10/100/1000Mbps

24-port + 1 Mini-GBIC

Managed Gigabit Ethernet Switch

WGSW-24010

User's Manual

Trademarks

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User 's Manual. PLANET makes no commitment to update or keep current the information in this User 's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

FCC Warning

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

CE Mark Warning

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.

Revision

PLANET Gigabit Ethernet Switch User's Manual
FOR MODELS: WGSW-24010
Part No.: EM_WGSW24010

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Package Contents

Check the contents of your package for following parts:

- Managed Gigabit Ethernet Switch x1
- CD-ROM user's manual x1
- Quick installation guide x1
- 19” rack mounting kit x1
- Power cord x1
- Rubber feet x 4

If any of these are missing or damaged, please contact your dealer immediately, if possible, retain the carton including the original packing material, and use them against to repack the product in case there is a need to return it to us for repair.

1.2 How to Use This Manual

This Web Smart Gigabit Ethernet Switch User Manual is structured as follows:

- Section 2, **Installation**
  It explains the functions of WGSW-24010 and how to physically install the WGSW-24010.
- Section 3, **Configuration**
  It contains information about the Smart function of WGSW-24010.
- Section 4, **Switch operation**
  It contains specifications of WGSW-24010.
- **Appendices**
  It contains cable information of WGSW-24010.

In the following section, terms “**Switch**” with upper case means the two switches, i.e. WGSW-24010. Terms with lower case “switch” means any Ethernet switches.

1.3 Product Features

- Complies with IEEE802.3, 10Base-T, IEEE802.3u, 100Base-TX and IEEE802.3ab, 1000Base-T and IEEE802.z 1000Base-SX/LX Ethernet standard
- 24 10/100/1000Mbps Ethernet ports, Auto MDI/MDI-X, Virtual Cable Test Support
- 1 Mini-GBIC for 1000Base-SX/LX fiber-optic interface with various connection media and distances
- Features Store-and-Forward mode with wire-speed filtering and forwarding rates
- Hardware based 10/100Mbps, half/full duplex and 1000Mbps full duplex mode, flow control and auto-negotiation
- IEEE802.3x flow control for full duplex operation and backpressure for half duplex operation
- Integrated address look-up engine, support 4K absolute MAC addresses, automatic address learning and address aging
- 400KB on chip frame buffer
- 9K Jumbo packet size support
- IEEE802.1q VLAN, up to 256 VLANS, IEEE802.1p four priority with Weight Round Robins
- LACP Link aggregation, port mirroring support
- IGMP Snooping, Storm control

- IEEE802.1d, IEEE802.1w, classic Spanning Tree Algorithm or Rapid Spanning Tree support
- Web, Telnet/Console Command Line management, SNMP v1, v2C
- RMON Group 1, 2, 3, 9
- Virtual Cable Test (VCT) technology provides the mechanism to detect and report potential cabling issues, such as cable opens, cable shorts, etc. on Copper Links
- 100~240VAC, 50~60Hz universal Power input
- FCC, CE class A compliant

1.4 Product Specifications

Model	WGSW-24010	
Hardware Specification		
Network Ports	24 10/100/100 Base-T STP ports 1 Mini-GBIC for 1000Base-SX/LX fiber-optic interface (shared with port 12)	
Switch Processing Scheme	Store-and-Forward	
Switch fabric	48Gbps	
Throughput (packet per second)	35.7Mbps	
Address Table	4K entries	
Share data Buffer	512KB	
Flow Control	Back pressure for half duplex, IEEE 802.3x Pause Frame for full duplex	
Dimensions	440 x 200 x 44 mm (1U height)	
Weight	2.64 kg	
Power Requirement	100~240 VAC, 50-60 Hz	
Temperature	Operating: 0~50 degree C, Storage -20~70 degree	
Humidity	Operating: 10% to 90%, Storage: 5% to 95% (Non-condensing)	
Management		
Management Interface	Web, Console, Telnet and SNMP	
Features	RFC 1157 SNMP v1/v2 RFC 1213 MIB II RFC 1493 Bridge MIB RFC 1643 Ethernet MIB RFC 1757 RMON 4 groups: stats, history, Alarms & Events	
Standards Conformance		
Regulation Compliance	FCC Part 15 Class A, CE	
Standards Compliance	IEEE 802.3 Ethernet IEEE 802.3u Fast Ethernet IEEE 802.3z/802.3ab Gigabit Ethernet IEEE 802.3x Flow Control IEEE 802.1p QoS priority IEEE 802.1Q VLAN tag IEEE 802.1D Spanning Tree Protocol IEEE802.1w Rapid Spanning Tree	RFC 768 UDP RFC 783 TFTP RFC 791 IP RFC 792 ICMP RFC 826 ARP RFC 854 Telnet RFC 2068 HTTP RFC 2236 IGMPv2

2. INSTALLATION

This section describes the functionalities of the Switch 's components and guides how to install it on the desktop or shelf. Basic knowledge of networking is assumed. Please read this chapter completely before continuing.

2.1 Product Description

The WGSW-24010 is a powerful, high-performance 24G + 1 Mini-GBIC 10/100/1000Mbps Fast Ethernet and Gigabit managed switch with twenty-four 10/100/1000Mbps ports and 1-SFP Mini-GBIC interfaces. The SFP Mini-GBIC interfaces for fiber extension is ideal for backbone connection to other workgroup products.

2.1.1 Product Overview

All RJ-45 copper interfaces of WGSW-24010 support 10/100/1000Mbps Auto-Negotiation for optimal speed detection through RJ-45 Category 6, 5 or 5e cables. Also, all the ports support Auto-MDI/MDI-X that can detect the type of connection to any Ethernet device without requiring special straight or crossover cables.

The powerful management capabilities of the device can be managed using the console, telnet or the web. SNMP MIB-II. Entity MIB and RMON are supported to provide maximum management functionality, providing a useful platform for system managers to monitor and administer the system efficiently. A complete set of diagnostic LED's are provided to simplify troubleshooting and provide a visible operating status. The IEEE 802.1Q VLAN tagging feature makes logically separating nodes easier with up to 256 VLAN groups allowed. Port trunking is also supported with up to 8 trunk groups on single switch. To simplify network troubleshooting when using sniffer software, the WGSW-24010 also supports port mirroring to duplicate up to 2 ports' transmitting and receiving packets to a specified sniffer port.

2.1.2 Switch Front Panel

Figure 2-1 shows a front panel of the Switch.

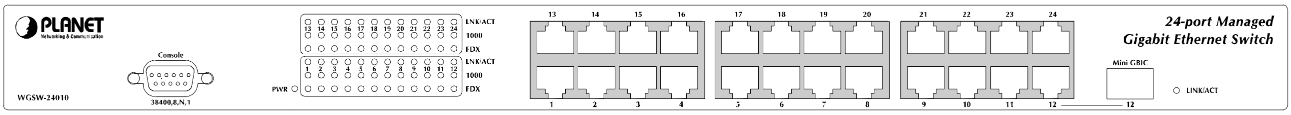


Figure 2-1 WGSW-24010 front panel

2.1.3 LED Indicators

LED	Color	Function
PWR	Green	Lights to indicate that the Switch has power.
LNK/ACT	Green	Lights to indicate that the Switch is successfully connecting to the network. Blinks to indicate the Switch is actively receiving or sending the data over the port.
1000	Orange	Lights to indicate that the port is operating at 1000 Mbps. Off to indicate that the port is operating at 100Mbps or 10 Mbps while the port 's Link is on.
FDX	Green	Lights to indicate that the port is operating in full duplex mode. Off to indicate that the port is operating in half duplex mode.

2.1.4 Switch Rear Panel

The rear panel of the Switch indicates an AC inlet power socket, which accepts input power from 100 to 240VAC, 50-60Hz.

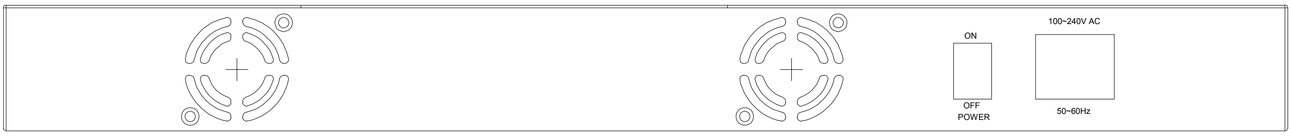


Figure 2-3 WGSW-24010 Rear Panel

Power Notice:

1. The device is a power-required device, it means, it will not work till it is powered. If your networks should active all the time, please consider using UPS (Uninterrupted Power Supply) for your device. It will prevent you from network data loss or network downtime.

2. In some area, installing a surge suppression device may also help to protect your switch from being damaged by unregulated surge or current to the Switch or the power adapter.

2.2 Installing the Switch

This section describes how to install your WGSW-24010 Managed Gigabit Ethernet Switch and make connections to the Switch. Please read the following topics and perform the procedures in the order being presented. PLANET Managed Gigabit Ethernet Switch do not need software configuration. To install the Switch on a desktop or shelf, simply complete the following steps.

2.2.1 Desktop Installation

To install a Switch on a desktop or shelf, simply complete the following steps:

Step1: Attach the rubber feet to the recessed areas on the bottom of the switch.

Step2: Place the Switch on a desktop or shelf near an AC power source.

Step3: Keep enough ventilation space between the switch and the surrounding objects.

✍ ***Note:*** When choosing a location, please keep in mind the environ mental restrictions discussed in Chapter 1, Section 4, in Specification.

Step4: Connect your Switch to network devices.

A. Connect one end of a standard network cable to the 10/100/1000 RJ-45 ports on the front of the Switch

B. Connect the other end of the cable to the network devices such as printer servers, workstations or routers …etc.

✍ ***Note:*** Connection to the Switch requires UTP Category 5 network cabling with RJ-45 tips. For more information, please see the Cabling Specification in Appendix A.

Step5**:** Supply power to the Switch.

A. Connect one end of the power cable to the SWITCH.

B. Connect the power plug of the power cable to a standard wall outlet.

When the Switch receives power, the Power LED should remain solid Green.

2.2.2 Rack Mounting

To install the switch in a **19-inch** standard rack, follow the instructions described below.

Step1: Place your Switch on a hard flat surface, with the front panel positioned towards your front side.

Step2: Attach a rack-mount bracket to each side of the switch with supplied screws attached to the package. Figure 2-5 shows how to attach brackets to one side of the switch.

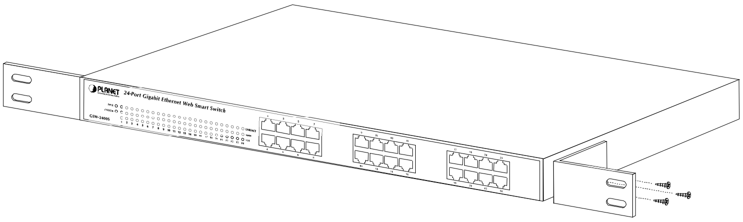


Figure 2-5 Attaching the brackets to the WGSW-24010

Caution:

You must use the screws supplied with the mounting brackets. Damage caused to the parts by using incorrect screws would invalidate your warranty.

Step3: Secure the brackets tightly.

Step4: Follow the same steps to attach the second bracket to the opposite side.

Step5: After the brackets are attached to the Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-6

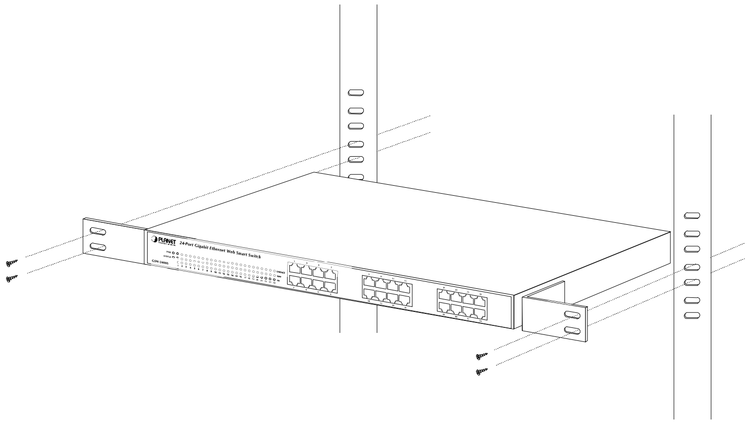


Figure 2-6 Mounting the Switch in a Rack

Step6: Proceeds with the steps 4 and steps 5 of session **2.2.1 Desktop Installation** to connect the network cabling and supply power to your switch.

3. CONFIGURATION

The WGSW-24010 is a managed Ethernet Switch that can be controlled by the RS-232 console interface, telnet interface, and Web interface. This chapter describer how to configure the Switch through these interfaces.

3.1 Configure through RS-232 console interface

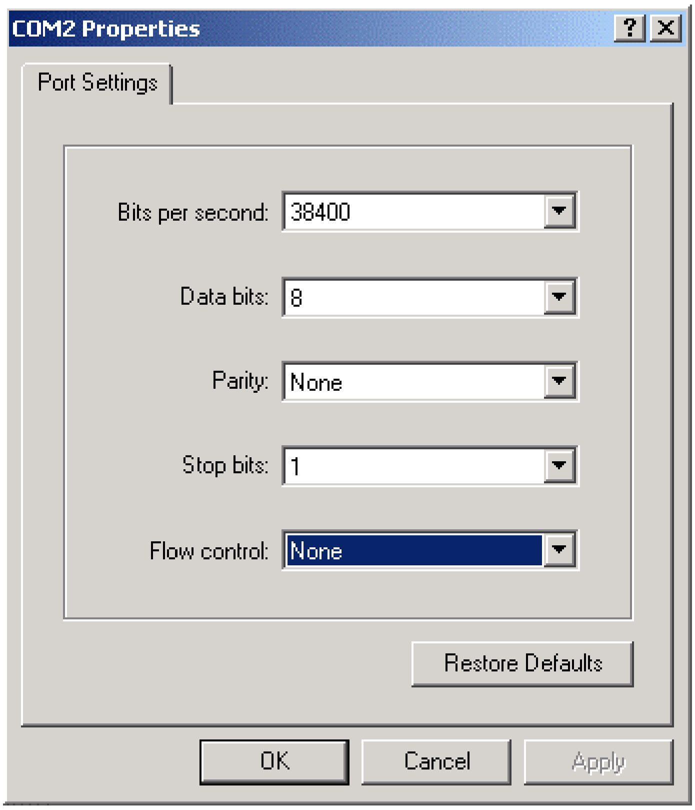
When you are ready to configure the smart functions of the Switch, make sure you had connected the supplied RS-232 serial cable to the RS-232 port at the front panel of your WGSW-24010 Switch and your PC.

3.1.1 Connect to PC's RS-232 serial port

Hyper Terminal

In Windows 98/2000/XP, launch "HyperTerminal", create a new connection, and adjust settings as below:

- Baud per second: 38400
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow Control: None



Bits per second: 38400

Data bits: 8

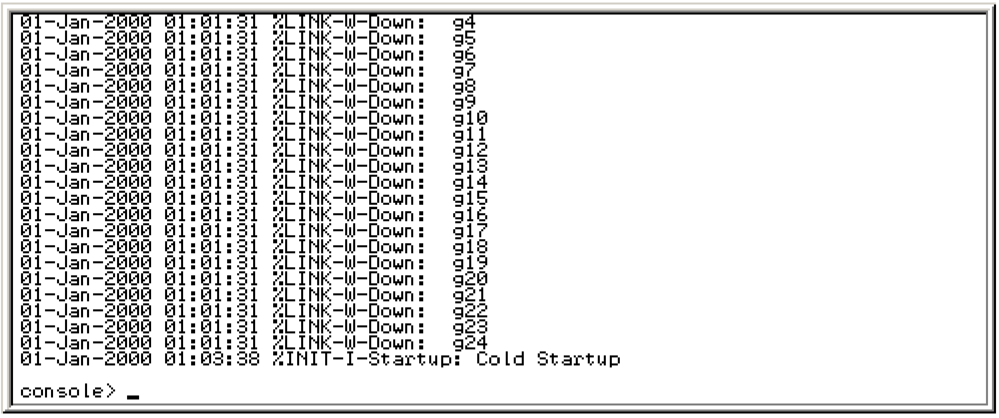
Parity: None

Stop bits: 1

Flow control: None

3.1.2 Configure IP Address

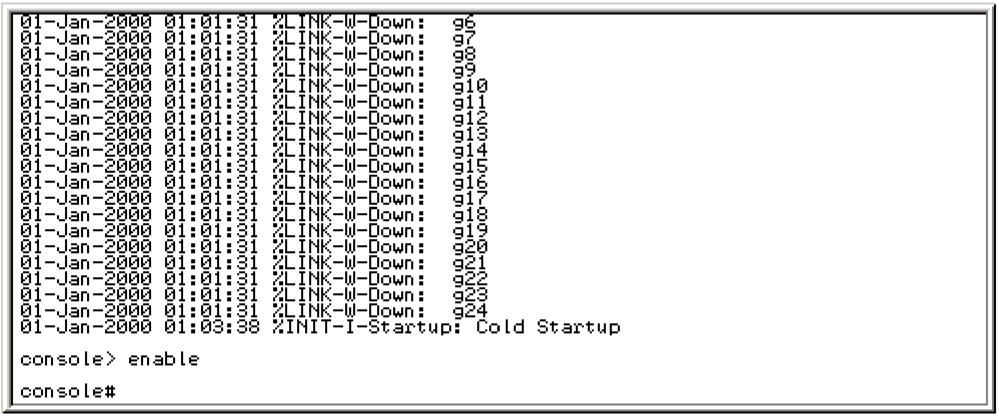
Power on the WGSW-24010, the terminal will display that it is running testing procedures. After boot, the following screen displayed.



```
01-Jan-2000 01:01:31 %LINK-W-Down:  g4
01-Jan-2000 01:01:31 %LINK-W-Down:  g5
01-Jan-2000 01:01:31 %LINK-W-Down:  g6
01-Jan-2000 01:01:31 %LINK-W-Down:  g7
01-Jan-2000 01:01:31 %LINK-W-Down:  g8
01-Jan-2000 01:01:31 %LINK-W-Down:  g9
01-Jan-2000 01:01:31 %LINK-W-Down:  g10
01-Jan-2000 01:01:31 %LINK-W-Down:  g11
01-Jan-2000 01:01:31 %LINK-W-Down:  g12
01-Jan-2000 01:01:31 %LINK-W-Down:  g13
01-Jan-2000 01:01:31 %LINK-W-Down:  g14
01-Jan-2000 01:01:31 %LINK-W-Down:  g15
01-Jan-2000 01:01:31 %LINK-W-Down:  g16
01-Jan-2000 01:01:31 %LINK-W-Down:  g17
01-Jan-2000 01:01:31 %LINK-W-Down:  g18
01-Jan-2000 01:01:31 %LINK-W-Down:  g19
01-Jan-2000 01:01:31 %LINK-W-Down:  g20
01-Jan-2000 01:01:31 %LINK-W-Down:  g21
01-Jan-2000 01:01:31 %LINK-W-Down:  g22
01-Jan-2000 01:01:31 %LINK-W-Down:  g23
01-Jan-2000 01:01:31 %LINK-W-Down:  g24
01-Jan-2000 01:03:38 %INIT-I-Startup: Cold Startup

console> _
```

