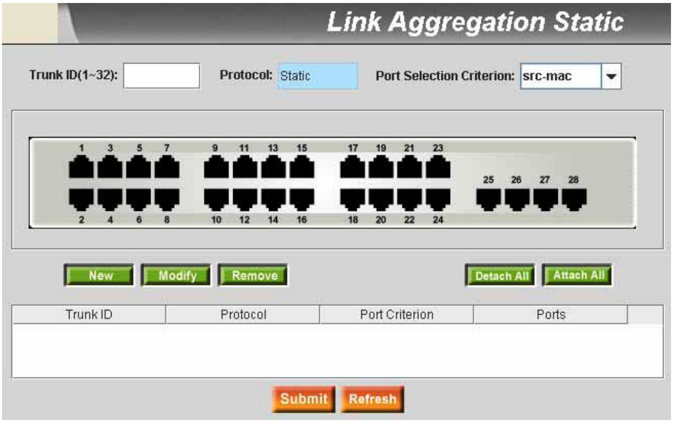
Link Type: By default, the link type is determined from the duplex mode of the interface: A full-duplex port is considered to have a point-to-point connection; a half-duplex port is considered to have a shared connection.

Edge Port: An edge port is the same as a Port Fast-enabled port, and you should enable it only on ports that connect to a single end-station.

Click “Submit” to commit the settings. Click “Refresh” to display current switch settings. To eventually make all changes permanent in Flash memory, click on “Save Configuration” (listed at the bottom of the Configuration Menu) and click “Save.”

2.2.7.2 Link Aggregation Static

This screen is for configuring the link aggregation static group (port trunking). The switch provides a maximum of 32 link aggregation groups, with the maximum achieved in a stacking configuration.



Trunk ID(1~32): Protocol: Static Port Selection Criterion: src-mac

Trunk ID	Protocol	Port Criterion	Ports

Trunk ID: This number identifies the trunk group in addition to the group name.

Port Selection Criterion: This is the algorithm to distribute packets among the ports of the link aggregation group according to the source MAC address, destination MAC address, source and destination MAC address, source IP address, destination IP address, or source and destination IP address.

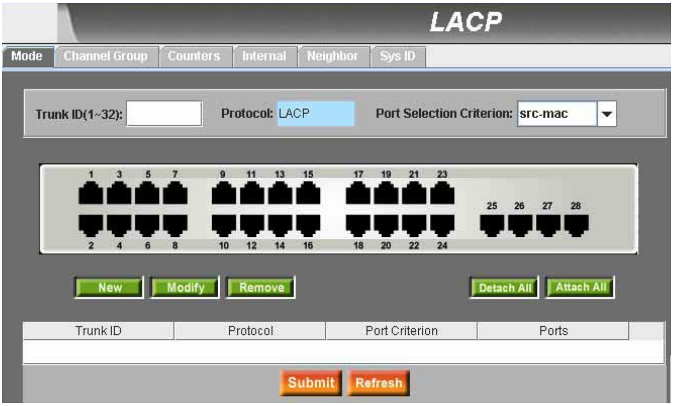
Port: These port icons are listed the same way as on the front panel. Click on the icon to select the group members; click the selected port again to remove it from the group.
Click “New” to create a new entry (temporary until “Submit” is clicked).
Click “Modify” to change the settings of an existing entry (temporary until “Submit” is clicked).
Click “Remove” to remove an existing entry (temporary until “Submit” is clicked).
Click “Attach All” to select all ports for a selected entry (temporary until “Submit” is clicked).
Click “Detach All” to unselect all ports for a selected entry (temporary until “Submit” is clicked).
Click “Submit” to commit the settings. Click “Refresh” to display current switch settings. To eventually make all changes permanent in Flash memory, click on “Save Configuration” (listed at the bottom of the Configuration Menu) and click “Save.”

It’s important that you check the runtime link speed and duplex mode to make sure the trunk is physically active. Go to Physical Interface (subsection 2.2.3.2) and check the link mode on the runtime status screen for the trunk ports. If all the trunk members are in the same speed and full-duplex mode, then the trunk group is set up successfully. If one of the members is not in the same speed or ful-duplex mode, the trunk is not set correctly. Check the link partner and change the settings to have the same speed and full-duplex mode for all the members of your trunk group. To reiterate:

- All ports in the link aggregation group *must* operate in full-duplex mode at the same speed.
- All ports in the link aggregation group *must* be configured in auto-negotiation mode or full-duplex mode. This configuration will make the full-duplex link possible. If you set the ports in full-duplex force mode, then the link partner *must* have the same setting; otherwise, the link aggregation could operate abnormally.
- All ports in the link aggregation group *must* have the same VLAN setting.
- All ports in the link aggregation group are treated as a single logical link; that is, if any member changes an attribute, the others will change also. For example, a trunk group consists of Port 1 and 2. If the VLAN of Port 1 changes, the VLAN of Port 2 also changes with Port 1.

2.2.7.3 LACP

This screen series is for configuring the LACP (Link Aggregation Control Protocol) group (port trunking). The switch provides a maximum of 32 link aggregation groups and up to eight ports per group, with the maximum achieved in a stacking configuration. For a stand-alone switch, the maximum number of groups is six since it supplies only 12 ports.

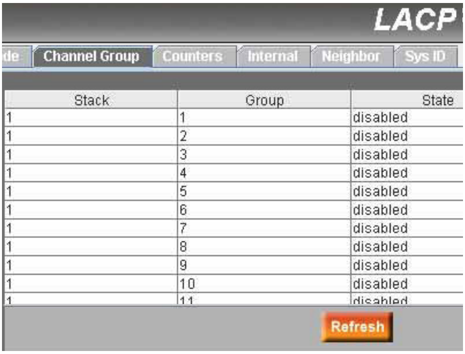


Trunk ID(1~32):
Protocol: LACP
Port Selection Criterion: src-mac

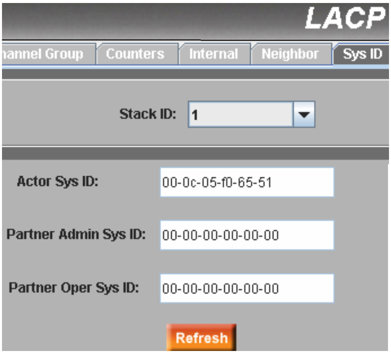
Trunk ID	Protocol	Port Criterion	Ports

2.2.7.3.1 Mode

Trunk ID: This number identifies the trunk group in addition to the group name.
Port Selection Criterion: This is the algorithm to distribute packets among the ports of the link aggregation group according to source MAC address, destination MAC address, source and destination MAC address, source IP address, destination IP address or source and destination IP address.
Port: These port icons are listed the same way as on the front panel. Click on the icon to select the group members; click the selected port again to remove it from the group.



Stack	Group	State
1	1	disabled
1	2	disabled
1	3	disabled
1	4	disabled
1	5	disabled
1	6	disabled
1	7	disabled
1	8	disabled
1	9	disabled
1	10	disabled
1	11	disabled



Stack ID: 1

Actor Sys ID: 00-0c-05-f0-65-51

Partner Admin Sys ID: 00-00-00-00-00-00

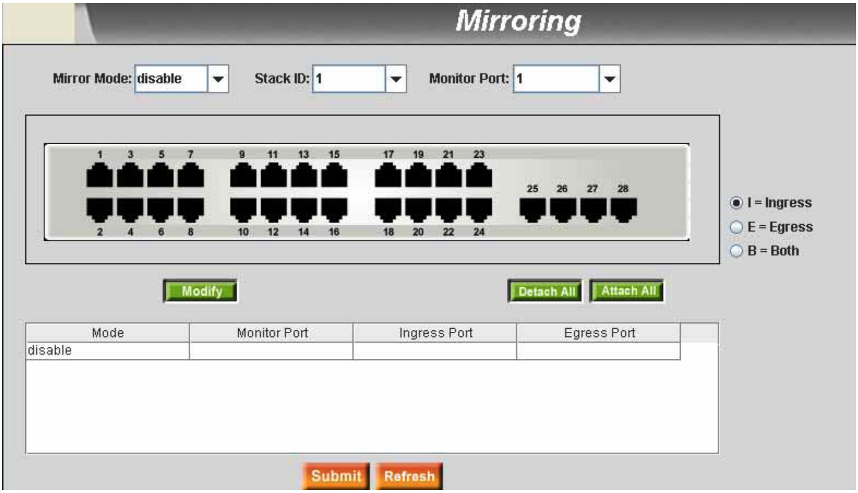
Partner Oper Sys ID: 00-00-00-00-00-00

2.2.7.3.2–6 Channel Group, Counters, Internal, Neighbor, Sys ID

Five additional screens (two shown) are available in this subsection for viewing various statistics and data, such as Channel Group (above left) and Sys ID (above right).

2.2.7.4 Mirroring

Port Mirroring, together with a network traffic analyzer, helps you monitor network traffic. You can monitor the selected ports for egress or ingress packets.



Mirror Mode: disable Stack ID: 1 Monitor Port: 1

● I = Ingress
○ E = Egress
○ B = Both

Mode	Monitor Port	Ingress Port	Egress Port
disable			

Mirror Mode: Enables or disables the mirror function for the selected group.

Stack ID: For a stand-alone switch, only ID “1” is available.

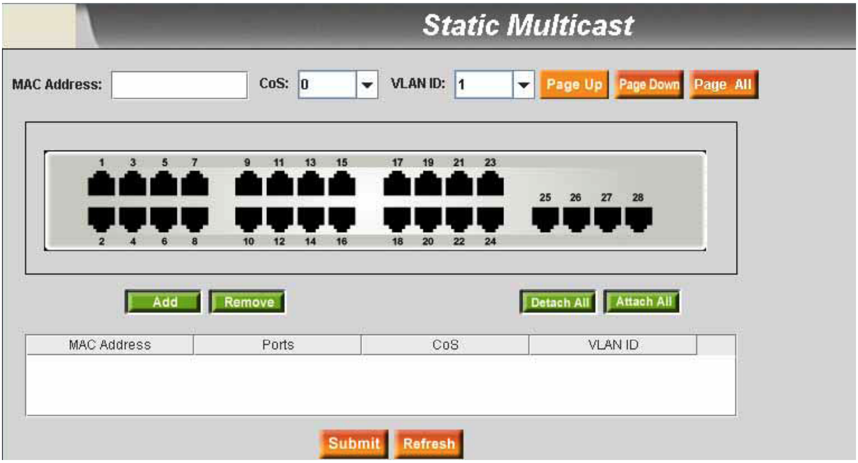
Monitor Port: Receives the copies of all the packets in the selected mirrored ports. ***NOTE:*** The monitor port cannot belong to any link aggregation group, and cannot operate as a normal switch port. It does not switch packets or do address learning.

Ingress, Egress, Both: Mirrors a port selected from the selection panel.

Click “Submit” to set the changes to the connected switch. Click “Refresh” to display the values of the switch. To eventually make all changes permanent in Flash memory, click on “Save Configuration” (listed at the bottom of the Configuration Menu) and click “Save.”

2.2.7.5 Static Multicast

This screen is for adding multicast addresses into the multicast table. The switch can hold up to 256 multicast entries. All the ports in the group will forward the specified multicast packets to other ports in the group.



Static Multicast

MAC Address: CoS: 0 VLAN ID: 1

MAC Address	Ports	CoS	VLAN ID

Select a port from the selection panel or select an existing group address from the window list.

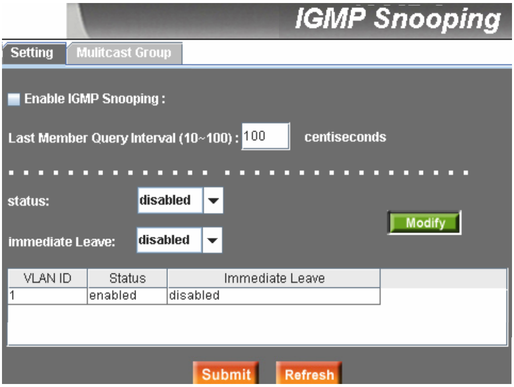
MAC Address: Assign the multicast address.

