



MEN-6532

***24 slot Gigabit Multi-rate SFP + 4 Gigabit Combo
Managed Aggregation Switch***

User Manual



**Version 1.0
Mar 2013**

COPYRIGHT

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, whether electronic, mechanical, photo copying, recording or otherwise, without the prior written permission of the publisher.

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.

Take special care to read and understand all the content in the warning boxes:



Warning

Table of Contents

| | |
|---|-----------|
| About This Manual | 6 |
| <i>Welcome</i> | <i>6</i> |
| <i>Purpose</i> | <i>6</i> |
| <i>Terms/ Usage.....</i> | <i>6</i> |
| <i>Features</i> | <i>6</i> |
| <i>Specifications</i> | <i>7</i> |
| Hardware Description | 10 |
| <i>Connectors</i> | <i>10</i> |
| Multirate (100/1000) Gigabit Ports | 10 |
| 10/100/1000Base-T Ports | 10 |
| SFP Slots for SFP modules | 11 |
| Installation | 11 |
| <i>Desktop Installation</i> | <i>11</i> |
| <i>Mounting on a Rack.....</i> | <i>11</i> |
| <i>Getting Connected</i> | <i>12</i> |
| <i>Powering On the Unit</i> | <i>12</i> |
| <i>Installing the SFP modules and Fiber Cable</i> | <i>12</i> |
| <i>Connecting a Copper Cable</i> | <i>14</i> |
| <i>Connecting the Console Port Cable</i> | <i>14</i> |
| <i>Connecting to Computers or a LAN.....</i> | <i>15</i> |
| <i>Power On the Unit</i> | <i>15</i> |
| LED Indicators | 16 |
| Management Options | 17 |
| <i>Web-based Management Interface.....</i> | <i>17</i> |
| <i>SNMP-based Management.....</i> | <i>17</i> |
| <i>Configuring the Switch via a Console Port (RS-232 DCE)</i> | <i>17</i> |
| Using HyperTerminal to Set an IP Address..... | 17 |
| <i>Telnet</i> | <i>19</i> |
| <i>SNMP Settings</i> | <i>20</i> |
| <i>Traps</i> | <i>21</i> |
| <i>MIBs</i> | <i>21</i> |
| First Time Connecting to the Switch | 21 |
| Web Management | 25 |
| <i>Log into Web Management.....</i> | <i>25</i> |
| <i>Status</i> | <i>25</i> |

| | |
|---|----|
| System Information | 25 |
| <i>Basic Setting</i> | 25 |
| General Setup | 25 |
| User Account | 26 |
| IP Setup | 27 |
| Port Setup | 28 |
| Interface Config | 28 |
| Runtime Status | 29 |
| Bandwidth Limitation | 30 |
| DHCP Relay | 31 |
| IGMP Snooping | 32 |
| General Setting | 32 |
| Querier Mode | 33 |
| Multicast MAC Address | 34 |
| Multicast VLAN Registration | 34 |
| Link Aggregation | 36 |
| Configuration | 36 |
| LACP | 36 |
| Port Priority | 37 |
| Loop Detection | 38 |
| MAC Forwarding | 40 |
| Dynamic MAC Addresses | 40 |
| Static MAC Addresses | 41 |
| Static Multicast MAC Addresses | 42 |
| Mirroring | 43 |
| Port Isolation | 44 |
| QoS | 46 |
| CoS Queue Mapping | 47 |
| 802.1p Priority | 47 |
| Spanning Tree | 48 |
| STP Status | 48 |
| Current Roots | 49 |
| Bridge Parameters | 50 |
| Port Parameters | 51 |
| Storm Control | 53 |
| VLAN Configuration | 53 |
| Static VLAN | 53 |
| Dynamic VLAN | 57 |
| Q-in-Q | 59 |
| <i>Security</i> | 63 |
| DHCP Binding Table | 63 |
| DHCP Snooping | 64 |
| DHCP Snooping Setting | 64 |
| DHCP Snooping VLAN Setting | 65 |
| DHCP Static Binding Table | 66 |
| ARP Inspection | 67 |
| ARP Inspection Setting | 67 |
| ARP Inspection VLAN Setting | 68 |
| Access Control List | 69 |
| 802.1x | 70 |
| Management | 73 |
| Reboot | 73 |
| Firmware Upgrade | 73 |
| Save Configuration & Reload Default | 75 |

| | |
|---|-----------|
| Command Line Interface | 76 |
| <i>Power On</i> | <i>76</i> |
| <i>Login and Logout</i> | <i>76</i> |
| <i>CLI Commands</i> | <i>76</i> |
| ACL..... | 77 |
| QoS..... | 78 |
| Bandwidth Management..... | 79 |
| Bandwidth Limitation..... | 79 |
| Storm Control..... | 79 |
| DHCP Client | 79 |
| DHCP Relay..... | 80 |
| DHCP Option 82..... | 80 |
| IGMP Snooping..... | 81 |
| IP Source Guard..... | 82 |
| DHCP Snooping | 82 |
| DHCP Snooping Binding Table..... | 82 |
| ARP Inspection | 83 |
| Blacklist Filter | 83 |
| Link Aggregation (Trunk) | 83 |
| Static Link Aggregation | 83 |
| 802.3ad Link Aggregation Control Protocol (LACP)..... | 84 |
| Loopback Detection..... | 85 |
| MAC Address Management | 85 |
| Port Management | 86 |
| Port Mirror | 87 |
| Port Security..... | 87 |
| SNMP | 89 |
| STP & RSTP | 89 |
| Configuration Management | 91 |
| Firmware Upgrade..... | 92 |
| System Management | 92 |
| System Management | 92 |
| User Account..... | 92 |
| VLAN..... | 94 |
| VLAN..... | 94 |
| Port Isolation..... | 94 |
| GARP | 95 |
| GVRP | 95 |
| Dot 1x | 96 |
| Customer Support | 98 |

About This Manual

Welcome

Congratulations on choosing the MEN-6532 24-port Gigabit SFP + 4 Gigabit Combo Managed Aggregation Switch. The MEN-6532 is a high-performance managed SNMP Layer 2 switch that provides users with 24 Multi-rate (100/1000) Gigabit SFP slots and four Gigabit Combo ports with both SFP slot and RJ-45. The Web/SNMP management provides remote control capability that provides flexible network management and monitoring options. Whether managed via an "in-band" SNMP management station, an Internet Web browser, or via an "out-of-band" RS-232 console port, the MEN-6532 facilitates network operational control and diagnostics.

The management functions enable efficient network usage. VLAN reduces the collisions caused by broadcasting. QoS secures the bandwidth for some bandwidth-hungry applications like VoIP and video conferencing. The Switch also supports Port Mirroring that allows web manager to watch abnormal traffic.

Purpose

This manual discusses how to install and configure your Managed Layer 2 Aggregation Switch.

Terms/ Usage

In this manual, the term "Switch" (first letter upper case) refers to the MEN-6532 Switch, and "switch" (first letter lower case) refers to other switches.

Features

- 24-port 100/1000 SFP plus a choice of four Gigabit copper or fiber ports
- Supports per-port Egress/Ingress rate control
- Supports 802.3x flow control for Full-duplex mode and collision-based backpressure for half-duplex mode
- Provides trunk groups of up to eight member ports per trunk, up to eight groups
- Broadcast storm prevention
- Supports jumbo frames of up to 10K bytes
- QoS with eight Priority Queues
- Automatic learning of up to 32K MAC addresses
- Supports STP and RSTP
- Tagged VLAN 802.1q with 802.1p up to 4K VLANs
- Double VLAN tagging (Q-in-Q)
- Supports 802.1X EAP and RADIUS Authentication
- IGMP Snooping V1/V2/V3 with Multicast Filtering
- Access Control List (Layer 2, 3, and 4)
- QoS Supports 802.1p, WRR, Strict Scheduling Priority Queue (SPQ), Bandwidth Management

- SNMP V1, V2c with RMON groups 1, 2, 3, and 9
- FCC Class A & CE approved

* Available in future firmware upgrade.

Specifications

Performance:

| | |
|---------------------|---|
| Throughput: | 14,880 packets per second (pps) to 10 Mbps ports 148,800 pps to 100Mbps ports 1,488,000 pps to 1000Mbps ports |
| Address Table Size: | 32K MAC entries |
| VLANs: | Port-based Tag-based (4096VLANs) |
| Link Aggregation: | Up to eight aggregation groups |
| Max. Distance: | UTP: 100 meters |
| Fiber: | Based on Mini GBIC module |
| Management via: | SNMP V1, V2c Web Management Command Line Interface (CLI) RS-232 console |

Connectors and Cabling:

| | |
|----------------|---|
| Ports: | 24 x Multirate 100/1000 SFP slots 4 x Gigabit Combo Ports (10/100/1000 RJ-45 Ethernet ports / Gigabit fiber SFP slots) |
| Smart Control: | RS-232 |

SNMP Standards & Protocols:

| | |
|----------|------------------------------------|
| RFC 1157 | Simple Network Management Protocol |
| RFC 1213 | MIB II |
| RFC 1493 | Bridge MIB |
| RFC 1643 | Ethernet Interface MIB |
| RFC 1757 | RMON |

Network Management:

| | |
|-----------------------------|--|
| System Configuration: | Console port, Telnet, Web browser, and SNMP/RMON |
| Management Agent: | SNMP Support: MIB II, Bridge MIB, Ethernet MIB, and RMON MIB |
| RMON Groups: | 1, 2, 3, and 9 (Statistics, History, Alarm and Event) |
| Spanning Tree Algorithm: | IEEE 802.1D and 802.1w provide redundant link support |
| Port-based or 802.1Q VLANs: | Up to 4096 VLANs, with GVRP for dynamic VLAN registration |
| Link Aggregation: | 2~8 ports can be combined into a fat pipe |

Standards and Compliance:

IEEE 802.3 10Base-T Ethernet
 IEEE 802.3u 100Base-TX Ethernet
 IEEE 802.3ab 1000Base-T Ethernet
 IEEE 802.3z 1000Base-SX/LX/LHX
 IEEE 802.3 NWay Auto-negotiation
 IEEE 802.3x Flow Control
 IEEE 802.1D Spanning Tree protocol
 IEEE 802.1w Rapid Spanning Tree protocol
 IEEE 802.1p Class of Service, Priority protocols
 IEEE 802.1Q VLAN Tagging
 IEEE 802.1X Port Authentication
 IEEE 802.1ad VLAN Stacking
 IEEE 802.3ad LACP Aggregation

Power Characteristics:

| | |
|--------------------|---|
| Input voltage: | 100 to 240V AC (auto-ranging) 50 to 60 Hz or DC-48V |
| Power Consumption: | 55-Watts max. |

Environmental Characteristics:

| | |
|-----------|---|
| Operating | Temperature: 0°C to 50°C Relative Humidity: 10% to 80%, non-condensing |
| Storage | Temperature: -20°C to 70°C Humidity: 5% to 90% (non-condensing) |

Dimensions:

44mm (H) x 440mm (W) x 284mm (D)

Weight:

4.5kg

Mounting:

Standard 19" Rack-mountable case

Electromagnetic Compatibility:

Emissions: FCC Class A, & CE approved

Hardware Description

The MEN-6532 is a high-performance managed SNMP Layer 2 switch that provides users with 24 x Gigabit Ethernet SFP slots and four Gigabit Combo ports. The Web/SNMP management provides remote control capability that gives user-friendly and flexible network management and monitoring options.

For increased bandwidth applications, the MEN-6532 can accommodate trunk groups with eight ports in each trunk, up to eight trunking groups.

Moreover, these trunk ports ship with fail-over function to provide redundant backup if one or more of the ports are malfunctioning. It also supports both Port-based VLAN and Tag-based VLAN, thereby simplifying network traffic segmentation, broadcast domain extension and other associated benefits of constructing VLANs. This abundance of features translates into increased efficiency and performance in network administration.

Being SNMP-ready, the Switch enables network managers to remotely monitor the entire network status quickly and easily via RJ-45 (in-band), or console port (out-of-band) connection. This managed Switch can extend the enterprise LAN configuration range up to 110km while simultaneously minimizing the troubleshooting time. The Switch is designed for 'plug-n-play' to enable hassle-free integration in today's managed mixed cabling network configurations.

Featuring auto MDI/MDI-X detection for direct connections to a workstation, switch or hub, network managers no longer need to worry about the cable configuration (crossover or straight through) when establishing connections between RJ-45 ports.

The Switch has auto-negotiation capabilities that allow it to support connection with leading NWay switches. In full-duplex mode, this unit can sustain distances of up to 550m (with multi-mode fiber) and 110km (with long-haul single-mode fiber) between a LAN switch and another switch or data/file server.

Connectors

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

Multi-rate (100/1000) Gigabit Ports

The 100/1000 ports support network speeds of either 100Mbps or 1000Mbps (1Gbps) and are designed to house 100Mbps/Gigabit SFP modules.

10/100/1000Base-T Ports

The Switch has four Gigabit 10/100/1000Base-T ports for RJ-45 connectors that support auto-negotiation and MDI/MDI-X. The only difference is that the Gigabit copper ports support network speeds of 10/100/1000Mbps.

These four ports are located next to the four SFP-type fiber slots and each one 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 correspondingly numbered RJ-45 port (25, 26, 27 or 28) will not function.

SFP Slots for SFP modules

The four uplink SFP slots are designed to house Gigabit SFP modules that support network speeds of 1000Mbps. 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 and 28) will not function.

Installation

The location chosen for installing the Switch may greatly affect its performance. When selecting a site, we recommend considering the following rules:

- Install the Switch in an appropriate place. See Technical Specifications for the acceptable temperature and humidity ranges.
- Install the Switch in a location that is not affected by strong electromagnetic field generators (such as motors), vibration, dust, and direct sunlight.
- Leave at least 10cm of space at the front and rear of the unit for ventilation.
- Affix the provided rubber pads to the bottom of the Switch to protect the case from scratching.

Desktop Installation

Follow the instructions listed below to install the Switch in a desktop location.

1. Locate the Switch in a clean, flat and safe position that has convenient access to AC power.
2. Affix the four self-adhesive rubber pads to the underside of the Switch.
3. Apply AC power to the Switch (The green PWR LED on the front panel should light up).
4. Connect cables from the network partner devices to the ports on the front panel (The green LNK LED on the upper right of the port should light).

This Switch can also be mounted on a vertical surface. Simply use the underside of the unit as a template to measure and mark out the position of the holes on to the surface where the unit is to be installed. Then use the two screws provided to mount the Switch firmly in place.



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

Mounting on a Rack

Attach brackets to each side of the switch and place the brackets in the rack's slots. Insert and tighten two screws to securely attach the bracket to the rack on each side.

Getting Connected

The Switch is capable of connecting up to 26 network devices employing a combination of twisted-pair and fiber cabling paths at Ethernet, Fast Ethernet, or Gigabit Ethernet speeds.

Powering On the Unit

The Switch uses an AC power supply 100~240V AC, 50~60 Hz, or DC -48V. 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. Insert the power cable plug 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. You must use a power cord set that has been approved for the receptacle type and electrical current in your country.

3. Check the front-panel LEDs as the device is powered on to verify that the Power LED is lit. If not, check that the power cable is correctly and securely plugged in.

Installing the SFP modules and Fiber Cable

- 1) The MEN-6532 has two Gigabit SFP slots situated under the RS-232 port:



- 2) Slide the selected SFP module into the selected SFP slot. (Make sure the SFP module is aligned correctly with the inside of the slot):



3) Insert and slide the module into the SFP slot until it clicks into place:



4) Remove any rubber plugs that may be present in the SFP module's mouth.

5) Align the fiber cable's connector with the SFP module's mouth and insert the connector:



6) Slide the connector in until a click is heard:



7) If you want to pull the connector out, first push down the release clip on top of the connector to release the connector from the SFP module.

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.

Note: When inserting the cable, be sure the tab on the plug clicks into position to ensure that it is properly seated.

Check the corresponding port LED on the Switch to be sure that the connection is valid. (Refer to the LED chart)

Connecting a 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 (see recommendation above) type 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 Switch to ensure that the connection is valid. (Refer to LED chart)

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 Switch and the other end into the COM port of the computer.
- 2 Configure the Hyper Terminal settings as mentioned in chapter 5 or 6.3.1.

Connecting to Computers or a LAN

You can use Ethernet cable to connect computers directly to the switch ports. You can also connect hubs/switches to the switch ports by Ethernet cables. You can use either the crossover or straight-through Ethernet cable to connect computers, hubs, or switches.

Use a twisted-pair Category 5 Ethernet cable to connect the 1000BASE-T port, otherwise the link speed will not be able to reach 1Gbps.

Power On the Unit

Connect the AC power cord to the POWER receptacle on the front of the Switch and plug the other end of the power cord into a wall outlet or a power strip.

Check the front LED indicators with the description in the next chapter. If the LEDs light up as described, the Switch's hardware is working properly.

LED Indicators

This Switch is equipped with Unit LEDs to enable you to determine the status of the Switch, as well as Port LEDs to display what is happening in all your connections. They are as follows:

| <i>Unit LEDs</i> | | |
|---|------------------|-----------------------------------|
| LED | Condition | Status |
| POST | Flashing | Self test fails |
| | On | System ready to use |
| PWR | On (Green) | Primary power normal |
| | Off | Primary power off or failure |
| (25 th ~28 th G E Ports) Link/Act | On (Green) | The port is linked. |
| | Flashing (Green) | Data traffic passing through port |
| | Off | No valid link established on port |
| (25 th ~28 th G E Ports) 100M | On (Green) | The port linked at 100Mbps |
| (25 th ~28 th G E Ports) 1000M | On (Green) | The port linked at 1000Mbps |

Management Options

This system may be managed out-of-band through the console port on the front panel or in-band by using Telnet. The user may also choose web-based management, accessible through a Web browser.

Web-based Management Interface

After you have successfully installed the Switch, you can configure the Switch, monitor the LED panel, and display statistics graphically using a Web browser.

SNMP-based Management

You can manage the Switch with SNMP Manager software. The SNMP agent decodes the incoming SNMP messages and responds to requests with MIB objects stored in the database. The SNMP agent updates the MIB objects to generate statistics and counters.

Configuring the Switch via a Console Port (RS-232 DCE)

Prior to accessing the switch's onboard agent via a network connection, you must first configure it 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 within the attached network or via internet. The onboard configuration program can be accessed by using Telnet from any computer attached to the network. It can also be managed with any computer 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. Configure your own terminal to match the following:

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

Note: Ensure that the terminal or PC you are using to make this connection is configured to match the above settings. Otherwise the connection will not work.

A console port cable is provided with the Switch to connect the PC's COM port with the Switch's serial console (RJ-45) port.

Using HyperTerminal to Set an IP Address

Prior to following the instructions listed below for HyperTerminal, verify that a console cable (RJ45 to DB9) connection between the Switch and workstation exists. Then follow the steps below:

1. Launch the terminal emulation program on the remote workstation and power on the Switch. Be sure to select the correct COM port.



2. Enter the correct parameters according to the defaults given on the previous page:



3. The prompt screen will appear after clicking the **OK** button. The default log-in name is "admin" with no password. If you want to enter the privileges mode, execute the command "enable." The default log-in name is "admin" with password "admin."
4. The prompt **Switch>** will appear. For a list of main commands, type "?" and <Enter>. For a list of sub-commands, type a main command like "list" and <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 successful log-in, type the following command line to change the device IP, Network Mask, and Gateway address:

```
Switch#config terminal
Switch(config)#interface eth0
Switch(config-if)#ip address xxx.xxx.xxx.xxx/dd
Switch(config-if)#exit
```

The **xxxs** represent values between **0** and **255** and the user should enter their own IP address in this form. The **/dd** represents the total bits of the subnet mask. The configuration program will not accept anything outside this format. Remember to separate each part of the address with a period (dot).