Figure 3-1 Console Main Screen of WGSW-24010

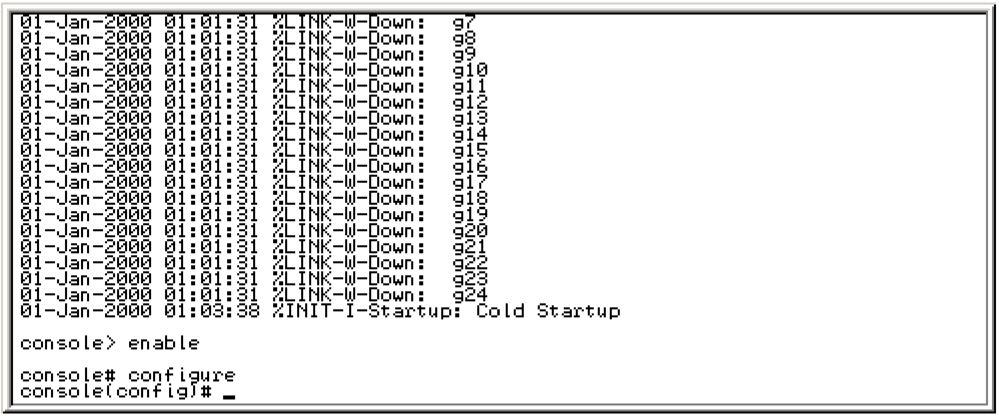
1. On **“console>”** prompt, enter **“enable”** to enable the privileged commands. The original prompt, **“console>”** will become **“console#”.** As show in Figure 3-2.



```
01-Jan-2000 01:01:31 %LINK-W-Down:  g6
01-Jan-2000 01:01:31 %LINK-W-Down:  g7
01-Jan-2000 01:01:31 %LINK-W-Down:  g8
01-Jan-2000 01:01:31 %LINK-W-Down:  g9
01-Jan-2000 01:01:31 %LINK-W-Down:  g10
01-Jan-2000 01:01:31 %LINK-W-Down:  g11
01-Jan-2000 01:01:31 %LINK-W-Down:  g12
01-Jan-2000 01:01:31 %LINK-W-Down:  g13
01-Jan-2000 01:01:31 %LINK-W-Down:  g14
01-Jan-2000 01:01:31 %LINK-W-Down:  g15
01-Jan-2000 01:01:31 %LINK-W-Down:  g16
01-Jan-2000 01:01:31 %LINK-W-Down:  g17
01-Jan-2000 01:01:31 %LINK-W-Down:  g18
01-Jan-2000 01:01:31 %LINK-W-Down:  g19
01-Jan-2000 01:01:31 %LINK-W-Down:  g20
01-Jan-2000 01:01:31 %LINK-W-Down:  g21
01-Jan-2000 01:01:31 %LINK-W-Down:  g22
01-Jan-2000 01:01:31 %LINK-W-Down:  g23
01-Jan-2000 01:01:31 %LINK-W-Down:  g24
01-Jan-2000 01:03:38 %INIT-I-Startup: Cold Startup

console> enable

console#
```

Figure 3-2 Enable privileged commands

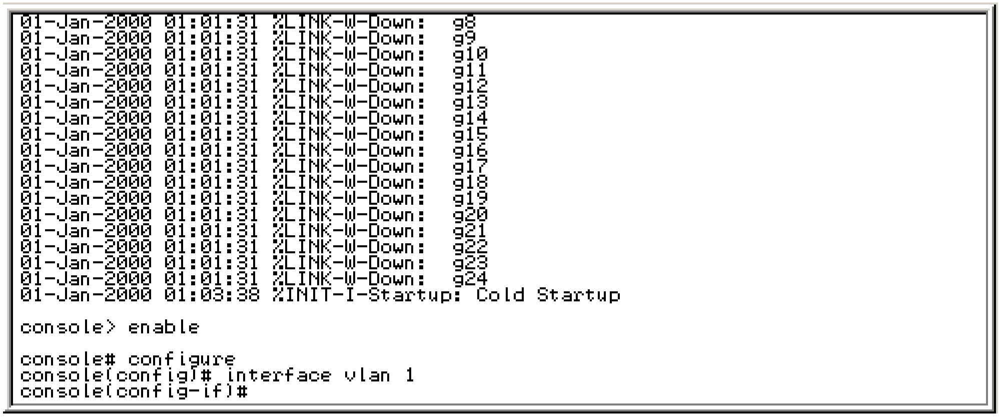
2. On **“console#”** prompt, enter “configure” to enter the configuration mode. The prompt **“console#”** then become **”console(config)#”.** As show in Figure 3-3.



```
01-Jan-2000 01:01:31 %LINK-W-Down:  g7
01-Jan-2000 01:01:31 %LINK-W-Down:  g8
01-Jan-2000 01:01:31 %LINK-W-Down:  g9
01-Jan-2000 01:01:31 %LINK-W-Down:  g10
01-Jan-2000 01:01:31 %LINK-W-Down:  g11
01-Jan-2000 01:01:31 %LINK-W-Down:  g12
01-Jan-2000 01:01:31 %LINK-W-Down:  g13
01-Jan-2000 01:01:31 %LINK-W-Down:  g14
01-Jan-2000 01:01:31 %LINK-W-Down:  g15
01-Jan-2000 01:01:31 %LINK-W-Down:  g16
01-Jan-2000 01:01:31 %LINK-W-Down:  g17
01-Jan-2000 01:01:31 %LINK-W-Down:  g18
01-Jan-2000 01:01:31 %LINK-W-Down:  g19
01-Jan-2000 01:01:31 %LINK-W-Down:  g20
01-Jan-2000 01:01:31 %LINK-W-Down:  g21
01-Jan-2000 01:01:31 %LINK-W-Down:  g22
01-Jan-2000 01:01:31 %LINK-W-Down:  g23
01-Jan-2000 01:01:31 %LINK-W-Down:  g24
01-Jan-2000 01:03:38 %INIT-I-Startup: Cold Startup

console> enable

console# configure
console(config)# _
```

Figure 3-3 Enter configuration mode

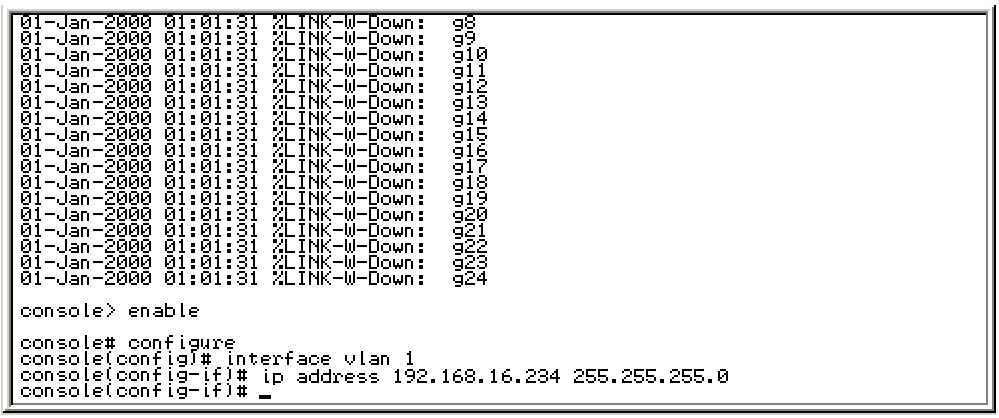
3. On **“console(config)#”** prompt, enter **“interface vlan 1”** to configure the default IEEE 802.1 VLAN. The prompt **“console(config)#”** then change to **“console(config-if)#”.** As show in Figure 3-4.



```
01-Jan-2000 01:01:31 %LINK-W-Down:  g8
01-Jan-2000 01:01:31 %LINK-W-Down:  g9
01-Jan-2000 01:01:31 %LINK-W-Down:  g10
01-Jan-2000 01:01:31 %LINK-W-Down:  g11
01-Jan-2000 01:01:31 %LINK-W-Down:  g12
01-Jan-2000 01:01:31 %LINK-W-Down:  g13
01-Jan-2000 01:01:31 %LINK-W-Down:  g14
01-Jan-2000 01:01:31 %LINK-W-Down:  g15
01-Jan-2000 01:01:31 %LINK-W-Down:  g16
01-Jan-2000 01:01:31 %LINK-W-Down:  g17
01-Jan-2000 01:01:31 %LINK-W-Down:  g18
01-Jan-2000 01:01:31 %LINK-W-Down:  g19
01-Jan-2000 01:01:31 %LINK-W-Down:  g20
01-Jan-2000 01:01:31 %LINK-W-Down:  g21
01-Jan-2000 01:01:31 %LINK-W-Down:  g22
01-Jan-2000 01:01:31 %LINK-W-Down:  g23
01-Jan-2000 01:01:31 %LINK-W-Down:  g24
01-Jan-2000 01:03:38 %INIT-I-Startup: Cold Startup

console> enable

console# configure
console(config)# interface vlan 1
console(config-if)#
```

Figure 3-4 Configure interface VLAN 1

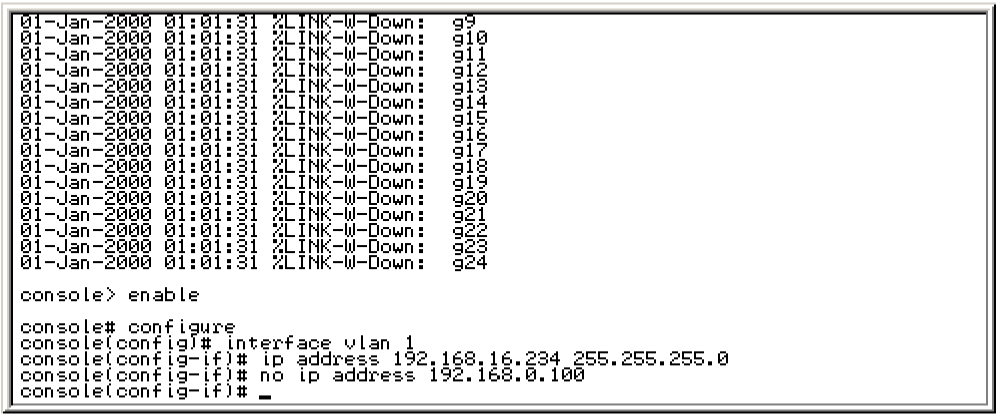
4. On **"console(config-if)#"** prompt, enter **"ip address A.B.C.D E.F.G.H"** to add a new IP address. Note that A.B.C.D is your new IP address and E.F.G.H is needed for the subnet mask. For example, enter **"ip address 192.168.16.234 255.255.255.0"** will add a new IP address to WGSW-24010. As show in Figure 3-5.



```
01-Jan-2000 01:01:31 %LINK-W-Down:  g8
01-Jan-2000 01:01:31 %LINK-W-Down:  g9
01-Jan-2000 01:01:31 %LINK-W-Down:  g10
01-Jan-2000 01:01:31 %LINK-W-Down:  g11
01-Jan-2000 01:01:31 %LINK-W-Down:  g12
01-Jan-2000 01:01:31 %LINK-W-Down:  g13
01-Jan-2000 01:01:31 %LINK-W-Down:  g14
01-Jan-2000 01:01:31 %LINK-W-Down:  g15
01-Jan-2000 01:01:31 %LINK-W-Down:  g16
01-Jan-2000 01:01:31 %LINK-W-Down:  g17
01-Jan-2000 01:01:31 %LINK-W-Down:  g18
01-Jan-2000 01:01:31 %LINK-W-Down:  g19
01-Jan-2000 01:01:31 %LINK-W-Down:  g20
01-Jan-2000 01:01:31 %LINK-W-Down:  g21
01-Jan-2000 01:01:31 %LINK-W-Down:  g22
01-Jan-2000 01:01:31 %LINK-W-Down:  g23
01-Jan-2000 01:01:31 %LINK-W-Down:  g24

console> enable

console# configure
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.234 255.255.255.0
console(config-if)# _
```

Figure 3-5 Add IP address

5. If you want to delete the default ip address, enter **"no ip address 192.168.0.100".** As show in Figure 3-6.



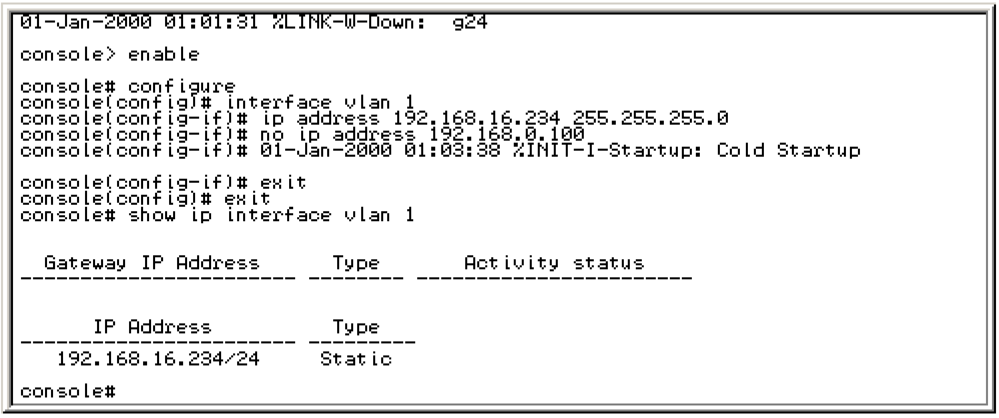
```
01-Jan-2000 01:01:31 %LINK-W-Down:  g9
01-Jan-2000 01:01:31 %LINK-W-Down:  g10
01-Jan-2000 01:01:31 %LINK-W-Down:  g11
01-Jan-2000 01:01:31 %LINK-W-Down:  g12
01-Jan-2000 01:01:31 %LINK-W-Down:  g13
01-Jan-2000 01:01:31 %LINK-W-Down:  g14
01-Jan-2000 01:01:31 %LINK-W-Down:  g15
01-Jan-2000 01:01:31 %LINK-W-Down:  g16
01-Jan-2000 01:01:31 %LINK-W-Down:  g17
01-Jan-2000 01:01:31 %LINK-W-Down:  g18
01-Jan-2000 01:01:31 %LINK-W-Down:  g19
01-Jan-2000 01:01:31 %LINK-W-Down:  g20
01-Jan-2000 01:01:31 %LINK-W-Down:  g21
01-Jan-2000 01:01:31 %LINK-W-Down:  g22
01-Jan-2000 01:01:31 %LINK-W-Down:  g23
01-Jan-2000 01:01:31 %LINK-W-Down:  g24

console> enable

console# configure
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.234 255.255.255.0
console(config-if)# no ip address 192.168.0.100
console(config-if)# _
```

Figure 3-6 Delete default IP address

6. Enter **"exit"** to exit the vlan configuration mode. The prompt **"console (config-if)#"** will change to **"console(config)#".**

7. Enter **"exit"** again to exit the configuration mode. The prompt **"console(config)#"** will become **"console#".**

8. On **"console#"** prompt, enter **"show ip interface vlan 1"** to check if the IP address is changed. As show in Figure 3-7.



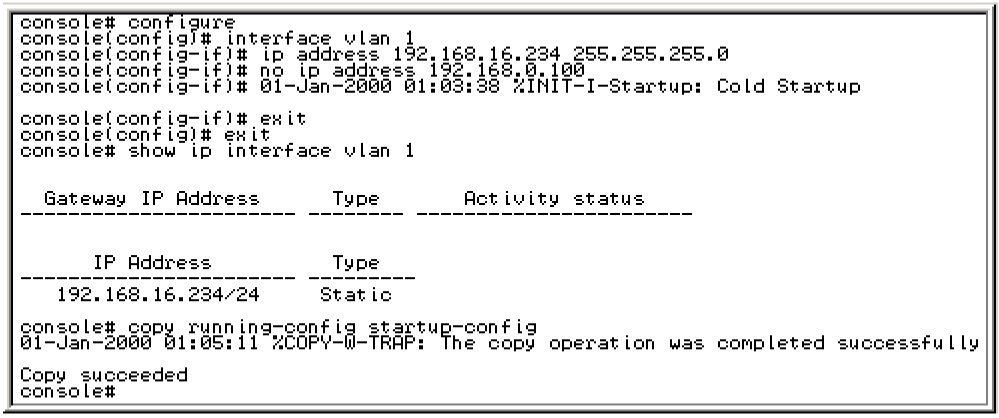
```
01-Jan-2000 01:01:31 %LINK-W-Down:  g24

console> enable

console# configure
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.234 255.255.255.0
console(config-if)# no ip address 192.168.0.100
console(config-if)# 01-Jan-2000 01:03:38 %INIT-I-Startup: Cold Startup

console(config-if)# exit
console(config)# exit
console# show ip interface vlan 1

  Gateway IP Address      Type       Activity status
----------------------- -------- ------------------------


       IP Address         Type
----------------------- ---------
   192.168.16.234/24     Static

console#
```

Figure 3-7 Show IP address

3.1.3 Change Username and Password

For security reason, we strongly suggest that you change user name and password immediately.

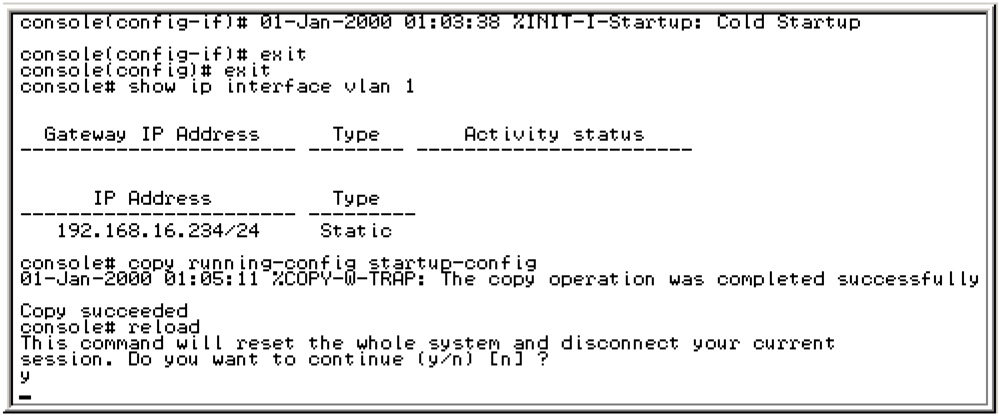
1. On **"console#"** prompt, enter "configure" to enter the configuration mode. The prompt **"console#"** then become**"console(config)#".**
2. On **"console(config)#"** prompt, enter **"no username admin"** to delete the default user. As show in Figure 3-8.



```
console# configure
console(config)# interface vlan 1
console(config-if)# ip address 192.168.16.234 255.255.255.0
console(config-if)# no ip address 192.168.0.100
console(config-if)# 01-Jan-2000 01:03:38 %INIT-I-Startup: Cold Startup

console(config-if)# exit
console(config)# exit
console# show ip interface vlan 1

  Gateway IP Address      Type       Activity status
----------------------- -------- ------------------------


       IP Address         Type
----------------------- ---------
   192.168.16.234/24     Static

console# copy running-config startup-config
01-Jan-2000 01:05:11 %COPY-W-TRAP: The copy operation was completed successfully

Copy succeeded
console#
```

Figure 3-8 Delete default user

3. Enter **"username AAAA password BBBB level N"** to add a new username/password. Where **AAAA** is the new username, **BBBB** is the new password and **N** is the access level, upper case and lower case is sensitive for username and password. For example, if you want to add **"supervisor"** as a new username and **"99888899"** as the relative password and with full management privilege, the command will be **"username supervisor password 99888899 level 15"**. As show in Figure 3-9.