CoS: Assign the priority for the Class of Service of VLAN frames.

VLAN ID: Select the VLAN group (a VLAN-based feature).

Click “Submit” to commit the settings. Click “Refresh” to display current switch settings. To eventually make all changes permanent in Flash memory, click on “Save Configuration” (listed at the bottom of the Configuration Menu) and click “Save.”

2.2.7.6 IGMP Snooping



IGMP Snooping

□ Enable IGMP Snooping :

Last Member Query Interval (10~100) : 100 centiseconds

status: disabled

immediate Leave: disabled

VLAN ID	Status	Immediate Leave
1	enabled	disabled

This screen — with subsections of Setting and Multicast Group, which displays current settings — provides options that help reduce the multicast traffic on the network by allowing the IGMP snooping function to be turned on or off.

2.2.7.6.1 Setting

Enable IGMP Snooping: Select to globally enable IGMP snooping in all existing VLAN interfaces. By default, IGMP snooping is globally enabled on the switch. If global snooping is disabled, you cannot enable VLAN snooping. If global snooping is enabled, you *can* enable or disable VLAN snooping.

Last Member Query Interval: Without Immediate Leave (see below), when the switch receives an IGMP leave message from a subscriber on a receiver port, it sends out an IGMP query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership.

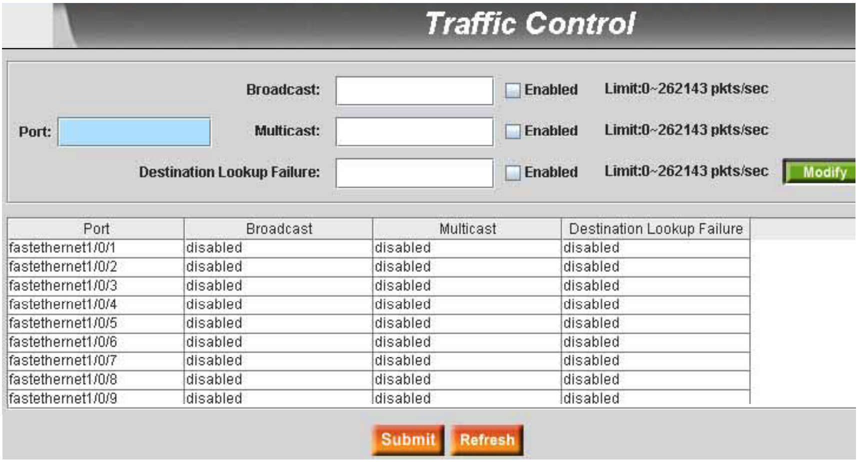
Status: If global snooping is enabled, you can enable or disable VLAN snooping.

Immediate Leave: When enabled, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port. You should use the Immediate Leave feature only when there is a single host present on every port in the VLAN. Immediate Leave is supported with only IGMP version 2 hosts.

If the static entries occupy all 256 spaces, IGMP snooping normally does not work. The switch only allows 256 Layer 2 multicast groups.

2.2.7.7 Traffic Control

Traffic Control protects the switch bandwidth from flooding packets — including broadcast packets, multicast packets and unicast packets — caused by destination address lookup failure. The limit number is a threshold that limits the total number of the selected type of packets. For example, if the broadcast and multicast options are selected, the total amount of packets per second for those two types will not exceed the limit value. Select an interface and assign the desirable settings, then click “Modify.”


Traffic Control
Port:
Broadcast: □ Enabled Limit:0~262143 pkts/sec
Multicast: □ Enabled Limit:0~262143 pkts/sec
Destination Lookup Failure: □ Enabled Limit:0~262143 pkts/sec
Modify
Submit
Refresh

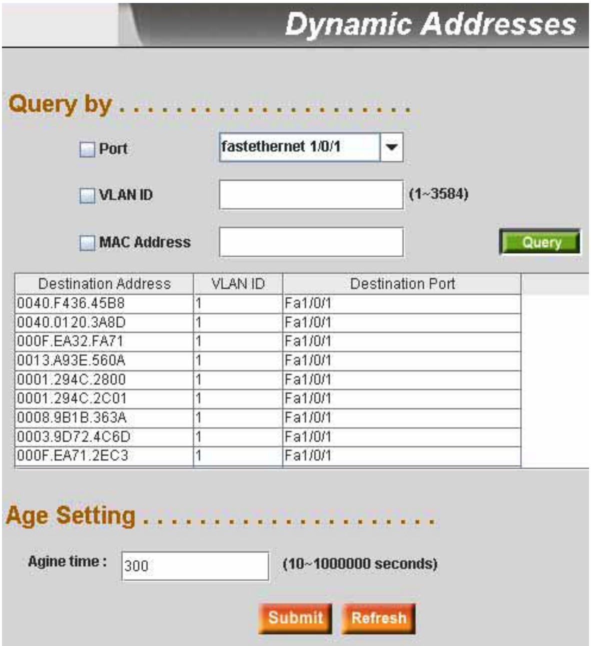
Port	Broadcast	Multicast	Destination Lookup Failure
fastethernet1/0/1	disabled	disabled	disabled
fastethernet1/0/2	disabled	disabled	disabled
fastethernet1/0/3	disabled	disabled	disabled
fastethernet1/0/4	disabled	disabled	disabled
fastethernet1/0/5	disabled	disabled	disabled
fastethernet1/0/6	disabled	disabled	disabled
fastethernet1/0/7	disabled	disabled	disabled
fastethernet1/0/8	disabled	disabled	disabled
fastethernet1/0/9	disabled	disabled	disabled

Click “Submit” to commit the settings. Click “Refresh” to display current switch settings. To eventually make all changes permanent in Flash memory, click on “Save Configuration” (listed at the bottom of the Configuration Menu) and click “Save.”

2.2.7.8 Dynamic Addresses

This screen displays the results of dynamic MAC address lookups by port, VLAN ID or specified MAC address. The dynamic address is the MAC address learned by the switch. It will age out of the address table if the address is not learned again within the aging time limit. Set the aging time by entering 10 to 1,000,000 in seconds.

Click “Submit” to commit the settings. Click “Refresh” to display current switch settings. Look up MAC addresses by checking and filling in the options for port, VLAN ID and/or MAC address, then clicking “Query.” The address window will display the results of the query.

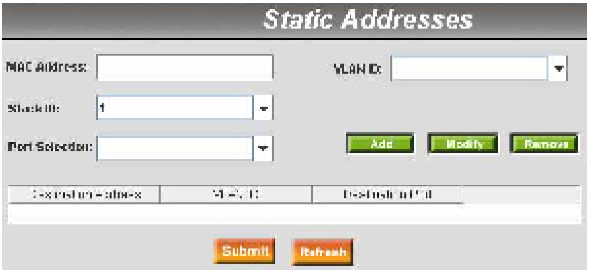


Port: fastethernet 1/0/1

Destination Address	VLAN ID	Destination Port
0040.F436.45B8	1	Fa1/0/1
0040.0120.3A8D	1	Fa1/0/1
000F.EA32.FA71	1	Fa1/0/1
0013.A93E.560A	1	Fa1/0/1
0001.294C.2800	1	Fa1/0/1
0001.294C.2C01	1	Fa1/0/1
0008.9B1B.363A	1	Fa1/0/1
0003.9D72.4C6D	1	Fa1/0/1
000F.EA71.2EC3	1	Fa1/0/1

Agine time : 300 (10~1000000 seconds)

2.2.7.9 Static Addresses



This screen allows you to add a MAC address to the switch address table. The MAC address added in this way will not age out from the address table. These are called static addresses.

MAC Address: Enter the MAC address.

VLAN ID: Enter the VLAN ID that the MAC belongs to.

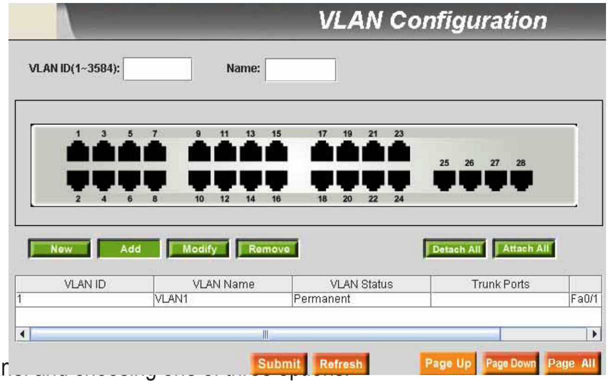
Stack ID: For a stand-alone switch, only ID “1” is available.

Port Selection: Select the port which the MAC belongs to.

Click “Add” to create a new static MAC address with the above information (temporary until “Submit” is clicked). Click “Remove” to remove a selected entry (temporary until “Submit” is clicked). Click “Modify” to update an existing MAC address entry (temporary until “Submit” is clicked).

Click “Submit” to commit the settings. Click “Refresh” to display current switch settings. To eventually make all changes permanent in Flash memory, click on “Save Configuration” (listed at the bottom of the Configuration Menu) and click “Save.”

2.2.7.10 VLAN Configuration



VLAN ID	VLAN Name	VLAN Status	Trunk Ports	
1	VLAN1	Permanent		Fa0/1

You can create up to 4094 VLAN groups and show them on this screen. VLAN1 is the default VLAN, which is created by the system and can’t be removed. This feature prevents the switch from malfunctioning. You can remove any existing VLAN except VLAN1.

You can assign the port to be a tagged port or an untagged port by clicking on the port on the selection panel and choosing one of three options:

- An untagging port will remove VLAN tags from the transmitted packets.
- A tagging port will tag all packets transmitted from this port.
- If the port is left “blank,” it is not a member of the selected VLAN group.

If one untagging port belongs to two or more VLAN groups at the same time, it will confuse the switch and cause flooding traffic. To prevent this, the switch only allows one untagging port to belong to one VLAN at the same time. To assign an untagging port from one VLAN to another, it first needs to be changed into something else in the original VLAN.

VLAN ID: Requires the VLAN ID to be entered when a new VLAN is created.

Name: Requires that a name be assigned for the VLAN.

DHCP-Snooping: (If displayed) Requires that a name be assigned for the VLAN.

Click “New” to create a new entry (temporary until “Submit” is clicked).

Click “Add” to add new entry to list of entries (temporary until “Submit” is clicked).

Click “Modify” to temporarily save changes to an existing entry (temporary until “Submit” is clicked).

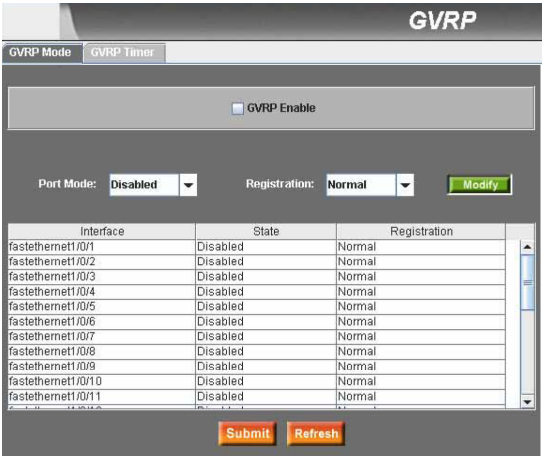
Click “Remove” to remove selected entry (temporary until “Submit” is clicked).

Click “Attach All” to select all ports for a selected entry (temporary until “Submit” is clicked).

Click Detach All to unselect all ports for a selected entry (temporary until Submit is clicked).

Click “Submit” to commit the settings. Click “Refresh” to display current switch settings. To eventually make all changes permanent in Flash memory, click on “Save Configuration” (listed at the bottom of the Configuration Menu) and click “Save.”