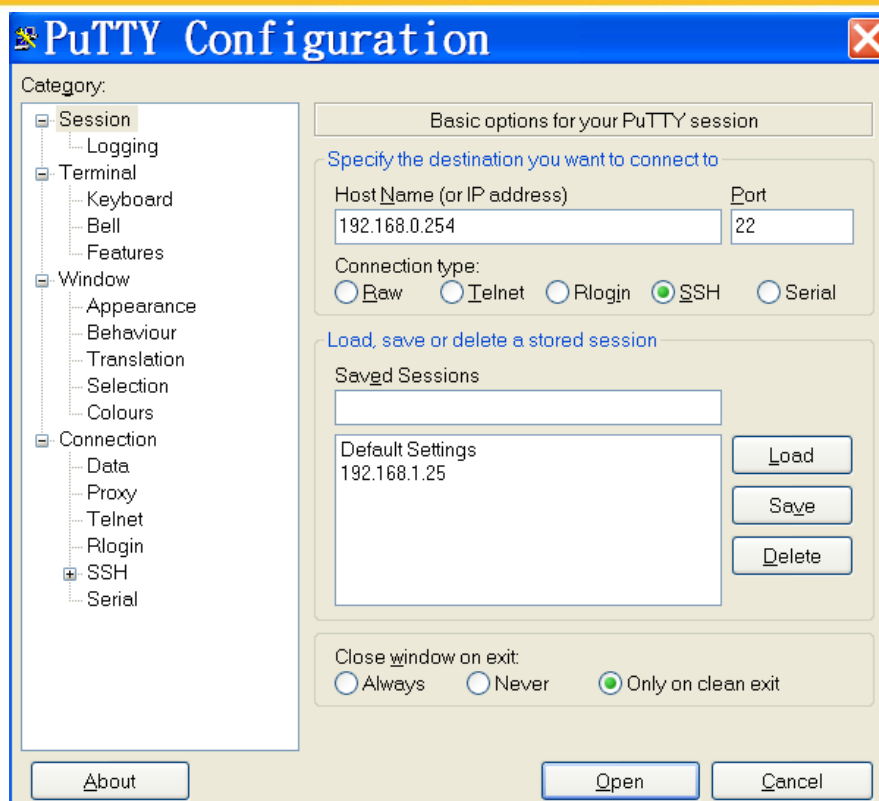
When the address has been changed, please make a note of the new address, and keep it in a safe place. With HyperTerminal, the command lines are the same as that for telnet. Users can continue to use Hyper Terminal along with the instructions given in next sections. Otherwise, log out by typing 'exit' and pressing the **<ENTER>** key. Then, the user can choose to configure the Switch via HTTP Web Browser or Telnet with Menu Driven or Command Line interfaces.

Note: *IP addresses are unique. If an address isn't available, please contact the appropriate authorities to apply for one.*

Telnet

Activate your workstation's command prompt program and access your Switch via the Internet by typing in the correct IP address (factory default IP address is **192.168.0.254** – connect directly via console port to configure a unique IP address). Your command prompt program will allow use of the Telnet protocol.

Example where IP address is typed in and Telnet is selected (using a command prompt program such as Putty):



After opening the program, a command prompt screen will appear. At the **Switch login** line, type the pre-set password – the factory default is **admin**. Type '?' for a list of main commands. For example, a user has typed the **list** command below the last listed main command:

```
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 in conf
```

SNMP Settings

Simple Network Management Protocol (SNMP) is an Application Layer designed specifically 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, monitoring performance, and detecting potential problems in the Switch, switch group, or network. Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like 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.

MIBs

The Switch in the MIB stores management and counter information. It uses the standard MIB-II Management Information Base module. 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.

First Time Connecting to the Switch

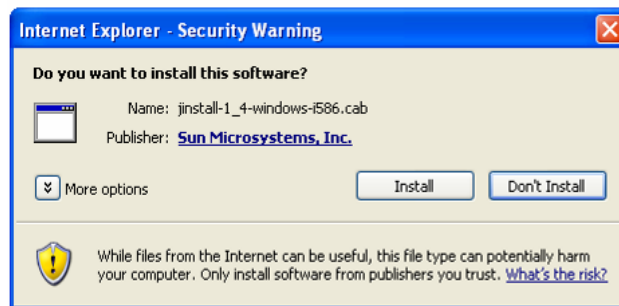
The Switch supports user-based security that can allow you to prevent unauthorized users from accessing the Switch or changing its settings. This section tells you how to log into the Switch. If you don't have the correct version of Java on your computer, the following will apply to you:

Installing the Java Runtime Environment Software:

If you don't already have the correct Java Runtime Environment (JRE) on your computer, this manual will help you to install it. To test if you already have the correct software, open your network browser (**you must be connected to the internet for the following function**) and type in 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.

Note: Depending on your connection speed, this process will take between 5 to 30 minutes to complete.

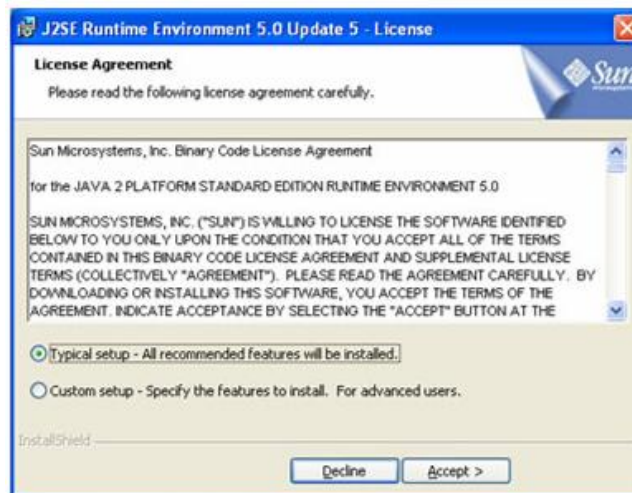
Step 1: If you get this Internet Explorer Security Warning, click **Install**.



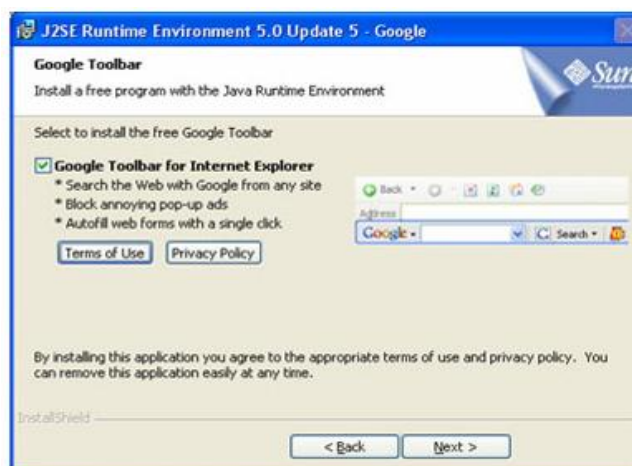
Step 2: The installation page will appear. Wait until the next screen appears.



Step 3: This is the User's Agreement page. Read through it and click on the **Accept >** button. (The page also gives you the option to choose "Typical setup" or "Custom setup". (The software vendor strongly suggests that the user select "Typical setup".)

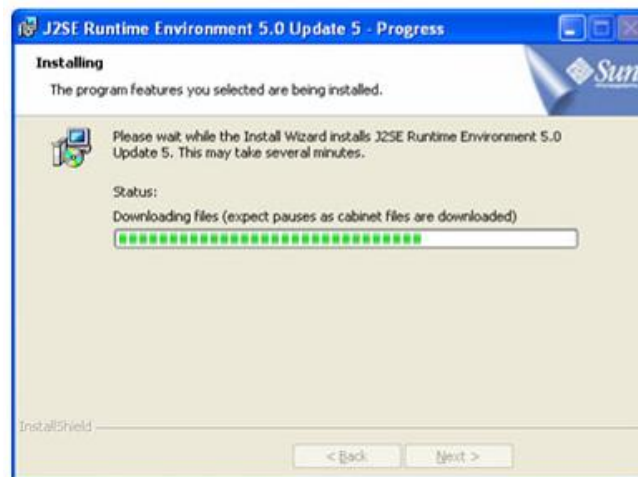


Step 4: If Internet Explorer is set as the default browser on your system, then the Java Runtime Environment 5.0 Update 5 – Google Programs dialog box will appear. By default, Google Toolbar for Internet Explorer is checked. Click the **Next >** button. This will start installing selected program features, including the JRE, on your system.



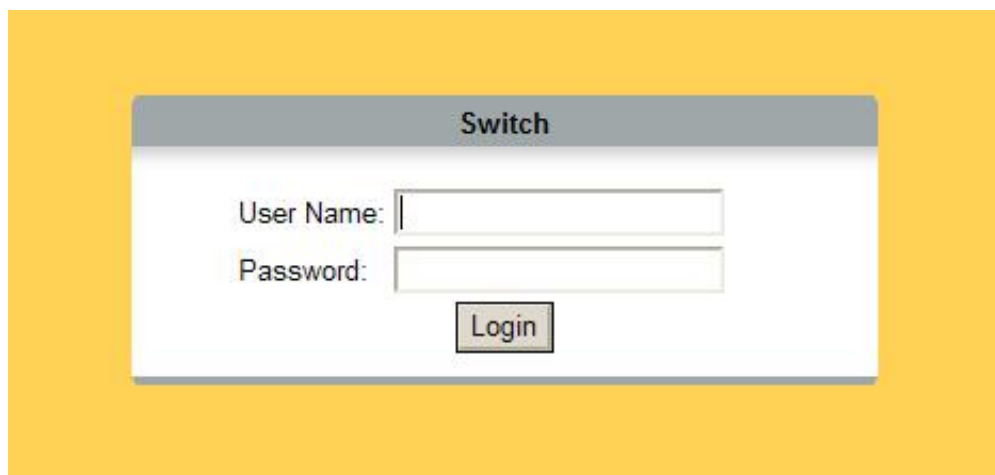
Note: You can choose to install or ignore this useful additional program by checking or un-checking the check box.

Step 5: This page appears when the installation process has started and shows you how far the process has progressed. Depending on your connection speed, the process can take between 5 and 30 minutes.



Step 6: A few brief dialog boxes will confirm the last steps of the installation process, and a concluding message will appear with the confirmation "Installation Completed OK." Click **Finish**.

Step 7: After finishing the installation process, the program will show this page every time you type the IP address. **The default User Name and Password is "admin" and "admin".**



Click **OK** to enter the management interface of the MEN-6532.

TROUBLESHOOTING:

If you still have problems accessing the hyperlink, check the following:

- 1) Check the firewall in your PC or the firewall that your company uses. This firewall could be blocking access to the hyperlink.
- 2) 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 Apple's Mac OSX and Unix.

Web Management

The 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 section 7 above).

Log into Web Management

From a PC, open your Web browser, type the following in the Web address (or location) box: **http://192.168.0.254** and then press **<Enter>**.

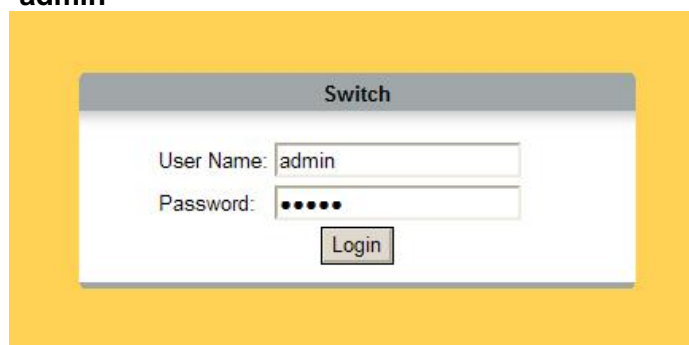
This is the factory default IP address for the switch. A login dialog is displayed, as shown in the figure on the right:

Enter your user name and password, then click **OK**.

Use the following defaults the first time you log into the program. You can change the password at any time through CLI interface.

Default User Name: **admin**

Default Password: **admin**



Status

The Status folder contains a read-only window for System Information.

System Information

The **System Information** window appears each time you log into the program. Alternatively, this window can be accessed by clicking **Status > Switch Information**.

Basic Setting

The Basic Setting folder contains configuration windows for General Setup, User Account, IP Setup, DHCP Client, and Port Setup.

General Setup

The **General Setup** window contains the following information:

- **Model Name:** The Switch model name.
- **MAC Address:** The Switch MAC address.

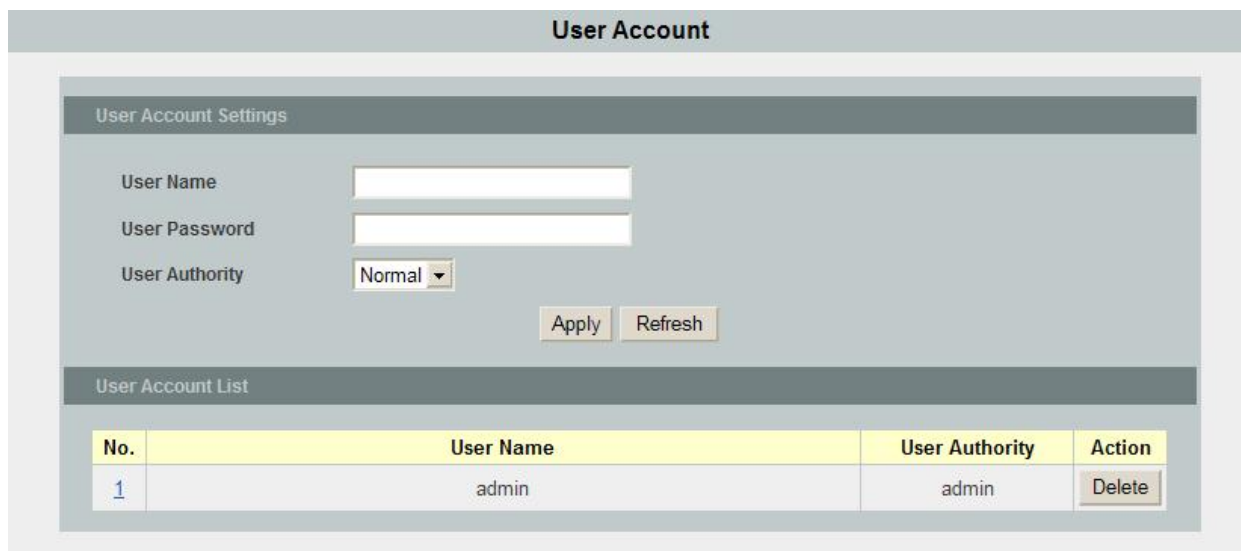
- **Firmware Version:** The Switch's firmware version.
- **Host Name:** The name of this Switch. Users can modify the name if desired. Please note that no space is allowed in the host name.

Click **Submit** to commit the settings. Click **Refresh** to display current settings of the Switch.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

User Account

The **User Account** window allows users to modify the access account info.



User Account window

| Parameter | Description |
|---------------|---|
| User Name | Enter a new user name. |
| User Password | Enter the password. |
| User Level | Choose either admin (read and write) or normal (read only) for this user. |
| Action | After you put in the new user, choose add . To delete an existing user, first select it from the table first. |
| Submit | Click Submit to commit the settings. |
| Refresh | Click Refresh to display the current settings of the Switch. |

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

IP Setup

The **IP Setup** window contains the following information:

- **IP Address:** The IP address for the Switch.
- **Subnet Mask:** The subnet mask for this network.

Click to modify the IP Address and/or the Subnet Mask if there is a need to change either.

The screenshot shows the 'General Settings' window with three tabs: 'System', 'Jumbo Frame', and 'SNTP'. The 'System' tab is selected, and the 'System Settings' section is visible. It contains the following fields and controls:

| Field | Value |
|-------------------|-----------------------------------|
| Hostname | L2SWITCH |
| DHCP Client | Disable (dropdown) [Renew button] |
| Static IP Address | 192.168.0.254 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 0.0.0.0 |
| Management VLAN | 1 |

At the bottom right of the 'System Settings' section are two buttons: 'Apply' and 'Refresh'.

IP Setup window

Click **Submit** to commit the settings. Click **Refresh** to display current settings of the Switch.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

Port Setup

Interface Config

The **Port Setup** window **Interface Config** tab displays the Ethernet port status in real time. Users can configure ports in the fields described in the table below.

Port Settings

Port
 From: To:

State

Speed/Duplex

(Port range must be port1~24 or port25~28)

Port Status

| Port | State | Speed/Duplex | Link Status |
|------|---------|--------------|--------------------|
| 1 | Enabled | Auto | Link Down |
| 2 | Enabled | Auto | Link Down |
| 3 | Enabled | Auto | Link Down |
| 4 | Enabled | Auto | Link Down |
| 5 | Enabled | Auto | Link Down |
| 6 | Enabled | Auto | Link Down |
| 7 | Enabled | Auto | Link Down |
| 8 | Enabled | Auto | Link Down |
| 9 | Enabled | Auto | Link Down |
| 10 | Enabled | Auto | Link Down |
| 11 | Enabled | Auto | Link Down |
| 12 | Enabled | Auto | Link Down |
| 13 | Enabled | Auto | Link Down |
| 14 | Enabled | Auto | Link Down |
| 15 | Enabled | Auto | Link Down |
| 16 | Enabled | Auto | Link Down |
| 17 | Enabled | Auto | Link Down |
| 18 | Enabled | Auto | Link Down |
| 19 | Enabled | Auto | Link Down |
| 20 | Enabled | Auto | Link Down |
| 21 | Enabled | Auto | Link Down |
| 22 | Enabled | Auto | Link Down |
| 23 | Enabled | Auto | Link Down |
| 24 | Enabled | Auto | Link Down |
| 25 | Enabled | Auto | 1000M / Full / Off |
| 26 | Enabled | Auto | Link Down |
| 27 | Enabled | Auto | Link Down |
| 28 | Enabled | Auto | Link Down |

Port Setup window - Interface Config tab

| Parameter | Description |
|--------------|--|
| Interface | Select the port that you are going to configure by clicking the corresponding port in the below table (1~26 port). Port 25 and 26 are the uplink SFP/RJ-45 combo ports. |
| Status | This enables or disables the port. |
| Flow Control | This enables or disables the 802.3x flow control mechanism. |
| Duplex | Set the half or full duplex mode. |
| Speed | Set the speed of each port. Port 1~24 supports 10/100 Base-T while port 25 and 26 supports 10/100/1000. |
| NWay | The enables or disables auto-negotiation (NWay) on each port. |
| Priority | Set the priority (0~7) on the port basis. The packets from higher port priority will be transmitted faster than the packets with lower priority. |
| Jumbo Frame | <p>The normal Ethernet frame size cannot exceed the boundary of 1522 bytes; any packet more than this value will be fragmented into smaller data grams. Jumbo frames extend this maximum frame size of the Ethernet from 1518 up to 2048 bytes (including Ethernet headers).</p> <p>The more the frames that the network device has to handle, the less the TCP throughput and the more the CPU overhead. By allowing the frame to extend in size from 1518 to 2048 bytes jumbo frames, the Switch will handle lower number of frames or data grams.</p> |
| Modify | After all the configurations are set, click Modify to apply the configurations to the port. The field changed will update the content of the display window. However, the new settings do not take effect until the Submit button is clicked. |
| Submit | Click Submit to commit the settings. |
| Refresh | Before submitting the configurations, users can click Refresh to clear the current configurations. |

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

Runtime Status

The **Port Setup** window **Runtime Status** tab displays at-a-glance interface information for each port:

- **Ethernet Link:** The link is connected or not connected.
- **Duplex:** The port state is full duplex or half duplex.
- **Speed:** The port link speed.
- **NWay:** The port is enabled or disabled for auto-negotiation (NWay).
- **Flow Control:** The setting of the 802.3x flow control mechanism on both directions of the port.

Advanced Setting

Advanced Setting folders contain configuration windows for Bandwidth Control, DHCP Relay, IGMP Snooping, Link Aggregation, Loop Detection, MAC Forwarding (Dynamic MAC Addresses, Static MAC Addresses, and Static Multicast MAC Addresses), Mirroring, Port Isolation, QoS, Spanning Tree, Storm Control, and VLAN Configuration (Static VLAN and Dynamic VLAN).

Bandwidth Limitation

The **Bandwidth Limitation** window allows a rate limit to be applied on ingress or egress packets. Select an interface from the list and set the ingress/egress traffic based on the unit of 125 kbits per second (the maximum for Fast Ethernet is 800 x 125kbits/s), then click **Apply**.

Storm Control

Bandwidth Limitation

Bandwidth Limitation Settings

| Port | Ingress | Egress |
|---------------|--------------|--------------|
| From: 1 To: 1 | 0 * 8(Kbits) | 0 * 8(Kbits) |

(Disable:0, Giga Ethernet:1~128000)

Bandwidth Limitation Status

| Port | Ingress (Kb) | Egress (Kb) | Port | Ingress (Kb) | Egress (Kb) |
|------|--------------|-------------|------|--------------|-------------|
| 1 | 0 | 0 | 2 | 0 | 0 |
| 3 | 0 | 0 | 4 | 0 | 0 |
| 5 | 0 | 0 | 6 | 0 | 0 |
| 7 | 0 | 0 | 8 | 0 | 0 |
| 9 | 0 | 0 | 10 | 0 | 0 |
| 11 | 0 | 0 | 12 | 0 | 0 |
| 13 | 0 | 0 | 14 | 0 | 0 |
| 15 | 0 | 0 | 16 | 0 | 0 |
| 17 | 0 | 0 | 18 | 0 | 0 |
| 19 | 0 | 0 | 20 | 0 | 0 |
| 21 | 0 | 0 | 22 | 0 | 0 |
| 23 | 0 | 0 | 24 | 0 | 0 |
| 25 | 0 | 0 | 26 | 0 | 0 |
| 27 | 0 | 0 | 28 | 0 | 0 |

Click **Refresh** to display current settings of the Switch.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

DHCP Relay

The **DHCP Relay** window allows users to take advantage of DHCP Relay and DHCP Option 82 on the Switch. To use DHCP Relay, select **Enable** in the first field and set up a DHCP Server by entering the appropriate IP address in the second field, choosing **Add** from the DHCP VLAN drop-down menu, and entering a VLAN ID in the next field. To globally enable DHCP Option 82, toggle this setting to **Enable**. Please note that the Switch should have a static IP address if DHCP is enabled. The Switch allows up to three DHCP servers to be configured.