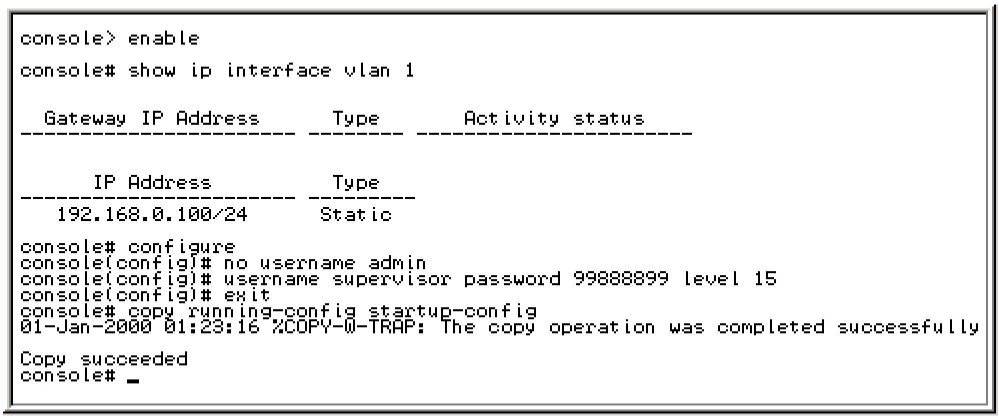
```
console(config-if)# 01-Jan-2000 01:03:38 %INIT-I-Startup: Cold Startup

console(config-if)# exit
console(config)# exit
console# show ip interface vlan 1

  Gateway IP Address      Type       Activity status
----------------------- -------- ------------------------


       IP Address         Type
----------------------- ---------
   192.168.16.234/24     Static

console# copy running-config startup-config
01-Jan-2000 01:05:11 %COPY-W-TRAP: The copy operation was completed successfully

Copy succeeded
console# reload
This command will reset the whole system and disconnect your current
session. Do you want to continue (y/n) [n] ?
y
_
```

Figure 3-9 Add new username/password

3.1.4 Save your configuration

The configurations you modified in console will **NOT** save to next startup until you copy the running configuration to the startup configuration.

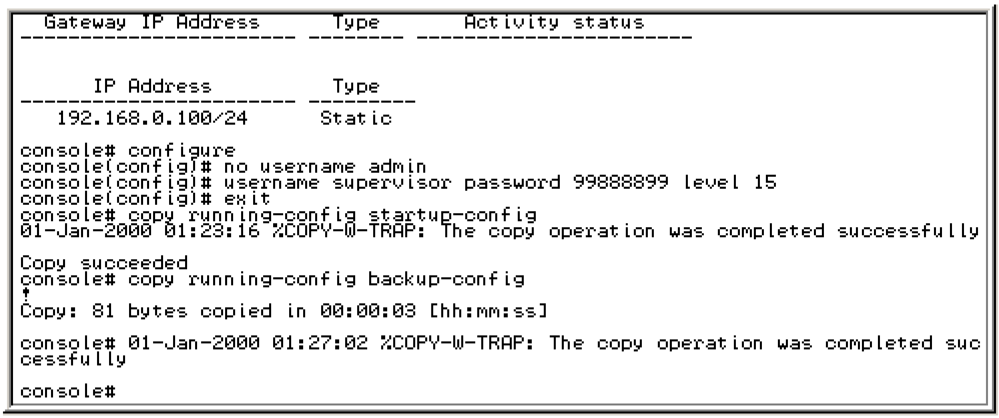
1. Enter **“exit”** to exit the configuration mode. The prompt **“console(config)#”** will return to **“console#”.**
2. Enter **“copy running-config startup-config”** on **“console#”** prompt to save the changes. As show in Figure 3-10.



```
console> enable

console# show ip interface vlan 1

  Gateway IP Address      Type       Activity status
----------------------- -------- -----------------------


       IP Address         Type
----------------------- ---------
   192.168.0.100/24      Static

console# configure
console(config)# no username admin
console(config)# username supervisor password 99888899 level 15
console(config)# exit
console# copy running-config startup-config
01-Jan-2000 01:23:16 %COPY-W-TRAP: The copy operation was completed successfully

Copy succeeded
console# _
```

Figure 3-10 Copy running-config to startup-config

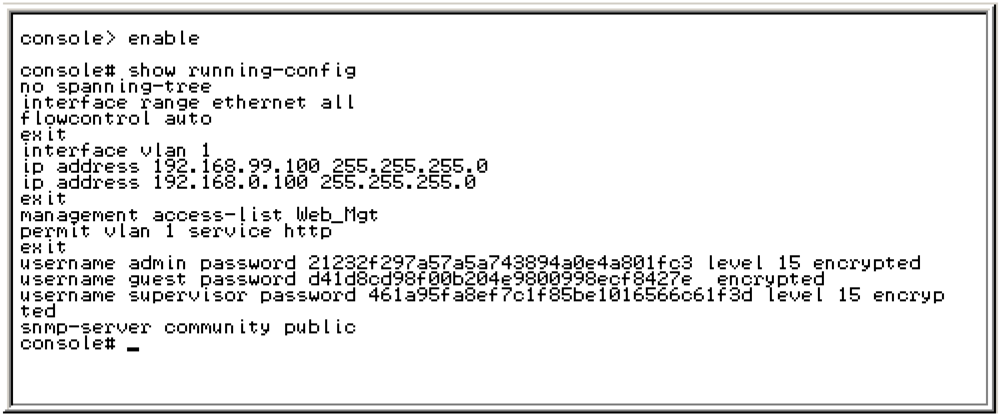
3. You can also make a copy of the running configuration to a backup configuration. As show in Figure 3-11.



```
  Gateway IP Address      Type       Activity status
----------------------- -------- -----------------------


       IP Address         Type
----------------------- ---------
   192.168.0.100/24      Static

console# configure
console(config)# no username admin
console(config)# username supervisor password 99888899 level 15
console(config)# exit
console# copy running-config startup-config
01-Jan-2000 01:23:16 %COPY-W-TRAP: The copy operation was completed successfully

Copy succeeded
console# copy running-config backup-config
!
Copy: 81 bytes copied in 00:00:03 [hh:mm:ss]

console# 01-Jan-2000 01:27:02 %COPY-W-TRAP: The copy operation was completed suc
cessfully

console#
```

Figure 3-11 Copy running-configure to backup-configure.

4. To ensure the configuration is saved and copied correctly, on “console#” prompt, enter **“show running-config”** to check the running configure, enter **“show startup-config”** to check the startup configuration, and **“show backup-config”** to check the backup configuration. Figure 3-12 show an example.



```
console> enable

console# show running-config
no spanning-tree
interface range ethernet all
flowcontrol auto
exit
interface vlan 1
ip address 192.168.99.100 255.255.255.0
ip address 192.168.0.100 255.255.255.0
exit
management access-list Web_Mgt
permit vlan 1 service http
exit
username admin password 21232f297a57a5a743894a0e4a801fc3 level 15 encrypted
username guest password d41d8cd98f00b204e9800998ecf8427e  encrypted
username supervisor password 461a95fa8ef7c1f85be1016566c61f3d level 15 encryp
ted
snmp-server community public
console# _
```

Figure 3-12 Show running configuration

✍ ***Note:*** If you are not familiar with console command or the related parameter, enter “help” anytime in console to get the help description.

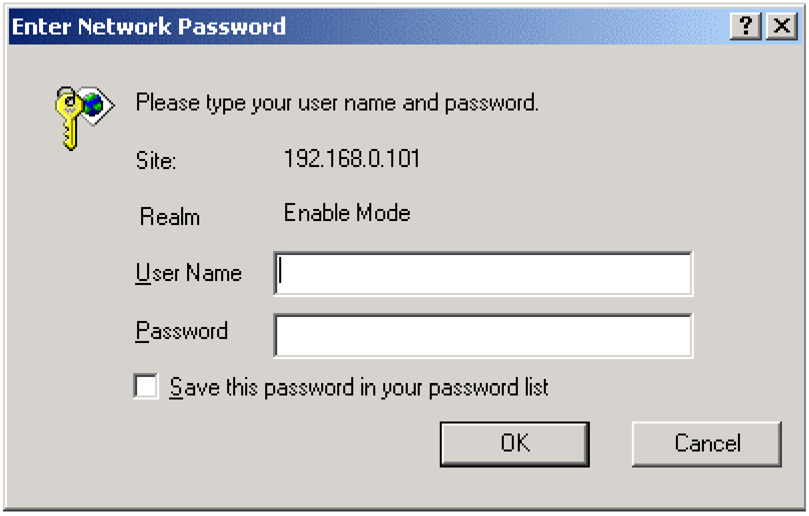
✍ ***Note:*** See Appendix B for factory default configuration.

3.2 Configure through Web browser interface

Besides the console interface, WGSW-24010 can be configured through an Ethernet connection, make sure the manager PC must be set on same the **IP subnet address** with the switch. For example, if you have changed the default IP address of the Switch to **192.168.16.234** with subnet mask **255.255.255.0** via console, then the manager PC should be set at **192.168.16.x** (where x is a number between 2 and 254) with subnet mask **255.255.255.0**. Or you can use the factory default IP address **192.168.0.100** to do the relative configuration on manager PC.

Use Internet Explorer 5.0 or above Web browser. Enter IP address **http://192.168.0.100** (the factory-default IP address or that you have changed via console) to access the Web interface.

When the following login screen appears, please enter the default username **"admin"** and password **“admin”** (or the username/password you have changed via console) to login the main screen of Switch. The login screen in Figure 3-13 appears.



Enter Network Password

Please type your user name and password.

Site: 192.168.0.101

Realm Enable Mode

User Name

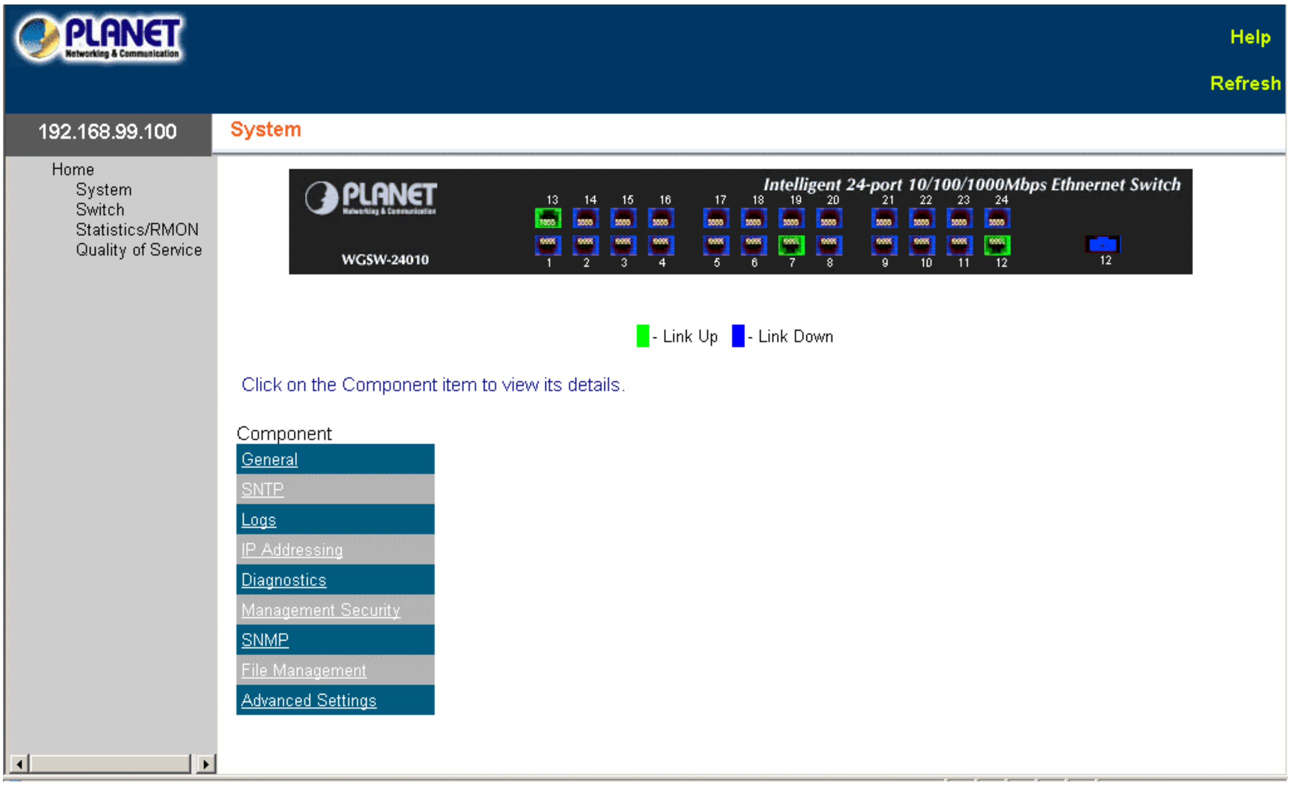
Password

□ Save this password in your password list

Figure 3-13 Login screen

Manin Menu

After a successful login, the main screen appears, the main screen displays the port status and a list of System section and the topics it provide. As showed in Figure 3-14.



Click on the Component item to view its details.

Figure 3-14 main menu screen

3.2.2 Configure System Information

The System section provides information for devining system parameters including security featrues, device software. Under system the folling topics are provided to devine and view the system informatin:

- **General**
- **SNTP**
- **Logs**
- **IP Addressing**
- **Diagnostics**
- **Management Security**
- **SNMP**
- **File Management**
- **Advanced Settings**

3.2.2.1 General

The General page contains links to pages that allow network managers to configure device parameters.

The General page contains links to the following topics:

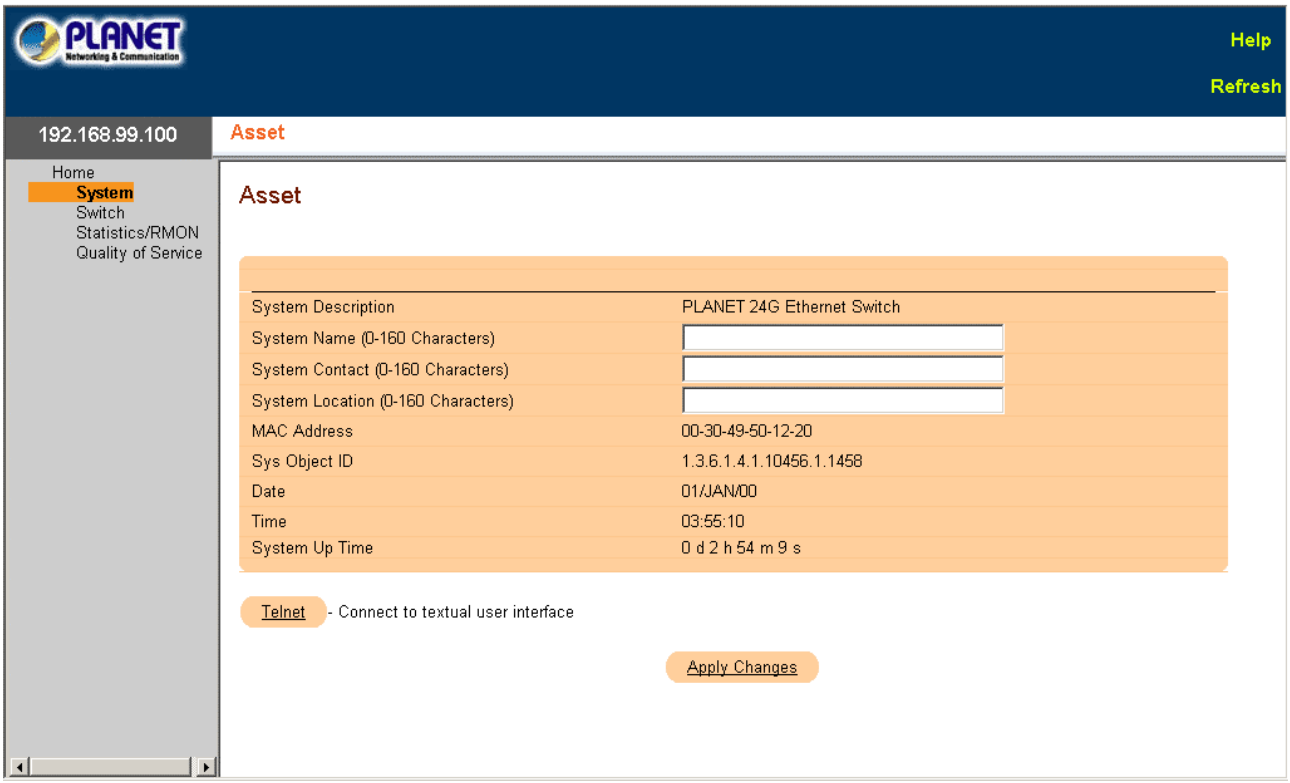
- **Asset**
- **Time Synchronization**
- **Health**
- **Versions**
- **Reset**

3.2.2.1.1 Assert

The **Asset** page contains parameters for configuring general device information, including the system name, location, and contact, the system MAC Address, System Object ID, date, time, and System Up Time.

To open **Access** screen perform the folling:

1. Click System -> General -> Assert
2. The Access information screen is displayed as in Figure 3-15.



System Description	PLANET 24G Ethernet Switch
System Name (0-160 Characters)	
System Contact (0-160 Characters)	
System Location (0-160 Characters)	
MAC Address	00-30-49-50-12-20
Sys Object ID	1.3.6.1.4.1.10456.1.1458
Date	01/JAN/00
Time	03:55:10
System Up Time	0 d 2 h 54 m 9 s

Figure 3-15 Asset information screen

The page includes the following fields:

- **System Name (0-160 Characters)** -- Defines the user-defined device name.
- **System Contact (0-160 Characters) --** Specifies the name of the contact person.
- **System Location (0-160 Characters)** -- The location where the system is currently running.
- **MAC Address** -- Specifies the device MAC address.
- **Sys Object ID** -- The vendor's authoritative identification of the network management subsystem contained in the entity.
- **Service Tag** -- The service reference number used when servicing the device.
- **Asset Tag (0-16 Characters) --** Specifies the user-defined device reference.
- **Serial No**. -- The device serial number.
- **Date (DD/MM/YY) --** The current date. The format is month, day, year, for example, 11/10/02 is November 10, 2002.
- **Time (HH:MM:SS)** -- Specifies the time. The format is hour, minute, second, for example, 20:12:03 is eight twelve and three seconds in the evening.
- **System Up Time** -- Specifies the amount of time since the last device reset. The system time is displayed in the following format: Days, Hours, Minutes and Seconds. For example, 41 days, 2 hours, 22 minutes and 15 seconds.

After entering the information, **"click Apply Changes"** to update the device.