2.2.7.11 GVRP

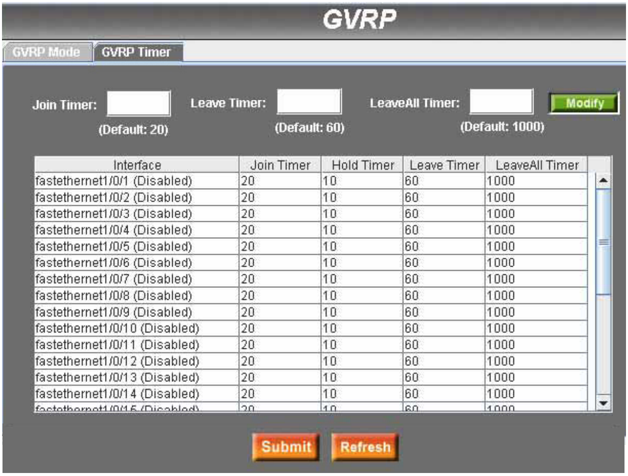


Interface	State	Registration
fastethernet1/0/1	Disabled	Normal
fastethernet1/0/2	Disabled	Normal
fastethernet1/0/3	Disabled	Normal
fastethernet1/0/4	Disabled	Normal
fastethernet1/0/5	Disabled	Normal
fastethernet1/0/6	Disabled	Normal
fastethernet1/0/7	Disabled	Normal
fastethernet1/0/8	Disabled	Normal
fastethernet1/0/9	Disabled	Normal
fastethernet1/0/10	Disabled	Normal
fastethernet1/0/11	Disabled	Normal

The Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) is an application defined in the IEEE 802.1Q standard that allows for the control of VLANs. GVRP will run only on 802.1Q trunk ports and is used primarily to prune traffic from VLANs that doesn’t need to be passed between trunking switches. There are some parameters for configuring GVRP on the GVRP Mode screen; the second screen option is GVRP Timer (shown below):

GVRP Enable: By default, GVRP is not enabled for the switch. You must first enable GVRP on the switch before you can configure the 802.1Q ports for GVRP operation.

Port Mode: Enable/disable GVRP on the individual 802.1Q trunk port. GVRP must be configured on both sides of the trunk to work correctly.



Interface	Join Timer	Hold Timer	Leave Timer	LeaveAll Timer
fastethernet1/0/1 (Disabled)	20	10	60	1000
fastethernet1/0/2 (Disabled)	20	10	60	1000
fastethernet1/0/3 (Disabled)	20	10	60	1000
fastethernet1/0/4 (Disabled)	20	10	60	1000
fastethernet1/0/5 (Disabled)	20	10	60	1000
fastethernet1/0/6 (Disabled)	20	10	60	1000
fastethernet1/0/7 (Disabled)	20	10	60	1000
fastethernet1/0/8 (Disabled)	20	10	60	1000
fastethernet1/0/9 (Disabled)	20	10	60	1000
fastethernet1/0/10 (Disabled)	20	10	60	1000
fastethernet1/0/11 (Disabled)	20	10	60	1000
fastethernet1/0/12 (Disabled)	20	10	60	1000
fastethernet1/0/13 (Disabled)	20	10	60	1000
fastethernet1/0/14 (Disabled)	20	10	60	1000
fastethernet1/0/15 (Disabled)	20	10	60	1000

Registration: By default, GVRP ports are in normal registration mode. These ports use GVRP “join” messages from neighboring switches to prune the VLANs running across the 802.1Q trunk link. If the device on the other side is not capable of sending GVRP messages, or if you do not want to allow the switch to prune any of the VLANs, use the fixed mode. Fixed-mode ports will forward for all VLANs that exist in the switch database. Ports in forbidden mode forward only for VLAN 1.

2.2.7.12 QoS/CoS

Three screens are presented in QoS/CoS (Quality of Service/Class of Service): 802.1p Priority, QoS Queue Mapping and QoS Bandwidth.

2.2.7.12.1 802.1p Priority

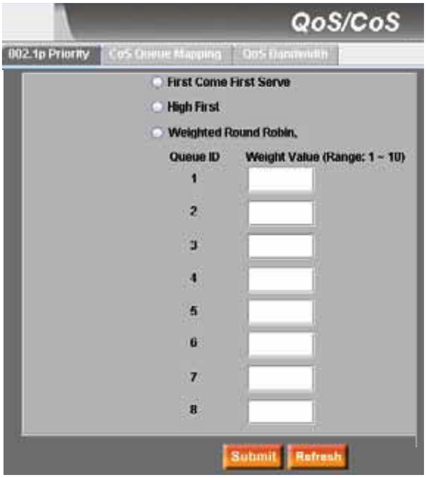
Each port has eight egress queues. These queues can either be configured with the Weighted Round Robin (WRR) scheduling algorithm, or with one queue as a strict priority queue and the other queues for WRR. The strict priority queue must be empty before the other queues are serviced. You can use the strict priority queue for mission-critical and time-sensitive traffic. There are three options.

First Come First Service: The first-come frame has the highest priority.

High First: A packet's priority depends on its CoS value.

Weighted Round Robin (WRR): If WRR scheduling algorithm is enabled, the ratio of the weights is the ratio of frequency in which the WRR scheduler de-queues packets from each queue.

Click "Submit" to commit the settings. Click "Refresh" to display current switch settings. To eventually make all changes permanent in Flash memory, click on "Save Configuration" (listed at the bottom of the Configuration Menu) and click "Save."

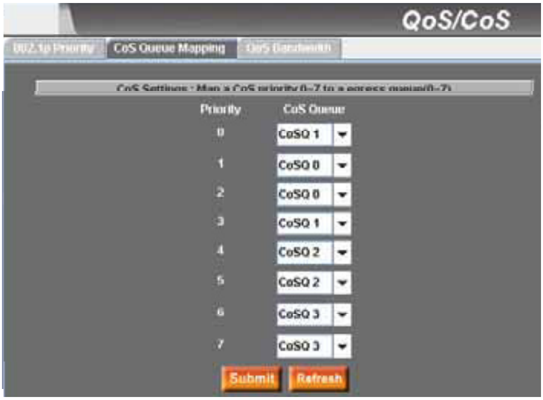


○ First Come First Serve
○ High First
○ Weighted Round Robin,

Queue ID	Weight Value (Range: 1 ~ 10)
1	
2	
3	
4	
5	
6	
7	
8	

2.2.7.12.2 QoS Queue Mapping

The switch supports eight egress queues for each port with a strict priority scheduler; that is, each CoS value can map into one of the eight queues. Queue 8 has the highest priority to transmit packets. Click "Submit" to commit the settings. Click "Refresh" to display current switch settings. To eventually make all changes permanent in Flash memory, click on "Save Configuration" (listed at the bottom of the Configuration Menu) and click "Save."



CoS Settings : Map a CoS priority 0~7 to a egress queue(0~7)

Priority	CoS Queue
0	CoSQ 1
1	CoSQ 0
2	CoSQ 0
3	CoSQ 1
4	CoSQ 2
5	CoSQ 2
6	CoSQ 3
7	CoSQ 3

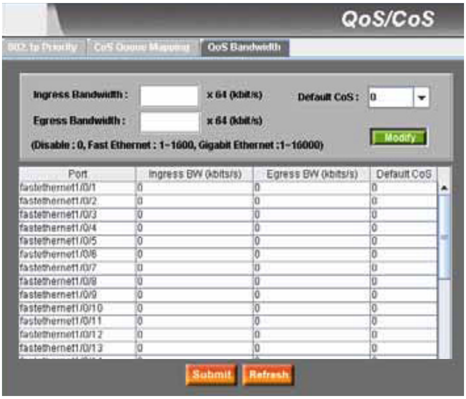
2.2.7.12.3 QoS Bandwidth

Some VLAN tag-related field settings for each port are included on this screen. Select a port to configure from the list window.

Ingress Bandwidth: Enter the maximum ingress bandwidth in 64kbps steps for the selected port.

Egress Bandwidth: Enter the maximum egress bandwidth in 64kbps steps for the selected port.

Default CoS: Every untagged packet received from this port will be assigned to this CoS value in the VLAN tagged.



Ingress Bandwidth : x 64 (kbit/s)
Egress Bandwidth : x 64 (kbit/s)
Default CoS : 0
(Disable : 0, Fast Ethernet : 1~1600, Gigabit Ethernet :1~16000)

Port	Ingress BW (kbits/s)	Egress BW (kbits/s)	Default CoS
fastethernet1/0/1	0	0	0
fastethernet1/0/2	0	0	0
fastethernet1/0/3	0	0	0
fastethernet1/0/4	0	0	0
fastethernet1/0/5	0	0	0
fastethernet1/0/6	0	0	0
fastethernet1/0/7	0	0	0
fastethernet1/0/8	0	0	0
fastethernet1/0/9	0	0	0
fastethernet1/0/10	0	0	0
fastethernet1/0/11	0	0	0
fastethernet1/0/12	0	0	0
fastethernet1/0/13	0	0	0

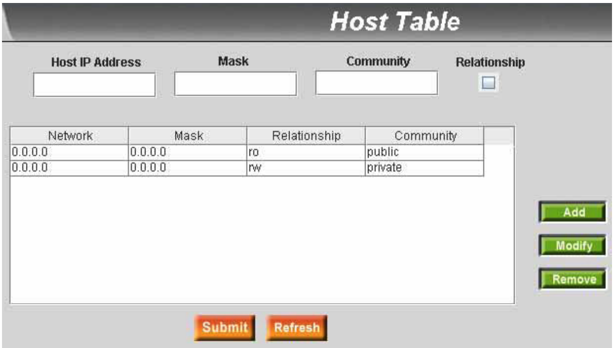
Click "Modify" to change the content in the selected port's window (temporary until "Submit" is clicked).

Click "Submit" to commit the settings. Click "Refresh" to display current switch settings. To eventually make all changes permanent in Flash memory, click on "Save Configuration" (listed at the bottom of the Configuration Menu) and click "Save."

2.2.8 SNMP

This series of screens — Host Table, Trap Setting and SNMPv3 VGU Table (with subsections) — presents SNMP configuration options.

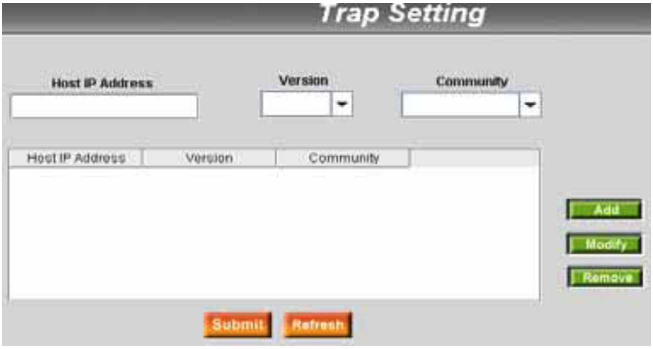
2.2.8.1 Host Table



Network	Mask	Relationship	Community
0.0.0.0	0.0.0.0	ro	public
0.0.0.0	0.0.0.0	rw	private

This screen links the host IP address to a community name. Enter an IP address and community name, then click “Add” to add the new entry to the list (temporary until “Submit” is clicked). Click “Modify” to temporarily save changes to an existing entry (temporary until “Submit” is clicked). Click “Remove” to remove a selected entry (temporary until “Submit” is clicked). Check “Relationship” to create a Set Community name; uncheck “Relationship to create a Get Community name. Click “Submit” to commit the settings. Click “Refresh” to display current switch settings. To eventually make all changes permanent in Flash memory, click on “Save Configuration” (listed at the bottom of the Configuration Menu) and click “Save.”