DHCP Relay

DHCP Relay Settings

State Disable ▾

VLAN State Add ▾

DHCP Server IP

Option 82 State Disable ▾

Option 82 Information

Apply
Refresh

DHCP Relay Status

| | |
|-----------------------|----------|
| DHCP Relay State | Disabled |
| Enabled on VLAN | None |
| DHCP Server IP | 0.0.0.0 |
| Option 82 State | Disabled |
| Option 82 Information | None |

DHCP Relay window

| Parameter | Description |
|----------------|--|
| DHCP Relay | Enable or disable the DHCP Relay for the Switch. |
| DHCP Server | Enter the DHCP Server IP address. |
| DHCP Option 82 | Globally Enable or Disable the DHCP Relay Option 82 for the Switch. |
| Information | The information for the DHCP Relay Option 82. If the DHCP Option 82 is enabled, the Switch will append the Information into the DHCP discover and request packets. |
| DHCP VLAN | Enable or disable the DHCP Relay on these VLANs. |
| Submit | Click Submit to commit the settings. |
| Refresh | Before submitting the configurations, users can click Refresh to clear the current configurations. |

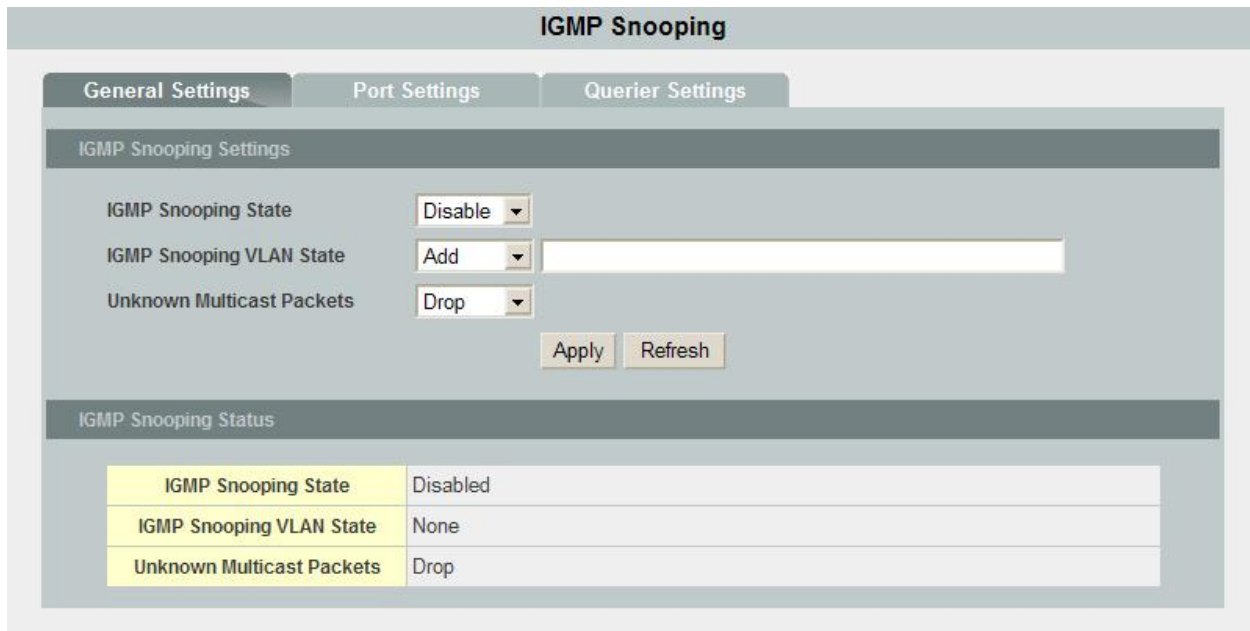
To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

IGMP Snooping

General Setting

Internet Group Management Protocol (IGMP) is a protocol through which hosts can register with their local router for multicast services. If there is more than one multicast router on a given sub-network, one of the routers is elected and assumes the responsibility of keeping track of group membership.

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.



| IGMP Snooping | |
|---|----------|
| General Settings | |
| IGMP Snooping Settings | |
| IGMP Snooping State | Disable |
| IGMP Snooping VLAN State | Add |
| Unknown Multicast Packets | Drop |
| <input type="button" value="Apply"/> <input type="button" value="Refresh"/> | |
| IGMP Snooping Status | |
| IGMP Snooping State | Disabled |
| IGMP Snooping VLAN State | None |
| Unknown Multicast Packets | Drop |

IGMP Snooping window – General Setting tab

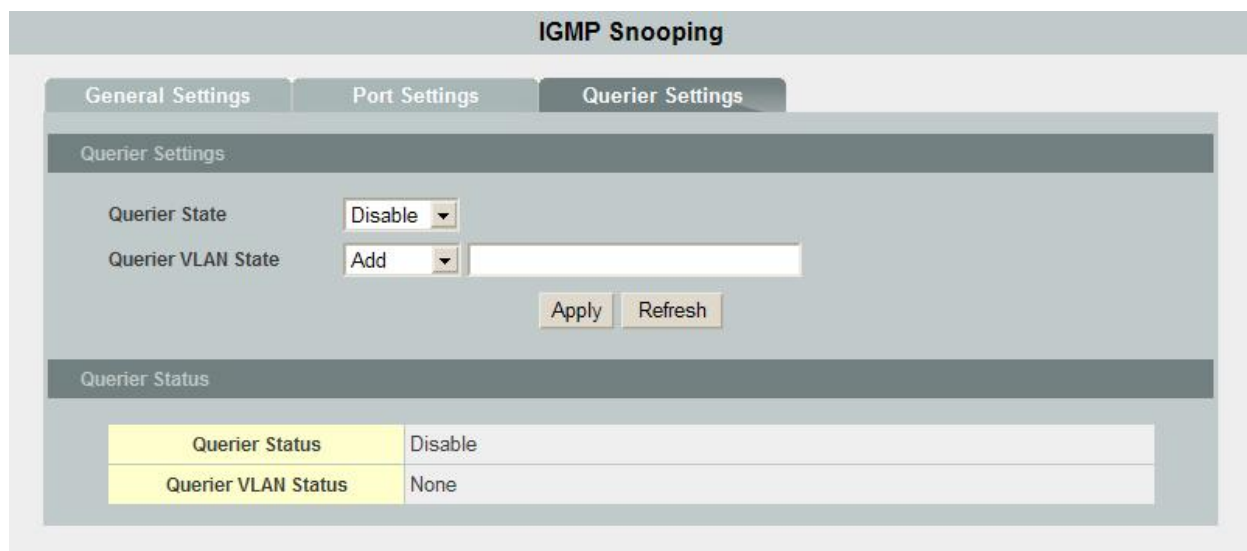
| Parameter | Description |
|-------------------------------|---|
| IGMP Snooping | IGMP Snooping is a global setting to enable or disable the IGMP queries for the Switch. |
| The Unknown Multicast Packets | Decide how to deal with unknown multicast packets, Drop or Flooding . |
| IGMP Snooping VLAN | IGMP Snooping VLAN enables or disables IGMP snooping on a specific VLAN. |

| | |
|---------|---|
| Submit | Click Submit to commit the settings. |
| Refresh | Before submitting the configurations, users can click Refresh to clear the current configurations. |

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

Querier Mode

The **Querier Mode** tab allows users to have the Switch forward IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router or server. Please note that IGMP snooping must also be enabled (see the previous tab).



IGMP Snooping window – Querier Mode tab

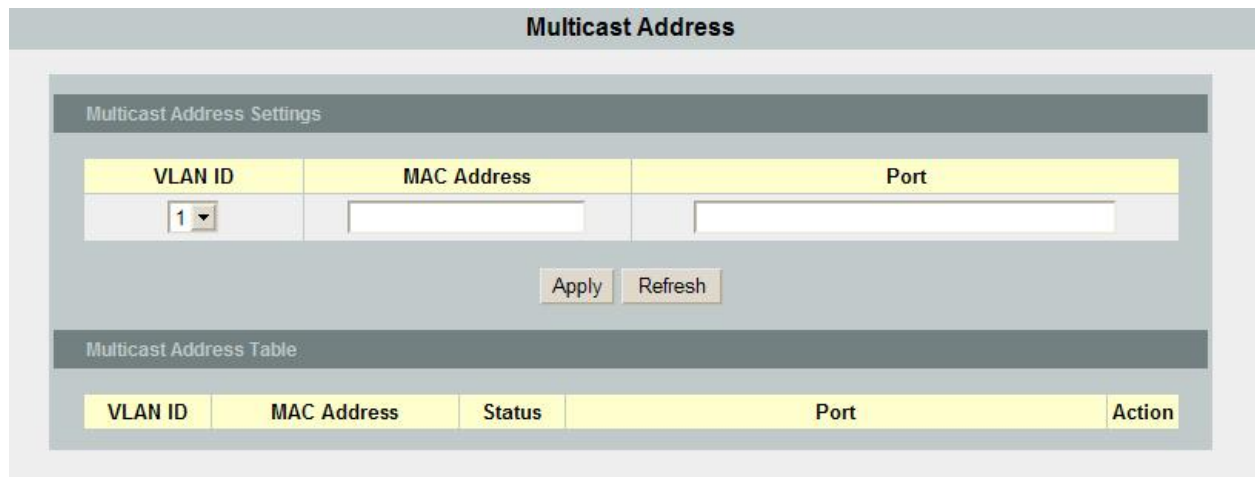
| Parameter | Description |
|----------------------------|--|
| IGMP Snooping Querier | IGMP Snooping Querier is a global setting to enable or disable IGMP queries for the Switch. |
| IGMP Snooping Querier VLAN | IGMP Snooping Querier VLAN enables or disables IGMP queries for a specific VLAN. If the IGMP Snooping Querier is enabled, the Switch is a Querier. Normally there is only one Querier per physical network. All multicast routers start up as a Querier on each attached network. If a multicast router hears a query message from a router with a lower IP address, it MUST become a Non-Querier on that network. If a router has not heard a query message from another router (Other Querier Present Interval), it resumes the role as Querier. Routers periodically (Query Interval) send a General Query on each attached network for which this router is the Querier to solicit membership information. On startup, a router SHOULD send [Startup Query Count] General Queries spaced closely together [Startup Query Interval] in order to quickly and reliably determine membership information. A General Query is addressed to the all-systems multicast group (224.0.0.1), has a Group Address field of 0, and has a Max Response Time of [Query Response Interval]. |
| Interface | Click the Interface to be modified in the table. |
| Querier Mode | Select the desired setting, Auto , Fixed , or Edge . Auto means the Switch |

| | |
|---------|--|
| | uses the port as an IGMP query port if the port receives IGMP query packets. Fixed means the Switch always treats the port(s) as IGMP query port(s). This is for when connecting an IGMP multicast server to the port(s). Edge means the Switch does not use the port as an IGMP query port. In this case, the Switch does not keep a record of an IGMP router being connected to this port and the Switch does not forward IGMP join or leave packets to this port. |
| Modify | Click the Querier Mode setting to be changed, and then click Modify . |
| Submit | Click Submit to commit the settings. |
| Refresh | Before submitting the configurations, users can click Refresh to clear the current configurations. |

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

Multicast MAC Address

The **Multicast MAC Address** tab allows users to see the updated status of the multicast members, both static and dynamic. Please note if the static entries occupy all 256 spaces, IGMP snooping does not work normally. The Switch only allows 256 Layer 2 multicast groups.



Multicast Address

Multicast Address Settings

| VLAN ID | MAC Address | Port |
|---------|-------------|------|
| 1 | | |

Apply Refresh

Multicast Address Table

| VLAN ID | MAC Address | Status | Port | Action |
|---------|-------------|--------|------|--------|
|---------|-------------|--------|------|--------|

IGMP Snooping window – Multicast MAC Address tab

Click **Refresh** to display current settings of the Switch.

Multicast VLAN Registration

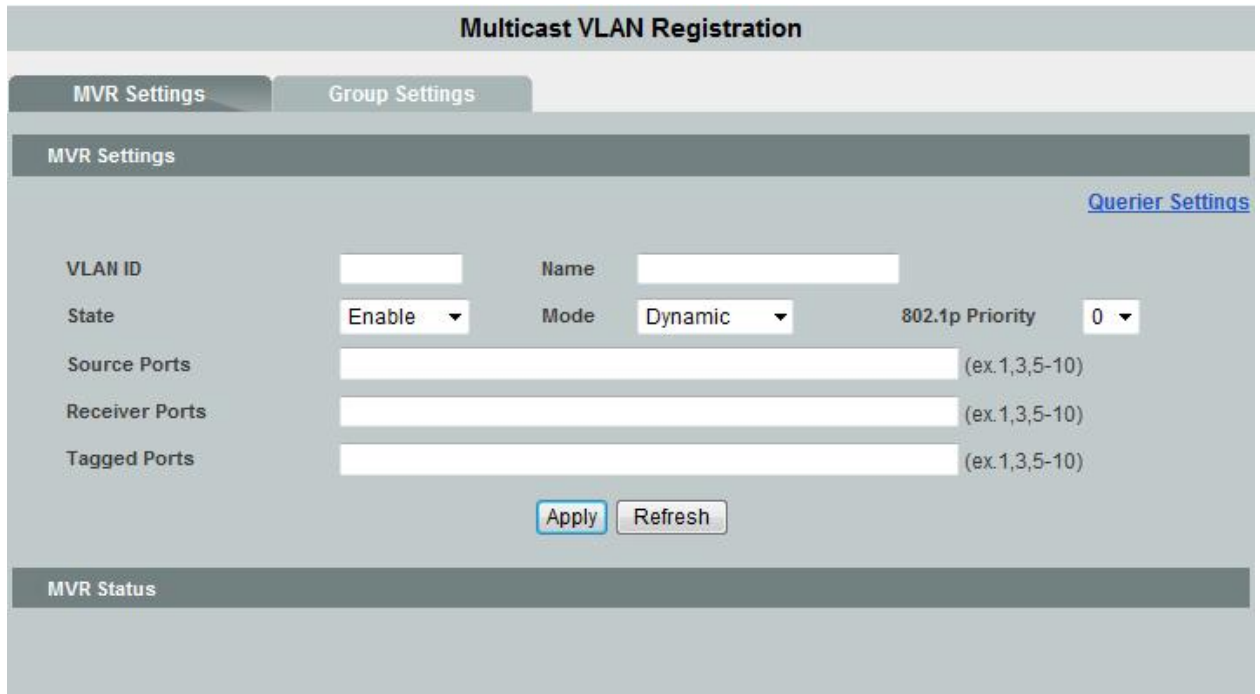
Multicast VLAN Registration (MVR) allows the network administrator to multicast packets from a particular VLAN in order to prevent multiple multicast streams being sent in the core network and degrading network performance.

On the Multicast VLAN Registration page, enter the VLAN ID and Name of the Multicast VLAN. Select the required mode (Dynamic or Compatible) and, optionally, the 802.1p (CoS) Priority of the VLAN. In Dynamic mode the Switch performs standard IGMP snooping. IGMP information packets are sent to the switch CPU, but multicast data packets are not sent to the CPU.

Dynamic mode allows the multicast router to run normally because the switch sends the IGMP join messages to the router, and the router only forwards multicast streams for a particular group to an interface if it has received a join message from the interface for the group. Receiver ports are treated as members of the multicast VLAN for MVR multicast control and data traffic. IGMP reports for MVR groups are sent out source ports in the multicast VLAN.

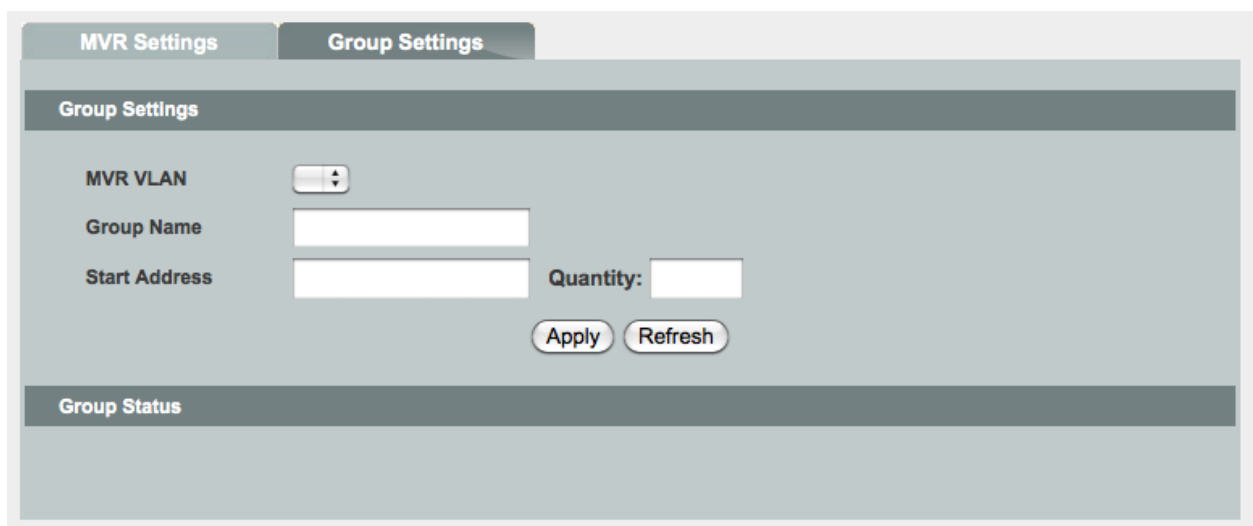
Compatible mode works the same as dynamic mode for all multicast data packets and IGMP query and leave packets. However, received IGMP report packets for MVR groups are not sent out on the multicast VLAN source ports. In contrast to dynamic mode, the switch does not send join messages to the router. The router must be statically configured for the interface to receive the multicast stream. Therefore, in this mode, MVR does not support dynamic membership joins on source ports.

Enter the Source, Receiver and Tagged Ports, and then click **Apply** to save.



The Group Settings tab allows the administrator to group IP addresses under a specific MVR.

Set the VLAN the group will belong to, followed by a Group Name and the Start Address and Quantity. For example, if IP addresses in the range from 192.168.2.101 to 192.168.2.150 then the Start Address should be 192.168.2.101, with the Quantity as 50. Once the correct numbers have been entered, click **Apply** to save.



Link Aggregation

Configuration

The **Configuration** tab allows user to set up static port trunking. Up to eight port trunk groups are supported. To start, select an entry from the table (the Group ID will be displayed in the first field), decide on the type of Load Balancing algorithm for the trunk group, **src-mac** (source MAC), **dst-mac** (destination MAC), **src-dst-mac** (source-destination MAC), **src-ip** (source IP), **dst-ip** (destination IP), or **src-dst-ip** (source-destination IP), choose which ports will be in the trunk (clicking **Attach All** selects every port while clicking **Detach All** clears every port) and then toggle Active to **Enable**.

To change a configured port trunk, select it, follow the same steps above, and then click **Modify**.

Click **Submit** to commit the settings. Click **Refresh** to display current settings of the Switch.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

LACP

The **LACP** tab allows users to set up Link Aggregation Control Protocol-compliant devices to negotiate the aggregated link in order that the group may be changed dynamically. Up to eight LACP port trunk groups of up to eight member ports per trunk are supported. The port trunk groups must first be set up on the previous tab.

To enable or disable LACP globally, toggle the first LACP field to **Enable**.

To enable and/or modify an individual LACP port, select the group from the table (the Group ID appears in the field above), make the desired change, and then click **Modify**.

Link Aggregation

StaticTrunk **LACP** Port Priority

LACP Settings

State:

System Priority:

Group LACP:

LACP Group Status

| Group ID | LACP State |
|----------|------------|
| 1 | Disabled |
| 2 | Disabled |
| 3 | Disabled |
| 4 | Disabled |
| 5 | Disabled |
| 6 | Disabled |
| 7 | Disabled |
| 8 | Disabled |

Link Aggregation window - LACP tab

Click **Submit** to commit the settings. Click **Refresh** to display current settings of the Switch. To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

Port Priority

The **Port Priority** tab provides users with a read-only view of the system priority for each port.

Link Aggregation

StaticTrunk
LACP
Port Priority

Port Priority Settings

Port

Priority

From: 1 To: 1

Apply
Refresh

Port Priority Status

| Port | Priority | Port | Priority |
|------|----------|------|----------|
| 1 | 32768 | 2 | 32768 |
| 3 | 32768 | 4 | 32768 |
| 5 | 32768 | 6 | 32768 |
| 7 | 32768 | 8 | 32768 |
| 9 | 32768 | 10 | 32768 |
| 11 | 32768 | 12 | 32768 |
| 13 | 32768 | 14 | 32768 |
| 15 | 32768 | 16 | 32768 |
| 17 | 32768 | 18 | 32768 |
| 19 | 32768 | 20 | 32768 |
| 21 | 32768 | 22 | 32768 |
| 23 | 32768 | 24 | 32768 |
| 25 | 32768 | 26 | 32768 |
| 27 | 32768 | 28 | 32768 |

Link Aggregation window – Port Priority tab

Click **Refresh** to display current settings of the Switch.