3.2.2.1.2 Time Synchronization

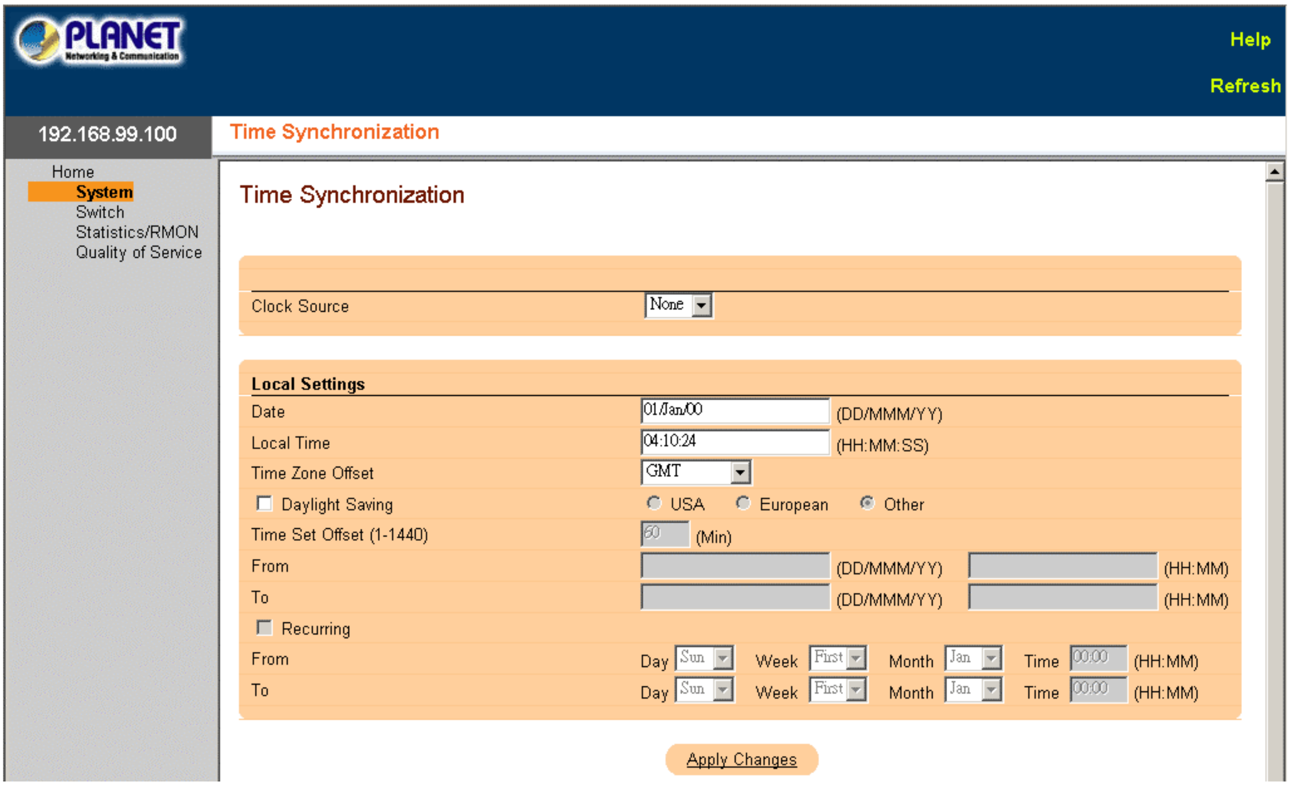
The **Time Synchronization** page contains fields for defining system time parameters for both the local hardware clock, and the external SNTP clock. If the system time is kept using an external SNTP clock, and the external SNTP clock fails, the system time reverts to the local hardware clock. Daylight Savings Time can be enabled on the device. Daylight Time start and end times in specific countries:

- Albania -- Last weekend of March until the last weekend of October.
- Australia -- From the end of October until the end of March.
- Australia - Tasmania -- From beginning of October until the end of March.
- Armenia -- Last weekend of March until the last weekend of October.
- Austria -- Last weekend of March until the last weekend of October.
- Bahamas -- From April to October, in conjunction with U.S. summer hours.
- Belarus -- Last weekend of March until the last weekend of October.
- Belgium -- Last weekend of March until the last weekend of October.
- Brazil -- From the 3rd Sunday in October until the 3rd Saturday in March. During the period of Daylight Saving Time, Brazilian clocks go forward one hour in most of the Brazilian southeast.
- Chile -- Easter Island 9th March until the 12th October. The first Sunday in March or after 9th March.
- China -- China does not operate Daylight Saving Time.
- Canada -- From the first Sunday in April until the last Sunday of October. Daylight Saving Time is usually regulated by provincial and territorial governments. Exceptions may exist in certain municipalities.
- Cuba -- From the last Sunday of March to the last Sunday of October.
- Cyprus -- Last weekend of March until the last weekend of October.
- Denmark -- Last weekend of March until the last weekend of October.
- Egypt -- Last Friday in April until the last Thursday in September.
- Estonia -- Last weekend of March until the last weekend of October.
- Finland -- Last weekend of March until the last weekend of October.
- France -- Last weekend of March until the last weekend of October.
- Germany -- Last weekend of March until the last weekend of October.
- Greece -- Last weekend of March until the last weekend of October.
- Hungary -- Last weekend of March until the last weekend of October.
- India -- India does not operate Daylight Saving Time.
- Iran -- From 1st Farvardin until the 1st Mehr.
- Iraq -- From 1st April until the 1st October.
- Ireland -- Last weekend of March until the last weekend of October.
- Israel -- Varies year-to-year.
- Italy -- Last weekend of March until the last weekend of October.
- Japan -- Japan does not operate Daylight Saving Time.
- Jordan -- Last weekend of March until the last weekend of October.
- Latvia -- Last weekend of March until the last weekend of October.
- Lebanon -- Last weekend of March and for the winter, until the last weekend of October.
- Lithuania -- Last weekend of March until the last weekend of October.
- Luxembourg -- Last weekend of March until the last weekend of October.
- Macedonia -- Last weekend of March until the last weekend of October.
- Mexico -- From the first Sunday in April at 02:00 to the last Sunday in October at 02:00.
- Moldova -- Last weekend of March until the last weekend of October.
- Montenegro -- Last weekend of March until the last weekend of October.
- Netherlands -- Last weekend of March until the last weekend of October.
- New Zealand -- From the first Sunday in October until the first Sunday on or after 15th March.

- Norway -- Last weekend of March until the last weekend of October.
- Paraguay -- From 6th April until 7th September.
- Poland -- Last weekend of March until the last weekend of October.
- Portugal -- Last weekend of March until the last weekend of October.
- Romania -- Last weekend of March until the last weekend of October.
- Russia -- From the 29th March until the 25th October.
- Serbia -- Last weekend of March until the last weekend of October.
- Slovak Republic -- Last weekend of March until the last weekend of October.
- South Africa -- South Africa does not operate Daylight Saving Time.
- Spain -- Last weekend of March until the last weekend of October.
- Sweden -- Last weekend of March until the last weekend of October.
- Switzerland -- Last weekend of March until the last weekend of October.
- Syria -- From 31st March until 30th October.
- Taiwan -- Taiwan does not operate Daylight Saving Time
- Turkey -- Last weekend of March until the last weekend of October.
- United Kingdom -- Last weekend of March until the last weekend of October.
- United States of America -- From the first Sunday in April at 02:00 to the last Sunday in October at 02:00.

To open **Time Synchronization** screen perform the folling:

1. Click System -> General -> Time Synchronization
2. The Time Synchronization screen is displayed as in Figure 3-16.



Time Synchronization

Clock Source: None

Local Settings

Date: 01/Jan/00 (DD/MMM/YY)

Local Time: 04:10:24 (HH:MM:SS)

Time Zone Offset: GMT

□ Daylight Saving ○ USA ○ European ● Other

Time Set Offset (1-1440): 60 (Min)

From: (DD/MMM/YY) (HH:MM)

To: (DD/MMM/YY) (HH:MM)

□ Recurring

From: Day Sun Week First Month Jan Time 00:00 (HH:MM)

To: Day Sun Week First Month Jan Time 00:00 (HH:MM)

Figure 3-16 Time Synchronization information screen

The Time Synchronization page is divided into the following sections:

- **Clock Source**
- **Local Settings**

Clock Source

The Clock Source section contains the following fields:

- **Clock Source --** The source used to set the system clock. The possible field values:
- **SNTP --** Specifies that the system time is set via an SNTP server. For more information, see "SNTP Global Settings".
- **None --** Specifies that the system time is not set by an external source.

Local Settings

The Local Settings section contains the following fields:

- **Date --** Defines the system date. The field format is Day:Month:Year, for example, 04 May 2050.
- **Local Time --** Defines the system time. The field format is HH:MM:SS, for example, 21:15:03.
- **Time Zone Offset --** The difference between Greenwich Mean Time (GMT) and local time. For example, the Time Zone Offset for Paris is GMT +1, while the local time in Taipei is GTM +8.
- There are two types of daylight settings, either by a specific date in a particular year or a recurring setting irrespective of the year. For a specific setting in a particular year complete the Daylight Savings area, and for a recurring setting, complete the Recurring area.
- **Daylight Savings --** Enables the Daylight Savings Time (DST) on the device based on the devices location. The possible field values are:
- **USA --** The device switches to DST at 2 a.m. on the first Sunday of April, and reverts to standard time at 2 a.m. on the last Sunday of October.
- **European --** The device switches to DST at 1:00 am on the last Sunday in March and reverts to standard time at 1:00 am on the last Sunday in October. The European option applies to EU members, and other European countries using the EU standard.
- **Other --** The DST definitions are user-defined based on the device locality. If Other is selected, the From and To fields must be defined.
- **Time Set Offset (1-1440) --** For non USA and European countries, the amount of time for DST can be set in minutes. The default time is 60 minutes.
- **From --** Defines the time that DST begins in countries other than USA or Europe, in the format DayMonthYear in one field and time in another. For example, DST begins on the 25th October 2007 5:00 am, the two fields will be 25Oct07 and 5:00. The possible field values are:
- **Date --** The date at which DST begins. The possible field range is 1-31.
- **Month --** The month of the year in which DST begins. The possible field range is Jan-Dec.
- **Year--** The year in which the configured DST begins.
- **Time --** The time at which DST begins. The field format is Hour:Minute, for example, 05:30.
- **To --** Defines the time that DST ends in countries other than USA or European in the format DayMonthYear in one field and time in another. For example, DST ends on the 23rd March 2008 12:00 am, the two fields will be 23Mar08 and 12:00. The possible field values are:
- **Date --** The date at which DST ends. The possible field range is 1-31.
- **Month --** The month of the year in which DST ends. The possible field range is Jan-Dec.
- **Year--** The year in which the configured DST ends.
- **Time --** The time at which DST starts. The field format is Hour:Minute, for example, 05:30.
- **Recurring --** Defines the time that DST starts in countries other than USA or Europe where the DST is constant year to year. The possible field values are:
- **From --** Defines the time that DST begins each year. For example, DST begins locally every second Sunday in April at 5:00 am. The possible field values are:
- **Day --** The day of the week from which DST begins every year. The possible field range is Sunday-Saturday.
- **Week --** The week within the month from which DST begins every year. The possible field range is 1-5.
- **Month --** The month of the year in which DST begins every year. The possible field range is Jan.-Dec.
- **Time --** The time at which DST begins every year. The field format is Hour:Minute, for example, 02:10.
- **To --** Defines the recurring time that DST ends each year. For example, DST ends locally every fourth Friday in October at 5:00 am. The possible field values are:
- **Day --** The day of the week at which DST ends every year. The possible field range is Sunday-Saturday.
- **Week --** The week within the month at which DST ends every year. The possible field range is 1-5.

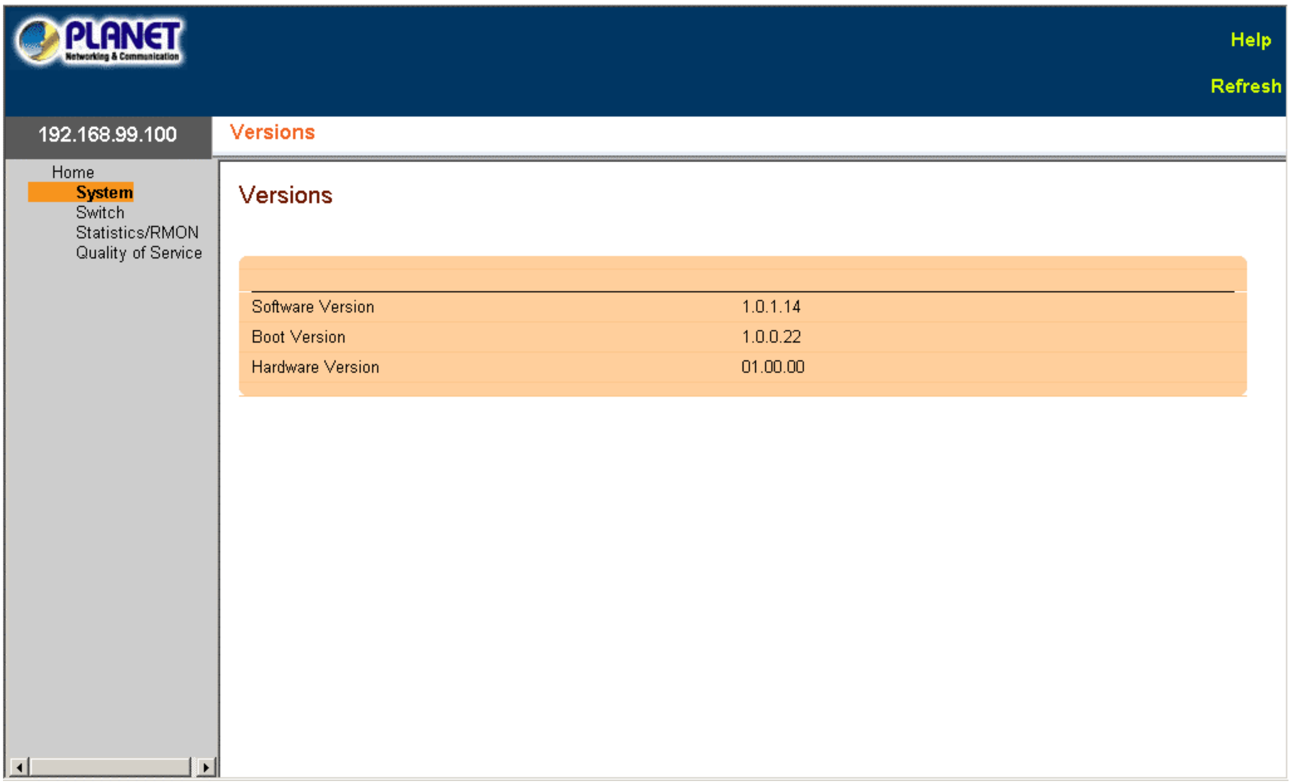
- **Month --** The month of the year in which DST ends every year. The possible field range is Jan.-Dec.
- **Time --** The time at which DST ends every year. The field format is Hour:Minute, for example, 05:30.

3.2.2.1.3 Versions

The **Versions** page contains information about the hardware and software versions currently running.

To open **Versions** screen perform the folling:

1. Click System -> General -> Versions
2. The Versions screen is displayed as in Figure 3-17.



Versions

Software Version	1.0.1.14
Boot Version	1.0.0.22
Hardware Version	01.00.00

Figure 3-17 Versions

The page includes the following fields:

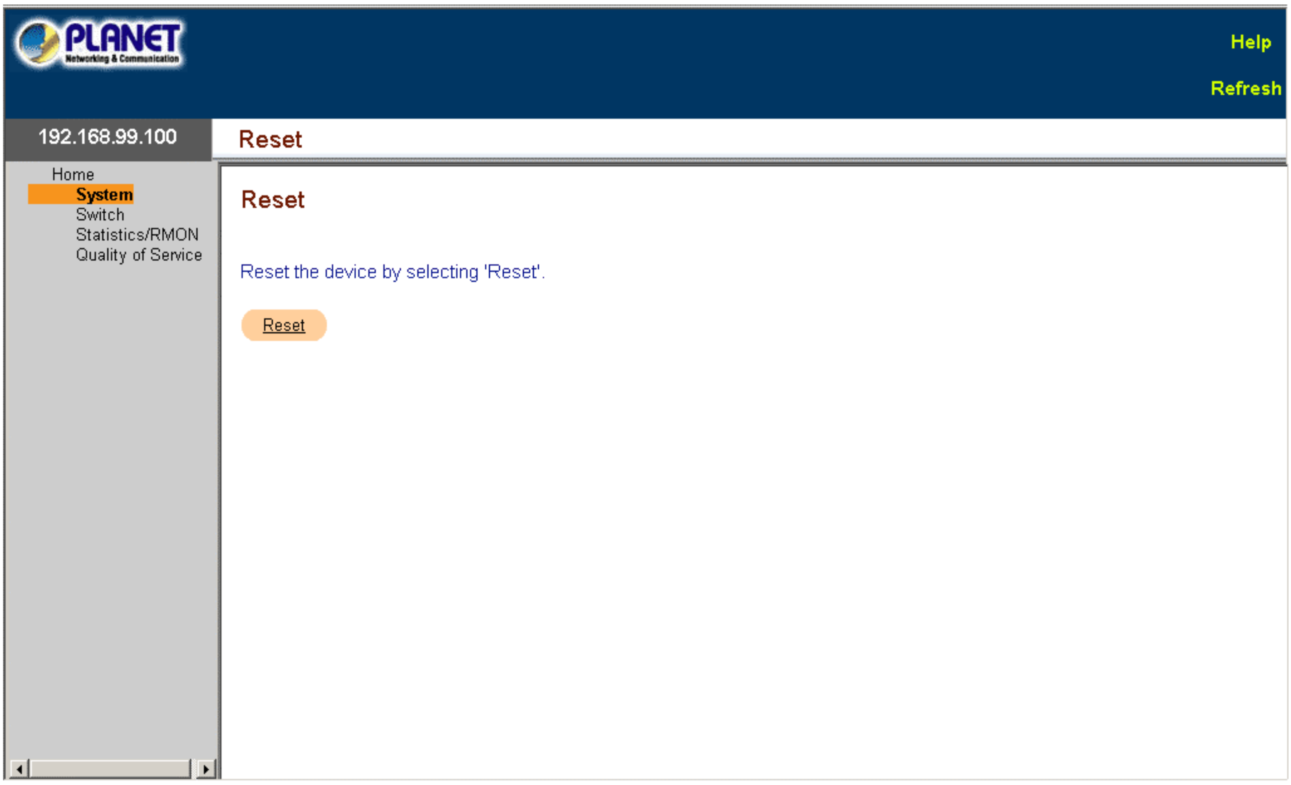
- **Software Version --** The current software version running on the device.
- **Boot Version --** The current Boot version running on the device.
- **Hardware Version --** The current hardware versions running on the device.

3.2.2.1.4 Reset

The **Reset** page enables the device to be reset from a remote location.

To open **Reset** screen perform the folling:

1. Click System -> General -> Reset
2. The Reset screen is displayed as in Figure 3-18.



Reset the device by selecting 'Reset'.

Figure 3-18 Reset screen

3.2.2.2 SNTP

The device supports the Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. SNTP operates only as a client, and cannot provide time services to other systems.

The device can poll the following server types for the server time:

- **Unicast**
- **Anycast**
- **Broadcast (Multicast)**

Time sources are established by Stratums. Stratums define the distance from the device to the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock. The device receives time from stratum 1 and above.

The following is an example of stratums:

- **Stratum 0 --** Indicates a real time clock is used as the time source, for example, a GPS system.
- **Stratum 1 --** Indicates that a server that is directly linked to a Stratum 0 time source is used. Stratum 1 time servers provide primary network time standards.
- **Stratum 2 --** Indicates that the time source is distanced from the Stratum 1 server over a network path. For example, a Stratum 2 server receives the time over a network link, via NTP, from a Stratum 1 server.

Information received from SNTP servers is evaluated based on the Time level and server type.

SNTP time definitions are assessed and determined by the following time levels:

- **T1 --** The time at which the original request was sent by the client.
- **T2 --** The time at which the original request was received by the server.
- **T3 --** The time at which the server sent the server a reply.
- **T4 --** The time at which the client received the server's reply.

Polling for Unicast Time Information

Polling for Unicast information is used for polling a server for which the IP address is known. T1 - T4 are used to determine the server time. This is the preferred method for synchronizing device time.