2.2.8.2 Trap Setting



Host IP Address	Version	Community

By setting trap destination IP addresses and community names, you can enable the SNMP trap function to send trap packets in different versions (v1 or v2c).
Click “Submit” to commit the settings. Click “Refresh” to display current switch settings. To eventually make all changes permanent in Flash memory, click on “Save Configuration” (listed at the bottom of the Configuration Menu) and click “Save.”

2.2.8.3 SNMPv3 VGU Table

Two concepts — delineated on the three subsection screens that follow — represent the new security features defined by SNMPv3:

1. The User-based Security Model (USM), which provides authentication, encryption and decryption of SNMPv3 packets, and
2. The View-based Access Control Model (VACM), which provides access control.

On each of these option screens, click “Add” to add the new entry to the list (temporary until “Submit” is clicked). Click “Modify” to temporarily save changes to an existing entry (temporary until “Submit” is clicked). Click “Remove” to remove a selected entry (temporary until “Submit” is clicked). Check “Relationship” to create a Set Community name; uncheck “Relationship to create a Get Community name.
Click “Submit” to commit the settings. Click “Refresh” to display current switch settings. To eventually make all changes permanent in Flash memory, click on “Save Configuration” (listed at the bottom of the Configuration Menu) and click “Save.”

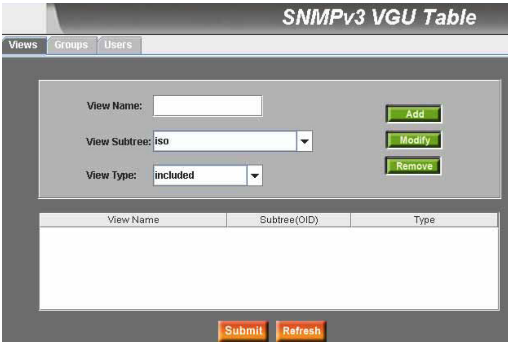
2.2.8.3.1 View

VACM View is used to view the information of SNMPv3 VACM Group.

View Name: Enter the security group name.

View Subtree: Enter the view subtree that the view belongs to. The subtree is the OID to match the OID in the SNMPv3 message. The match is good when the subtree is shorter than the OID in the SNMPv3 message.

View Type: Select the view type — “Included” or “Excluded” — when the view subtree matches the Oid in the SNMPv3 message.



View Name:

View Subtree: iso

View Type: included

View Name	Subtree(OID)	Type

2.2.8.3.2 Groups

This screen is used to configure the information of SNMPv3 VACM Group.

Group Name: Enter the security group name.

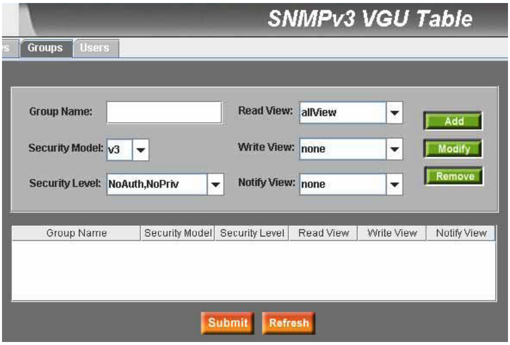
Read View: Enter the Read View name the group belongs to. The related SNMP messages are Get, GetNext and GetBulk.

Write View: Enter the Write View name the group belongs to. The related SNMP message is Set.

Notify View: Enter the Notify View name the group belongs to. The related SNMP messages are Trap and Report.

Security Model: Enter the security model the group belongs to. Any is suitable for v1, v2 or v3. USM is SNMPv3-related.

Security Level: Enter the Security Level name the group belongs. Only NoAuth, AuthNopriv or AuthPriv can be chosen.



Group Name:

Security Model: v3

Security Level: NoAuth,NoPriv

Read View: allView

Write View: none

Notify View: none

Group Name	Security Model	Security Level	Read View	Write View	Notify View

2.2.8.3.3 Users

This screen is used to configure the information of SNMPv3 USM User.

User Name: Enter the user name of a specific security group.

Group Name: Enter the security group name.

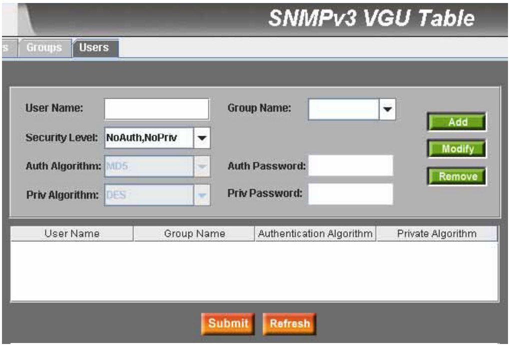
Auth Algorithm: Select the protocol that SNMP User and Security Group belong to: “NoAuth,” “MD5” or “SHA1.” If “NoAuth” is selected, there’s no need to enter a password.

Auth Password: Enter the password that the Auth Algorithm (Protocol) belongs to. The password needs to be at least eight digits or characters.

Priv Algorithm: Select the protocol that SNMP User and Security Group belong to: “NoPriv” or “DES.” If “NoPriv” is selected, there’s no need to enter a password.

Priv Password: Enter the password that the Priv Algorithm (Protocol) belongs to. The password needs to be at least eight digits or characters.

Security Level: Select the level the group belongs to: “NoAuth,” “AuthNopriv” or “AuthPriv.”



User Name:

Security Level: NoAuth,NoPriv

Auth Algorithm: MD5

Priv Algorithm: DES

Group Name:

Auth Password:

Priv Password:

User Name	Group Name	Authentication Algorithm	Private Algorithm

2.2.9 Filters

The switch can filter certain traffic types according to packet header information from Layer 2 to Layer 4. Each filter set includes a couple of rules. You have to attach the filter set to certain ports to make the filter work.

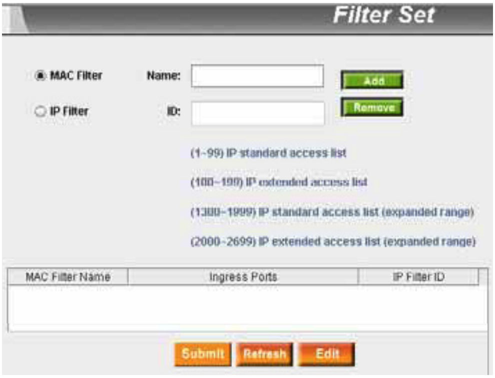
2.2.9.1 Filter Set

The switch defines two modes of rules: MAC mode and IP mode. Only the same mode of rules can be bundled together to form a filter set. Each mode has different fields to configure (e.g., you can use IP mode rules to filter FTP packets).

You can select MAC Filter, enter a name and then add it. You also can select IP Filter, enter an ID/name and then add it. Click "Submit" to commit the settings. Click "Refresh" to display current switch settings.

You can also edit entries or selections. Click on a filter set you want to edit or remove, then click "Edit" to display the Filter Rule page (or click "Remove" to remove the filter set). A filter set consists of a particular type of rules, with rules having the same fields for filtering packets belonging to the same type (e.g., two rules that filter packets with two destination IP addresses would be of the same type, but a rule filtering a source IP address does not belong to that same type). Four types of rules can apply to ports at the same time. If there are more than four types applied, the system automatically disables the rules.

The Filter Rule screens present attributes of rule modes: one for MAC rule; one for IP rule. If the MAC field is left blank, the rules will disregard the MAC value. In the IP rule setup, you can select any of the five types: source IP, destination IP, protocol, source application port or destination application port. The Action field determines if the packet should be dropped or forwarded when it matches the rule. If a packet matches two rules with different actions, the packet will follow the rule listed first.



Filter Set

● MAC Filter Name:

○ IP Filter ID:

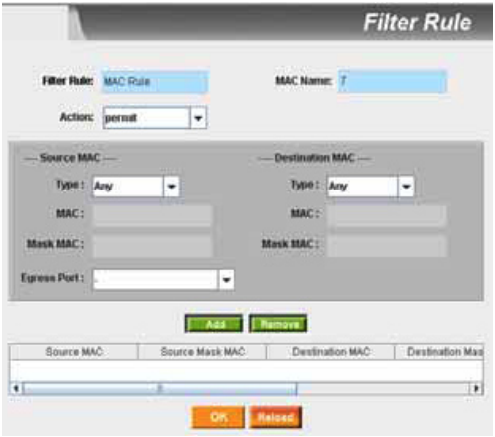
(1~99) IP standard access list

(100~199) IP extended access list

(1300~1999) IP standard access list (expanded range)

(2000~2699) IP extended access list (expanded range)

MAC Filter Name	Ingress Ports	IP Filter ID



Filter Rule

Filter Rule: MAC Rule

MAC Name: 7

Action: permit

— Source MAC —

Type: Any

MAC:

Mask MAC:

Egress Port:

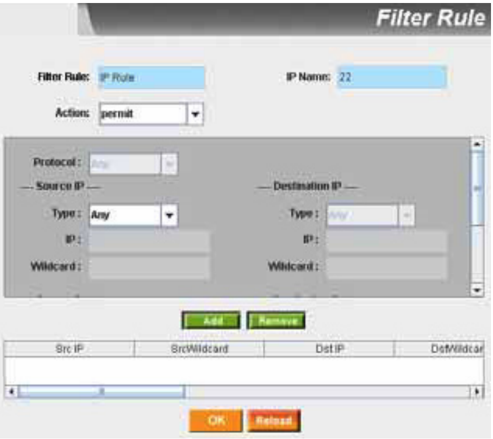
— Destination MAC —

Type: Any

MAC:

Mask MAC:

Source MAC	Source Mask MAC	Destination MAC	Destination Mas



Filter Rule

Filter Rule: IP Rule

IP Name: 22

Action: permit

Protocol: Any

— Source IP —

Type: Any

IP:

Wildcard:

— Destination IP —

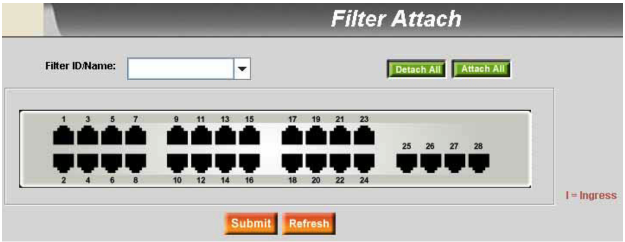
Type: Any

IP:

Wildcard:

Src IP	SrcWildcard	Dst IP	DstWildcar

2.2.9.2 Filter Attach



Filter ID/Name:

A filter set is idle if you did not attach it to any ingress port. Use this screen to attach a filter set to ingress ports. Click “Attach All” to apply the filter set to all the ports of the system. Click “Detach All” to remove all the filters from the attached ports. Click “Submit” to commit the settings. Click “Refresh” to display current switch settings. To eventually make all changes permanent in Flash memory, click on “Save Configuration” (listed at the bottom of the Configuration Menu) and click “Save.”

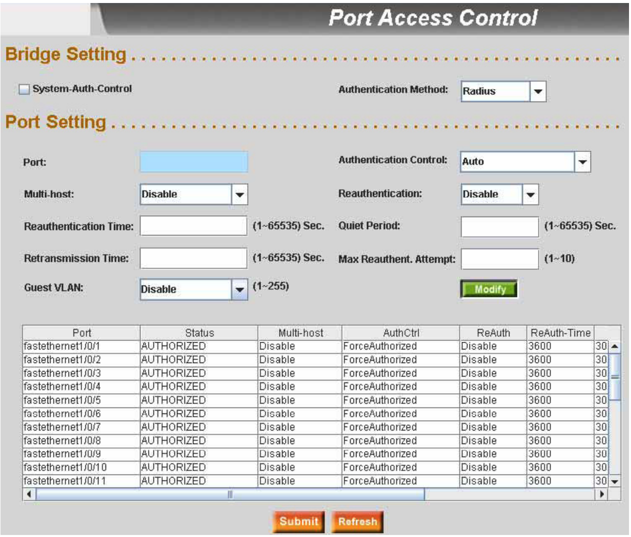
NOTE: You may not detach certain ports after issuing an “Attach All” command. If you wish to detach ports, use the “Detach All” command.