Loop Detection

The loop detection function sends special packets periodically to detect if the network is in loop. The Switch shuts down a port if it detects that packets loop back to the same port on the Switch.

Loop Detection

Loop Detection Settings

State Disable ▾

MAC Address 01:a0:c5:21:22:23

| Port | State | Action | Loop Recovery | Recovery Time (min) |
|-------------------|-----------|--------|---------------|---------------------|
| From: 1 ▾ To: 1 ▾ | Disable ▾ | None ▾ | Enable ▾ | 3 (Range: 1-60) |

Apply
Refresh

Loop Detection Status

| Port | State | Status | Loop Recovery | Recovery Time (min) |
|------|----------|--------|---------------|---------------------|
| 1 | Disabled | Normal | Enabled | 3 |
| 2 | Disabled | Normal | Enabled | 3 |
| 3 | Disabled | Normal | Enabled | 3 |
| 4 | Disabled | Normal | Enabled | 3 |
| 5 | Disabled | Normal | Enabled | 3 |
| 6 | Disabled | Normal | Enabled | 3 |
| 7 | Disabled | Normal | Enabled | 3 |
| 8 | Disabled | Normal | Enabled | 3 |
| 9 | Disabled | Normal | Enabled | 3 |
| 10 | Disabled | Normal | Enabled | 3 |
| 11 | Disabled | Normal | Enabled | 3 |
| 12 | Disabled | Normal | Enabled | 3 |
| 13 | Disabled | Normal | Enabled | 3 |
| 14 | Disabled | Normal | Enabled | 3 |
| 15 | Disabled | Normal | Enabled | 3 |
| 16 | Disabled | Normal | Enabled | 3 |
| 17 | Disabled | Normal | Enabled | 3 |
| 18 | Disabled | Normal | Enabled | 3 |
| 19 | Disabled | Normal | Enabled | 3 |
| 20 | Disabled | Normal | Enabled | 3 |
| 21 | Disabled | Normal | Enabled | 3 |
| 22 | Disabled | Normal | Enabled | 3 |
| 23 | Disabled | Normal | Enabled | 3 |
| 24 | Disabled | Normal | Enabled | 3 |
| 25 | Disabled | Normal | Enabled | 3 |
| 26 | Disabled | Normal | Enabled | 3 |
| 27 | Disabled | Normal | Enabled | 3 |
| 28 | Disabled | Normal | Enabled | 3 |

Loop Detection window

| Parameter | Description |
|-------------|--|
| Loop Detect | Set Loop Detect to Enable or Disable the global Loop Detection function on the Switch. Ethernet Loop Detection is used to detect Ethernet Loop conditions on active ports. |

| | |
|--------------|--|
| MAC | Use the default MAC address or enter a specific MAC as the destination MAC address for Ethernet Loop Detection. |
| Interface | The specific interface being configured for loop detection. |
| Status | Enable or Disable an interface on the table at the top of the window. |
| Retry Time | The retry time allows the Switch to retry more times before it blocks any specific ports with looping. Note: The default value is 0. |
| Retry Period | The Retry Period allows the Switch to retry the looping with delay. Note: The default value is 0 seconds. |
| Submit | Click Submit to commit the settings. |
| Refresh | Before submitting the configurations, users can click Refresh to clear the current configurations. |

To enable or disable loop detection on a specific port, first click the port from the list below, choose to enable or disable Port Loop Detect, and click **Modify** to make the setting.

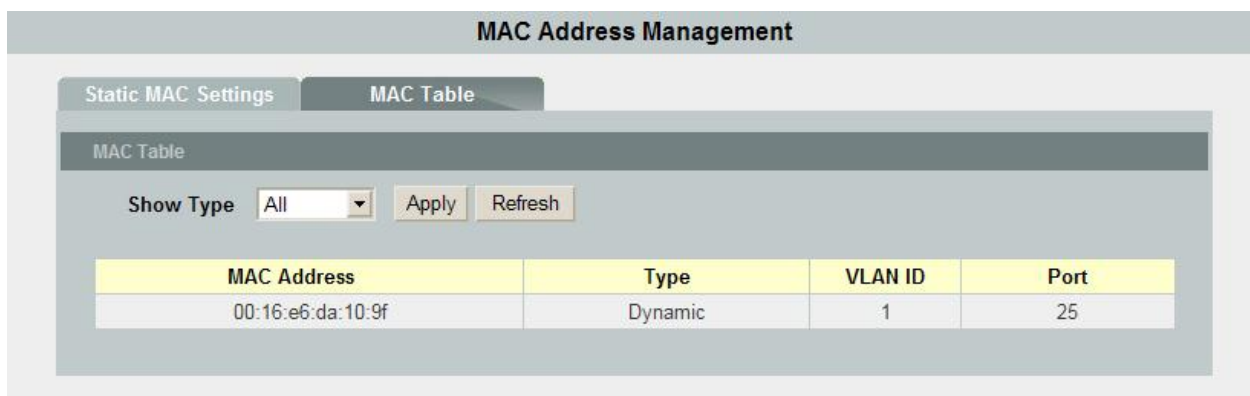
If the Switch detects a loop, it will automatically block that port. The user can manually unblock the port by choosing the port in the Port Unblocking table at the bottom of the window.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

MAC Forwarding

Dynamic MAC Addresses

The **Dynamic MAC Address** window allows the Switch's dynamic MAC address forwarding table to be displayed. When the Switch learns an association between a MAC address and a port number, it enters the information in the table. These entries are used to forward packets through the Switch.



MAC Address Management

Static MAC Settings | **MAC Table**

MAC Table

Show Type:

| MAC Address | Type | VLAN ID | Port |
|-------------------|---------|---------|------|
| 00:16:e6:da:10:9f | Dynamic | 1 | 25 |

Dynamic MAC Addresses window

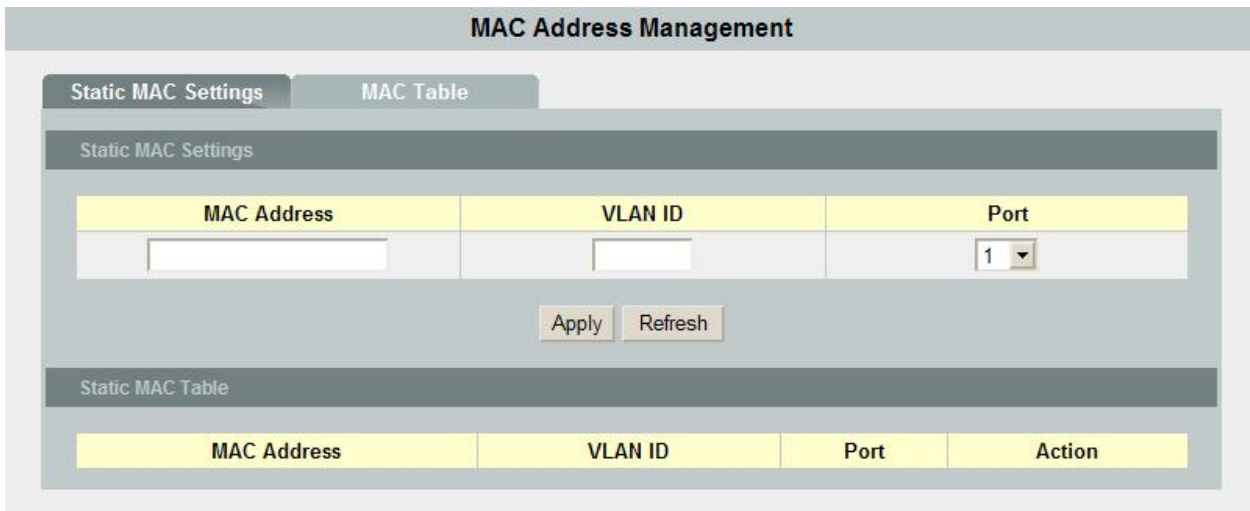
| Parameter | Description |
|-------------|---|
| Port | Tick the check box and enter a port or CPU . |
| VLAN ID | Tick the check box and enter a VLAN ID between 1 and 4094 . |
| MAC Address | Tick the check box and enter a MAC address. |

| | |
|------------|---|
| Query | Click to move to a sector of the database corresponding to a user-defined port, VLAN, or MAC Address. |
| Aging Time | Configure an aging time between 10 and 1000000 seconds |
| Submit | Click Submit to commit the settings. |
| Refresh | Before submitting the configurations, users can click Refresh to clear the current configurations. |

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

Static MAC Addresses

The **Static MAC Address** window allows users to add, remove, or modify a static MAC address from the Switch's static MAC address table. Enter a destination MAC Address, VLAN ID, and destination Port, and then click **Add**, or choose an entry from the table to either **Modify** or **Remove** it.



The screenshot shows the 'Static MAC Addresses' window. At the top is a header 'MAC Address Management'. Below it are two tabs: 'Static MAC Settings' (selected) and 'MAC Table'. Under 'Static MAC Settings', there is a form with three input fields: 'MAC Address', 'VLAN ID', and 'Port'. The 'Port' field has a dropdown menu showing '1'. Below these fields are 'Apply' and 'Refresh' buttons. At the bottom, there is a section titled 'Static MAC Table' which contains a table with four columns: 'MAC Address', 'VLAN ID', 'Port', and 'Action'.

Static MAC Addresses window

Click **Submit** to commit the settings. Click **Refresh** to display current settings of the Switch.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

Static Multicast MAC Addresses

The **Static Multicast Addresses** window allows users to add or remove static multicast MAC addresses from the Switch's static multicast MAC address table. Enter a MAC Address, VLAN ID, and Port (click **Detach All** to clear all the ports or **Attach All** to select all the ports), and then click **Add**, or choose an entry from the table to **Remove** it.

Multicast Address

Multicast Address Settings

| VLAN ID | MAC Address | Port |
|---------|--|--|
| 1 ▾ | <input style="width: 90%;" type="text"/> | <input style="width: 90%;" type="text"/> |

Multicast Address Table

| VLAN ID | MAC Address | Status | Port | Action |
|---------|-------------|--------|------|--------|
|---------|-------------|--------|------|--------|

Static Multicast MAC Addresses window

Click **Submit** to commit the settings. Click **Refresh** to display current settings of the Switch.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

Mirroring

Port Mirroring, together with a network traffic analyzer, helps to monitor network traffic. Users can monitor the selected ports for egress and/or ingress packets.

Port Mirroring

Port Mirroring Settings

State Disable ▾

Monitor Port 1 ▾

All Ports : Disable ▾

| Source Port | Mirror Mode | Source Port | Mirror Mode |
|-------------|---|-------------|---|
| 1 | Disable ▾ | 2 | Disable ▾ |
| 3 | Disable ▾ | 4 | Disable ▾ |
| 5 | Disable ▾ | 6 | Disable ▾ |
| 7 | Disable ▾ | 8 | Disable ▾ |
| 9 | Disable ▾ | 10 | Disable ▾ |
| 11 | Disable ▾ | 12 | Disable ▾ |
| 13 | Disable ▾ | 14 | Disable ▾ |
| 15 | Disable ▾ | 16 | Disable ▾ |
| 17 | Disable ▾ | 18 | Disable ▾ |
| 19 | Disable ▾ | 20 | Disable ▾ |
| 21 | Disable ▾ | 22 | Disable ▾ |
| 23 | Disable ▾ | 24 | Disable ▾ |
| 25 | Disable ▾ | 26 | Disable ▾ |
| 27 | Disable ▾ | 28 | Disable ▾ |

Apply
Refresh

Mirroring window

| Parameter | Description |
|---------------------|---|
| Mirror Mode | Enables or disables the mirror function for the selected group. |
| Monitor Port | Receives the copies of all the packets in the selected mirrored ports. The monitor port cannot belong to any link aggregation group. |
| Ingress/Egress/Both | Check the box of ingress/egress/both on the right. After you have the box checked, click on the port to be monitored. For example, if you want to monitor port 18's egress packets, you have to check the Egress box on the right first, and then click port 18. You will see an E on that port. |

| | |
|------------|---|
| Detach All | After you do some settings on the diagram, click Detach All , and all the settings on the diagram will be cleaned. |
| Attach All | After you check Ingress, Egress or Both, click Attach All , and the setting will be attached to all ports on the diagram. |
| Modify | Click Modify to apply the settings on the diagram to the ports. The field changed will update the content of the display window. |

Click **Submit** to set the changes to the connected Switch. Click **Refresh** to show the values of the Switch.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

Port Isolation

Port isolation allows the user to manage connections between ports. Select a port and then click the port on the front panel display to mark "V," meaning the port can forward packets to ports marked "V" only.

Port Isolation

Port Isolation Settings

Port

From:
To:

Egress Port :

☐ Select All
☐ Deselect All

☐ 1 ☐ 3 ☐ 5 ☐ 7

☐ 9 ☐ 11 ☐ 13 ☐ 15

☐ 17 ☐ 19 ☐ 21 ☐ 23

☐ 25 ☐ 27

☐ 2 ☐ 4 ☐ 6 ☐ 8

☐ 10 ☐ 12 ☐ 14 ☐ 16

☐ 18 ☐ 20 ☐ 22 ☐ 24

☐ 26 ☐ 28

☒ 0 (CPU)

Apply

Refresh

Port Isolation Status

| | Egress Port | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------|-------------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--|
| Port | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | |
| 1 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 2 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 3 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 4 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 5 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 6 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 7 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 8 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 9 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 10 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 11 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 12 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 13 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 14 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 15 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 16 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 17 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 18 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 19 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 20 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 21 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 22 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 23 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 24 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 25 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 26 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 27 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |
| 28 | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | V | |

Port Isolation window

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

Note: Port 0 is for packets to transmit to the CPU. If port 0 is unchecked under port ID 1, the user cannot configure the settings through port 1.

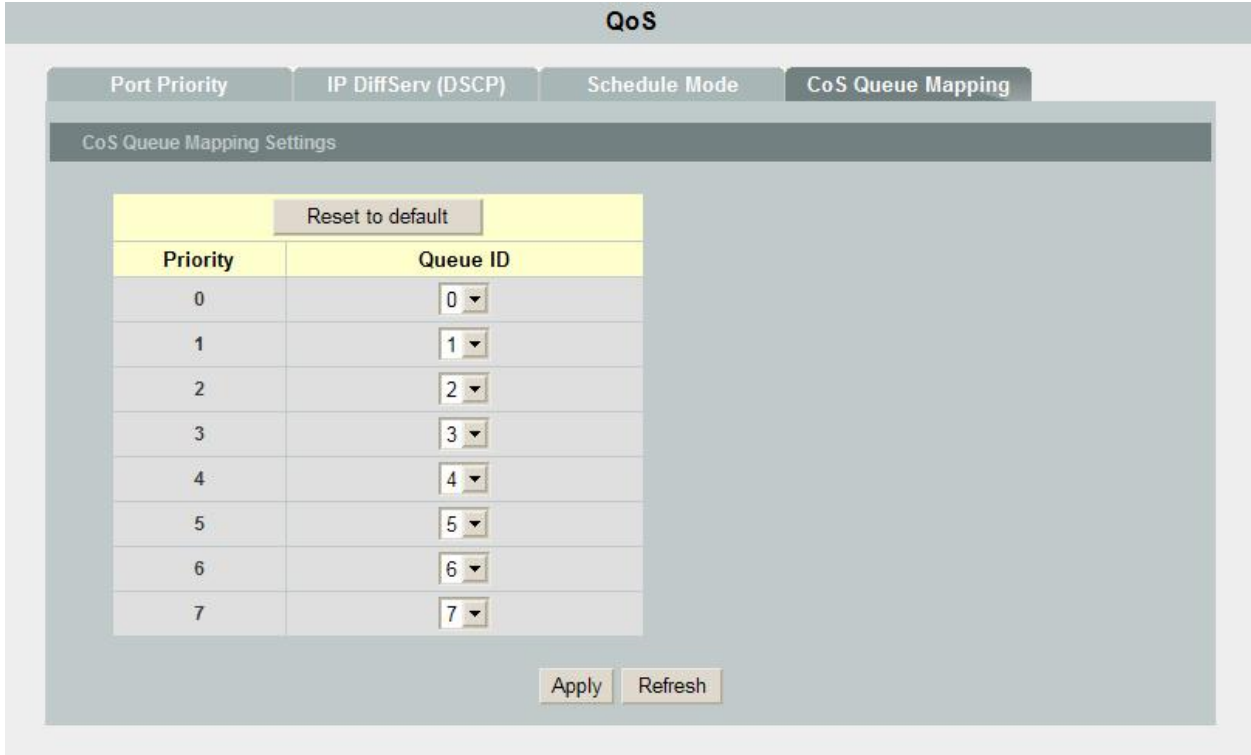
QoS

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When a user configures the QoS feature, specific network traffic can be selected and prioritized according to relative importance. Use congestion-management and congestion-avoidance techniques to give preferential treatment. Implementing QoS in a network makes network performance more predictable and bandwidth utilization more effective.

CoS Queue Mapping

The Switch supports four egress queues for each port with a strict priority scheduler. That is, each CoS value can map into one of the four queues. Queue three has the highest priority to transmit packets.



QoS

Port Priority | IP DiffServ (DSCP) | Schedule Mode | **CoS Queue Mapping**

CoS Queue Mapping Settings

Reset to default

| Priority | Queue ID |
|----------|----------|
| 0 | 0 |
| 1 | 1 |
| 2 | 2 |
| 3 | 3 |
| 4 | 4 |
| 5 | 5 |
| 6 | 6 |
| 7 | 7 |

Apply Refresh

QoS window – CoS Queue Mapping tab

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

802.1p Priority

Each port has four egress queues. These queues can either be configured with the Weighted Round Robin (WRR) scheduling algorithm or High First (SPQ). The Strict Priority Queue must be empty before the WRR queues are serviced. You can use the strict priority queue for mission-critical and time-sensitive traffic. There are two options:

- **High First (SPQ):** Packet's priority depends on its CoS value. This queuing processes as many packets as possible in Queue[3] before processing any packets in Queue[2], then processes as many packets as possible in Queue[2] before processing any packets in Queue[1] or Queue[0].
- **Weighted Round Robin (WRR):** If WRR scheduling algorithm is enabled, the ratio of the weights is the ratio of the bandwidth. For example, by default, Queue[3] has the weight value of eight. This means Queue[3] has eight times the bandwidth as Queue[0]. After Queue[3] uses up all the bandwidth, the next queue (queue[2]) moves up and shares four times the bandwidth of queue [0].

QoS

Port Priority
IP DiffServ (DSCP)
Schedule Mode
CoS Queue Mapping

Port Priority Settings

All Ports 802.1p priority : -

| Port | 802.1p priority | Port | 802.1p priority |
|------|---|------|---|
| 1 | 0 | 2 | 0 |
| 3 | 0 | 4 | 0 |
| 5 | 0 | 6 | 0 |
| 7 | 0 | 8 | 0 |
| 9 | 0 | 10 | 0 |
| 11 | 0 | 12 | 0 |
| 13 | 0 | 14 | 0 |
| 15 | 0 | 16 | 0 |
| 17 | 0 | 18 | 0 |
| 19 | 0 | 20 | 0 |
| 21 | 0 | 22 | 0 |
| 23 | 0 | 24 | 0 |
| 25 | 0 | 26 | 0 |
| 27 | 0 | 28 | 0 |

Apply
Refresh

QoS window - 802.1p Priority tab

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

Spanning Tree

This section configures two types of Spanning Tree Protocol, Spanning Tree Protocol and Rapid Spanning Tree Protocol.

STP Status

The **STP Status** tab enables or disables STP. Two modes can be enabled, STP and RSTP.

The Spanning Tree Protocol (STP) is used for detecting and disabling network loops, and to provide backup links between switches, bridges or routers. This allows the Switch to communicate and interact with other bridging devices (i.e. STA-compliant devices) in a network to ensure that only one route exists between any two stations, and it provides redundant or backup links that automatically takeover when a primary link goes down.

Rapid Spanning Tree Protocol (RSTP) is a refinement of STP. RSTP provides faster spanning tree convergence than STP after a topology change. While STP can take 30 to 50 seconds to

respond to a topology change, RSTP is typically able to respond to changes within a second.