Polling for Anycast Time Information

Polling for Anycast information is used when the server IP address is unknown. The first anycast server to return a response is used to set the time value. Time levels T3 and T4 are used to determine the server time. Using Anycast time information for synchronizing device time is preferred to using Broadcast time information.

Polling for Broadcast Time Information

Polling for Broadcast information is used when the server IP address is unknown. When a Multicast message is sent to Multicast group, the SNTP client listens for the response. The SNTP client neither sends time information requests nor receives responses from the Broadcast server.

MD5 (Message Digest 5) Routing Authentication safeguards device synchronization paths to SNTP servers. MD5 is an algorithm that produces a 128-bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication, authenticates the origin of the communication.

The SNTP page contains links to the following topics:

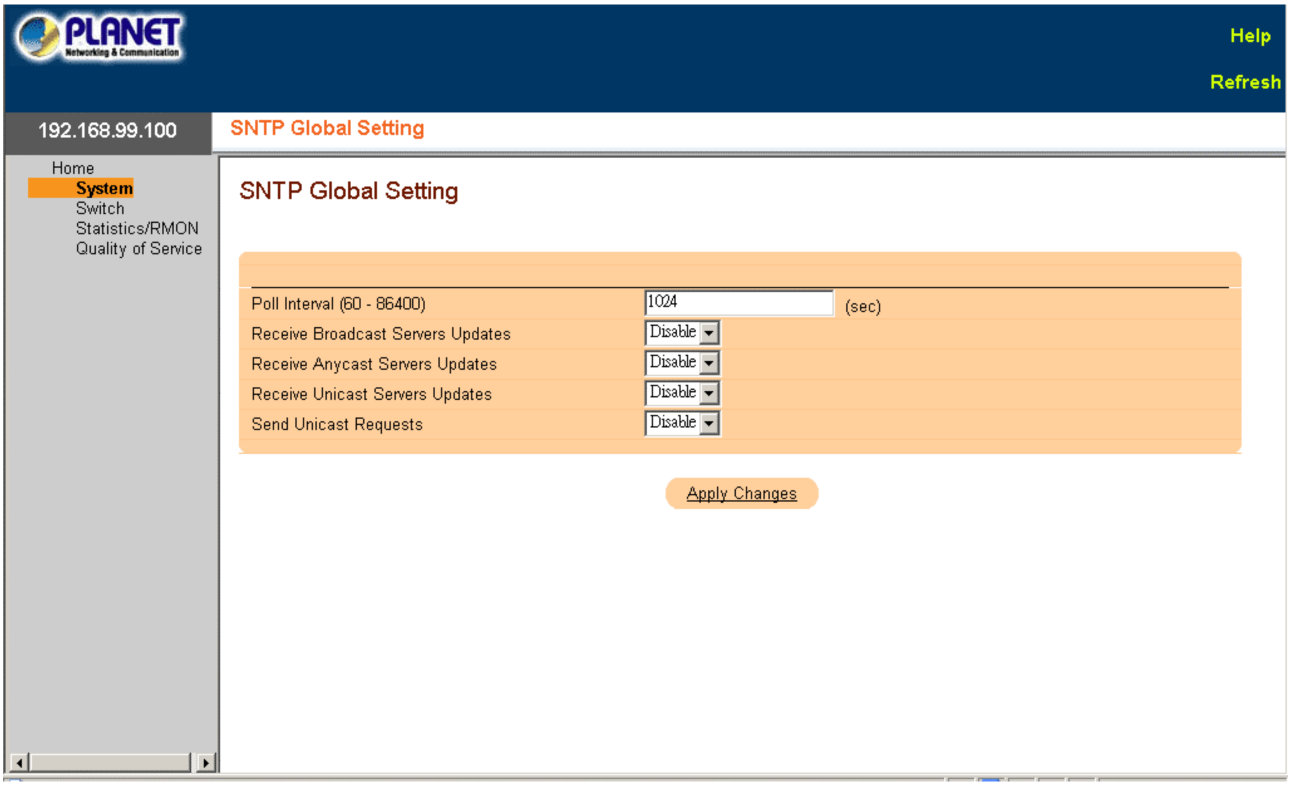
- **Global Settings**
- **Authentication**
- **Servers**
- **Interface Settings**

3.2.2.2.1 SNTP Global Settings

The **SNTP Global Settings** page provides information for defining SNTP parameters globally.

To open **SNTP Global Settings** screen perform the folling:

1. Click System -> SNTP -> Global Settings
2. The SNTP Global Settings screen is displayed as in Figure 3-19.



SNTP Global Setting

Poll Interval (60 - 86400)	1024	(sec)
Receive Broadcast Servers Updates	Disable	
Receive Anycast Servers Updates	Disable	
Receive Unicast Servers Updates	Disable	
Send Unicast Requests	Disable	

Figure 3-19 SNTP Global Settings screen

The page includes the following fields:

- **Poll Interval (60-86400) --** Defines the interval (in seconds) at which the SNTP server is polled for Unicast information.
- **Receive Broadcast Servers Updates --** Polls the SNTP servers for Broadcast server time information on the selected interfaces, when enabled.

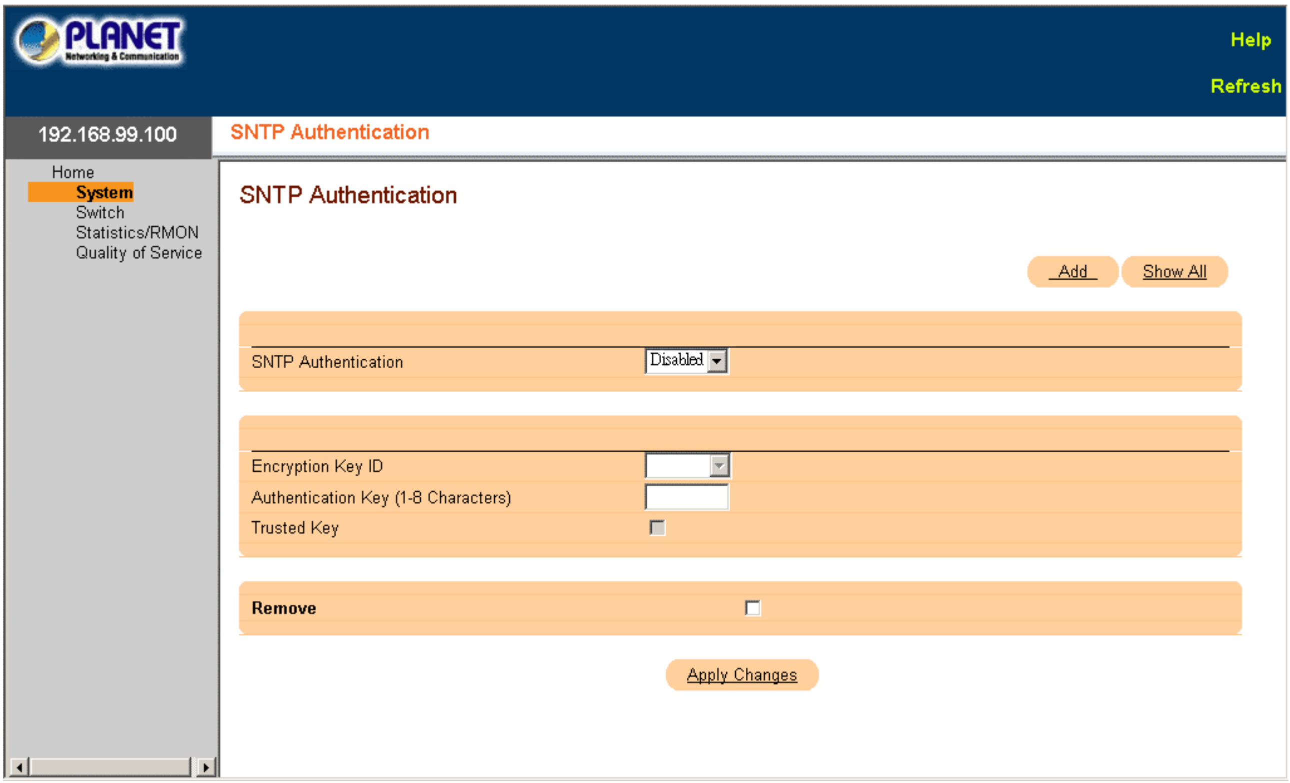
- **Receive Anycast Servers Updates --** Polls the SNTP server for Anycast server time information, when enabled. If both the Receive Anycast Servers Update, and the Receive Broadcast Servers Update fields are enabled, the system time is set according the Anycast server time information.
- **Receive Unicast Servers Updates --** Polls the SNTP server for Unicast server time information, when enabled. If the Receive Broadcast Servers Updates, Receive Anycast Servers Updates, and the Receive Unicast Servers Updates fields are all enabled, the system time is set according the Unicast server time information.
- **Poll Unicast Servers --** Sends SNTP Unicast forwarding information to the SNTP server, when enabled.

3.2.2.2.2 SNTP Authentication

The **SNTP Authentication** page enables SNTP authentication between the device and an SNTP server. The means by which the SNTP server is authenticated is also selected in the SNTP Authentication page.

To open **SNTP Authentication** screen perform the folling:

1. Click System -> SNTP -> Authentication
2. The SNTP Authentication screen is displayed as in Figure 3-20.



SNTP Authentication

SNTP Authentication	Disabled
Encryption Key ID	
Authentication Key (1-8 Characters)	
Trusted Key	☐
Remove	☐

Figure 3-20 SNTP Authentication screen

The page includes the following fields:

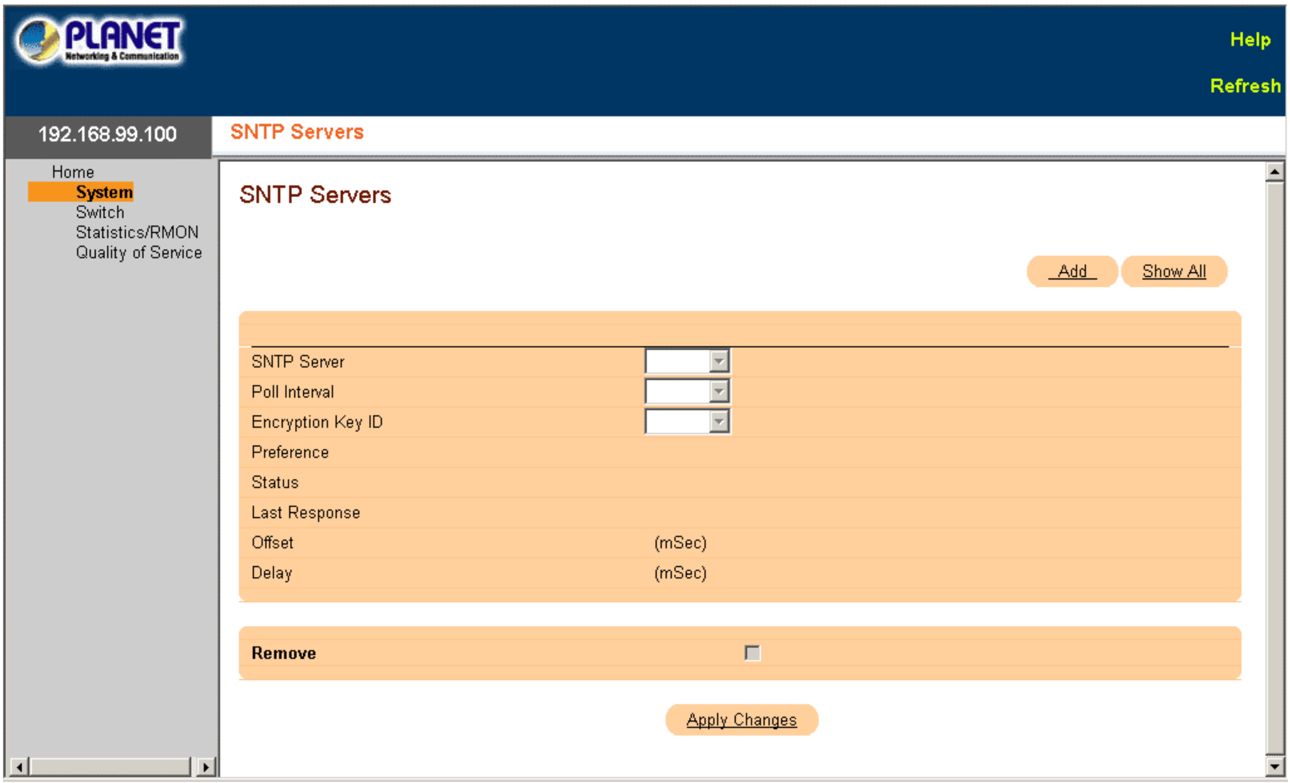
- **SNTP Authentication --** Enables authenticating an SNTP session between the device and an SNTP server, when enabled.
- **Encryption Key ID --** Defines the Key Identification used to authenticate the SNTP server and device. The field value is up to 4294967295 characters.
- **Authentication Key (1-8 Characters) --** The key used for authentication.
- **Trusted Key --** The Encryption Key elected to authenticate the SNTP server.
- **Remove --** Removes the selected ID key. Keys are removed one by one and not grouped for removal with other keys.

3.2.2.2.3 SNTP Servers

The **SNTP Servers** page contains information for enabling SNTP servers, as well as adding new SNTP servers. In addition, the SNTP Servers page enables the device to request and accept SNTP traffic from a server.

To open **SNTP Servers** screen perform the folling:

1. Click System -> SNTP -> Servers
2. The SNTP Servers screen is displayed as in Figure 3-21.



SNTP Servers

SNTP Server	
Poll Interval	
Encryption Key ID	
Preference	
Status	
Last Response	
Offset	(mSec)
Delay	(mSec)

Remove □

Figure 3-21 SNTP Servers screen

The page includes the following fields:

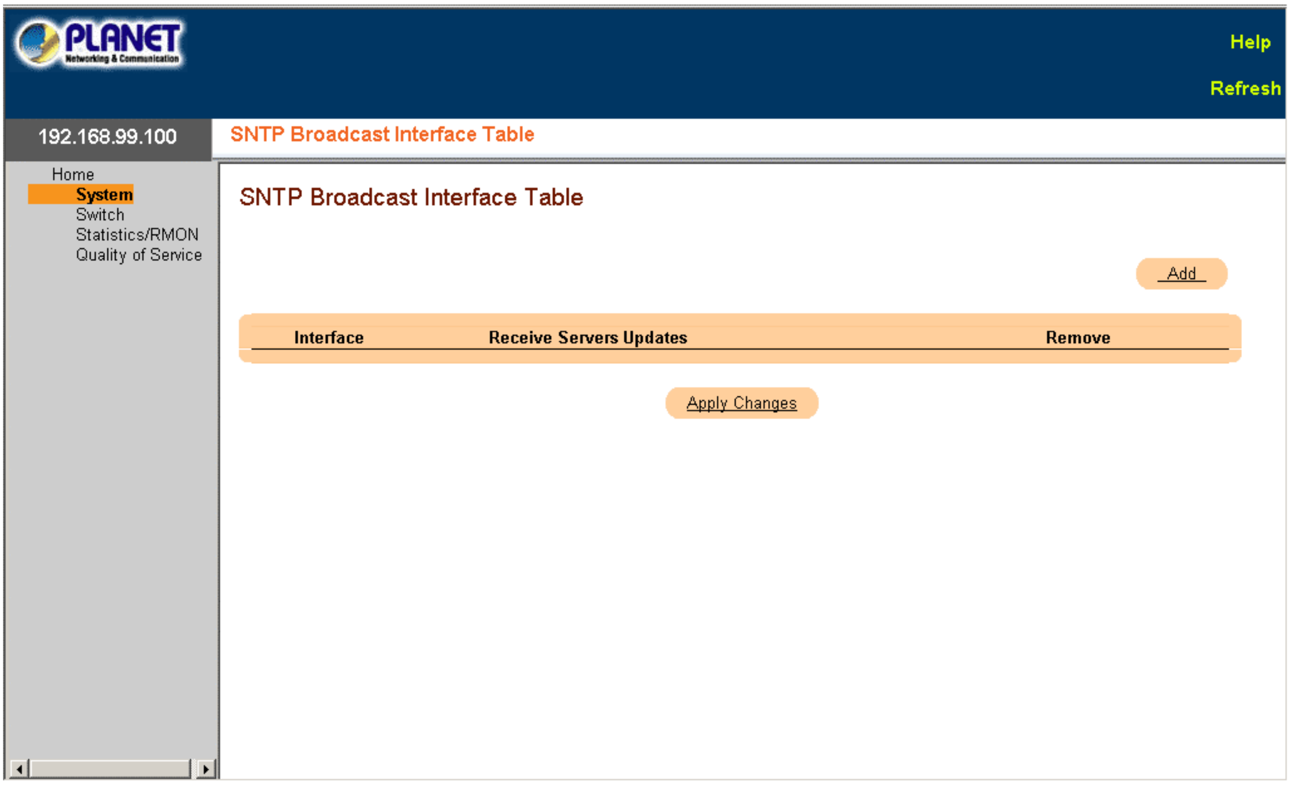
- **SNTP Server --** Enter a user-defined SNTP server IP addresses or hostname. Up to eight SNTP servers can be defined. This field can contain 1 - 158 characters.
- **Poll Interval --** Enables polling the selected SNTP Server for system time information, when enabled.
- **Encryption Key ID --** Specifies the Key Identification used to communicate between the SNTP server and device. The range is 1 - 4294967295.
- **Preference --** The SNTP server providing SNTP system time information. The possible field values are:
- **Primary --** The primary server provides SNTP information.
- **Secondary --** The backup server provides SNTP information.
- **Status --** The operating SNTP server status The possible field values are:
- **Up --** The SNTP server is currently operating normally.
- **Down --** The SNTP server is currently not operating normally.
- **Unknown --** The SNTP server status is currently unknown.
- **Last Response --** The last time a response was received from the SNTP server.
- **Offset --** Timestamp difference between the device local clock and the aquired time from the SNTP server.
- **Delay --** The amount of time it takes to reach the SNTP server.
- **Remove --** Removes a specific SNTP server from the SNTP Server list, when selected.

3.2.2.2.4 SNTP Interface Settings

The **SNTP Broadcast Interface Table** contains fields for setting SNTP on different interfaces.

To open **SNTP Broadcast Interface Table** screen perform the folling:

1. Click System -> SNTP -> Interface Settings
2. The SNTP Interface Settings screen is displayed as in Figure 3-22.



SNTP Broadcast Interface Table

Interface	Receive Servers Updates	Remove

Figure 3-22 SNTP Broadcast Interface Table screen

The page includes the following fields:

- **Interface --** Contains an interface list on which SNTP can be enabled.
- **Receive Server Updates --** The amount of time that passes before the SNTP server is polled for information. The field range is 3600 - 4294967295 seconds.
- **Remove --** Disables SNTP on a specific interface, when selected.

3.2.2.3 Logs

The **Logs** page contains links to the following topics:

- **Global Parameters**
- **RAM Log**
- **Log File**
- **Remote Log Server**
-

3.2.2.3.1 Global Parameters

The Global Log Parameters page contains fields for enabling logs globally, and fields for defining log parameters. The Severity log messages are listed from the highest severity to the lowest.