NOTE: Once the filter set is attached to the ingress ports, it will filter the packets according to the ingress port and the packet fields in the rules (e.g., a set with a single rule to filter out the destination MAC address 00:10:20:30:40:50 is attached to Ingress Port 3, but a packet with the destination MAC 00:10:20:30:40:50 from Port 3 is not permitted).

2.2.10 Security

The switch supports the 802.1x port-based security feature. Only authorized hosts are allowed to access the switch port. Traffic from unauthenticated hosts will be blocked. Authentication can be provided via a RADIUS server or the local database in the switch. The switch also supports dynamic VLAN assignment through the 802.1x authentication process. ***NOTE:*** The VLAN information for the users/ports should be configured in the authentication server before enabling this feature.

2.2.10.1 Port Access Control



□ System-Auth-Control

Authentication Method: Radius

Port:

Authentication Control: Auto

Multi-host: Disable

Reauthentication: Disable

Reauthentication Time: (1~65535) Sec.

Quiet Period: (1~65535) Sec.

Retransmission Time: (1~65535) Sec.

Max Reauthent. Attempt: (1~10)

Guest VLAN: Disable (1~255)

Port	Status	Multi-host	AuthCtrl	ReAuth	ReAuth-Time	
fastethernet1/0/1	AUTHORIZED	Disable	ForceAuthorized	Disable	3600	30
fastethernet1/0/2	AUTHORIZED	Disable	ForceAuthorized	Disable	3600	30
fastethernet1/0/3	AUTHORIZED	Disable	ForceAuthorized	Disable	3600	30
fastethernet1/0/4	AUTHORIZED	Disable	ForceAuthorized	Disable	3600	30
fastethernet1/0/5	AUTHORIZED	Disable	ForceAuthorized	Disable	3600	30
fastethernet1/0/6	AUTHORIZED	Disable	ForceAuthorized	Disable	3600	30
fastethernet1/0/7	AUTHORIZED	Disable	ForceAuthorized	Disable	3600	30
fastethernet1/0/8	AUTHORIZED	Disable	ForceAuthorized	Disable	3600	30
fastethernet1/0/9	AUTHORIZED	Disable	ForceAuthorized	Disable	3600	30
fastethernet1/0/10	AUTHORIZED	Disable	ForceAuthorized	Disable	3600	30
fastethernet1/0/11	AUTHORIZED	Disable	ForceAuthorized	Disable	3600	30

This screen — split into Bridge (Global) Setting and Port Setting — is used to configure various parameters of 802.1x, which uses either a RADIUS server or a local database to authenticate port users.

System-Auth-Control: Select to enable the authentication.

Authentication Method: “RADIUS” or “Local database” can be selected to authenticate the port user.

Port: Highlight a port to configure from the port list window at the bottom of the screen.

Multi-host: If enabled, *all* hosts connected to the selected port are allowed to use the port if *one* of the hosts passed the authentication. If disabled, only *one* host is allowed to use the port.

Authentication Control: If “Force Authorized” is selected, the selected port is force-authorized;

i.e., traffic from all hosts is allowed to pass. If “Force Unauthorized” is selected, the selected port is blocked and no traffic can go through. If “Auto” is selected, the behavior of the selected port is controlled by the 802.1x protocol. All ports should be set to “Auto” under normal conditions.

Reauthentication: Once enabled, the switch will try to authenticate the port user again when the re-authentication time is up.

Reauthentication Time: If “Reauthentication” is enabled, this is the time period the switch uses to re-send authentication request to the port user (see above).

Quiet Period: If authentication failed, the switch waits upon this time period before sending another authentication request to the port user.

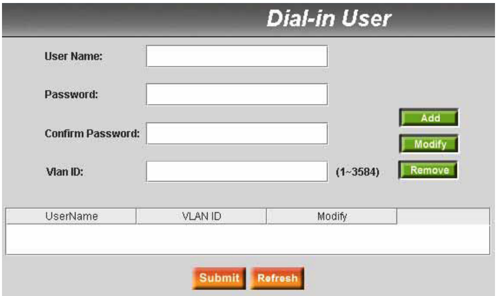
Retransmission Time: If the port user failed to respond to authentication request from the switch, the switch waits for this time period before sending another authentication request to the port user.

Max Reauthent. Attempt: This is the re-try count if the port user failed to respond to authentication requests from the switch.

Guest VLAN: Specify a guest VLAN to clients that are not 802.1x-capable.

Click “Submit” to commit the settings. Click “Refresh” to display current switch settings. To eventually make all changes permanent in Flash memory, click on “Save Configuration” (listed at the bottom of the Configuration Menu) and click “Save.”

2.2.10.2 Dial-In User



This screen is used to define users in the local database of the switch.

User Name: Enter a new username.

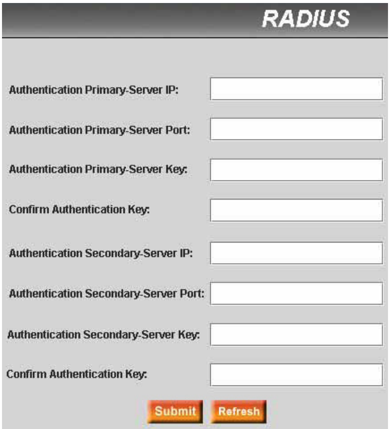
Password: Enter a password for the new user.

Confirm Password: Enter the password again.

Vlan ID: Specify the VLAN ID assigned to the 802.1x-authenticated clients.

Click “Add” to add the new user. Click “Modify” when the modifications are complete. Click “Remove” to remove a selected user. Click “Submit” to make the settings permanent. Click “Refresh” to refresh the settings to current values.

2.2.10.3 RADIUS


RADIUS
Authentication Primary-Server IP:
Authentication Primary-Server Port:
Authentication Primary-Server Key:
Confirm Authentication Key:
Authentication Secondary-Server IP:
Authentication Secondary-Server Port:
Authentication Secondary-Server Key:
Confirm Authentication Key:
Submit
Refresh

This screen is configured — with primary and secondary field options — in order to use an external RADIUS server.

Authentication Server IP: The IP address of the RADIUS server.

Authentication Server Port: The port number that the RADIUS server is listening to.

Authentication Server Key: The key that is used for communications between the switch and the RADIUS server.

Confirm Authentication Key: Re-enter the key entered above.

NOTE: The VLAN of the RADIUS server connected to the switch must be the same as the VLAN of the system management interface.

Click “Submit” to commit the settings. Click “Refresh” to display current switch settings. To eventually make all changes permanent in Flash memory, click on “Save Configuration” (listed at the bottom of the Configuration Menu) and click “Save.”

2.2.11 Traffic Chart

These statistical chart screens present network flow information. You can specify the time limits for chart refresh updates, and the charts let you monitor different types of network traffic. Most MIB-II counters are displayed in these charts.

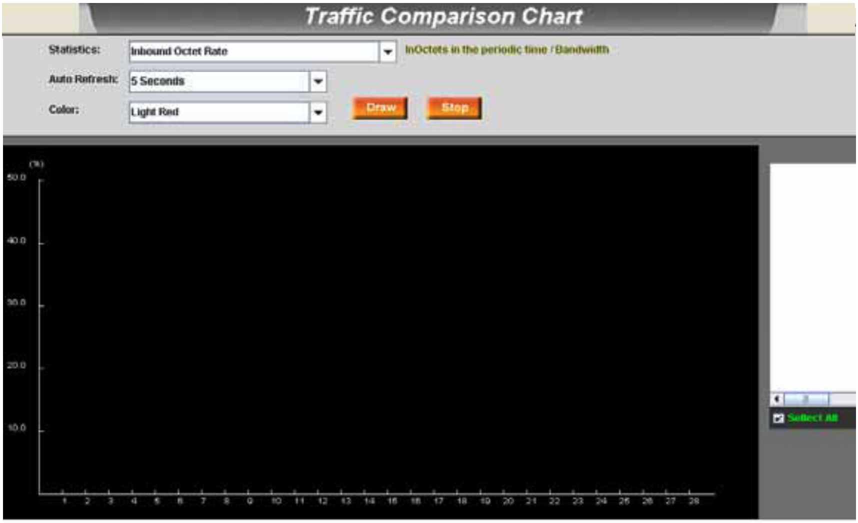
Auto Refresh: Set the time interval at which new data is retrieved from the switch.

Color: Assign a different color to each variable.

After the variables have been set, click “Draw” to allow the browser to draw the graphic chart. Each new drawing will reset the *Statistics:* display.

2.2.11.1 Traffic Comparison Chart

This screen shows one statistic for all the ports in one graphic chart.



Traffic Comparison Chart

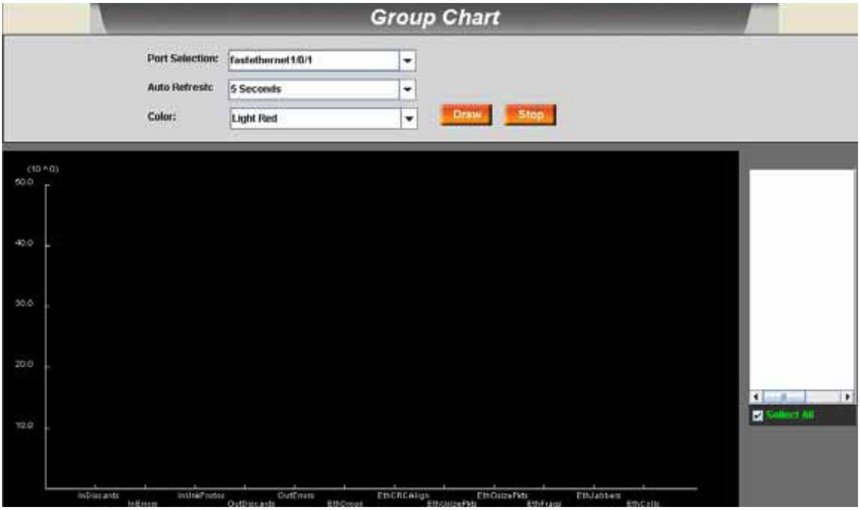
Statistics: Inbound Octet Rate — InOctets in the periodic time / Bandwidth

Auto Refresh: 5 Seconds

Color: Light Red

2.2.11.2 Group Chart

The statistics window shows all the discards or error counts for the specified port.



Group Chart

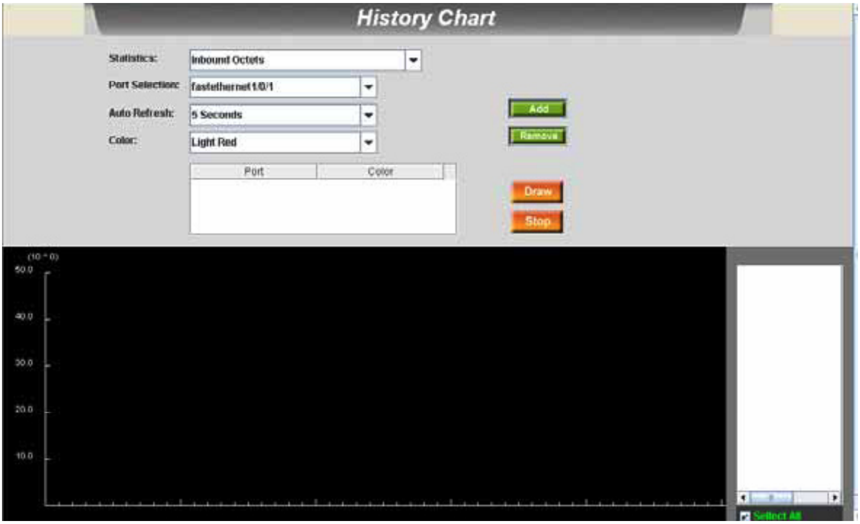
Port Selection: fastethernet1/0/1

Auto Refresh: 5 Seconds

Color: Light Red

2.2.11.3 History Chart

Display information for different ports and statistics items on this chart. Since this shows the history of the statistics information, the line chart keeps the old data even when it is refreshed.