Spanning Tree Protocol

General Settings
Port Parameters
STP Status

Current Root Status

| | | | | |
|-------------|----------|---------|------------|---------------|
| MAC Address | Priority | Max Age | Hello Time | Forward Delay |
|-------------|----------|---------|------------|---------------|

Current Bridge Status

| | | | | | | |
|-------------|----------|---------|------------|---------------|-----------|-----------|
| MAC Address | Priority | Max Age | Hello Time | Forward Delay | Path Cost | Root Port |
|-------------|----------|---------|------------|---------------|-----------|-----------|

Spanning Tree window – STP Status tab

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

Current Roots

The **Current Roots** tab displays information of the current root bridge, which includes:

- MAC Address of root bridge
- Priority of root bridge
- Maximum age of root bridge
- Hello time of root bridge
- Forwarding delay timer of root bridge

Path Cost of Root Bridge Telnet

Activate your workstation's command prompt program (like Putty) and access your Switch via the Internet by typing in the correct IP address (the factory default IP address is 192.168.0.254 – connect directly via the console port to configure a unique IP address). A command prompt program like Putty will allow you to access the Switch via Telnet.

Bridge Parameters

The **Bridge Parameters** tab allows users to configure spanning tree parameters for BPDU transmission.

The screenshot shows the 'Spanning Tree Protocol' configuration window with the 'Bridge Parameters' tab selected. The window has three tabs: 'General Settings', 'Port Parameters', and 'STP Status'. Under 'Spanning Tree Protocol Settings', the 'State' is set to 'Disable' and the 'Mode' is set to 'RSTP'. The 'Bridge Parameters' section contains the following fields:

| Parameter | Value |
|--------------|-------|
| Forward Time | 15 |
| Max Age | 20 |
| Hello Time | 2 |
| Priority | 32768 |
| Path Cost | Short |

At the bottom of the window are 'Apply' and 'Refresh' buttons.

Spanning Tree window – Bridge Parameters tab

| Parameter | Description |
|---------------|--|
| Priority | Set the bridge priority. The range is between 0 (the highest priority) and 61440 (the lowest priority). Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will become the root device. |
| Forward Delay | Set the Forward Delay. The range is from 4 to 30 seconds. This is the maximum time (in seconds) the root device will wait before changing states (i.e., listening to learning to forwarding). |
| Max Age | Set the waiting time for receiving packets before attempting to reconfigure the link. The range is from 6 to 40 seconds. |
| Hello Time | Set the time at which the root switch transmits a configuration message. The range is from 1 to 10 seconds. |

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

Port Parameters

The **Port Parameters** tab allows users to show and edit the current configurations for each port. Select a port then edit it. Click the port in the below table first, and then click **Modify** to change the port setting for spanning tree.

Spanning Tree Protocol

General Settings
Port Parameters
STP Status

Port Parameters Settings

| Port | Path Cost | Port Priority | Edge Port | BPDU Filter | BPDU Guard |
|---|--|--|---|---|---|
| From: 1 To: 1 | <input style="width: 100px;" type="text"/> | <input style="width: 100px;" type="text"/> | Disable | Disable | Disable |

Apply
Refresh

Port Status

| Port | Status | Path Cost | Port Priority | Edge Port | BPDU Filter | BPDU Guard |
|------|------------|-----------|---------------|-----------|-------------|------------|
| 1 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 2 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 3 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 4 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 5 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 6 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 7 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 8 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 9 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 10 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 11 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 12 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 13 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 14 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 15 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 16 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 17 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 18 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 19 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 20 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 21 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 22 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 23 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 24 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 25 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 26 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 27 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |
| 28 | Discarding | 250 | 128 | Disabled | Disabled | Disabled |

Spanning Tree window – Port Parameters tab

| Parameter | Description |
|-----------|---|
| Path Cost | The valid value is from 1 to 200000000 . Higher cost paths are more likely to be blocked by STP if a network loop is detected. |
| 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. This function can only be enabled in RSTP mode. |
| Priority | Set the port priority in the switch. Low numeric value indicates a high priority. A port with lower priority is more likely to be blocked by STP if a network loop is detected. The valid value is from 0 to 240 . |

After the configurations are done, click **Modify** to apply the configurations to the port. The field you change will update the content of the display window.

Click **Submit** to commit the settings. Click **Refresh** to display current settings of the Switch.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

Storm Control

Storm Control protects the Switch bandwidth from flooding packets, including broadcast packets, multicast packets, and destination lookup failure (DLF). The Rate 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 from the list and assign the desirable settings, then click **Modify**.

Rate Limitation

Storm Control
Bandwidth Limitation

Storm Control Settings

Port

From: 1
To: 1

Rate

0
(pps)

Type

(Disable: 0, Giga Ethernet: 1~1488000)

Apply
Refresh

Storm Control Status

| Port | Rate (pps) | Type | Port | Rate (pps) | Type |
|------|------------|------|------|------------|------|
| 1 | 0 | - | 2 | 0 | - |
| 3 | 0 | - | 4 | 0 | - |
| 5 | 0 | - | 6 | 0 | - |
| 7 | 0 | - | 8 | 0 | - |
| 9 | 0 | - | 10 | 0 | - |
| 11 | 0 | - | 12 | 0 | - |
| 13 | 0 | - | 14 | 0 | - |
| 15 | 0 | - | 16 | 0 | - |
| 17 | 0 | - | 18 | 0 | - |
| 19 | 0 | - | 20 | 0 | - |
| 21 | 0 | - | 22 | 0 | - |
| 23 | 0 | - | 24 | 0 | - |
| 25 | 0 | - | 26 | 0 | - |
| 27 | 0 | - | 28 | 0 | - |

Storm Control window

Click **Submit** to commit the settings. Click **Refresh** to display current settings of the Switch.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

VLAN Configuration

Static VLAN

VLAN Member Setting

The **VLAN Member Setting** tab allows users to set up VLANs on the Switch. Users can create

up to 4094 VLAN groups and display the VLAN groups on this tab.

VLAN

VLAN Settings Tag Settings Port Settings

VLAN Settings

| VLAN ID | VLAN Name | Member Port |
|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> |

Apply Refresh

VLAN List

| VLAN ID | VLAN Name | VLAN Status | Member Port | Action |
|---------|-----------|-------------|-------------|--------|
| 1 | VLAN1 | Static | 1-28 | Delete |

Static VLAN window – VLAN Member Setting tab

To create a new VLAN, the user can enter the VLAN ID, Name and select the ports belonging to this VLAN, and then click **Add**. The VLAN will display in the below table. The **VLAN Member Setting** will not become *Permanent* from *Unused* before you submit the settings. Or you can use **Attach All/Detach All** for quick configuration.

To modify the existing settings, select the VLAN from the list below, and then click **Modify** after the settings are reconfigured.

To remove a VLAN, select the VLAN from the list at the bottom of the window and then click the **Remove** button. VLAN1 is the default VLAN, which is created by the system. It cannot be removed. This feature prevents the Switch from malfunctioning. Users can remove any existing VLAN except VLAN1.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

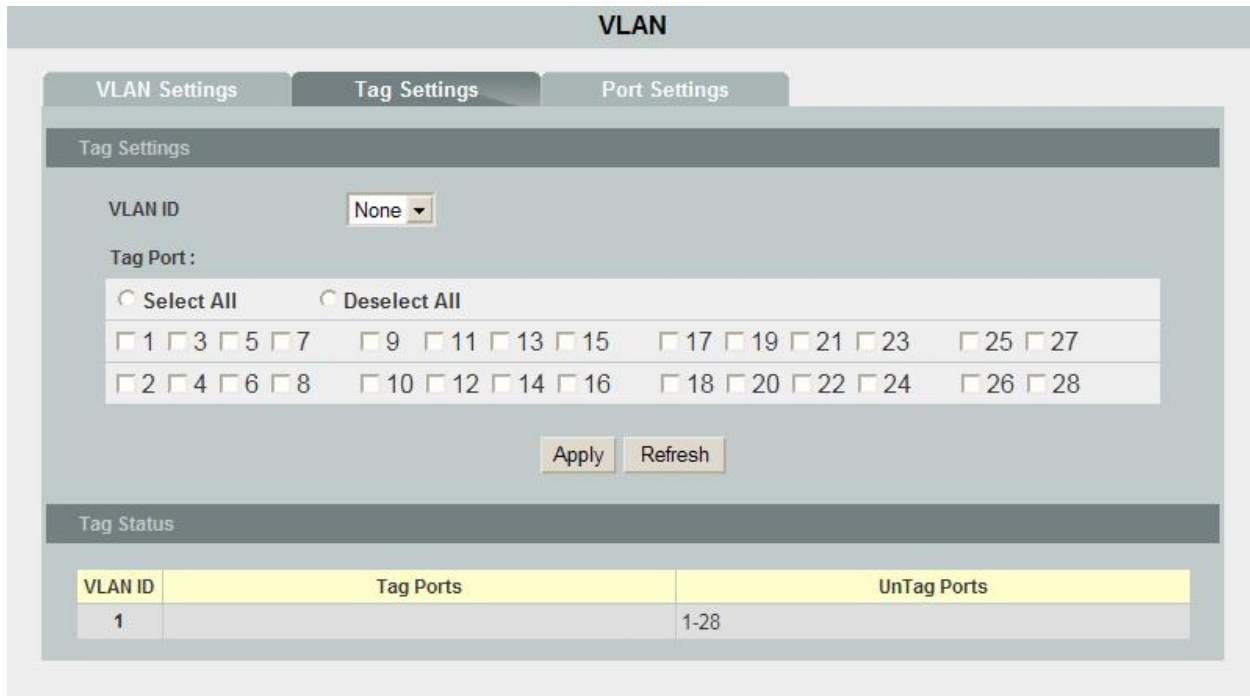
Tag Setting

The **Tag Setting** tab allows users to assign the port to be a tagged port or an untagged port. First, select the existing VLAN from the list at the bottom of the window. Then click on the port on the picture to determine the port to be tagged or untagged.

“**U**” **type**: An un-tagging port that will remove VLAN tags from the transmitted packets.

“**T**” **type**: All packets transmitted from this port will be tagged.

Click **Modify** to commit the settings, and the new settings will display in the below window. The untagged ports are displayed next to VLAN Status. Drag the bar to the right to see Tagged ports.



VLAN

VLAN Settings **Tag Settings** Port Settings

Tag Settings

VLAN ID: None ▾

Tag Port:

☐ Select All ☐ Deselect All

| | | | | | | | | | | | | | |
|----------------------------|----------------------------|----------------------------|----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|
| <input type="checkbox"/> 1 | <input type="checkbox"/> 3 | <input type="checkbox"/> 5 | <input type="checkbox"/> 7 | <input type="checkbox"/> 9 | <input type="checkbox"/> 11 | <input type="checkbox"/> 13 | <input type="checkbox"/> 15 | <input type="checkbox"/> 17 | <input type="checkbox"/> 19 | <input type="checkbox"/> 21 | <input type="checkbox"/> 23 | <input type="checkbox"/> 25 | <input type="checkbox"/> 27 |
| <input type="checkbox"/> 2 | <input type="checkbox"/> 4 | <input type="checkbox"/> 6 | <input type="checkbox"/> 8 | <input type="checkbox"/> 10 | <input type="checkbox"/> 12 | <input type="checkbox"/> 14 | <input type="checkbox"/> 16 | <input type="checkbox"/> 18 | <input type="checkbox"/> 20 | <input type="checkbox"/> 22 | <input type="checkbox"/> 24 | <input type="checkbox"/> 26 | <input type="checkbox"/> 28 |

Apply Refresh

Tag Status

| VLAN ID | Tag Ports | UnTag Ports |
|---------|-----------|-------------|
| 1 | | 1-28 |

Static VLAN window – Tag Setting tab

Click **Submit** to save changes to RAM memory. Click **Refresh** to view the effect of the changes.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

VLAN Port Setting

The **VLAN Port Setting** tab allows users to set a port VLAN ID (PVID) per port. Set the VLAN ID between 1 and 4094. The VLAN ID is assigned to all untagged frames received on this port.

Set Ingress Check to enabled or disabled. When enabled, the Switch discards incoming frames on a port for VLANs that do not include this port in its member set.

Click the interface below, enter the PVID, and click **Modify** to make the changes.

VLAN

VLAN Settings
Tag Settings
Port Settings

Port Settings

Port
 From: To:

PVID

Acceptable Frame

Port Status

| Port | PVID | Acceptable Frame | Port | PVID | Acceptable Frame |
|------|------|------------------|------|------|------------------|
| 1 | 1 | All | 2 | 1 | All |
| 3 | 1 | All | 4 | 1 | All |
| 5 | 1 | All | 6 | 1 | All |
| 7 | 1 | All | 8 | 1 | All |
| 9 | 1 | All | 10 | 1 | All |
| 11 | 1 | All | 12 | 1 | All |
| 13 | 1 | All | 14 | 1 | All |
| 15 | 1 | All | 16 | 1 | All |
| 17 | 1 | All | 18 | 1 | All |
| 19 | 1 | All | 20 | 1 | All |
| 21 | 1 | All | 22 | 1 | All |
| 23 | 1 | All | 24 | 1 | All |
| 25 | 1 | All | 26 | 1 | All |
| 27 | 1 | All | 28 | 1 | All |

Static VLAN window – VLAN Port Setting tab

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

Dynamic VLAN

GVRP Mode

The **GVRP Mode** tab allows users to determine whether the Switch will share VLAN configuration information with other GARP VLAN Registration Protocol-enabled switches. Tick the GVRP Enable check box to enable the global GVRP function, select the desired Interface, toggle the State between **Enabled** and **Disabled**, and determine the Registration to be used, **Normal** or **Forbidden**.

To change an entry in this table, select it (the Interface appears In the field above), make the desired changes, and then click **Modify**.

GARP VLAN Registration Protocol

GVRP
GARP Timer

GVRP Settings

GVRP State Disable

Port
From: 1 To: 1

State
Disable

Registration Mode
Normal

Apply
Refresh

GVRP Status

| Port | State | Registration Mode | Port | State | Registration Mode |
|------|----------|-------------------|------|----------|-------------------|
| 1 | Disabled | - | 2 | Disabled | - |
| 3 | Disabled | - | 4 | Disabled | - |
| 5 | Disabled | - | 6 | Disabled | - |
| 7 | Disabled | - | 8 | Disabled | - |
| 9 | Disabled | - | 10 | Disabled | - |
| 11 | Disabled | - | 12 | Disabled | - |
| 13 | Disabled | - | 14 | Disabled | - |
| 15 | Disabled | - | 16 | Disabled | - |
| 17 | Disabled | - | 18 | Disabled | - |
| 19 | Disabled | - | 20 | Disabled | - |
| 21 | Disabled | - | 22 | Disabled | - |
| 23 | Disabled | - | 24 | Disabled | - |
| 25 | Disabled | - | 26 | Disabled | - |
| 27 | Disabled | - | 28 | Disabled | - |

Dynamic VLAN window – GVRP Mode tab

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

GARP Timer

The **GARP Timer** tab allows users to display and configure General Attribute Registration Protocol (GARP) timers, including Join Time, Leave Time, and Leave All Time.

To change an entry on this table, select it, make the desired changes in the three fields at the top of the window, and then click **Modify**.

GARP VLAN Registration Protocol

GVRP
GARP Timer

GARP Timer Settings

| Port | Join Time | Leave Time | Leave All Time |
|---|--|--|--|
| From: 1 To: 1 | 20 | 60 | 1000 |

2*Join Time < Leave Time < Leave All Time
Time unit:(centi-sec)

Apply
Refresh

GARP Timer Status

| Port | Join Time | Hold Time | Leave Time | Leave All Time |
|------|-----------|-----------|------------|----------------|
| 1 | 20 | 10 | 60 | 1000 |
| 2 | 20 | 10 | 60 | 1000 |
| 3 | 20 | 10 | 60 | 1000 |
| 4 | 20 | 10 | 60 | 1000 |
| 5 | 20 | 10 | 60 | 1000 |
| 6 | 20 | 10 | 60 | 1000 |
| 7 | 20 | 10 | 60 | 1000 |
| 8 | 20 | 10 | 60 | 1000 |
| 9 | 20 | 10 | 60 | 1000 |
| 10 | 20 | 10 | 60 | 1000 |
| 11 | 20 | 10 | 60 | 1000 |
| 12 | 20 | 10 | 60 | 1000 |
| 13 | 20 | 10 | 60 | 1000 |
| 14 | 20 | 10 | 60 | 1000 |
| 15 | 20 | 10 | 60 | 1000 |
| 16 | 20 | 10 | 60 | 1000 |
| 17 | 20 | 10 | 60 | 1000 |
| 18 | 20 | 10 | 60 | 1000 |
| 19 | 20 | 10 | 60 | 1000 |
| 20 | 20 | 10 | 60 | 1000 |
| 21 | 20 | 10 | 60 | 1000 |
| 22 | 20 | 10 | 60 | 1000 |
| 23 | 20 | 10 | 60 | 1000 |
| 24 | 20 | 10 | 60 | 1000 |
| 25 | 20 | 10 | 60 | 1000 |
| 26 | 20 | 10 | 60 | 1000 |
| 27 | 20 | 10 | 60 | 1000 |
| 28 | 20 | 10 | 60 | 1000 |

Dynamic VLAN window – GARP Timer tab

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

Q-in-Q

Q-in-Q, IEEE 802.1ad, also known as **stackable VLANs**, is a function allowing a group of VLANs to be wrapped in a carrier VLAN for security and ease of management. This involves “double-tagging” a frame with two VLAN IDs; the ID of the original VLAN (usually assigned at the Layer 2 Switch) and the tag of the Tag VLAN (usually assigned at the Layer 3 switch).

To enable VLAN Stacking, select the VLAN Stacking tab then select Enable from the Action drop-down menu. Select the ports to be included and the role this stack (tunnel) will play (choose between Normal, Access, and Tunnel). The Normal setting uses 802.1q standard VLAN tagging; Access identifies ingress ports that then have the Tag (wrapper) VLAN ID added to the frame header. Tunnel is used for Egress ports, so the tagged VLAN acts as an aggregated VLAN, incorporating all the stacked VLANs within the group. If the Tunnel role is selected, a Tag Protocol Identifier (TPID) must also be chosen for the Tag VLAN. Once the appropriate selections have been made, click **Apply** to save.

Q-in-Q

VLAN Stacking
Port-based Q-in-Q
Selective Q-in-Q

VLAN Stacking Setting

Action Disable ▾

Port
 From: 1 ▾ To: 1 ▾

Role
Normal ▾

Tunnel TPID

8100
(0000~ffff)

Apply
Refresh

VLAN Stacking Status

| Port | Role | Tunnel TPID | Port | Role | Tunnel TPID |
|------|--------|-------------|------|--------|-------------|
| 1 | Normal | 8100 | 2 | Normal | 8100 |
| 3 | Normal | 8100 | 4 | Normal | 8100 |
| 5 | Normal | 8100 | 6 | Normal | 8100 |
| 7 | Normal | 8100 | 8 | Normal | 8100 |
| 9 | Normal | 8100 | 10 | Normal | 8100 |
| 11 | Normal | 8100 | 12 | Normal | 8100 |
| 13 | Normal | 8100 | 14 | Normal | 8100 |
| 15 | Normal | 8100 | 16 | Normal | 8100 |
| 17 | Normal | 8100 | 18 | Normal | 8100 |
| 19 | Normal | 8100 | 20 | Normal | 8100 |
| 21 | Normal | 8100 | 22 | Normal | 8100 |
| 23 | Normal | 8100 | 24 | Normal | 8100 |
| 25 | Normal | 8100 | 26 | Normal | 8100 |
| 27 | Normal | 8100 | 28 | Normal | 8100 |

Port-based Q-in-Q assigns all incoming frames on a particular port to a certain Service Provider VLAN ID (SPVID). Select the port range required, the SPVID tag to be added, and the priority (based on priority levels set in the CoS menu option). Click **Apply** to save.

VLAN Stacking
Port-based Q-in-Q
Selective Q-in-Q

Port-based Q-in-Q

| Port | SPVID | Priority |
|---|---|--------------------------------|
| From: <input type="text" value="1"/> To: <input type="text" value="1"/> | <input type="text" value="1"/> (1~4094) | <input type="text" value="0"/> |

Port-based Q-in-Q Status

| Port | SPVID | Priority | Port | SPVID | Priority |
|------|-------|----------|------|-------|----------|
| 1 | 1 | 0 | 2 | 1 | 0 |
| 3 | 1 | 0 | 4 | 1 | 0 |
| 5 | 1 | 0 | 6 | 1 | 0 |
| 7 | 1 | 0 | 8 | 1 | 0 |
| 9 | 1 | 0 | 10 | 1 | 0 |
| 11 | 1 | 0 | 12 | 1 | 0 |
| 13 | 1 | 0 | 14 | 1 | 0 |
| 15 | 1 | 0 | 16 | 1 | 0 |
| 17 | 1 | 0 | 18 | 1 | 0 |
| 19 | 1 | 0 | 20 | 1 | 0 |
| 21 | 1 | 0 | 22 | 1 | 0 |
| 23 | 1 | 0 | 24 | 1 | 0 |
| 25 | 1 | 0 | 26 | 1 | 0 |
| 27 | 1 | 0 | 28 | 1 | 0 |

The **Selective Q-in-Q** tab allows the administrator to assign an outer Tag VLAN based on incoming VLAN IDs from particular ports. First, name the Selective Q-in-Q group, followed by the member ports for this group. Next, select the Customer VLAN IDs to be covered by this group, for example CVIDs 100 to 299. Choose a Service Provider VLAN ID (SPVID) for this group, select a priority level (as defined in the CoS settings) and select **Enable** from the **Action** drop-down menu. Click **Apply** to save.