Event messages have a unique format, as per the SYSLOG RFC recommended message format for all error reporting. For example, Syslog+ local device reporting. Messages are assigned a severity code, and include a message mnemonic, which identifies the source application generating the message. Messages are filtered based on their urgency or relevancy. The severity of each message determines the set of event logging devices to which are sent for each event logging device. The following table contains the Log Severity Levels:

Severity Type	**Severity Level**	**Description**	**Example**
Emergency	0	The system is not functioning.	Memory overflow.
Alert	1	The system needs immediate attention.	Main system memory pool overflow.
Critical	2	The system is in a critical state.	Cannot bind to SNMP.

Error	3	A system error has occurred.	Failed to delete entry.
Warning	4	A system warning has occurred.	Port down.
Notice	5	The system is functioning properly, but system notice has occurred.	Bad route.
Informational	6	Provides device information.	Link up.
Debug	7	Provides detailed information about the log. If a Debug error occurs, contact Dell Online Technical Support	Method list created.
Severity Type	**Severity Level**	**Description**	**Example**

The page includes the following fields:

- **Logging --** Enables device global logs for Cache, File, and Server Logs. Console logs are enabled by default.
- **Severity --** The following are the available severity logs:
- **Emergency --** The highest warning level. If the device is down or not functioning properly, an emergency log message is saved to the specified logging location.
- **Alert --** The second highest warning level. An alert log is saved if there is a serious device malfunction, for example, all device features are down.
- **Critical --** The third highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.
- **Error --** A device error has occurred, for example, if a single port is offline.
- **Warning --** The lowest level of a device warning. The device is functioning, but an operational problem has occurred.
- **Notice --** Provides device information.
- **Informational --** Provides device information.
- **Debug --** Provides debugging messages.

✍ ***Note:*** When a severity level is selected, all severity level choices above the selection are selected automatically.

The Global Log Parameters page also contains check boxes which correspond to a distinct logging system:

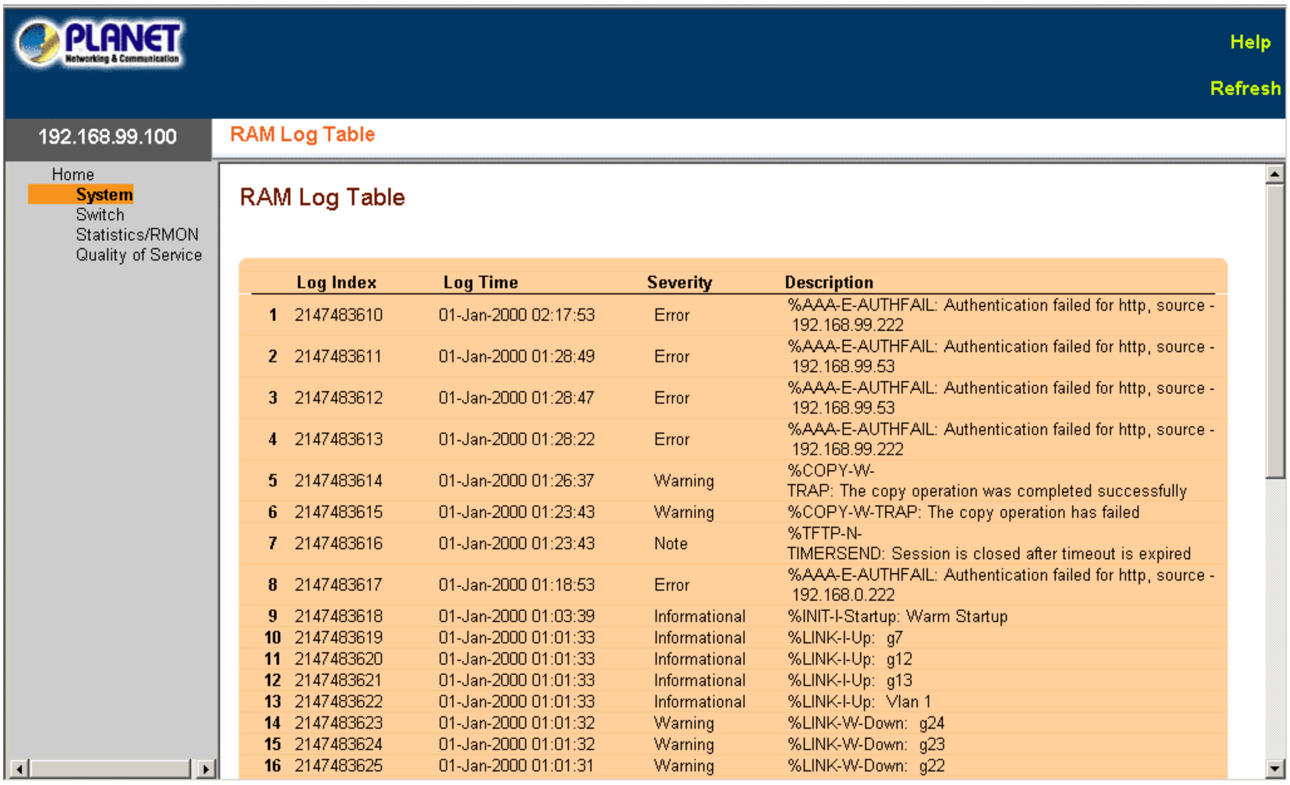
- **Console --** The minimum severity level from which logs are sent to the console.
- **RAM Logs --** The minimum severity level from which logs are sent to the Log File kept in RAM (Cache).
- **Log File --** The minimum severity level from which logs are sent to the Log File kept in FLASH memory

3.2.2.3.2 RAM Log

The **RAM Log Table** contains information about log entries kept in RAM, including the time the log was entered, the log severity, and a description of the log.

To open **RAM Log Table** screen perform the folling:

1. Click System -> Logs -> RAM Log
2. The RAM Log Table Interface Settings screen is displayed as in Figure 3-23.



RAM Log Table

	Log Index	Log Time	Severity	Description
1	2147483610	01-Jan-2000 02:17:53	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 192.168.99.222
2	2147483611	01-Jan-2000 01:28:49	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 192.168.99.53
3	2147483612	01-Jan-2000 01:28:47	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 192.168.99.53
4	2147483613	01-Jan-2000 01:28:22	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 192.168.99.222
5	2147483614	01-Jan-2000 01:26:37	Warning	%COPY-W-TRAP: The copy operation was completed successfully
6	2147483615	01-Jan-2000 01:23:43	Warning	%COPY-W-TRAP: The copy operation has failed
7	2147483616	01-Jan-2000 01:23:43	Note	%TFTP-N-TIMERSEND: Session is closed after timeout is expired
8	2147483617	01-Jan-2000 01:18:53	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 192.168.0.222
9	2147483618	01-Jan-2000 01:03:39	Informational	%INIT-I-Startup: Warm Startup
10	2147483619	01-Jan-2000 01:01:33	Informational	%LINK-I-Up: g7
11	2147483620	01-Jan-2000 01:01:33	Informational	%LINK-I-Up: g12
12	2147483621	01-Jan-2000 01:01:33	Informational	%LINK-I-Up: g13
13	2147483622	01-Jan-2000 01:01:33	Informational	%LINK-I-Up: Vlan 1
14	2147483623	01-Jan-2000 01:01:32	Warning	%LINK-W-Down: g24
15	2147483624	01-Jan-2000 01:01:32	Warning	%LINK-W-Down: g23
16	2147483625	01-Jan-2000 01:01:31	Warning	%LINK-W-Down: g22

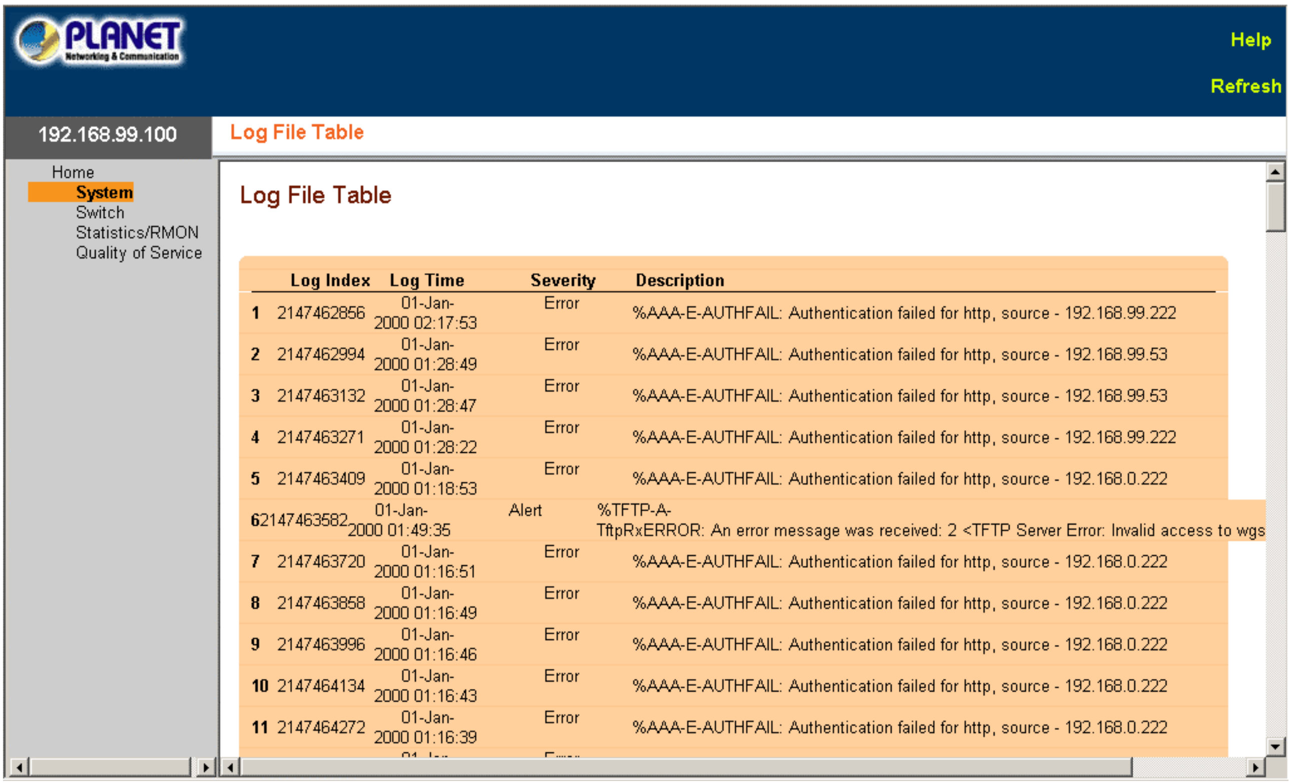
Figure 3-23 RAM Log Tables

3.2.2.3.3 Log File

The **Log File Table** contains information about log entries saved to the Log File in FLASH, including the time the log was entered, the log severity, and a description of the log message.

To open **Log File Table** screen perform the folling:

1. Click System -> Logs -> Log File
2. The Log File Table Interface Settings screen is displayed as in Figure 3-24.



Log File Table

	Log Index	Log Time	Severity	Description
1	2147462856	01-Jan-2000 02:17:53	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 192.168.99.222
2	2147462994	01-Jan-2000 01:28:49	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 192.168.99.53
3	2147463132	01-Jan-2000 01:28:47	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 192.168.99.53
4	2147463271	01-Jan-2000 01:28:22	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 192.168.99.222
5	2147463409	01-Jan-2000 01:18:53	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 192.168.0.222
6	2147463582	01-Jan-2000 01:49:35	Alert	%TFTP-A-TftpRxERROR: An error message was received: 2 <TFTP Server Error: Invalid access to wgs
7	2147463720	01-Jan-2000 01:16:51	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 192.168.0.222
8	2147463858	01-Jan-2000 01:16:49	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 192.168.0.222
9	2147463996	01-Jan-2000 01:16:46	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 192.168.0.222
10	2147464134	01-Jan-2000 01:16:43	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 192.168.0.222
11	2147464272	01-Jan-2000 01:16:39	Error	%AAA-E-AUTHFAIL: Authentication failed for http, source - 192.168.0.222

Figure 3-24 Log File Table screen

The page includes the following fields:

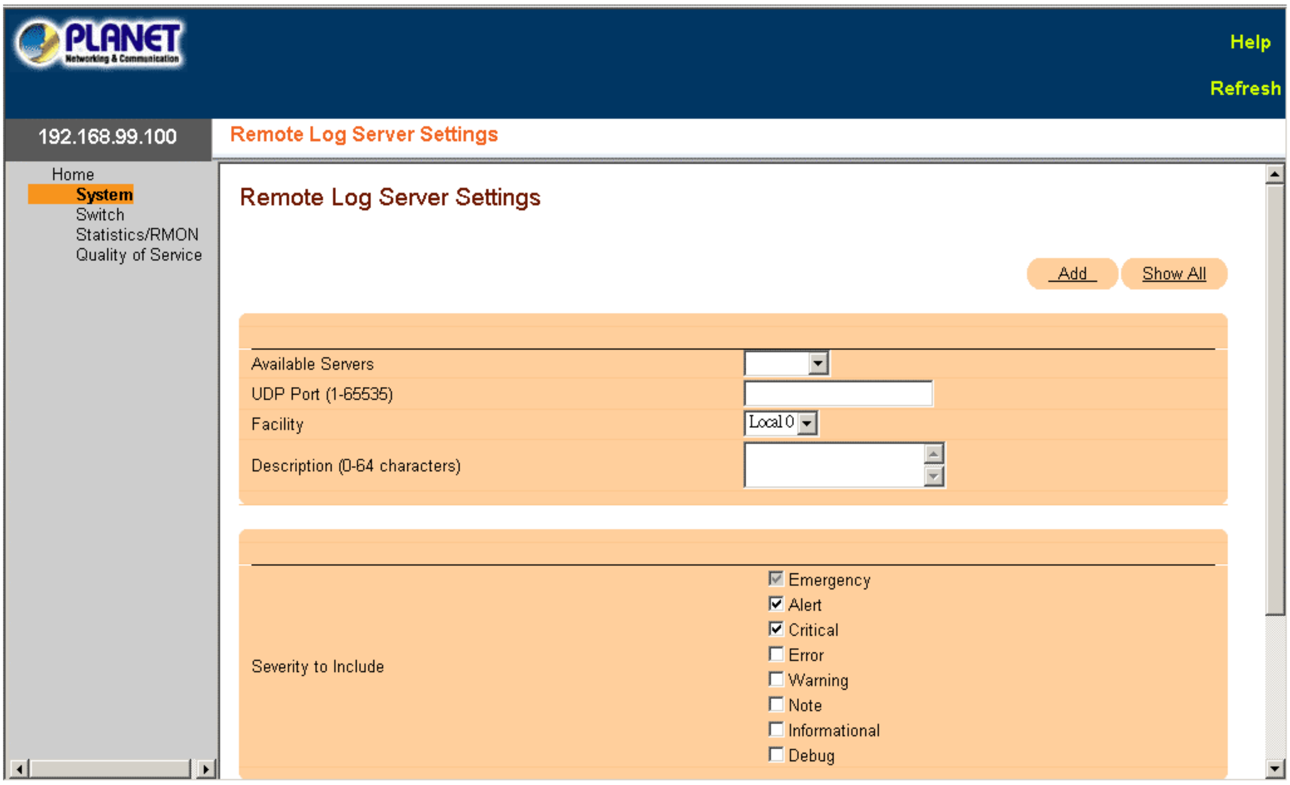
- **Log Index --** The log number in the Log File Table.
- **Log Time --** Specifies the time at which the log was entered in the Log File Table.
- **Severity --** Specifies the log severity.
- **Description --** The log message text.

3.2.2.3.4 Remote Log Server

The **Remote Log Server Settings** page contains fields for viewing and configuring the available Log Servers. In addition, new log servers can be defined, and the log severity sent to each sever.

To open **Remote Log Server Settings** screen perform the folling:

1. Click System -> Logs -> Remote Log Server Settings
2. The Remote Log Server Settings screen is displayed as in Figure 3-25.



Remote Log Server Settings

Available Servers	
UDP Port (1-65535)	
Facility	Local 0
Description (0-64 characters)	
Severity to Include	☑ Emergency ☑ Alert ☑ Critical □ Error □ Warning □ Note □ Informational □ Debug

Figure 3-25 Remote Log Server Settings screen

The page includes the following fields:

- **Available Servers --** Contains a list of servers to which logs can be sent.
- **UDP Port (1-65535) --** The UDP port to which the logs are sent for the selected server. The possible range is 1 - 65535. The default value is 514.
- **Facility --** Defines a user-defined application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility level is overridden. All applications defined for a device utilize the same facility on a server. The possible field values are: Local 0 - Local 7.
- **Description (0-64 Characters) --** The user-defined server description.
- **Delete Server --** Deletes the currently selected server from the Available Servers list, when selected.

The **Remote Log Server Settings** page also contains a severity list. The severity definitions are the same as the severity definitions in the Global Log Parameters page.

3.2.2.4 IP Addressing

The **IP Addressing** page contains links for assigning interface and default gateway IP addresses, and defining ARP and DHCP parameters for the interfaces.

The **IP Addressing** page contains links to the following topics:

- **Default Gateway**
- **IP Interface Parameters**
- **DHCP IP Interface**
- **Domain Name System**
- **Default Domain Name**
- **Host Name Mapping**
- **ARP**

3.2.2.4.1 Default Gateway

The **Default Gateway** page contains fields for assigning Gateway devices. Packets are forwarded to the default IP when frames are sent to a remote network. The configured IP address must belong to the same IP address subnet of one of the IP interfaces.