Statistics: Inbound Octets

Port Selection: fastethernet1/0/1

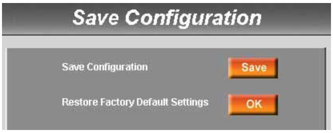
Auto Refresh: 5 Seconds

Color: Light Red

2.2.12 Save Configuration

Click “Save” to make the settings permanent by saving to the Flash memory (“Submit” only saves changes to the RAM memory; such changes will be lost if the switch is turned off). If you want to reset the switch’s configuration, click “OK” to reset the configuration file to factory defaults. A system reboot will follow this restoration process.

NOTE: You will lose all of your own configurations when you choose to restore the factory default configurations.



2.3 Command Line Interface

This section describes how to use console interface to configure the switch. The switch provides RS-232 connectors to connect to your PC. Use a terminal emulator on your PC — such as HyperTerminal or command line interpreter — to configure the switch. Configure the terminal emulator with a baud rate of 9600, 8-bit data, no parity, 1-stop bit and no flow control. Once you’re in CLI mode, typing “?” will display all available command help messages. This is very useful if you’re unfamiliar with the CLI commands. All the CLI commands are case sensitive.

2.3.1 Power On

Power On Self Test (POST) is executed during the system booting period. It tests system memory, LEDs and hardware chips on the switchboard. It displays system information as the result of system testing and initialization. You can ignore all information until the prompt “Switch login:” appears.

2.3.1.1 Boot ROM Command Mode

During the POST process, you can enter a Boot ROM Command mode by pressing the “Enter” key. Type the “?” key to show the help messages for all available commands.

NOTE: Although the commands are helpful in some situations, it is *strongly* recommended that users not use them if they don’t know the command function.

2.3.1.2 Boot ROM Commands

Two types of boot ROM commands can be used:

- "command" — The current settings will be displayed.
- "command" with new setting — The current setting will be replaced by a specified new setting.

Command	Parameters	Usage	Notes
Baudrate	Baud rate	9600 38400 57600 115200	You must set up the terminal emulator with the same baud rate to make it work.
bdinfo	none	none	print Board Info structure
echo	string	none	echo the string to console
ethaddr	none	none	get MAC address
gatewayip	IP address	xxx.xxx.xxx.xxx	set gateway IP address
go	none	none	boot firmware image
? or help	none	none	print online help
imls	none	none	list all images found in flash
ipaddr	IP address	xxx.xxx.xxx.xxx	set tftp client IP address
loadbx	none	none	load binary file over serial line (X modem)
netmask	mask	xxx.xxx.xxx.xxx	set network mask
ping	host	xxx.xxx.xxx.xxx	send ICMP ECHO_REQUEST to network host
pwd	none	none	reset switch password
reset	none	none	perform reset of the CPU
serverip	IP address	xxx.xxx.xxx.xxx	set tftp server IP address
slot	slot	1, 2, auto	select boot slot to boot
tftpboot	filename	Example: 3112single.img	load image via network using TFTP protocol
version	none	none	print monitor version

2.3.2 Login and Logout

To enter the CLI mode, you must present a valid username and password. With the first login, you can enter "admin" as the username (without a password). For security reasons, change the username and password after login. If you forget the username and password, you can contact the support team or restore the default user account in the Boot ROM Command mode — "pwd." If you select the second choice, the default username "admin" will be restored. Type "exit" to leave the CLI mode safely. This action allows you to secure the CLI mode. The next user has to log in again with an authorized username and password.

2.3.3 CLI Commands

The switch provides CLI commands for all managed functions so you can set up the switch as easily as using a Web interface.

NOTE: Always use "?" or "list" to get the available commands list and help. Always use "end" to get back to the root directory (enable mode).

2.3.3.1 User Account

2.3.3.1.1 Add User

Add a new user or modify an existing user's password.
CLI Syntax: add user user-name password
Example: SWITCH# add admin 123

2.3.3.1.2 Delete User

Delete an existing user.
CLI Syntax: delete user user-name
Example: SWITCH# delete user admin

2.3.3.2 Backup and Restore

2.3.3.2.1 Backup Startup Configuration File

Backup the startup configuration file “Quagga.conf” of the switch to the TFTP server.
CLI Syntax: copy startup-config tftp: URL
Example: SWITCH# copy startup-config tftp: 192.168.8.56

2.3.3.2.2 Restore Startup Configuration File

Restore the startup configuration file “Quagga.conf” of the switch from TFTP server.
CLI Syntax: copy tftp: URL startup-config
Example: SWITCH# copy tftp: 192.168.1.2 startup-config

2.3.3.3 System Management Configuration

2.3.3.3.1 Firmware Upgrade

Upgrade new firmware into the switch.
CLI Syntax: archive download-sw /overwrite tftp: ImageFile
Example: SWITCH# archive download-sw /overwrite tftp:192.168.1.3/3112single.img
NOTE: It is strongly recommended that you back up “startup-config” before upgrading.

2.3.3.3.2 Configure Terminal

Use the write configuration command on the switch to configure.
CLI Syntax: configure terminal
Example: SWITCH# configure terminal

2.3.3.3.3 Enable

Enter enable mode and turn on privileged mode command.
CLI Syntax: enable
Example: SWITCH# enable

2.3.3.3.4 Disable

Enter enable mode and turn on privileged mode command.
CLI Syntax: enable
Example: SWITCH# enable

2.3.3.3.5 End

This command lets the user end the current mode and go to enable mode.
CLI Syntax: end
Example: SWITCH# end

2.3.3.3.6 Exit

This command lets the user end the current mode and go to the previous mode.
CLI Syntax: exit
Example: SWITCH# exit

2.3.3.3.7 Help

This command lists all the commands of the operational mode.
CLI Syntax: list
Example: SWITCH# list
Example: SWITCH# ?

2.3.3.3.8 Hostname

Displays the given name of the switch. This is an RFC-1213-defined MIB object in System Group, and provides administrative information on the managed node.
CLI Syntax: hostname WORD
Example: (config)# hostname Switch
If you enter a name in the Name Description field, the switch’s system name changes to the new one.

2.3.3.3.9 Date

2.3.3.3.10 System Contact

Displays contact information regarding the switch. This is an RFC-1213-defined MIB object in System Group, and provides contact information on the managed node.
CLI Syntax: snmp-server contact WORD
Example: (config)# snmp-server contact clerk@central.com.tw
If you enter the contact info in the Contact Description field, the switch's contact info will change to the new info.

2.3.3.3.11 System Location

Displays the physical location of the switch. This is an RFC-1213-defined MIB object in System Group, and provides the location information on the managed node.
CLI Syntax: snmp-server location WORD
Example: (config)# snmp-server location Central-Taipei
Type in the new location description in the location description field.

2.3.3.3.12 IP Address and Network Mask

Displays the switch's IP address. This IP address is used for managing purposes; i.e., network applications such as the http server, SNMP server, tftp server, SSH and Telnet server of the switch are all using this IP address in interface vlan1.
CLI Syntax: ip address A.B.C.D/M

```
Example: (config)# interface vlan 1
         (config-if)# ip address 192.168.20.121/24
```

2.3.3.3.13 Reboot

Use this command to reboot the system.
CLI Syntax: reboot
Example: reboot

2.3.3.3.14 Refresh Default-Config File

Use this command to copy a default-config file to replace the current one.
CLI Syntax: Refresh default-config file
Example: SWITCH# Refresh default-config file

2.3.3.3.15 Show Running-Config

To show running-config file.
CLI Syntax: show running-config
Example: SWITCH# show running-config

2.3.3.3.16 Write Memory

Use the write file configuration command on the switch stack or stand-alone switch to write configuration to the file.
CLI Syntax: write memory
Example: SWITCH# write memory

2.3.3.3.17 Assign a New User Account

Add a user; e.g., a user named Tony whose password is tony123456.
CLI Syntax: add user WORD WORD
Example: add user tony tony123456

2.3.3.3.18 Delete a New User Account

Delete a user account; e.g., for a user named Tony.
CLI Syntax: delete user WORD
Example: delete user tony

2.3.3.4 Physical Interface Commands

2.3.3.4.1 Interface Mode

Use the auto-negotiation configuration command on the switch to set the auto-negotiation status of the port.

CLI Syntax: auto-negotiation

Example: (config)# interface gi1/0/2

```
(config-if)# auto-negotiation
```

This example shows how to use the auto-negotiation configuration command on the switch to enable the auto-negotiation mode.

2.3.3.4.2 Interface Duplex

Use the duplex configuration command on the switch to set duplex status of the port.

CLI Syntax: duplex (full| half)

Example: (config)# interface gi1/0/2

```
(config-if)# duplex full
```

This example shows how to use the duplex configuration command on the switch to set full-duplex on the interface.

2.3.3.4.3 Interface Flow Control

Use the flow control configuration command on the switch to set flow control status of the port.

CLI Syntax: flowcontrol (rx| tx | both) (on|off)

Example: (config)# interface gi1/0/2

```
(config-if)# flowcontrol both on
```

This example shows how to use the flow control configuration command on the switch to set "flow control both on."

2.3.3.4.4 Show L2 Interface

Use the show l2_interface command on the switch to show l2 interface status.

CLI Syntax: show l2_interfaces IFNAME

Example: SWITCH# show l2_interface gi1/0/2

2.3.3.5 IP Interface

2.3.3.5.1 Show VLAN Name String

Use the show vlan user EXEC command to display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch.

CLI Syntax: show vlan name string

Example: SWITCH# show vlan VLAN1

NOTE: VLAN1 is for system purposes like firmware upgrade, management, etc.

2.3.3.5.2 Create a VLAN Entry

Use the vlan id command to create a vlan entry on the Switch. Use the name string command to create a vlan entry with a string on the Switch.

CLI Syntax: vlan id

Example: (config)# vlan 3

```
(config-vlan)# name vlan3
```

2.3.3.5.3 Interface VLAN VLAN-ID

This command changes the operation to vlan interface command mode.

CLI Syntax: interface vlan VLAN-ID

Example: interface vlan 1

2.3.3.5.4 IP Address

This command sets the ip address for a specific interface.

CLI Syntax: ip address A.B.C.D/M

Example: (config-if)# ip address 192.168.20.121/24

NOTE: This won't show you the interface name. (Remember which interface you're configuring.

2.3.3.5.5 IP Helper-Address

This command enables a DHCP relay for a specific interface.

CLI Syntax: ip helper-address A.B.C.D

Example: (config-if)# ip helper-address 192.168.1.180

2.3.3.5.6 IP OSPF

This command sets up OSPF interface parameters.
CLI Syntax: ip ospf
Example: (config-if)# ip ospf

2.3.3.5.7 IP PIM

This command sets up PIM-DM interface parameters.
CLI Syntax: ip pim
Example: (config-if)# ip pim dense-mode

2.3.3.5.8 IP RIP

This command sets up RIP interface parameters.
CLI Syntax: ip rip
Example: (config-if)# ip rip

2.3.3.6 RIP

2.3.3.6.1 Router RIP

The router rip command is necessary to enable RIP. To disable RIP, use the “no router rip” command. RIP must be enabled before carrying out any of the RIP commands.
CLI Syntax: router rip
Example: (config)# router rip

2.3.3.6.2 No Router RIP

Disable RIP.
CLI Syntax: no router rip
Example: (config)# no router rip

2.3.3.6.3 Version

RIP can be configured to process either Version 1 or Version 2 packets. The default mode is Version 2.
CLI Syntax: version 1|2
Example: (config-router)# version 1

2.3.3.6.4 Network

Set the RIP-enable interfaces via network. Interfaces with addresses matching the network’s are enabled.
CLI Syntax: network A.B.C.D/M
Example: (config-router)# network 35.0.0.0/8

2.3.3.7 OSPF

2.3.3.7.1 Router OSPF

Enable or disable the OSPF process. Multiple OSPF processes are not supported, so you can’t specify an OSPF process number.
CLI Syntax: router ospf
Example: (config)# router ospf

2.3.3.7.2 Router ID

Assign an OSPF Router ID in IP-address format.
CLI Syntax: ospf router-id a.b.c.d
Example: (config-router)# ospf router-id 10.0.0.3

2.3.3.7.3 Area

Set the OSPF area ID.
CLI Syntax: network a.b.c.d/m area a.b.c.d
Example: (config-router)# network 102.192.2/24 area 192.192.2.254

2.3.3.8 Multicast Route

Enable or disable Multicast Route functions, which include DVMRP and PIM-DM.