VLAN Stacking

Port-based Q-in-Q

Selective Q-in-Q

Selective Q-in-Q Setting

Name

Member Ports

(ex. 1,3,5-10)

CVID Range

(ex. 100-299 or 300-300)

SPVID

(1~4094)

Priority

0

Action

Disable

Apply

Refresh

Selective Q-in-Q Status

| No. | Name | Member Ports | CVID Range | SPVID | Priority | Action | Delete |
|-----|------|--------------|------------|-------|----------|--------|--------|
|-----|------|--------------|------------|-------|----------|--------|--------|

Security

Security folders contain configuration windows for DHCP Binding Table, DHCP Snooping, ARP Inspection, and Access Control List.

DHCP Binding Table

The DHCP snooping feature dynamically builds and maintains the database using information extracted from intercepted DHCP messages. In this screen, you can see dynamic binding table with leased IP addresses. The dynamic binding table is stored in volatile memory. If the Switch restarts, it loads static bindings from permanent memory but loses the dynamic bindings.

Apart from the dynamic binding, you can manually add the static binding using the DHCP Binding Configuration.

After all settings are done, click **Add** to commit the rule. If you want to delete an existing rule, click it from the list, and click **Remove**.

Click **Submit** to save changes to RAM memory. Click **Refresh** to view the effect of the changes.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

DHCP Snooping

DHCP Snooping Setting

DHCP snooping is a DHCP security feature that provides security by filtering un-trusted DHCP messages and by building and maintaining a DHCP snooping binding table. DHCP snooping acts like a firewall between un-trusted hosts and DHCP servers. By using DHCP snooping, unauthorized DHCP packets can be filtered on the network and the binding table can be built dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP server.

DHCP Snooping

DHCP Snooping Settings

State:

VLAN State:

Option 82 State:

Option 82 Information:

DHCP Snooping Status

| | |
|----------------------|----------|
| DHCP Snooping State | Disabled |
| Enabled on VLAN | None |
| Option82 State | Disabled |
| Option82 Information | None |

DHCP Snooping window – DHCP Snooping Setting tab

| Parameter | Description |
|--------------------|---|
| DHCP Snooping | To enable this function, use the drop-down menu on the top of the window. This enables global DHCP Snooping. |
| DHCP Option 82 | To enable this function, use the drop-down menu on the top of the window. |
| Information | The information for the DHCP Relay Option 82. If the DHCP Option 82 is enabled, the Switch will append the Information into the DHCP discover and request packets. |
| Interface | The interface the DHCP snooping settings are being made on. |
| Trusted | Click the port from the below list, and set the port to be trusted (Yes) or un-trusted (No). Normally, the trusted ports are connected to DHCP servers and the un-trusted ports are connected to subscribers/hosts. |
| Maximum Host Count | Determines the maximum number of hosts that can be learned in the binding table. The range is from 1 to 32 . |

| | |
|--------|---|
| Modify | After the configurations are done, click Modify to commit the changes. |
|--------|---|

Click **Submit** to save changes to RAM memory. Click **Refresh** to view the effect of the changes. To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

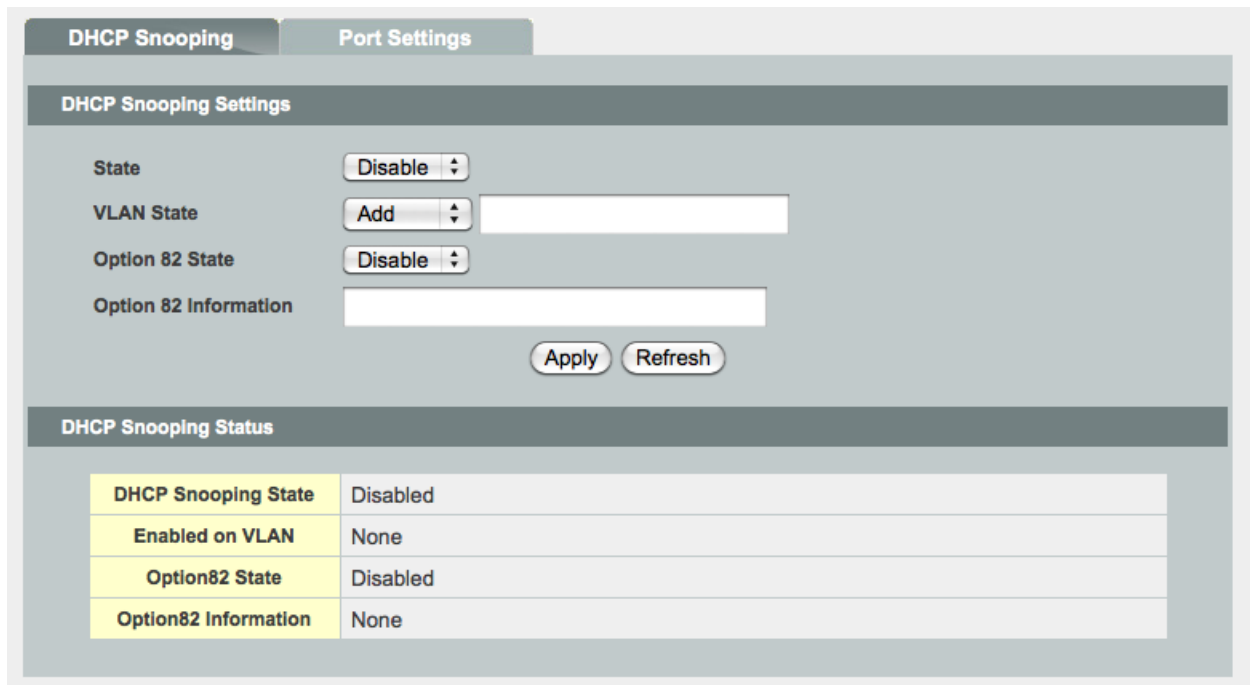
Note:

- The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.
- If the port link is down, the entries learned by this port in the DHCP snooping table will be deleted.
- You must enable the global DHCP snooping and DHCP Snooping for VLAN first.

DHCP Snooping VLAN Setting

The **DHCP Snooping** window **DHCP Snooping VLAN Setting** tab allows the user to set the VLANs to which DHCP Snooping will apply. Make sure that global and port DHCP snooping are enabled.

Choose the VLAN ID from the drop-down menu and enable or disable DHCP Snooping on the VLAN. After the configurations are done, click **Submit**.



| DHCP Snooping Settings | |
|---|---------|
| State | Disable |
| VLAN State | Add |
| Option 82 State | Disable |
| Option 82 Information | |
| <input type="button" value="Apply"/> <input type="button" value="Refresh"/> | |

| DHCP Snooping Status | |
|----------------------|----------|
| DHCP Snooping State | Disabled |
| Enabled on VLAN | None |
| Option82 State | Disabled |
| Option82 Information | None |

DHCP Snooping window – DHCP Snooping VLAN Setting tab

Click **Refresh** to display current settings of the Switch.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

DHCP Static Binding Table

The DHCP snooping feature dynamically builds and maintains the database using information extracted from intercepted DHCP messages. In this screen, you can see dynamic binding table with leased IP addresses. The dynamic binding table is stored in volatile memory. If the Switch restarts, it loads static bindings from permanent memory but loses the dynamic bindings.

Apart from the dynamic binding, you can manually add the static binding using the DHCP Binding Configuration.

After all settings are done, click **Add** to commit the rule. If you want to delete an existing rule, click it from the list, and click **Remove**.

| No. | MAC Address | IP Address | Lease(hour) | VLAN | Port | Type |
|---------|-------------|------------|-------------|------|------|------|
| Refresh | | | | | | |

DHCP Snooping widow – Static Binding Table

Click **Submit** to save changes to RAM memory. Click **Refresh** to view effect of changes.

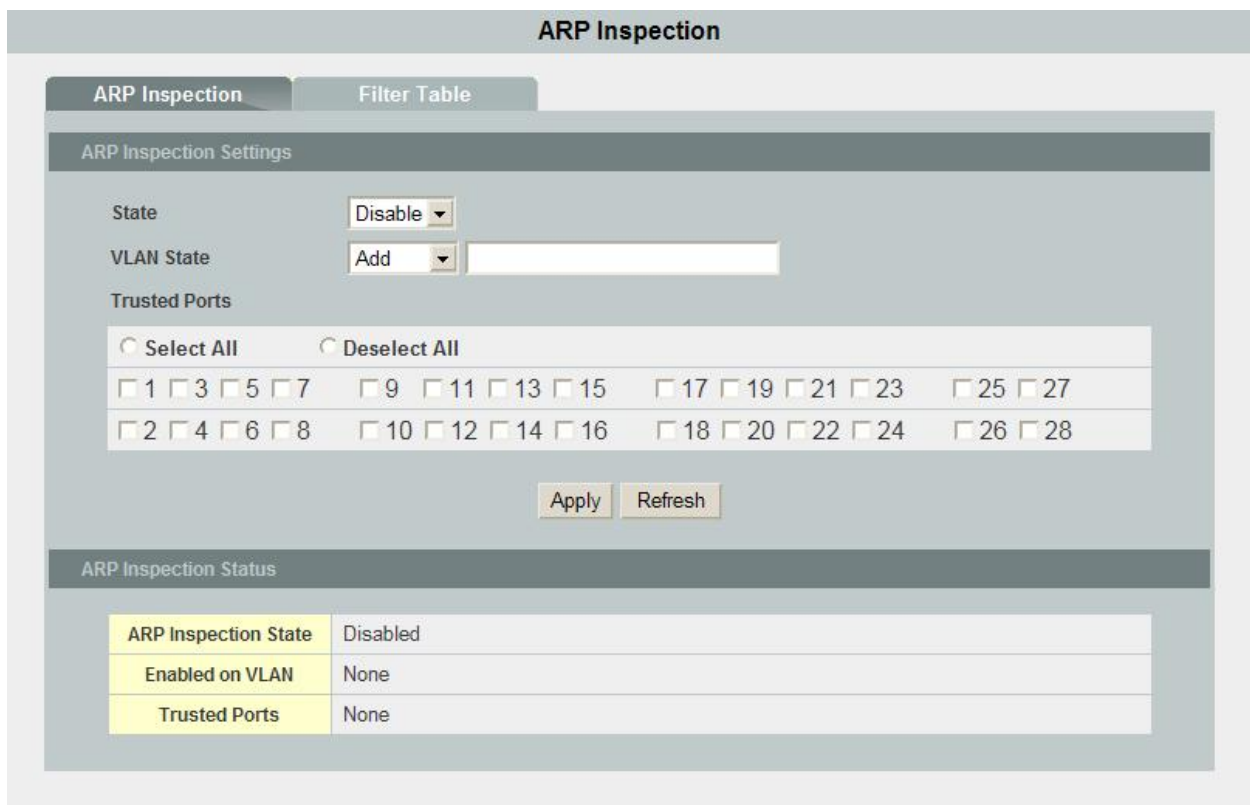
To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

ARP Inspection

ARP Inspection Setting

The Address Resolution Protocol (ARP) Inspection function filters unauthorized ARP packets on the network. This can prevent many kinds of man-in-the-middle attacks. The feature is running based on the DHCP snooping. DHCP Snooping creates a valid MAC-IP binding table for ARP Inspection reference. Therefore, be sure to enable DHCP snooping first.

The user first needs to enable global ARP Inspection by ticking the check box. In addition, the filtering age out time needs to be entered in the field at the top of the window. Click on the port to determine trusted or un-trusted. The Switch discards ARP packets on un-trusted ports when the sender's information in the ARP packets does not match any entries of the current binding tables.



ARP Inspection

ARP Inspection Filter Table

ARP Inspection Settings

State:

VLAN State:

Trusted Ports

☐ Select All ☐ Deselect All

| | | | | | | | | | | | | | |
|----------------------------|----------------------------|----------------------------|----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|
| <input type="checkbox"/> 1 | <input type="checkbox"/> 3 | <input type="checkbox"/> 5 | <input type="checkbox"/> 7 | <input type="checkbox"/> 9 | <input type="checkbox"/> 11 | <input type="checkbox"/> 13 | <input type="checkbox"/> 15 | <input type="checkbox"/> 17 | <input type="checkbox"/> 19 | <input type="checkbox"/> 21 | <input type="checkbox"/> 23 | <input type="checkbox"/> 25 | <input type="checkbox"/> 27 |
| <input type="checkbox"/> 2 | <input type="checkbox"/> 4 | <input type="checkbox"/> 6 | <input type="checkbox"/> 8 | <input type="checkbox"/> 10 | <input type="checkbox"/> 12 | <input type="checkbox"/> 14 | <input type="checkbox"/> 16 | <input type="checkbox"/> 18 | <input type="checkbox"/> 20 | <input type="checkbox"/> 22 | <input type="checkbox"/> 24 | <input type="checkbox"/> 26 | <input type="checkbox"/> 28 |

ARP Inspection Status

| | |
|----------------------|----------|
| ARP Inspection State | Disabled |
| Enabled on VLAN | None |
| Trusted Ports | None |

ARP Inspection window – ARP Inspection Setting tab

Click **Modify** to commit the setting, and it will display in the window. Click **Submit** to apply the setting.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

After enabling the ARP Inspection on specified port(s), go to the **ARP Inspection VLAN Setting** tab on the next page to enable ARP inspection on each VLAN.

ARP Inspection VLAN Setting

ARP Inspection

ARP Inspection
Filter Table

Filter Age Time Settings

Filter Age Time minutes (Range: 1-10080)

Apply
Refresh

Filter Table

| No. | MAC Address | VLAN | Port | Expiry(min) | Action |
|---------------------|-------------|------|------|-------------|--------|
| Total : 0 record(s) | | | | | |

ARP Inspection window – ARP Inspection VLAN Setting tab

Choose the VLAN first, then enable or disable the ARP Inspection on the VLAN.

Before enabling ARP Inspection on the VLAN, be sure to first enable the following functions:

- Global ARP Inspection
- Global DHCP Snooping
- Per-port DHCP Snooping
- Fixed VLAN DHCP Snooping

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

Access Control List

MAC Address List

The **MAC Access List** tab allows user to set up access control on the Switch. Use the fields at the top of the window to create rules and then click **Add**.

To change an entry on this table, select it, make the desired changes, and then click **Modify**.

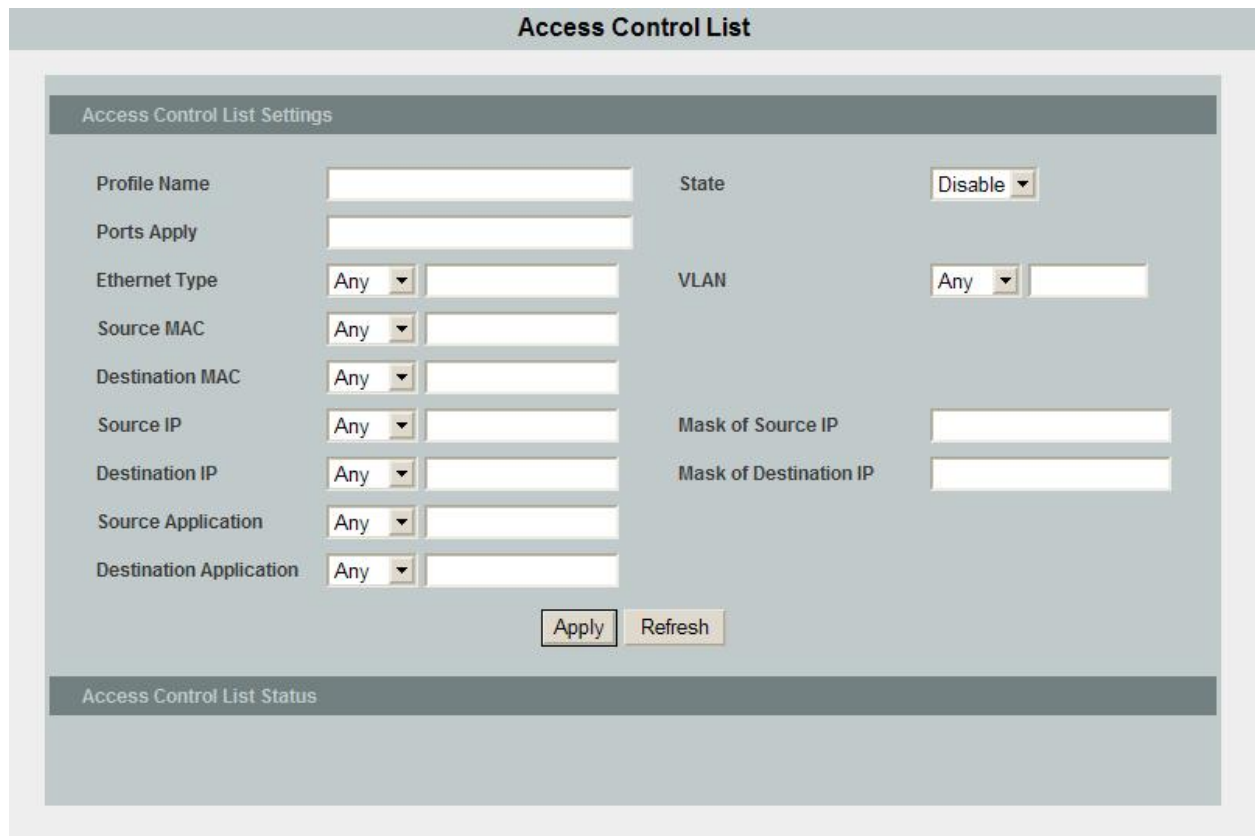
To delete an entry from this table, select it and then click **Remove**.

For example, if the Ethernet Type is **Any**, the Source MAC Address is **Any**, the Destination MAC Address is **Any**, and the Source Port is All (that is, **Detach All** has been clicked), packets with VID 2 tab will be dropped.

If the Ethernet Type is **0x0806**, the Source MAC Address is **Any**, the Destination MAC Address is **Any**, the Source Port is All (that is, **Detach All** has been clicked), and the VLAN is **Any**, packets with 0x0806 will be dropped.

If the Ethernet Type is **Any**, the Source MAC Address is **00:01:02:03:04:05**, the Destination MAC Address is **Any**, the Source Port is All (that is, **Detach All** has been clicked), and the VLAN is **Any**, packets with the source MAC address 00:01:02:03:04:05 will be dropped.

If the Ethernet Type is **0x0806**, the Source MAC address is **00:01:02:03:04:05**, the Destination MAC Address is **Any**, the Source Port is All (that is, **Detach All** has been clicked), and the VLAN is **Any**, packets with Ethernet type 0x0806 and source MAC address 00:01:02:03:04:05 will be dropped.



The screenshot shows the 'Access Control List' window with the 'MAC Access List' tab selected. The window has a title bar 'Access Control List' and a main content area. At the top of the content area is a section titled 'Access Control List Settings'. Below this, there are two columns of settings. The left column contains: 'Profile Name' (text input), 'Ports Apply' (text input), 'Ethernet Type' (dropdown menu with 'Any' selected), 'Source MAC' (dropdown menu with 'Any' selected), 'Destination MAC' (dropdown menu with 'Any' selected), 'Source IP' (dropdown menu with 'Any' selected), 'Destination IP' (dropdown menu with 'Any' selected), 'Source Application' (dropdown menu with 'Any' selected), and 'Destination Application' (dropdown menu with 'Any' selected). The right column contains: 'State' (dropdown menu with 'Disable' selected), 'VLAN' (dropdown menu with 'Any' selected), 'Mask of Source IP' (text input), and 'Mask of Destination IP' (text input). At the bottom of the settings section are two buttons: 'Apply' and 'Refresh'. Below the settings section is a section titled 'Access Control List Status' which is currently empty.

Access Control List window – MAC Access List tab

Click **Modify** to commit the setting, and it will display in the window. Click **Submit** to apply the setting.

To make all changes permanent in Flash memory, go to the **Save Configuration & Reload Default** window (**Management > Save Configuration & Reload Default**) and click **OK**.

802.1x

Port-based Network Access Control (known by the IEEE protocol number 802.1x) is a way of providing an authentication service to devices wishing to join a LAN or WLAN.

To enable, select **Enable** from the **State** drop-down menu. For the authentication method, select either **Local** (authentication is carried out at the Switch itself), or **RADIUS** for authentication at the RADIUS server site. If RADIUS Authentication is selected, then details of the primary RADIUS server (and secondary, if available) must be added below. For local authentication, enter the user name and password. Click **Apply** to save.