To open **Default Gageway** screen perform the folling:

1. Click System -> IP Addressing -> Default Gateway
2. The Default Gateway screen is displayed as in Figure 3-26.

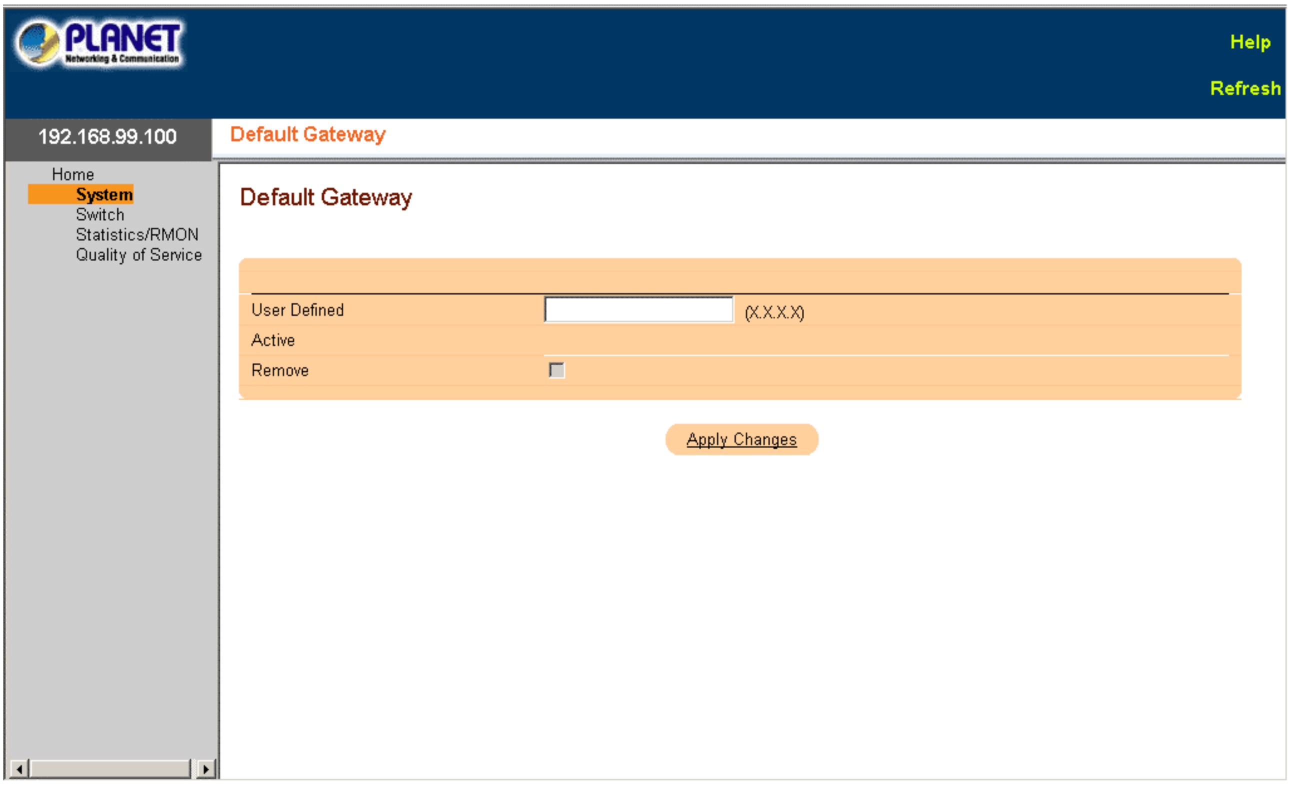


Figure 3-26 Default Gateway screen

The page includes the following fields:

- **Default Gateway --** The Gateway device IP address.
- **Remove --** Removes Gateway devices from the Default Gateway drop-down list, when selected

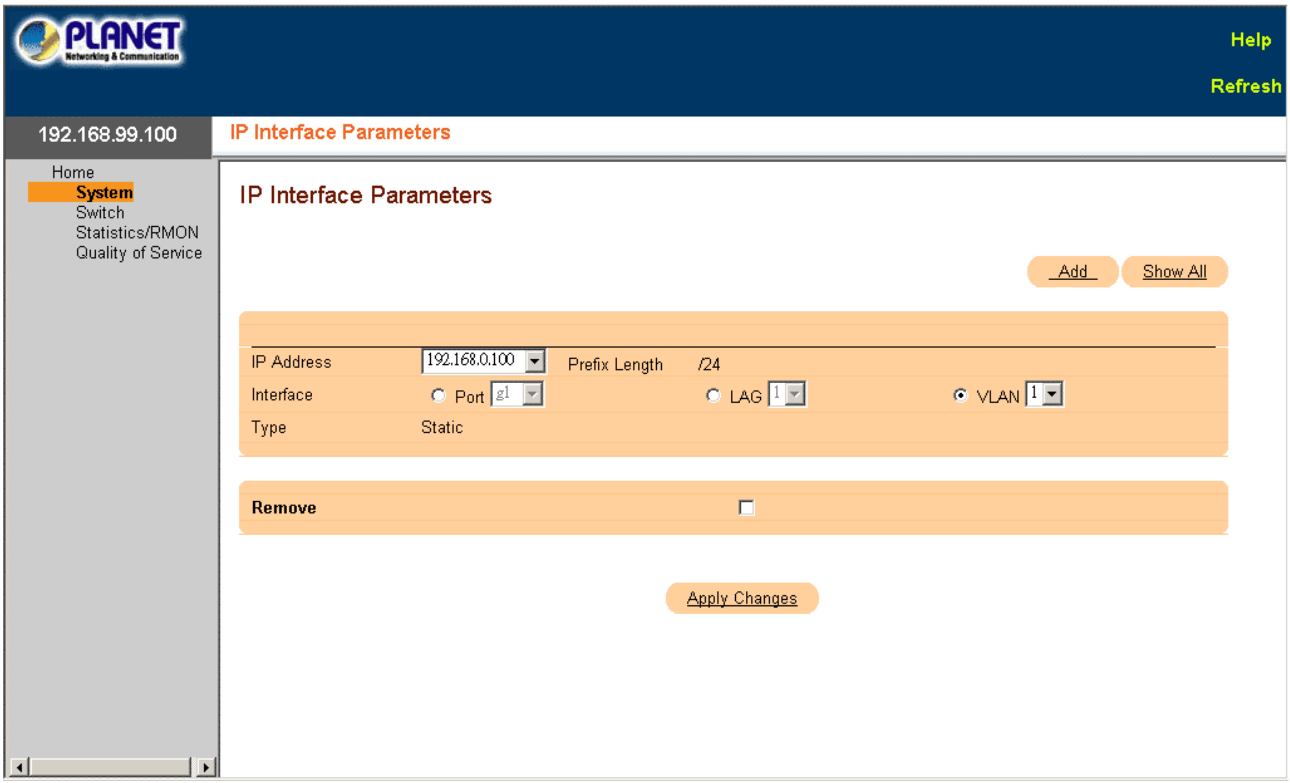
3.2.2.4.2 IP Interface Parameters

The **IP Interface Parameters** page contains fields for assigningIP parameters to interfaces.

To open **IP Interface Parameter** screen perform the folling:

1. Click System -> IP Addressing -> IP Interface Parameter

2. The IP Interface Parameter screen is displayed as in Figure 3-27.



IP Interface Parameters

IP Address	192.168.0.100	Prefix Length	/24
Interface	○ Port g1	○ LAG 1	● VLAN 1
Type	Static		

Remove □

Figure 3-27 IP Interface Parameter screen

The page includes the following fields:

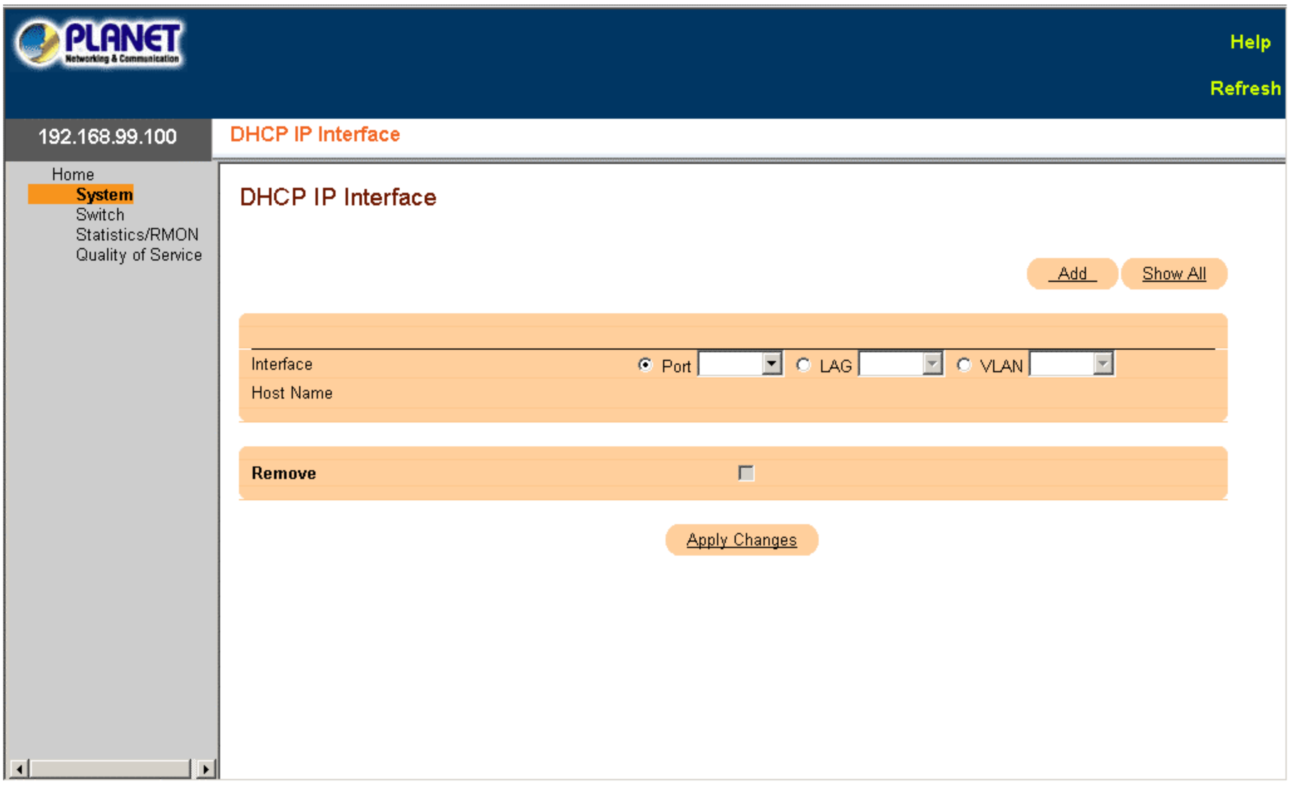
- **IP Address --** The interface IP address.
- **Prefix Length --** The number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- **Interface --** The interface type for which the IP address is defined. Select Port, LAG, or VLAN. For more information, see "Configuring VLANs".
- **Type --** Indicates whether or not the IP address was configured statically.
- **Remove --** When selected, removes the interface from the IP Address drop-down menu.

3.2.2.4.3 DHCP IP Interface

The DHCP IP Interface page contains fields for specifying the DHCP clients connected to the device.

To open **DHCP IP Interface** screen perform the folling:

1. Click System -> IP Addressing -> DHCP IP Interface
2. The DHCP IP Interface screen is displayed as in Figure 3-28.



Interface ● Port ○ LAG ○ VLAN

Host Name

Remove □

Figure 3-28 DHCP IP Interface screen

The page includes the following fields:

- **Interface --** The specific interface connected to the device. Click the option button next to Port, LAG, or VLAN and select the interface connected to the device.
- **Host Name --** The system name. This field can contain up to 20 characters.
- **Remove --** When selected, removes DHCP clients.

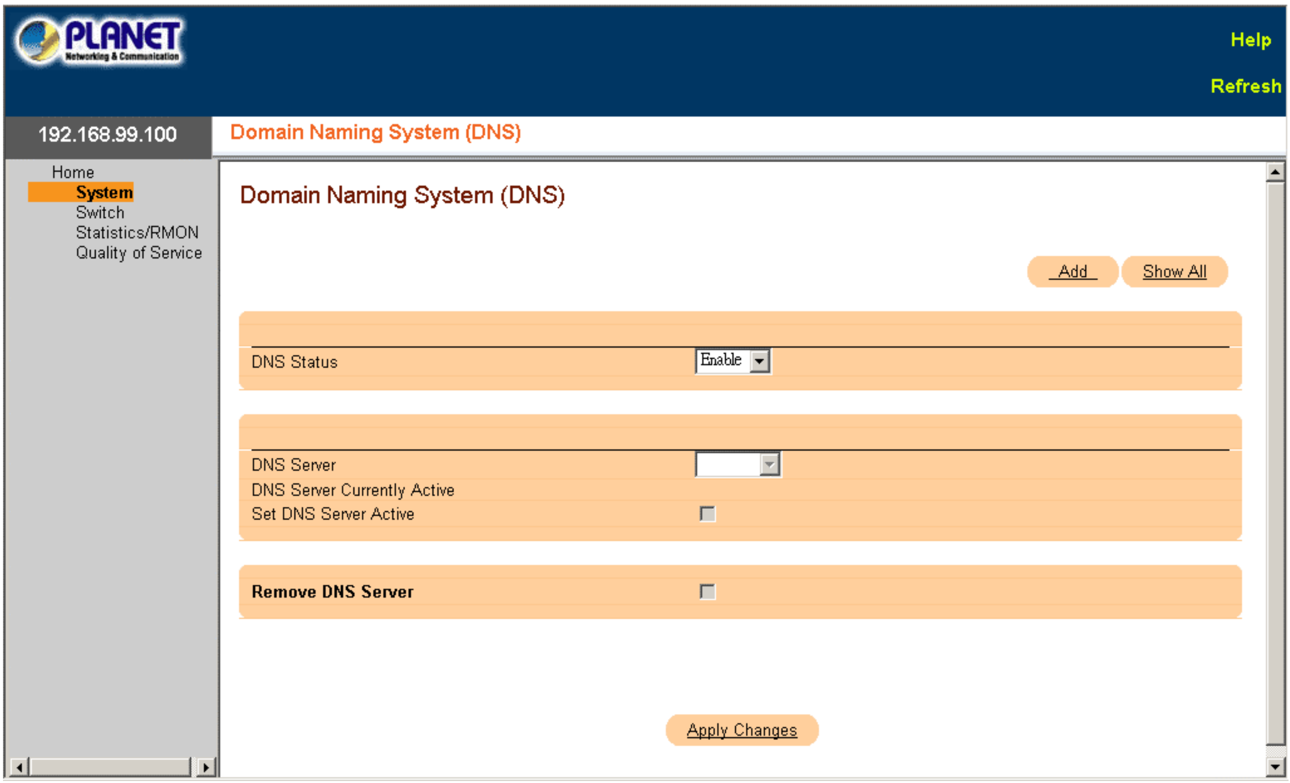
3.2.2.4.4 Domain Name System

Domain Name System (DNS) converts user-defined domain names into IP addresses. Each time a domain name is assigned the DNS service translates the name into a numeric IP address. For example, www.ipexample.com is translated to 192.87.56.2. DNS servers maintain domain name databases and their corresponding IP addresses.

The **Domain Naming System (DNS)** page contains fields for enabling and activating specific DNS servers.

To open **Domain Name System** screen perform the folling:

1. Click System -> IP Addressing -> Domain Name System
2. The Domain Name System screen is displayed as in Figure 3-29.



Domain Naming System (DNS)

DNS Status	Enable
DNS Server	
DNS Server Currently Active	
Set DNS Server Active	□
Remove DNS Server	□

Figure 3-29 Domain Name System screen

The page includes the following fields:

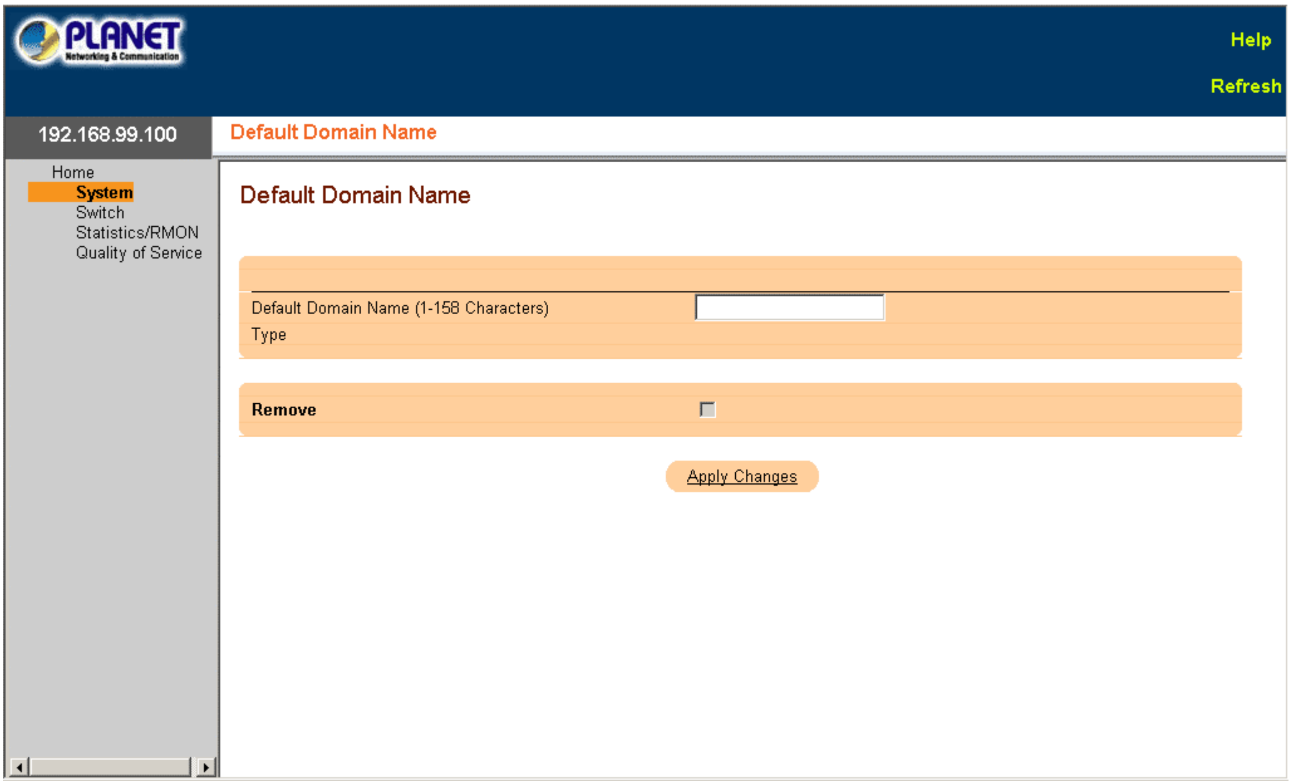
- **DNS Status --** Enables or disables translating DNS names into IP addresses.
- **DNS Server --** Contains a list of DNS servers. DNS servers are added in the Add DNS Server page.
- **DNS Server Currently Active --** The DNS server that is currently the active DNS server.
- **Set DNS Server Active --** Activates the DNS server selected in the DNS Server field.
- **Remove DNS Server --** When selected, removes DNS Servers.

3.2.2.4.5 Default Domain Name

The **Default Domain Name** page provides information for defining default DNS domain names.

To open **Domain Name System** screen perform the folling:

1. Click System -> IP Addressing -> Default Domain Name
2. The Default Domain Name screen is displayed as in Figure 3-30.



Default Domain Name

Default Domain Name (1-158 Characters)	
Type	
Remove	☐

Figure 3-30 Default Domain Name screen

The page includes the following fields:

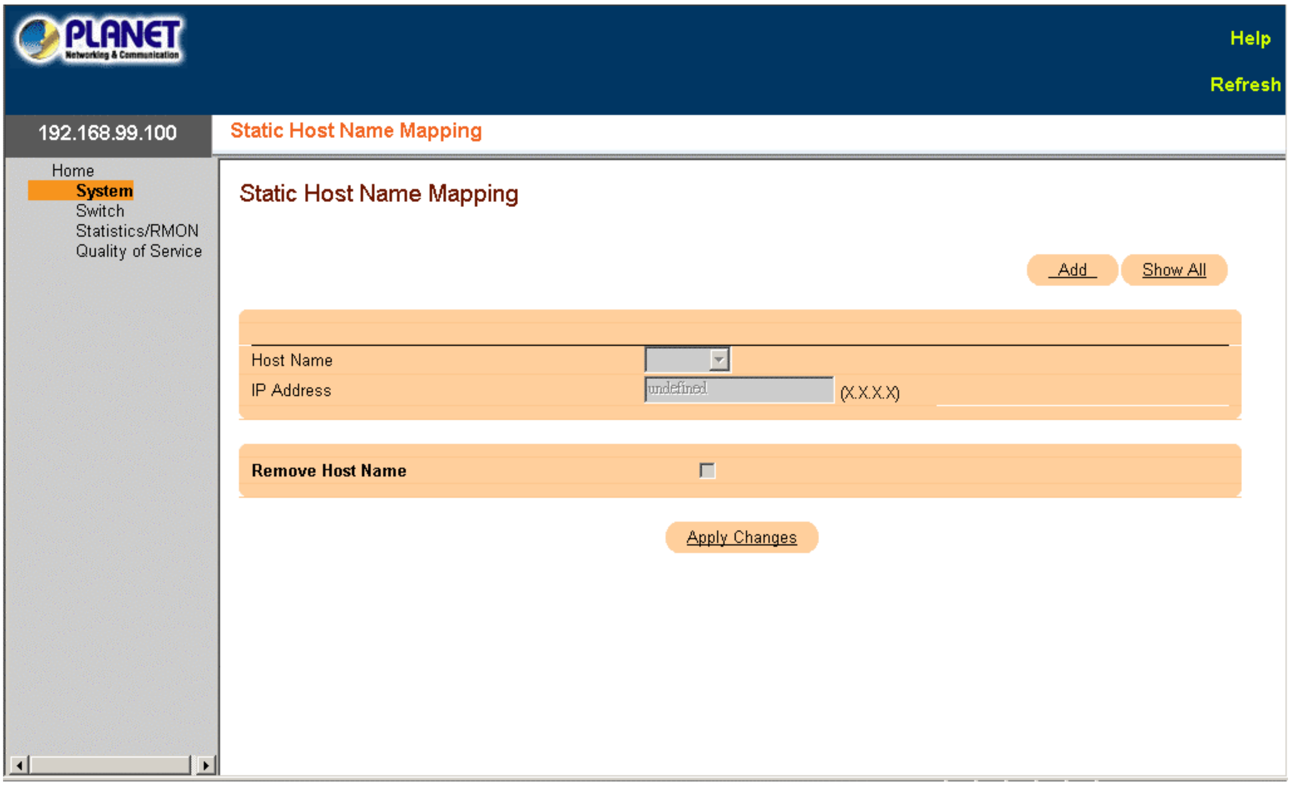
- **Default Domain Name (1-158 characters) --** Contains a user-defined DNS domain name server. When selected, the DNS domain name is the default domain.
- **Type --** The domain type if the domain was statically or dynamically created.
- **Remove --** When selected, removes a selected domain.