CLI Syntax: ip multicast-routing ROUTING-PROTOCOL
Example: (config-router)# ip multicast-routing PIM-DM

2.3.3.9 VRRP

Enable or disable VRRP functions for a specific IP interface.
CLI Syntax: standby VRID (1-255) ip a.b.c.d/m
Example: (config-if)# standby 1 ip 192.168.1.1/24

2.3.3.10 Spanning Tree

2.3.3.10.1 Clear Spanning-Tree Counters

Use the “clear spanning-tree counters” configuration command on the switch to clear spanning-tree statistics.
CLI Syntax: clear spanning-tree counters
Example: SWITCH# clear spanning-tree counters

2.3.3.10.2 Clear Spanning-Tree Counters Interface IFNAME

Use the “clear spanning-tree counters” configuration command on the switch to clear spanning-tree statistics on one interface.
CLI Syntax: clear spanning-tree counters interface IFNAME
Example: SWITCH# clear spanning-tree counters interface gi1/0/2

2.3.3.10.3 Default Spanning-Tree

This command sets spanning-tree parameters to default.
CLI Syntax: default spanning-tree
Example: SWITCH# default spanning-tree forward-time

2.3.3.10.4 Show Spanning-Tree Active

To ‘show spanning-tree active’.
CLI Syntax: show spanning-tree active
Example: SWITCH# show spanning-tree active

2.3.3.10.5 Spanning-Tree Enable and Disable

Enable/Disable the spanning tree.
CLI Syntax: spanning-tree (enable|disable)
Example: SWITCH# spanning-tree disable

2.3.3.11 Link Aggregation

2.3.3.11.1 Trunk Aggregation Group

Use the aggregation-link trunk group configuration command on the switch to configure trunk aggregation group.
CLI Syntax: aggregation-link trunk STACKID group <1-32> PORTLIST
Example: SWITCH#aggregation-link trunk 1 group 1 1,2

2.3.3.11.2 Trunk Load Balancing

Use the aggregation-link trunk group configuration command on the switch to configure trunk load balancing by using source-based or destination-based forwarding methods.
CLI Syntax: aggregation-link trunk STACKID load-balance group <1-32> (src-mac |dst-mac |src-dst-mac |src-ip |dst-ip |src-dst-ip)
Example: SWITCH#aggregation-link trunk 1 load-balance group 1

2.3.3.11.3 Show Aggregation-Link Trunk

To show aggregation-link trunk status.
CLI Syntax: show aggregation-link trunk STACKID [GROUPID]
Example: SWITCH# show aggregation-link trunk 1 1

2.3.3.12 LACP

2.3.3.12.1 Clear LACP Counters

Use the “clear lacp counters” configuration command on the switch to clear the statistics for

all aggregated port sets.
CLI Syntax: clear lacp counters [STACKID]
Example: clear lacp counters 1

2.3.3.12.2 LACP Aggregation-Link Trunk

This command sets the Link Aggregation Control Protocol (LACP) operation add/set for the trunk group ports on the switch.
CLI Syntax: lacp aggregation-link trunk STACKID (add/set) group <1-32> PORTLIST
Example: SWITCH# lacp aggregation-link trunk 1 set group 1 1,2

2.3.3.12.3 Disable LACP Aggregation-Link Trunk

This command sets the Link Aggregation Control Protocol (LACP) operation add/set or disable for the trunk group ports on the switch.
CLI Syntax: lacp aggregation-link trunk STACKID disable <1-12>
Example: SWITCH# lacp aggregation-link trunk 1 disable 2

2.3.3.12.4 LACP Port-Priority

This command sets the port priority for the Link Aggregation Control Protocol (LACP) on the switch.
CLI Syntax: lacp port-priority <1-65535>
Example: (config)# interface fa1/0/2
            (config-if)# lacp port-priority 1000

2.3.3.12.5 LACP System-Priority

This sets the system priority for the Link Aggregation Control Protocol (LACP) on the switch.
CLI Syntax: lacp system-priority <1-65535>
Example: (config)# lacp system-priority 20000

2.3.3.13 Mirroring

2.3.3.13.1 Mirror Mode

To set the port mirror mode.
CLI Syntax: mirror mode
Example: (config)# mirror mode l2

2.3.3.13.2 Mirror Setting

This command mirrors the source interface list traffic to the destination interface. The mirror type supports received traffic, transmitted traffic or both.
CLI Syntax: mirror IFLIST to IFNAME (rx|tx|both)
Example: (config)# mirror gi1/0/3-5 to gi1/0/9 both

2.3.3.13.3 Show Mirror

To show current mirror features.
CLI Syntax: Show mirror
Example: SWITCH# show mirror

2.3.3.13.4 No Mirror

This command resets the source interface’s received or transmitted traffic or both to the destination interface.
CLI Syntax: no mirror SRCIFLIST (rx|tx|both)
Example: (config)# no mirror gi1/0/1,gi1/0/4 rx

2.3.3.14 Static Multicast

2.3.3.14.1 MAC-Address-Table Multicast

Use the mac-address-table multicast configuration command on the switch to add multicast static addresses to the MAC address table.
CLI Syntax: mac-address-table multicast MACADDR vlan VLANID interface IFLIST
Example: (config)# mac-address-table multicast 0100.5e11.1111 vlan 2 interface gi1/0/3 1

2.3.3.14.2 No MAC-Address-Table Multicast

Use the no mac-address-table multicast configuration command on the switch to remove the multicast static port from the MAC address table.
CLI Syntax: no mac-address-table multicast MACADDR vlan VLANID interface IFLIST
Example: (config)# no mac-address-table multicast 0100.5e11.1111 vlan 2 interface gi1/0/3 1

2.3.3.14.3 Show MAC-Address-Table Multicast

Use the “show mac-address-table multicast” user EXEC command to display the Layer 2 multicast entries for all VLANs. Use the command in privileged EXEC mode to display specific multicast entries.
CLI Syntax: show mac-address-table multicast
Example: SWITCH# show mac-address-table multicast

2.3.3.15 IGMP Snooping

2.3.3.15.1 Default IP IGMP Snooping

This command sets the “ip igmp snooping” feature to default.
CLI Syntax: default ip igmp snooping
Example: (config)# default ip igmp snooping

2.3.3.15.2 IP IGMP Snooping

This command sets the IGMP snooping function to “enabled globally.”
CLI Syntax: ip igmp snooping
Example: (config)# ip igmp snooping

2.3.3.15.3 Interval Time

This command sets the interval time for the IGMP queries sent by the switch.
CLI Syntax: ip igmp snooping last-member-query-interval TIMEVALUE
Example: (config)# ip igmp snooping last-member-query-interval 100

2.3.3.16 Traffic Control

2.3.3.16.1 Storm-Control

Use the storm-control configuration command on the switch to set the limit rate of the port’s total bandwidth used by broadcast/dlf/multicast.
CLI Syntax: storm-control (broadcast|dlf|multicast) LIMIT_RATE
Example: (config)# storm-control broadcast 25

2.3.3.16.2 No Storm-Control

Use the no storm-control configuration command on the switch to disable the limit rate of the port’s total bandwidth used by broadcast/dlf/multicast.
CLI Syntax: no storm-control (broadcast|dlf|multicast)
Example: (config-if)# no storm-control broadcast

2.3.3.16.3 Show Storm-Control

Use the show storm-control configuration command on the switchto show the limit rate of the port’s total bandwidth used by broadcast/dlf/multicast.
CLI Syntax: show storm-control IFNAME (broadcast|dlf|multicast)
Example: SWITCH# show storm-control gi1/0/1 broadcast

2.3.3.17 Dynamic Addresses

2.3.3.17.1 Clear Dynamic MAC-Address

Use the write configuration command on the switch stack or stand-alone switch to clear dynamic L2 MAC addresses in the database.
CLI Syntax: clear mac-address-table dynamic address MAC_ADDR
Example: (config)# clear mac-address-table dynamic address 0000.1111.2222

2.3.3.17.2 Aging Time

Use the mac-address-table aging-time configuration command on the switch stack or on a stand-alone switch to set the length of time that a dynamic entry remains in the MAC address

table after the entry is used or updated. The real aging time is triple the command input radix number.
CLI Syntax: mac-address-table aging-time <1-255>
Example: (config)# mac-address-table aging-time 100
This example shows how to configure the mac-address-table aging time to 300 seconds.

2.3.3.17.3 No Aging Time

Disables the aging timer of the mac-address-table.
CLI Syntax: no mac-address-table aging-time
Example: (config)# no mac-address-table aging-time

2.3.3.17.4 Show MAC-Address-Table Aging-Time

CLI Syntax: show mac-address-table aging-time
Example: SWITCH# show mac-address-table aging-time

2.3.3.18 Static Addresses

2.3.3.18.1 Add Static MAC-Address

You can add a MAC address to the switch address table. The MAC address added this way will not age out from the address table.
CLI Syntax: mac-address-table static MAC_ADDR vlan VLANID interface IFNAME
Example: (config)# mac-address-table static 0000.1111.2222 1 gi1/0/2

2.3.3.18.2 Show MAC-Address-Table

This shows static and dynamic MAC addresses.
CLI Syntax: show mac-address-table
Example: SWITCH# show mac-address-table

2.3.3.19 VLAN

2.3.3.19.1 Show VLAN Name String

Use the ‘show vlan’ user EXEC command to display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch.
CLI Syntax: show vlan name string
Example: SWITCH# show vlan name VLAN1

2.3.3.19.2 VLAN VID

Use the vlan vid command to create a vlan entry on the switch.
CLI Syntax: vlan vid
Example: (config)# vlan 2

2.3.3.19.3 Name String

Use the ‘name string’ command to create a vlan entry with a string on the switch.
CLI Syntax: name string
Example: (config-vlan)# name VLAN2

2.3.3.19.4 Access VLAN

Set access mode characteristics of all interfaces and Set Virtual LAN.
CLI Syntax: switchport access vlan <1-4094>
Example: (config)# interface fa1/0/2

```
(config-if)# switchport access vlan 1
```

2.3.3.19.5 Allowed VLANs

Use the “switchport trunk allowed vlan” configuration command on the switch to add or remove the VLANs that are allowed to receive and send traffic on this interface in tagged format when in trunking mode.
CLI Syntax: switchport trunk allowed vlan (add|remove) VLANLIST
Example: (config)# interface fa1/0/2

```
(config-if)# switchport trunk allowed vlan add 1
```

2.3.3.20 GVRP

2.3.3.20.1 Clear GVRP Statistics

Use the “clear gvrp statistics” configuration command on the switch to clear all the GVRP statistics information on one or all interfaces.
CLI Syntax: clear gvrp statistics [IFNAME]
Example: SWITCH# clear gvrp statistics gi1/0/2

2.3.3.20.2 Default GVRP Configuration

This command sets the GVRP configuration to default.
CLI Syntax: default gvrp configuration
Example: SWITCH# default gvrp configuration