Global Settings

Port Settings

Global Settings

| | | | |
|-------------------------|--|---------------------------------|-----------------------------------|
| State | Disable | | |
| Authentication Method | Local | | |
| Primary Radius Server | IP : <input type="text"/> | UDP Port : <input type="text"/> | Shared Key : <input type="text"/> |
| Secondary Radius Server | IP : <input type="text"/> | UDP Port : <input type="text"/> | Shared Key : <input type="text"/> |
| Local Authentic User | <div>None</div> <div>User Name : <input type="text" value="admin"/></div> <div>Password : <input type="password" value="*****"/></div> | | |

Apply

Refresh

Global Status

| | | | |
|---------------------------|----------|--------------|----------------|
| State | Disabled | | |
| Authentication Method | Local | | |
| Primary Radius Server | IP : - | UDP Port : - | Shared Key : - |
| Secondary Radius Server | IP : - | UDP Port : - | Shared Key : - |
| Local Authentication User | None | | |

To configure the settings on a per-port basis, select the **Port Settings** tab. Select the port range and select **Enable** from the **802.1x State** drop-down menu. Choose the **Admin Control Direction** (Both or In) and **Re-authentication** from the drop-down menu. From the **Port Control Mode** drop-down menu, select **Auto**, **Force-Authorized** or **Force-Unauthorized**.

Selecting **Auto** causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the switch by using the client MAC address.

Selecting **Force-Authorized** disables IEEE 802.1x authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 802.1x-based authentication of the client.

Force-Unauthorized causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port.

After optionally selecting the **Guest VLAN** ID from the next drop-down menu, enter the **Max-req Time** (the maximum number of authentication requests issued by the Switch).

Reauth-Period: Sets the time after which an automatic re-authentication should be initiated.

Quiet Period: This timer sets the quiet-period. When a supplicant system fails to pass the authentication, the device quiets for the set period (set by the quiet-period timer) before it processes another authentication request re-initiated by the supplicant system. During this quiet period, the device does not perform any 802.1x authentication-related actions for the supplicant system.

Supp-timeout: This timer sets the supp-timeout period and is triggered by the device after the device sends a request/challenge packet to a supplicant system (The packet is used to request the supplicant system for the MD5 encrypted string.) The device sends another request/challenge packet to the supplicant system if the device does not receive the response from the supplicant system when this timer times out.

Server-timeout: Sets the RADIUS server timer. This timer sets the server-timeout period. After sending an authentication request packet to the RADIUS server, the device sends another authentication request packet if it does not receive the response from the RADIUS server when this timer times out.

Once the required changes have been made, click **Apply** to save.

802.1x

Global Settings

Port Settings

Port Settings

Port

From: To:

802.1x State

| Admin Control Direction | Reauthentication | Port Control Mode | Guest VLAN | Max-req Time |
|-------------------------------------|--|-------------------------------------|-------------------------------------|--------------------------------|
| <input type="button" value="Both"/> | <input type="button" value="Disable"/> | <input type="button" value="Auto"/> | <input type="button" value="None"/> | <input type="text" value="2"/> |
| Reauth-period | Quiet-period | Supp-timeout | Server-timeout | Reset to Default |
| <input type="text" value="3600"/> | <input type="text" value="60"/> | <input type="text" value="30"/> | <input type="text" value="30"/> | <input type="checkbox"/> |

Port Status

| Port | 802.1x State | Admin Control Direction | Reauthentication | Port Control Mode | Guest VLAN | Max-req Time | Reauth-period | Quiet-period | Supp-timeout | Server-timeout |
|------|--------------|-------------------------|------------------|-------------------|------------|--------------|---------------|--------------|--------------|----------------|
| 1 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 2 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 3 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 4 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 5 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 6 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 7 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 8 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 9 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 10 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 11 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 12 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 13 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 14 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 15 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 16 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 17 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 18 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 19 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 20 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 21 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 22 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 23 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 24 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 25 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 26 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 27 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |
| 28 | Disabled | Both | Disabled | Auto | 0 | 2 | 3600 | 60 | 30 | 30 |

Management

Management folders contain windows for Reboot, Firmware Upgrade, and Save Configuration & Reload Default.

Reboot

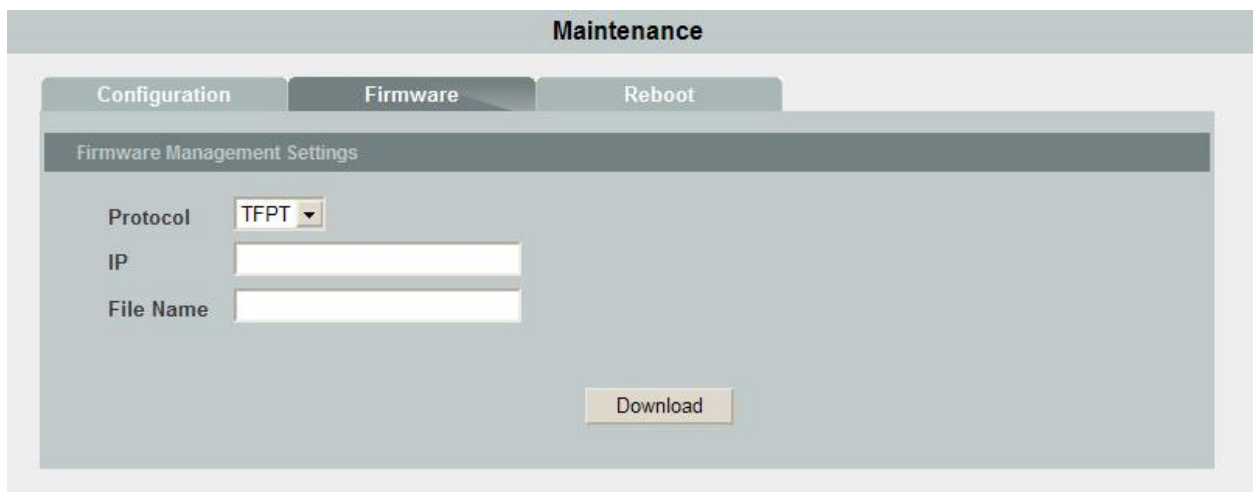
The **Reboot** window contains a **Reboot** button. Clicking this button reboots the system.

Rebooting the system stops the network traffic and terminates the Web interface connection.

Firmware Upgrade

The Switch provides three methods to upgrade firmware/configurations—TFTP, FTP, and HTTP.

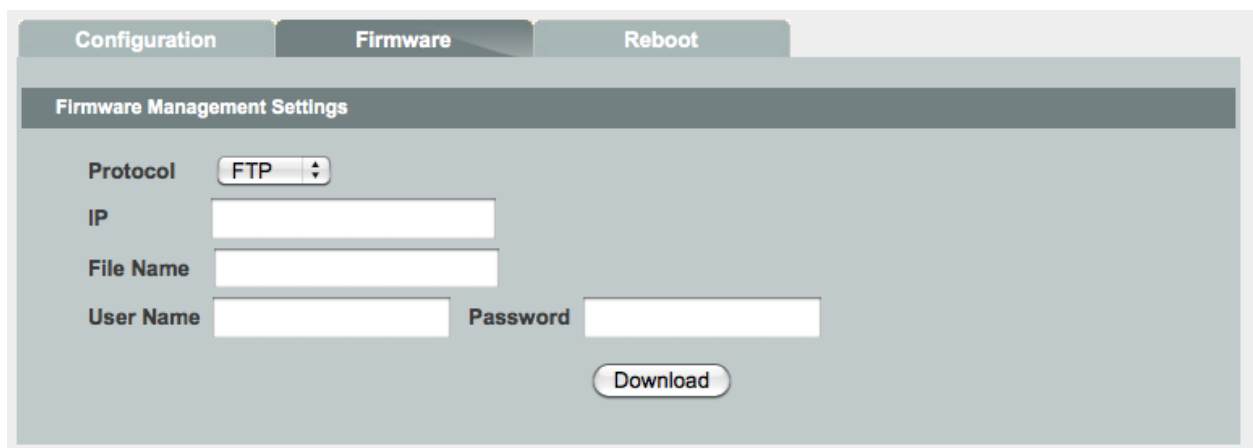
To download/upload firmware/configurations through TFTP and HTTP, select the desired Type and Mode and then enter the TFTP/HTTP/FTP server IP Address and the firmware File Name. Click **Upgrade** to update the Switch's firmware from the TFTP/HTTP/FTP server.



The screenshot shows the 'Maintenance' section of the web interface. Under the 'Firmware' tab, the 'Firmware Management Settings' section is active. It features a 'Protocol' dropdown menu set to 'TFTP', an 'IP' text input field, and a 'File Name' text input field. A 'Download' button is located at the bottom right of the settings area.

Firmware Upgrade window – TFTP

To download firmware/configurations through an FTP server, besides IP address and file name, users also need to enter the user name and password to access the FTP server.



The screenshot shows the 'Maintenance' section of the web interface. Under the 'Firmware' tab, the 'Firmware Management Settings' section is active. It features a 'Protocol' dropdown menu set to 'FTP', an 'IP' text input field, a 'File Name' text input field, a 'User Name' text input field, and a 'Password' text input field. A 'Download' button is located at the bottom right of the settings area.

Firmware Upgrade window - FTP

Clicking the **Upgrade** button loads the assigned firmware to the Switch, and then reboots the system after a successful firmware update. Users will need to log in to the Web interface again.

Save Configuration & Reload Default

Select **Save Configuration** from the drop-down menu to make the settings permanent by saving to the Flash memory and then click **OK** (**Submit** only saves changes to the RAM memory and such changes will be lost if the Switch is switched off).

To reset the Switch's configuration, select **Reload Default Configuration** from the drop-down menu and then click **OK**. This will reset the configuration file to factory default. A system reboot will follow this restoration process.

NOTE: All user configurations will be lost when you choose to restore the factory default configuration.

Maintenance

Configuration

Firmware

Reboot

Save Configurations

Save the parameter settings of the device :

Save

Save / Load Configurations to / from a TFTP server

☒ Save configurations to a TFTP server.
 ☐ Load configurations to device from a TFTP server.

Server IP

FILE NAME

2011-0318-1741.conf

Apply

Reset Configurations

Reset the factory default settings of the device :

- IP address will be 192.168.0.254

Reset

Maintenance

Configuration

Firmware

Reboot

Reboot

Press "Reboot" to restart the system.

Reboot

Save Configuration & Reload Default window

75

Command Line Interface

This chapter describes how to use console interface to configure the Switch. The Switch provides RS232 connectors to connect to a PC. Use a terminal emulator on the PC, such as HyperTerminal or command line interpreter, to configure the switch. The terminal emulator should be configured with a baud rate of 115200, 8 bit data, no parity, 1 stop bit, and no flow control.

In CLI mode, typing “?” or list will display all available command help messages. All the CLI commands are case sensitive.

Power On

Power On Self Test is executed during the system boot period. It tests system memory, LED and hardware chips on the switchboard. It displays system information as the result of system testing and initialization. The user can ignore all information until the prompt, “Switch login:” appears.

Login and Logout

To enter the CLI mode, a valid user name and password must be entered. For the first login, the user can enter “admin” as the user name, and the password too. For security reasons, please change the user name and password after login. If you forget the user name and password, you may 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 the user to secure the CLI mode. The next user has to log in again with an authorized user name and password.

CLI Commands

The Switch provides CLI commands for all managed functions. The user can follow the instructions and set up the Switch as easily as using the Web interface to configure the Switch.

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).

ACL

| Access Control List CLI Commands | |
|----------------------------------|---|
| Command | Parameters |
| show access-list | |
| | This command displays all of the access control profiles. |
| access-list | STRING |
| | This command creates a new access control profile. Where the STRING is the profile name. |
| show profile | |
| | This command displays the current access control profile. |
| active | |
| | This command activates this profile. |
| no active | |
| | This command disables the profile. |
| mac destination address | MACADDR MACADDR |
| | This command configures the destination MAC and mask for the profile. The second MACADDR parameter is the mask for the profile. |
| mac destination address | host MACADDR |
| | This command configures the destination MAC and mask for the profile. The mask is set to ff.ff.ff.ff.ff automatically. |
| no mac destination address | |
| | This command removes the destination MAC and mask from the profile. |
| mac ethertype | STRING |
| | This command configures the Ethernet type for the profile. Where the STRING is a hex-decimal value. e.g.: 08AA. |
| no mac ethertype | |
| | This command removes the limitation of the Ethernet type from the profile. |
| mac source address | MACADDR MACADDR |
| | This command configures the source MAC and mask for the profile. |
| mac source address | host MACADDR |
| | This command configures the source MAC and mask for the profile. The mask is set to ff.ff.ff.ff.ff automatically. |
| no mac source address | |
| | This command removes the source MAC and mask from the profile. |
| mac vlan | VLANID |
| | This command configures the VLAN for the profile. |
| no mac vlan | |
| | This command removes the limitation of the VLAN from the profile. |
| source-port | PORTLIST |
| | This command configures the source ports for the profile. |
| no source-port | PORTLIST |
| | This command removes the source ports from the profile. |

QoS

| QoS CLI Commands | |
|---------------------|---|
| Command | Parameters |
| show queue cos_map | |
| | This command displays the current 802.1p priority mapping to the service queue. |
| show qos mode | |
| | This command displays the current QoS scheduling mode of IEEE 802.1p. |
| queue cos_map | PRIORITY QUEUE_ID |
| | This command configures the 802.1p priority mapping to the service queue. |
| no queue cos_map | |
| | This command configures the 802.1p priority mapping to the service queue to default. Default: Priority: 0 1 2 3 4 5 6 7 Queue: 1 0 0 1 2 2 3 3 |
| qos mode | high_first |
| | This command configures the QoS scheduling mode to high_first, each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets. |
| qos mode | wrr_queue weights VALUE0 VALUE1 VALUE2 VALUE3 |
| | This command configures the QoS scheduling mode to wrr_queue (Weighted Round Robin). The VALUE0 is for queue 0. The VALUE1 is for queue 1. The VALUE2 is for queue 2. The VALUE3 is for queue 3. |
| no qos mode | |
| | This command configures the QoS scheduling mode to default (high-first). |
| default_priority | |
| | This command allows the user to specify default priority handling of untagged packets received by the Switch. The priority value entered with this command will be used to determine which of the four hardware priority queues the packet is forwarded to. Default: 0. |
| no default_priority | |
| | This command configures the default priority for the specific port to default (0). |

Bandwidth Management

Bandwidth Limitation

| Bandwidth Limitation CLI Commands | |
|-----------------------------------|--|
| Command | Parameters |
| show bandwidth-limit | |
| | This command displays the current rate control configurations. |
| bandwidth-limit | egress RATE_LIMIT interface PORTLISTS |
| | This command enables the bandwidth limit for outgoing packets and sets the limitation. |
| no bandwidth-limit | egress interface PORTLISTS |
| | This command disables the bandwidth limit for outgoing packets. |
| bandwidth-limit | ingress RATE_LIMIT interface PORTLISTS |
| | This command enables the bandwidth limit for incoming packets and sets the limitation. |
| no bandwidth-limit | ingress interface PORTLISTS |
| | This command disables the bandwidth limit for incoming packets. |

Storm Control

| Storm Control CLI Commands | |
|----------------------------|--|
| Command | Parameters |
| show bandwidth-limit | |
| | This command displays the current rate control configurations. |
| storm-control | rate RATE_LIMIT type (bcast mcast dlf bcast_mcast mcast_dlf bcast_dlf bcast_mcast_dlf) interface PORTLISTS |
| | This command enables the bandwidth limit for broadcast and/or multicast and/or DLF packets and set the limitation. |
| no storm-control | type (bcast mcast dlf bcast_mcast mcast_dlf bcast_dlf bcast_mcast_dlf) interface PORTLISTS |
| | This command disables the bandwidth limit for broadcast and/or multicast and/or DLF packets. |

DHCP Client

| DHCP Client CLI Commands | |
|--------------------------|--|
| Command | Parameters |
| show interface eth0 | |
| | This command displays the current Eth0 configurations. |
| ip dhcp client | (disable enable renew) |
| | This command configures a DHCP client function for the system. |

DHCP Relay

| DHCP Relay CLI Commands | |
|----------------------------|---|
| Command | Parameters |
| show dhcp relay | |
| | This command displays the current configurations for the DHCP relay. |
| dhcp relay | |
| | This command enables the global DHCP relay function. |
| no dhcp relay | |
| | This command disables the global DHCP relay function. |
| dhcp relay vlan | VLAN_RANGE |
| | This command enables the DHCP relay function on a VLAN or a range of VLANs. |
| no dhcp relay vlan | VLAN_RANGE |
| | This command disables the DHCP relay function on a VLAN or a range of VLANs. |
| dhcp helper-address | IP_ADDR |
| | This command configures the DHCP server's IP address. Note: The system allows up to three DHCP servers to be configured. |
| no dhcp helper-address | |
| | This command removes the DHCP server's IP address. |
| ip address default-gateway | A.B.C.D |
| | This command configures the system default gateway. |

DHCP Option 82

| DHCP Option 82 CLI Commands | |
|-----------------------------|---|
| Command | Parameters |
| show dhcp-snooping | |
| | This command displays the current DHCP snooping configurations. |
| show dhcp relay | |
| | This command displays the current DHCP Relay configurations. |
| dhcp option | |
| | This command enables the DHCP option 82 on the Switch. |
| no dhcp option | |
| | This command disables the DHCP option 82 on the Switch. |
| dhcp option information | STRING |
| | This command configures the information for the DHCP option 82. |
| no dhcp option information | |
| | This command removes the information for the DHCP option 82. |

IGMP Snooping

| IGMP Snooping CLI Commands | |
|----------------------------|--|
| Command | Parameters |
| show igmp-snooping | |
| | This command displays the current IGMP snooping configurations. |
| igmp-snooping | |
| | This command enables the IGMP snooping function for the Switch. |
| no igmp-snooping | |
| | This command disables the IGMP snooping function for the Switch. |
| igmp-snooping | vlan VLAN_ID |
| | This command enables the IGMP snooping function on a VLAN or range of VLANs. |
| no igmp-snooping | VLAN VLAN_ID |
| | This command disables the IGMP snooping function on a VLAN or range of VLANs. |
| igmp-snooping querier | |
| | This command enables the IGMP snooping querier for the Switch. |
| no igmp-snooping querier | |
| | This command disables the IGMP snooping querier for the Switch. |
| igmp-snooping querier | VLAN VLAN_ID |
| | This command enables the IGMP snooping querier function on a VLAN or range of VLANs. |
| no igmp-snooping querier | VLAN VLAN_ID |
| | This command disables the IGMP snooping querier function on a VLAN or range of VLANs. |
| igmp-snooping | unknown-multicast (drop flooding) |
| | This command configures the process for unknown multicast packets when the IGMP snooping function is enabled. <i>drop</i> : Drop all of the unknown multicast packets. <i>flooding</i> : Flooding all of the unknown multicast packets. |
| igmp-querier-mode | (auto fixed edge) |
| | This command specifies whether or not and under what conditions the port(s) is (are) IGMP query port(s). The Switch forwards IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well. (Default:auto) fixed: The Switch always treats the port(s) as IGMP query port(s). Select this when you connect an IGMP multicast server to the port(s). auto: The Switch uses the port as an IGMP query port if the port receives IGMP query packets. edge: The Switch does not use the port as an IGMP query port. The Switch does not keep any record of an IGMP router being connected to this port. The Switch does not forward IGMP join or leave packets to this port. Default: auto |
| igmp-immediate-leave | |
| | This command enables the IGMP snooping immediate leave function for the specific interface. |

| | |
|-------------------------|--|
| no igmp-immediate-leave | |
| | This command disables the IGMP snooping immediate leave function for the specific interface. |

IP Source Guard

DHCP Snooping

| DHCP Snooping CLI Commands | |
|----------------------------|--|
| Command | Parameters |
| show dhcp-snooping | |
| | This command displays the current DHCP snooping configurations. |
| dhcp-snooping | |
| | This command enables the DHCP snooping function for the Switch. |
| no dhcp-snooping | |
| | This command disables the DHCP snooping function for the Switch. |
| dhcp-snooping | vlan VLAN_ID |
| | This command enables the DHCP snooping function on a VLAN or range of VLANs. |
| no dhcp-snooping | vlan VLANID |
| | This command disables the DHCP snooping function on a VLAN or range of VLANs. |
| dhcp-snooping | host |
| | configures the maximum host count for the specific port. |
| no dhcp-snooping | host |
| | This command configures the maximum host count to default for the specific port. |
| dhcp-snooping | trust |
| | This command configures the trust port for the specific port. |
| no dhcp-snooping | trust |
| | This command configures the un-trust port for the specific port. |

DHCP Snooping Binding Table

| DHCP Snooping Binding Table CLI Commands | |
|--|---|
| Command | Parameters |
| show dhcp-snooping | binding |
| | This command displays the current DHCP snooping binding table. |
| dhcp-snooping | binding mac MAC_ADDR ip IP_ADDR vlan VLAN_ID interface PORT_NO |
| | This command configures a static host into the DHCP snooping binding table. |
| no dhcp-snooping | binding mac MAC_ADDR |
| | This command removes a static host from the DHCP snooping binding table. |