2.3.3.20.3 GVRP Mode

This command sets the GVRP feature to globally be enabled or disabled on the switch.
CLI Syntax: gvrp mode (enable|disable)
Example: SWITCH# gvrp mode enable

2.3.3.20.4 Show GVRP Configuration

To show gvrp configuration IFNAME status.
CLI Syntax: show gvrp configuration IFNAME
Example: SWITCH# show gvrp configuration gi1/0/1

2.3.3.20.5 Show GVRP Statistics

To show gvrp statistics IFNAME status.
CLI Syntax: show gvrp statistics [IFNAME]
Example: SWITCH# show gvrp statistics gi1/0/1

2.3.3.21 CoS/QoS

2.3.3.21.1 Queue CoS-Map

Use the “queue cos-map configuration” command on the switch to select the CoS queue that a given priority should map into.
CLI Syntax: queue cos-map PRIORITY QUEUE
Example: SWITCH# queue cos-map 1 3

2.3.3.21.2 Show Queue CoS-Map

This command shows the information of CoS and priority mapping.
CLI Syntax: show queue cos-map
Example: (config)# show queue cos-map

2.3.3.21.3 QoS Mode

This command sets qos mode to highfirst mode.
CLI Syntax: qos mode high_first
Example: (config)# qos mode high_first

2.3.3.21.4 Show QoS Mode

This command shows the qos mode.
CLI Syntax: show qos mode
Example: (config)# show qos mode

2.3.3.21.5 QoS Egress Bandwidth

This command is used to set the QoS bandwidth informational parameter for the outgoing packets.
CLI Syntax: qos egress bandwidth LIMIT_RATE BURST_RATE

```
Example: (config)# int gi1/0/2
         (config-if)# qos egress bandwidth 100 10
```

2.3.3.22 SNMP

2.3.3.22.1 Show RMON Statistics

To show rmon statistics IFNAME status.
CLI Syntax: show rmon statistics [IFNAME]
Example: SWITCH# show rmon statistics gi1/0/1

2.3.3.22.2 Show SNMP-Server Community

To show snmp-server community.
CLI Syntax: show snmp-server community
Example: SWITCH# show snmp-server community

2.3.3.22.3 SNMP-Server Host

This command sets the SNMP host information.
CLI Syntax: snmp-server host A.B.C.D
Example: (config)# snmp-server host 192.168.8.31

2.3.3.23 Filter

2.3.3.23.1 Deny Any Host

Use this deny MAC access list configuration command on the switch to prevent non-IP traffic from being forwarded if the conditions are matched. Use the “no” form of this command to remove a deny condition from the named MAC access list.
CLI Syntax: deny any host MACADDR [VLANID]
Example: (config)# deny any host c2f3.220a.12f4 1

2.3.3.23.2 Filter Set

This command defines an extended MAC access list using a name (enter access-list configuration mode).
CLI Syntax: mac access-list extended WORD
Example: (config)# mac access-list extended mac_acl_1

2.3.3.23.3 Filter Conditions

This command specifies one or more conditions (denied or permitted) to decide if the packet is forwarded or dropped.
CLI Syntax: (permit|deny) any any
Example: (config)# permit any any

2.3.3.23.4 Filter Attach

This command is used to assign filter rule for a specific port.
CLI Syntax: mac access-group WORD in
Example: (config-if)# mac access-group mac_acl_1 in

2.3.3.24 Port Access Control

2.3.3.24.1 Default System Authentication Control

This command sets dot1x system authentication control to default.
CLI Syntax: default dot1x system-auth-control
Example: (config)# default dot1x system-auth-control

2.3.3.24.2 Dot1x Default

This command resets the configurable 802.1x parameters to the default values.
CLI Syntax: dot1x default

```
Example: (config)# interface gi1/0/1
         (config-if)# dot1x default
```

2.3.3.24.3 Dot1x Guest-VLAN

Use the dot1x guest-vlan interface configuration command on the switch to specify an active VLAN as an 802.1X guest VLAN. Use the “no” form of this command to return to the default setting.
CLI Syntax: dot1x guest-vlan <1-255>

Example: (config)# interface gi1/0/1
(config-if)# dot1x guest-vlan 3

2.3.3.24.4 Dot1x Initialize Interface

Use the “dot1x initialize privileged” EXEC command on the switch to manually return the specified 802.1X-enabled interface to an unauthorized state before initiating a new authentication session on the interface.
CLI Syntax: dot1x initialize interface [IFNAME]
Example: (config)# dot1x initialize interface gi1/0/1

2.3.3.24.5 Dot1x Max-Req

Use the dot1x max-req interface configuration command on the switch to set the maximum number of times that the switch sends an Extensible Authentication Protocol (EAP)-request/identity frame (assuming that no response is received) to the client before restarting the authentication process. Use the “no” form of this command to return to the default setting.
CLI Syntax: dot1x max-req <1-10>
Example: (config)# interface fa1/0/1
(config-if)# dot1x max-req 2

2.3.3.24.6 Dot1x Port-Control

Use the dot1x port-control interface configuration command on the switch to enable manual control of the authorization state of the port. Use the “no” form of this command to return to the default setting.
CLI Syntax: dot1x port-control (auto|force-authorized| force-unauthorized)
Example: (config)# interface gi1/0/1
(config-if)# dot1x port-control force-authorized

2.3.3.25 Dial-In User

2.3.3.25.1 Dot1x Username Password

Add a user into the local radius database.
CLI Syntax: dot1x username WORD password WORD
Example: (config)# dot1x username test password 12345

2.3.3.25.2 Show Dot1x User

Show a dot1x dial-in user.
CLI Syntax: show dot1x username
Example: SWITCH# show dot1x test

2.3.3.26 RADIUS

2.3.3.26.1 RADIUS Settings

This command sets the radius server ip, radius key and radius port for 802.1X configuration.
CLI Syntax: dot1x radius server-ip A.B.C.D key RADIUS_KEY [PORTID]
Example: (config)# dot1x radius server-ip 192.168.1.38 key 123456 1812

2.3.3.26.2 Show Dot1x Radius

Show dot1x radius server ip, radius key and radius port for 802.1X configuration.
CLI Syntax: show dot1x radius
Example: SWITCH# show dot1x radius

2.3.3.27 Port Security

2.3.3.27.1 Show Port Security

This is used to show the port security configuration, status and MAC addresses information.
CLI Syntax: show port-security [address] [interface IFNAME]
Example: SWITCH# show port-security
SWITCH# show port-security interface gi1/0/1
SWITCH# show port-security address
SWITCH# show port-security interface gi1/0/1 address

2.3.3.27.2 Clear Port Security

This command is used to clear port security dynamic MAC addresses.
CLI Syntax: clear port-security dynamic [address MAC] | [interface IFNAME]
Example:

```
SWITCH# clear port-security dynamic
SWITCH# clear port-security dynamic address 0023.1313.2313
SWITCH# clear port-security dynamic interface gi1/0/1
```

2.3.3.27.3 Switchport Port-Security

This command is used to set the port security configuration and MAC addresses.
CLI Syntax: switchport port-security [mac-address MAC] | [maximum VALUE] | [violation {protect | restrict | shutdown}] | [reup]
Example:

```
(config)# interface gi1/0/1
(config-if)# switchport port-security
(config-if)# switchport port-security mac-address 0023.1313.2313
(config-if)# switchport port-security maximum 20
(config-if)# switchport port-security violation protect
(config-if)# switchport port-security reup
```

2.3.3.27.4 Switchport Port-Security Aging

This command is used to set the port security aging configuration.
CLI Syntax: switchport port-security aging {time TIME | type {absolute | inactivity}}
Example:

```
(config)# interface gi1/0/1
(config-if)# switchport port-security aging time 20
(config-if)# switchport port-security aging type absolute
```

2.3.4 Miscellaneous Commands

show monitor: Shows the environment variables, like temperature, fan speed and voltage.
show sysleds: Shows the three system LEDs: SYSTEM, RPS and FAN.
show modelname: Shows the model name of the switch.
show version: Shows the hardware, boot rom and firmware version.
ping: Ping the remote host.
show ip route: Display the entries in the routing table.

3 SPECIFICATIONS

Standards

- IEEE 802.1d (Spanning Tree Protocol)
- IEEE 802.1s (Multiple Spanning Tree Protocol)
- IEEE 802.1w (Rapid Spanning Tree Protocol)
- IEEE 802.1p (Traffic Prioritization)
- IEEE 802.1q (VLAN Tagging)
- IEEE 802.3 (10Base-T Ethernet)
- IEEE 802.3ab (Twisted Pair Gigabit Ethernet)
- IEEE 802.3ad (Link Aggregation)
- IEEE 802.3u (100Base-TX Fast Ethernet)
- IEEE 802.3x (flow control, for full duplex mode)
- IEEE 802.3z (1000Base-SX/LX/LHX)
- SNMPv1/v2c/v3 (Simple Network Management Protocol)

General

- Media support:
  - 10Base-T Cat3, 4, 5 UTP/STP RJ-45
  - 100Base-TX Cat5 UTP/STP RJ-45
  - 1000Base-T Cat5e UTP/STP RJ-45

- Packet filter/forwarding rate:
  - 1,488,000 pps (1000 Mbps)
  - 148,800 pps (100 Mbps)
  - 14,880 pps (10 Mbps)
- Buffer memory: 32 MBytes
- MAC address table: 16384 entries
- Backplane speed: 12.8 Gbps
- Switch architecture: store and forward
- Ports
  - 24 x RJ-45 Fast Ethernet ports
  - 4 RJ-45 Gigabit ports
  - 4 SFP Mini-GBIC transceiver module slots
- Certifications: FCC Class A, CE Mark, EN 60950

Configuration Options

- Full and half duplex per Fast Ethernet port
- Port link speed: 10 Mbps, 100 Mbps or auto-negotiation for Fast Ethernet ports
- Port ingress/egress control
- VLAN:
  - Port-based
  - Tag-based (4096 VLANs with GVRP for dynamic VLAN registration)
- Quality of Service (QoS):
  - 8 priority levels
  - 3 priority options (First Come First Serve, High First and Weighted Round Robin (WRR))
  - CoS Queue Mapping
  - Ingress/Egress bandwidth
- Port Mirroring for all ports with sniffer port configuration
- Port Aggregation/Trunking: 32 groups with up to 8 member ports per trunk
- SNMP Management with Host Table, Trap Setting and SNMPv3 VGU Table configuration
- Management Agent SNMP Support: MIB II, Bridge MIB, Ethernet MIB, RMON MIB
- SNMP Standards & Protocols:
  - RFC 1213 MIB II
  - RFC 1493 Bridge MIB
  - RFC 1643 Ethernet Interface MIB
  - RFC 1757 RMON
  - RFC 1112/2236 IGMP Snooping v1, v2
  - RFC 1350 TFTP

LEDs

- Power Supply 1
- Power Supply 2
- Post function
- Link Speed per Fast Ethernet port: 10/100 Mbps
- Link Speed per Gigabit port: 10/100/1000 Mbps
- Link/Activity per port

Power

- Internal power supply, 100 to 240 V AC, 50/60 Hz
- Power consumption: 40 Watts (maximum)

Environmental

- Metal housing, 19” rackmount, 1 U
- Dimensions: 440 (W) x 184 (L) x 44 (H) mm (17.4 x 7.2 x 1.7 in.); weight: 4.0 kg (8.8 lbs.)
- Operating temperature: 0 – 50°C (32 – 122°F)
- Operating humidity: 10 – 80% RH, non-condensing
- Storage temperature: -20 – 70°C (-4 – 158°F)

NOTES:

NOTES:

NOTES:

NOTES:

INTELLINET™

NETWORK SOLUTIONS

BRINGING NETWORKS TO LIFE

www.intellinet-network.com

Are you completely satisfied with this product?
Please contact your INTELLINET NETWORK SOLUTIONS™ dealer
with comments or questions.