ARP Inspection

| ARP Inspection CLI Commands | |
|-----------------------------|--|
| Command | Parameters |
| show arp-inspection | |
| | This command displays the current ARP Inspection configurations. |
| arp-inspection | |
| | This command enables the ARP Inspection function for the Switch. |
| no arp-inspection | |
| | This command disables the ARP Inspection function for the Switch. |
| arp-inspection | vlan VLAN_ID |
| | This command enables the ARP Inspection function on a VLAN or range of VLANs. |
| no arp-inspection | vlan VLAN_ID |
| | This command disables the ARP Inspection function on a VLAN or range of VLANs. |
| arp-inspection trust | |
| | This command configures the trust port for the specific port. |
| no arp-inspection trust | |
| | This command configures the un-trust port for the specific port. |

Blacklist Filter

| Blacklist Filter CLI Commands | |
|----------------------------------|---|
| Command | Parameters |
| show arp-inspection mac-filter | |
| | This command displays the current ARP Inspection filtered MAC. |
| -iarpnspection mac-filter age | VALUE |
| | This command configures the age time for the ARP inspection MAC filter entry. |
| no arp-inspection mac-filter mac | MAC_ADDR |
| | This command removes an entry from the ARP inspection MAC filter table. |

Link Aggregation (Trunk)

Static Link Aggregation

| Static Link Aggregation CLI Commands | |
|--------------------------------------|--|
| Command | Parameters |
| show link_aggregation | |
| | The commands displays the current trunk configurations. |
| link_aggregation | [GROUP_ID] |
| | The commands enables the trunk for a specific trunk group. |

| | |
|---------------------|--|
| no link_aggregation | [GROUP_ID] |
| | The commands disables the trunk for a specific trunk group. |
| link_aggregation | [GROUP_ID] interface PORTLISTS |
| | The commands adds ports to a specific trunk group. |
| no link_aggregation | [GROUP_ID] interface PORTLISTS |
| | The commands delete ports from a specific trunk group. |
| link_aggregation | [GROUP_ID] load-balance (src-mac dst-mac src-dst-mac src-ip dst-ip src-dst-ip) |
| | The commands configures the load-balance algorithm for a specific trunk group. src-mac: source mac. dst-mac: destination mac. src-dst-mac: source and destination mac. src-ip: source IP. dst-ip: destination IP. src-dst-ip: source and destination IP. |

802.3ad Link Aggregation Control Protocol (LACP)

| LACP CLI Commands | |
|-------------------------|--|
| Command | Parameters |
| show trunk | |
| | This command displays the current trunk configurations. |
| show lacp counters | [GROUP_ID] |
| | This command displays the LACP counters for the specific group or all groups. |
| show lacp internal | [GROUP_ID] |
| | This command displays the LACP internal information for the specific group or all groups. |
| show lacp neighbor | [GROUP_ID] |
| | This command displays the LACP neighbor's information for the specific group or all groups. |
| show lacp port_priority | |
| | This command displays the port priority for the LACP. |
| show lacp sys_id | |
| | This command displays the actor's and partner's system ID. |
| lacp | |
| | This command enables the global LACP function. |
| lacp | GROUP_ID |
| | This command enables the LACP for the specific trunk group. |
| clear lacp counters | [PORT_ID] |
| | This command clears the LACP statistics for the specific port or all ports. |
| lacp system-priority | <1-65535> |
| | This command configures the system priority for the LACP. Note: The default value is 32768. |
| no lacp system-priority | |
| | This command configures the default for the system priority for the LACP. |
| lacp port_priority | <1-65535> |
| | This command configures the priority for the specific port. Note: The default value is 32768. |

| | |
|-----------------------|---|
| no lacp port_priority | |
| | This command configures the default for the priority for the specific port. |

Loopback Detection

| Loopback Detection CLI Commands | |
|---------------------------------|---|
| Command | Parameters |
| show loop-detection | |
| | This command displays the current loop detection configurations. |
| loop-detection | |
| | This command enables the loop detection function for the Switch. |
| no loop-detection | |
| | This command disables the loop detection function for the Switch. |
| loop-detection | address MAC_ADDR |
| | This command configures the destination MAC for the loop detection special packets. |
| no loop-detection | address MAC_ADDR |
| | This command configures the destination MAC to default (00:F0:F0:00:00:00). |
| loop-detection | |
| | This command enables the loop detection function for the specific port. |
| no loop-detection | |
| | This command disables the loop detection function for the specific port. |
| no shutdown | |
| | This command enables the specific port. It can unblock port blocked by loop detection. |
| loop-detection retry | <0-5> |
| | This command configures the retry times. The retry time allows the Switch to retry more times before it blocks any specific ports with looping. |
| loop-detection retrial-period | <0-10> |
| | This command configures the retrial-period. The “retrial-period” allows the Switch to retry the loop detection with delay. |

MAC Address Management

| MAC Address Management CLI Commands | |
|-------------------------------------|---|
| Command | Parameters |
| show mac-address-table | aging-time |
| | This command displays the current MAC address table age time. |
| show mac-address-table | multicast |
| | This command displays the current static/dynamic multicast address entries. |
| show mac-address-table | (static dynamic) |

| | |
|--------------------------|--|
| | This command displays the current static/dynamic unicast address entries. |
| mac-address-table | aging-time TIMEVALUE |
| | This command configures the aging time in seconds. The range is 10 to 1000000. |
| mac-address-table | multicast MACADDR vlan VLAN_ID port PORTLISTS |
| | This command configures a static multicast entry. |
| no mac-address-table | multicast MACADDR |
| | This command removes a static multicast entry from the address table. |
| mac-address-table static | MACADDR vlan VLAN_ID port PORT_ID |
| | This command configures a static unicast entry. |
| no mac-address-table | static MACADDR |
| | This command removes a static unicast entry from the address table. |

Port Management

| Port Management CLI Commands | |
|------------------------------|--|
| Command | Parameters |
| show interface | IFNAME |
| | This command displays the port configurations. |
| speed | (10 100 1000) |
| | This command configures the port speed to 10M/100M/1000M. |
| shutdown | |
| | This command disables the specific port. |
| no shutdown | |
| | This command enables the specific port. |
| mdix | (auto normal xover) |
| | This command configures the MDIX state for the specific port. Default: auto. |
| loopback | (none mac phy) |
| | This command specifies the loopback mode of operation for the specific port. Default: none. |
| no loopback | |
| | This command disables the loopback mode of operation for the specific port. |
| flowcontrol | |
| | This command configures the receive and send flow-control value for the port. Default: On. |
| no flowcontrol | |
| | This command sets Flow Control to its default. |
| duplex | (full half) |
| | This command specifies the duplex mode of operation for the port. Default: full duplex. |
| no duplex | |
| | This command sets Duplex mode to its default. |
| auto-negotiation | |
| | This command enables auto-negotiation state for the port |

| | |
|---------------------|---|
| | Default: enable. |
| No auto-negotiation | |
| | This command sets auto-negotiation state to the default. |
| jumboframe | (1518 2048) |
| | This command configures jumbo frame size to 1518 or 2048. Default: 1518. |

Port Mirror

| Port Mirror CLI Commands | |
|--------------------------|---|
| Command | Parameters |
| show mirror | |
| | This command displays the current port mirroring configurations on the Switch. |
| mirror | |
| | This command enables the port mirroring without having to modify the port mirroring configuration. Default: disable. |
| no mirror | |
| | This command disables the port mirroring and reset all of the port mirroring configurations. |
| mirror destination | interface PORT_ID |
| | This command configures the target port for the port mirroring. |
| mirror source | interface PORT_LIST mode (both rx tx) |
| | This command allows a range of source ports to have all of their traffic also sent to a mirror port. In addition, users can specify that only traffic received by or sent by one or both is mirrored to the mirror port. PORT_LIST – This specifies a port or range of ports that will be mirrored. That is, the range of ports in which rx – Allows the mirroring of only packets received by the port or ports in the port list. tx – Allows the mirroring of only packets sent to the port or ports in the port list. both – Mirrors all the packets received or sent by the port or ports in the port list. |
| no mirror source | interface PORT_LIST |
| | This command removes a port or ports from the source ports of port mirroring. |

Port Security

| Port Security CLI Commands | |
|----------------------------|--|
| Command | Parameters |
| Show port-security | |
| | This command displays ports security configurations. |
| port-security | |
| | This command disables the new MAC addresses learning and aging activities function for the Switch. |
| no port-security | |
| | This command enables the new MAC addresses learning and aging activities for the Switch. |



SNMP

| SNMP CLI Commands | |
|----------------------|---|
| Command | Parameters |
| show snmp | |
| | This command displays the SNMP configurations. |
| snmp community | STRING (ro rw) trusted-host IPADDR |
| | This command displays the SNMP configurations. |
| snmp disable | |
| | This command disables the SNMP function. |
| snmp enable | |
| | This command enables the SNMP function. |
| snmp system-contact | STRING |
| | This command configures contact information for the system. |
| snmp system-location | STRING |
| | This command configures the location information for the system. |
| snmp system-name | STRING |
| | This command configures a name for the system. |
| snmp trap-receiver | IPADDR VERSION COMMUNITY |
| | This command configures the trap receiver's configurations, including the IP address, version (v1 or v2c), and community. |

STP & RSTP

| STP & RSTP CLI Commands | |
|----------------------------------|--|
| Command | Parameters |
| show spanning-tree active | |
| | This command displays the spanning tree information for only active port(s) |
| show spanning-tree blocked ports | |
| | This command displays the spanning tree information for only blocked port(s) |
| show spanning-tree port detail | IFNAME |
| | This command displays the spanning tree information for the interface port. |
| show spanning-tree statistics | IFNAME |
| | This command displays the spanning tree information for the interface port. |
| show spanning-tree summary | |
| | This command displays the summary of port states and configurations |
| clear spanning-tree counters | |
| | This command clears all spanning-tree statistics. |

| | |
|--|--|
| spanning-tree | |
| | This command enables the spanning tree function for the system. |
| no spanning-tree | |
| | This command disables the spanning tree function for the system. |
| spanning-tree algorithm-timer | forward-time TIME max-age TIME hello-time TIME |
| | This command configures the bridge times (forward-delay, max-age, and hello-time). |
| no spanning-tree algorithm-timer | |
| | This command configures the default values for forward-time, max-age, and hello-time. |
| spanning-tree forward-time | <4-30> |
| | This command configures the bridge forward delay time (sec). |
| no spanning-tree forward-time | |
| | This command configures the default values for forward-time. |
| spanning-tree hello-time | <1-10> |
| | This command configures the bridge hello time (sec). |
| no spanning-tree hello-time | |
| | This command configures the default values for hello-time. |
| spanning-tree max-age | <6-40> |
| | This command configures the bridge message max-age time (sec). |
| no spanning-tree max-age | |
| | This command configures the default values for max-age time. |
| spanning-tree mode | (stp rstp) |
| | This command configures the spanning mode. |
| spanning-tree pathcost method | (long short) |
| | This command configures |
| spanning-tree priority | <0-61440> |
| | This command configures the priority for the system. |
| no spanning-tree priority | |
| | This command configures the default values for the system priority. |
| spanning-tree transmission-limit | <1-10> |
| | This command configures ??? Note: The minimum interval between transmission of consecutive RSTP BPDUs |
| no spanning-tree transmission-limit | |
| | This command configures the default values for transmission-limit. |
| spanning-tree bpdufilter | (enable disable) |
| | This command configures enables/disables the BPDU filter function. Note: BPDU Filter is a feature to filter sending or receiving BPDUs on a switchport. |
| spanning-tree | (enable disable) |

| | |
|--------------------------------|--|
| bpduguard | |
| | This command configures enables/disables the BPDU guard function. Note: BPDU Guard is a feature to respond to invalid configurations in securely. |
| spanning-tree edge-port | (enable disable) |
| | This command enables/disables the edge port setting. Note: Edge ports if they are attached to a LAN that has no other bridges attached. |
| spanning-tree cost | VALUE |
| | This command configures the cost for the specific port. Cost range: 16-bit based value range 1-65535, 32-bit based value range 1-200000000. |
| no spanning-tree cost | |
| | This command configures the path cost to default for the specific port. |
| spanning-tree port-priority | <0-240> |
| | This command configures the port priority for the specific port. Default: 128. |
| no spanning-tree port-priority | |
| | This command configures the port priority to default for the specific port. |

Configuration Management

| Configuration Management CLI Commands | |
|---------------------------------------|---|
| Command | Parameters |
| write memory | |
| | This command writes configurations to the Flash. |
| show running-config | |
| | This command displays the current operating configurations. |
| reload default-config | |
| | This command copies a default-config file to replace the current one. |
| archive download-config | <URL PATH> |
| | This command downloads a new copy of configuration file from TFTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file |
| archive upload-config | <URL PATH> |
| | This command uploads the current operating configurations to the TFTP server. Where <URL PATH> can be: tftp://192.168.1.1/file |

Firmware Upgrade

| Firmware Upgrade CLI Commands | |
|-------------------------------|---|
| Command | Parameters |
| archive download-fw | <URL PATH> |
| | This command downloads a new copy of configuration file from TFTP server. Where <URL PATH> can be: ftp://user:pass@192.168.1.1/file http://192.168.1.1/file tftp://192.168.1.1/file |

System Management

System Management

| System Management CLI Commands | |
|--------------------------------|---|
| Command | Parameters |
| show interface eth0 | |
| | This command displays the current Eth0 configurations. |
| reboot | |
| | This command reboots the system. |
| hostname | |
| | This command sets the system's network name. |
| interface eth0 | |
| | This command enters the eth0 interface node to configure the system IP. |
| management vlan | VLAN_ID |
| | This command configures the management VLAN. |
| no management vlan | |
| | This command configures the management VLAN to default. |
| ip address | A.B.C.D/M |
| | This command configures a static IP for the system. |
| ip address default-gateway | A.B.C.D |
| | This command configures the system default gateway. |

User Account

| User Account CLI Commands | |
|---------------------------|---|
| Command | Parameters |
| show user account | |
| | This command displays the current user account. |
| add user | USER_ACCOUNT PASSWORD (normal admin) |
| | This command adds a new user account. |
| delete user | USER_ACCOUNT |

| | |
|--|--|
| | This command deletes a present user account. |
|--|--|

VLAN

VLAN

| VLAN CLI Commands | |
|-------------------|---|
| Command | Parameters |
| show vlan | |
| | This command displays the VLAN configurations. |
| vlan | <1~4094> |
| | This command enables a VLAN and enters the VLAN node. |
| acceptable frame | type (all discardall vlan tagged only) |
| | This command configures the frame type for the specific port to accept. |
| fixed | PORT_LIST |
| | This command assigns ports for permanent member of the VLAN group. |
| forbidden | PORT_LIST |
| | This command assigns ports to prohibit the port to join in the VLAN group. The ports should be one/some of the permanent members of the VLAN group. |
| untagged | PORT_LIST |
| | This command assigns ports for untagged member of the VLAN group. The ports should be one/some of the permanent members of the VLAN group. |
| name | STRING |
| | This command assigns a name for the specific VLAN. |
| no fixed | |
| | This command removes all fixed members from the VLAN. |
| no forbidden | |
| | This command removes all forbidden members from the VLAN. |
| no untagged | |
| | This command removes all untagged member from the VLAN. |
| no name | |
| | This command configures the VLAN name to default. Note: The default VLAN name is "VLAN"+vlan_ID, VLAN1, VLAN2,... |

Port Isolation

| Port Isolation CLI Commands | |
|-----------------------------|--|
| Command | Parameters |
| show port-isolation | |
| | This command displays the current port isolation configurations. |
| port-isolation | PORTLISTS |
| | This command configures the forwarding port group for the ingress packets for the specific port. |
| no port-isolation | |
| | This command allows the specific port to forward the ingress packets to all ports. |

GARP

| GARP CLI Commands | |
|------------------------|---|
| Command | Parameters |
| show garp timer | |
| | This command displays the General Attribute Registration Protocol timers. |
| garp join-timer | <1-2147483647> |
| | This command configures join time for the GARP. |
| garp leave-timer | <1-2147483647> |
| | This command configures leave time for the GARP. |
| garp leaveall-timer | <1-2147483647> |
| | This command configures leave all time for the GARP. |
| no garp join-timer | |
| | This command configures join time for the GARP to default. |
| no garp leave-timer | |
| | This command configures leave time for the GARP to default. |
| no garp leaveall-timer | |
| | This command configures leave all time for the GARP to default. |

GVRP

| GVRP CLI Commands | |
|-------------------------|---|
| Command | Parameters |
| show gvrp configuration | |
| | This command displays the configurations of the GVRP. |
| show gvrp statistics | |
| | This command displays statistics of the GVRP. |
| clear gvrp statistics | [IFNAME] |
| | This command clears the statistic of the GVRP for the specific port. |
| gvrp | |
| | This command enables the global GVRP function for the Switch. |
| no gvrp | |
| | This command disables the global GVRP function for the Switch. |
| no gvrp configuration | |
| | This command sets the GVRP configurations to defaults. |
| gvrp registration | (normal fixed forbidden) |
| | This command configures the registration mode for the specific port. Normal registration mode: Allows dynamic creation, registration, and deregistration of VLANs on the trunk port. Fixed registration mode: Allows manual creation and registration of VLANs, prevents VLAN deregistration, and registers all known VLANs on other ports on the trunk port. Forbidden registration mode: Deregisters all VLANs (except VLAN 1) and prevents any further VLAN creation or registration on the trunk port. |
| gvrp | |
| | This command enables the GVRP for the specific port. |

| | |
|---------|---|
| no gvrp | |
| | This command disables the GVRP for the specific port. |

Dot 1x

| Dot1x CLI Commands | |
|-------------------------------|---|
| Command | Parameters |
| show dot1x | |
| | This command displays the current 802.1X configurations. |
| show dot1x username | |
| | This command displays the current user accounts for the local authentication. |
| show dot1x accounting-record | |
| | This command displays the local accounting records. |
| dot1x system-auth-control | |
| | This command enables the 802.1X port authentication on the Switch. |
| no dot1x system-auth-control | |
| | This command disables the 802.1X port authentication on the Switch. |
| dot1x authentic-method | (local radius) |
| | This command configures the authentic method of 802.1X. (Default: local). |
| no dot1x authentic-method | |
| | This command configures the authentic method of 802.1X to default. |
| dot1x radius | primary-server-ip <IP> port PORTID |
| | This command configures the primary RADIUS server. |
| dot1x radius | primary-server-ip <IP> port PORTID key KEY |
| | This command configures the primary RADIUS server. |
| dot1x radius | secondary-server-ip <IP> port PORTID |
| | This command configures the secondary RADIUS server. |
| dot1x radius | secondary-server-ip <IP> port PORTID key KEY |
| | This command configures the secondary RADIUS server. |
| no dot1x radius | secondary-server-ip |
| | This command removes the secondary RADIUS server. |
| dot1x username | <STRING> passwd <STRING> |
| | This command configures the user account for local authentication. |
| no dot1x username | <STRING> |
| | This command deletes the user account for local authentication. |
| dot1x accounting | |
| | This command enables the dot1x accounting. |
| dot1x accounting-clean | |
| | This command cleans the local accounting records. |
| dot1x admin-control-direction | (both in) |
| | This command configures the control direction for blocking packets. |
| dot1x default | |

| | |
|---------------------------|--|
| | This command sets the port configuration to default settings. |
| dot1x max-req | <1-10> |
| | This command sets the max-req times of a port. (1~10). |
| dot1x port-control | (auto force-authorized force-unauthorized) |
| | This command configures the port control mode. auto → Users can access network after authenticating. force-authorized → Users can access network without authentication. force-unauthorized → Users can not access network. |
| dot1x port-enable | |
| | This command configures the port control mode to default. |
| no dot1x port-enable | |
| | This command configures the port control mode to default. |
| dot1x reauthentication | |
| | This command enables reauthentication of a port. |
| no dot1x reauthentication | |
| | This command disables reauthentication of a port. |
| dot1x timeout | quiet-period |
| | This command configures the quiet-period value, which is the period that an authenticator will not attempt to acquire a Supplicant in quiet period. |
| dot1x timeout | server-timeout |
| | This command configures the server-timeout value, which is used for timing out the Authentication Server. |
| dot1x timeout | reauth-period |
| | This command configures the reauth-period value, which determines when reauthentication of a Supplicant takes place. |
| dot1x timeout | supp-timeout |
| | This command configures the supp-timeout value which is the initialization value used for timing out a Supplicant |
| dot1x guest-vlan | VLAN_ID |
| | This command configures the guest VLAN. |
| no dot1x guest-vlan | VLAN_ID |
| | This command deletes the guest VLAN. |

Customer Support and Contact

For all questions related to the MEN-6532 or any other Volktek product, please contact Volktek customer support:

| | |
|---------|---|
| Address | Volktek Customer Support 4F, 192 Liancheng Road, Zhonghe District, New Taipei City 23553 Taiwan |
| Phone | +886-2-8242-1000 |
| Fax | +886-2-8242-3333 |
| Email | support@volktek.com |
| Website | www.volktek.com |