3.2.2.4.6 Host Name Mapping

The **Host Name Mapping** page provides parameters for assigning static host names IP addresses. The Host Name Mapping page provides up to eight IP addresses per host.

To open **Host Name Mapping** screen perform the folling:

1. Click System -> IP Addressing -> Host Name Mapping
2. The Host Name Mapping screen is displayed as in Figure 3-30.



Static Host Name Mapping

Static Host Name Mapping

Host Name	
IP Address	undefined (X.X.X.X)

Remove Host Name □

Figure 3-30 Host Name Mapping screen

The page includes the following fields:

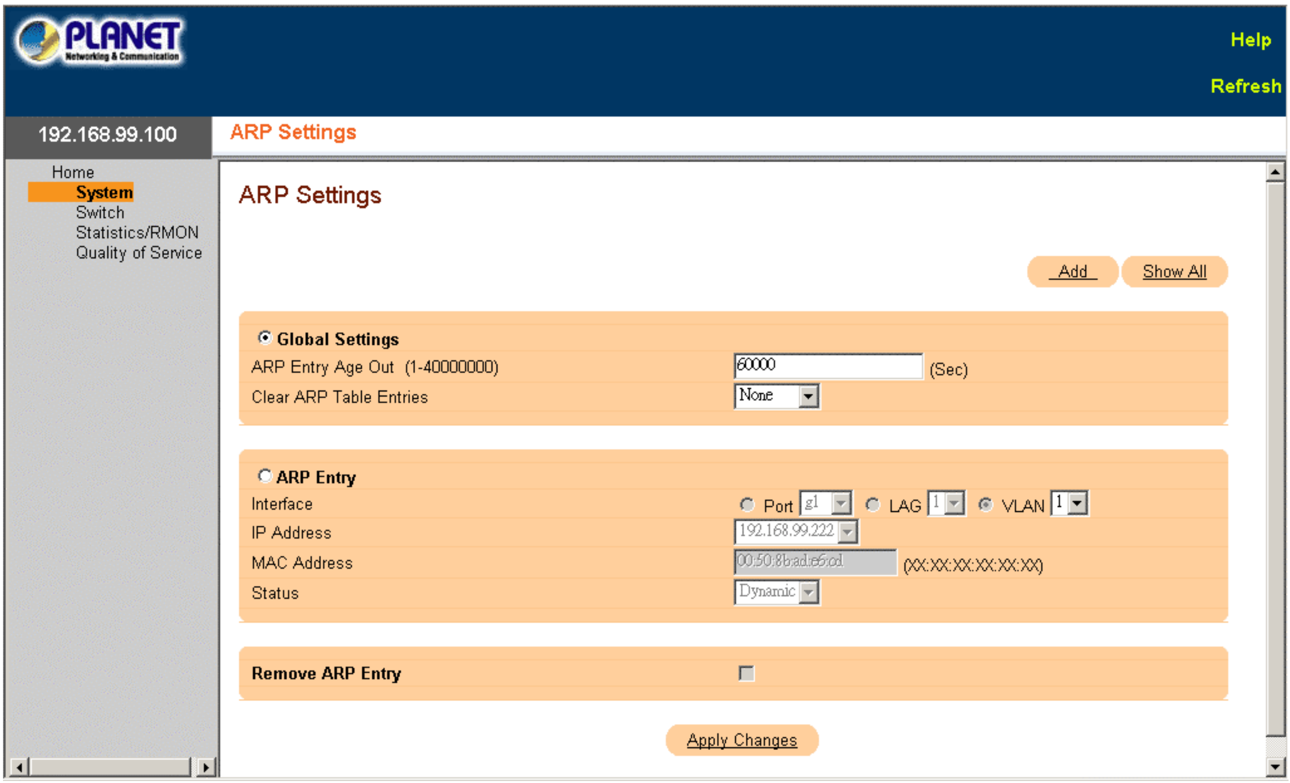
- **Host Name --** Contains a Host Name list. Host Name are defined in the Add Host Name Mapping page. Each host provides up to eight IP addresses. The field values for the Host Name field are:
- **IP Address (X.X.X.X) --** Provides up to eight IP address that are assigned to the specified host name.
- **Type --** The IP address type. The possible field values are:
- **Dynamic --** The IP address was created dynamically.
- **Static --** The IP address is a static IP address.
- **Remove Host Name Mapping --** When checked, removes the DNS Host Mapping.

3.2.2.4.7 ARP

The **Address Resolution Protocol (ARP)** is a TCP/IP protocol that converts IP addresses into physical addresses. The static entries can be defined in the ARP Table. When static entries are defined, a permanent entry is entered and used to translate IP addresses to MAC addresses.

To open **Host Name Mapping** screen perform the folling:

1. Click System -> IP Addressing -> ARP
2. The ARP screen is displayed as in Figure 3-31.



ARP Settings

● Global Settings

ARP Entry Age Out (1-40000000)	60000 (Sec)
Clear ARP Table Entries	None

○ ARP Entry

Interface	○ Port g1 ○ LAG 1 ● VLAN 1
IP Address	192.168.99.222
MAC Address	00:50:8b:ad:e6:cd (XX:XX:XX:XX:XX:XX)
Status	Dynamic

Remove ARP Entry □

Figure 3-31 ARP Settings screen

The page includes the following fields:

- **Global Settings --** Select this option to activate the fields for ARP global settings.
- **ARP Entry Age Out (1-40000000) --** For all devices, the amount of time (seconds) that passes between ARP requests about an ARP table entry. After this period, the entry is deleted from the table. The range is 1 - 4000000, where zero indicates that entries are never cleared from the cache. The default value is 60000 seconds.
- **Clear ARP Table Entries --** The type of ARP entries that are cleared on all devices. The possible values are:
- **None --** ARP entries are not cleared.
- **All --** All ARP entries are cleared.
- **Dynamic --** Only dynamic ARP entries are cleared.
- **Static --** Only static ARP entries are cleared.
- **ARP Entry --** Select this option to activate the fields for ARP settings on a single device.
- **Interface --** The interface number of the port, LAG, or VLAN that is connected to the device.
- **IP Address --** The station IP address, which is associated with the MAC address filled in below.
- **MAC Address --** The station MAC address, which is associated in the ARP table with the IP address.
- **Status --** The ARP Table entry status. Possible field values are:
- **Dynamic --** The ARP entry is learned dynamically.
- **Static --** The ARP entry is a static entry.
- **Remove ARP Entry --** When selected, removes an ARP entry.

3.2.2.5 Diagnostics

The **Diagnostics** page contains links to pages for performing virtual cable tests on copper and fiber optics cables.

The **Diagnostics** page contains links to the following topics:

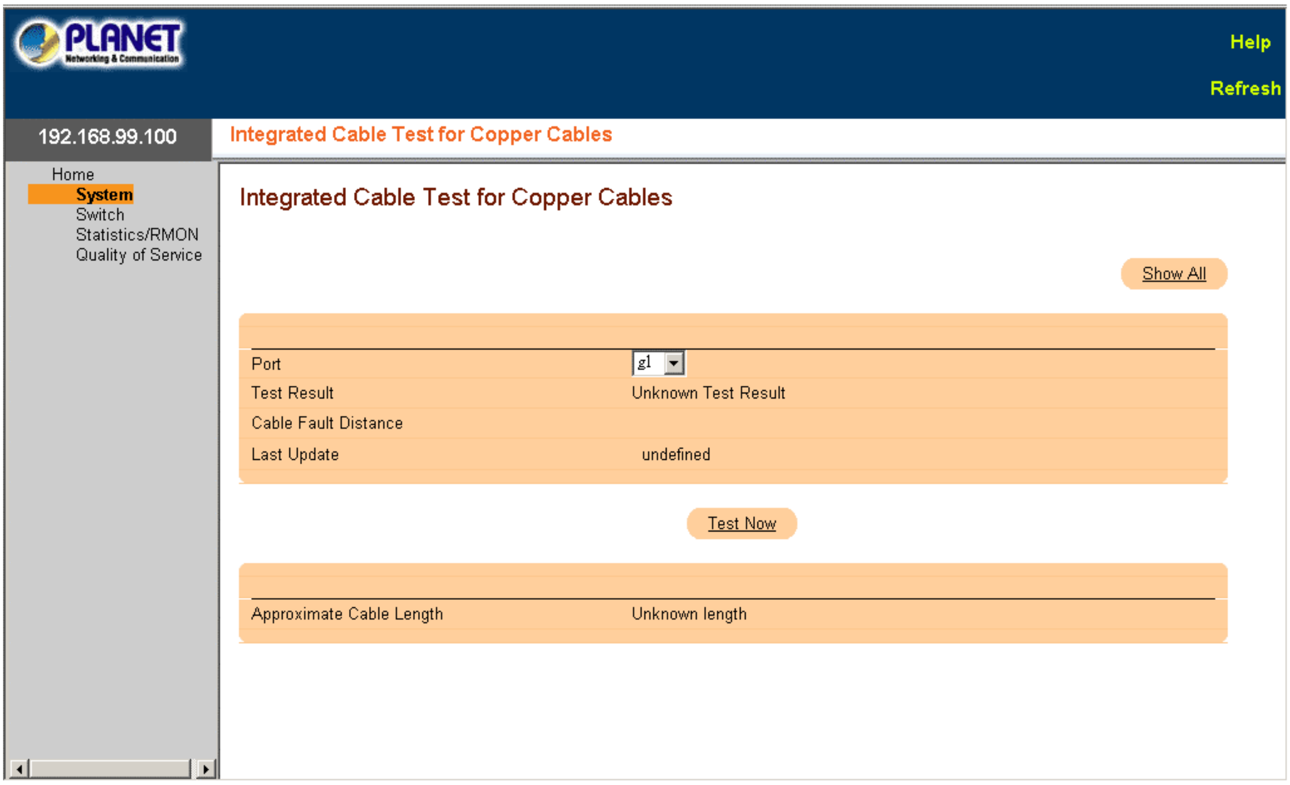
- **Integrated Cable Test**

3.2.2.5.1 Integrated Cable Test

The **Integrated Cable Test for Copper Cables** page contains fields for performing tests on copper cables. Cable testing provides information about where errors occurred in the cable, the last time a cable test was performed, and the type of cable error which occurred. The tests use Time Domain Reflectometry (TDR) technology to test the quality and characteristics of a copper cable attached to a port. Cables up to 120 meters long can be tested. Cables are tested when the ports are in the **"down"** state, with the exception of the Approximated Cable Length test.

To open **Integrated Cable Test** screen perform the folling:

1. Click System -> Diagnostics -> Integrated Cable Test
2. The Integrated Cable Test screen is displayed as in Figure 3-32.



Integrated Cable Test for Copper Cables

Port	g1
Test Result	Unknown Test Result
Cable Fault Distance	
Last Update	undefined

Approximate Cable Length	Unknown length

Figure 3-32 Integrated Cable Test screen

The page includes the following fields:

- **Port --** The port to which the cable is connected.
- **Test Result --** The cable test results. Possible values are:
- **No Cable --** There is no cable connected to the port.
- **Open Cable --** The cable is connected on only one side.
- **Short Cable --** A short has occurred in the cable.
- **OK --** The cable passed the test.
- **Fiber Cable --** A fiber cable is connected to the port.
- **Cable Fault Distance --** The distance from the port where the cable error occurred.
- **Last Update --** The last time the port was tested.
- **Approximate Cable Length --** The approximate cable length. This test can only be performed when the port is up and operating at 1 Gbps.

✍ ***Note:*** The cable length returned is an approximation in the ranges of up to 50 meters, 50m-80m, 80m-110m, 110m-120m, or more than 120m. The deviation may be up to 20 meters.

3.2.2.6 Management Security

The **Management Security** page provides access tosecurity pages that contain fields for setting security parameters for ports, device management methods, user, and server security.

- **Access Profiles**
- **Authentication Profiles**
- **Select Authentication**
- **Local User Database**
- **Line Password**
- **Enable Password**
- **TACACS+**
- **RADIUS**

3.2.2.6.1 Access Profile

The **Access Profiles** page contains fields for defining profiles and rules for accessing the device. Access to management functions can be limited to user groups, which are defined by ingress interfaces and source IP address and/or source IP subnets.

Management access can be separately defined for each type of management access method, including, Web (HTTP), Secure web (HTTPS), Telnet, Secure Telnet and SNMP.

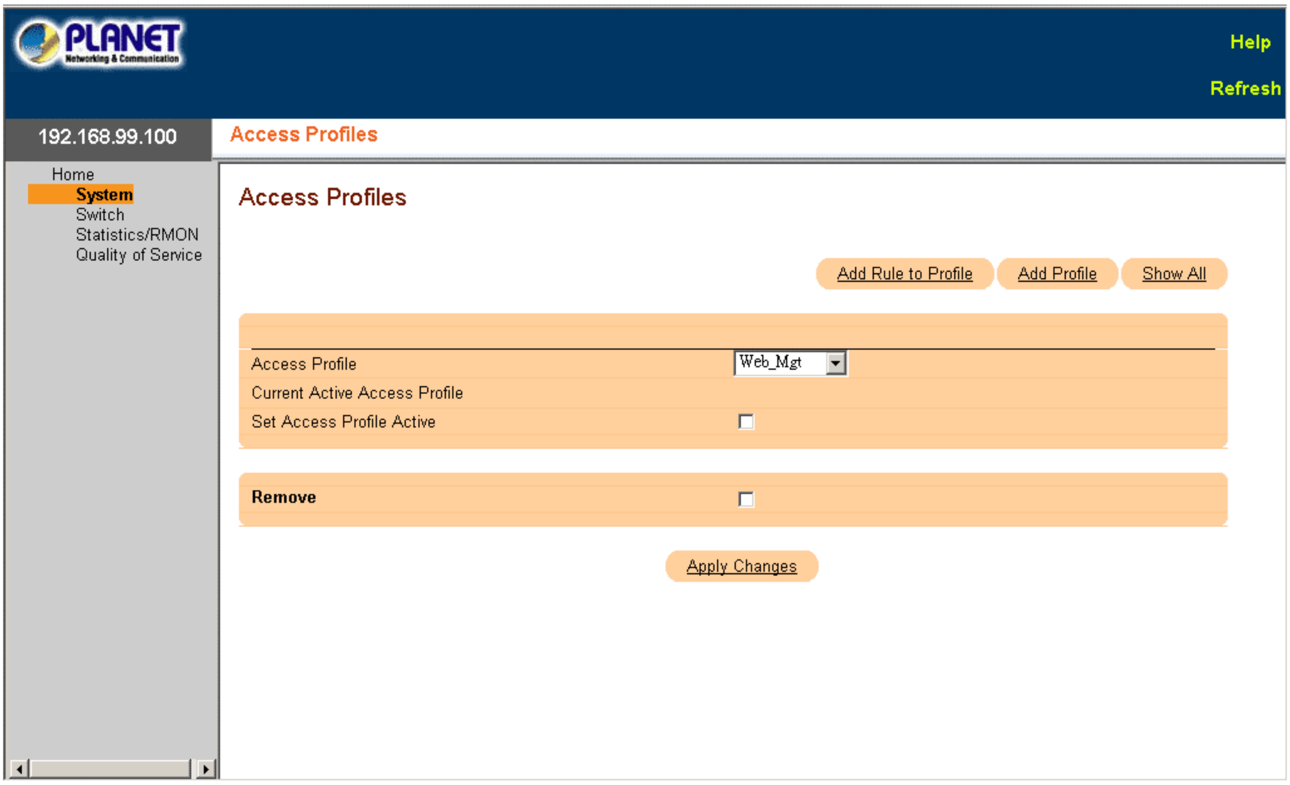
Access to different management methods may differ between user groups. For example, User Group 1 can access the device only via an HTTPS session, while User Group 2 can access the device via both HTTPS and Telnet sessions.

Management Access Lists contain the rules that determine which users can manage the device, and by which methods. Users can also be blocked from accessing the device.

The Access Profiles page contains fields for configuring Management Lists and applying them to specific interfaces.

To open **Access Profile** screen perform the folling:

1. Click System -> Management Security -> Access Profile
2. The Access Profile screen is displayed as in Figure 3-33.



Access Profile: Web_Mgt
Current Active Access Profile
Set Access Profile Active □
Remove □

Figure 3-33 Access Profile screen

The page and the add pages include the following fields:

- **Access Profile --** User-defined Access Profile lists. The Access Profile list contains a default value of Console List, to which user-defined access profiles are added. Selecting Console Only as the Access Profile name disconnects the session, and enables accessing the device from the console only.
- **Current Active Access Profile --** The access profile that is currently active.
- **Set Access Profile Active --** Activates an access profile.
- **Remove --** Removes an access profile from the Access Profile Name list, when selected.
- **Access Profile Name (1-32 Characters) --** User-defined name for the access profile.
- **Rule Priority (1-65535) --** The rule priority. When the packet is matched to a rule, user groups are either granted or denied device management access. The rule order is set by defining a rule number within the Profile Rules Table. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis. The rule priorities are assigned in the Profile Rules Table.
- **Management Method --** The management method for which the access profile is defined. Users with this access profile can access the device using the management method selected.
- **Interface --** The interface type to which the rule applies. This is an optional field. This rule can be applied to a selected port, LAG, or VLAN by selecting the check box and selecting the appropriate option button and interface.
- **Source IP Address --** The interface source IP address for which the rule applies. This is an optional field and indicates that the rule is valid for a subnetwork.
- **Network Mask --** The IP subnetwork mask.
- **Prefix Length --** The number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- **Action --** Defines whether to permit or deny management access to the defined interface.

✍ ***Note:*** Assigning an access profile to an interface denies access via other interfaces. If an access profile is not assigned to any interface, the device can be accessed by all interfaces.

3.2.2.6.2 Authentication Profile

The Authentication Profiles page contains fields for selecting the user authentication method on the device. User authentication occurs:

- **Locally**
- **Via an external server**

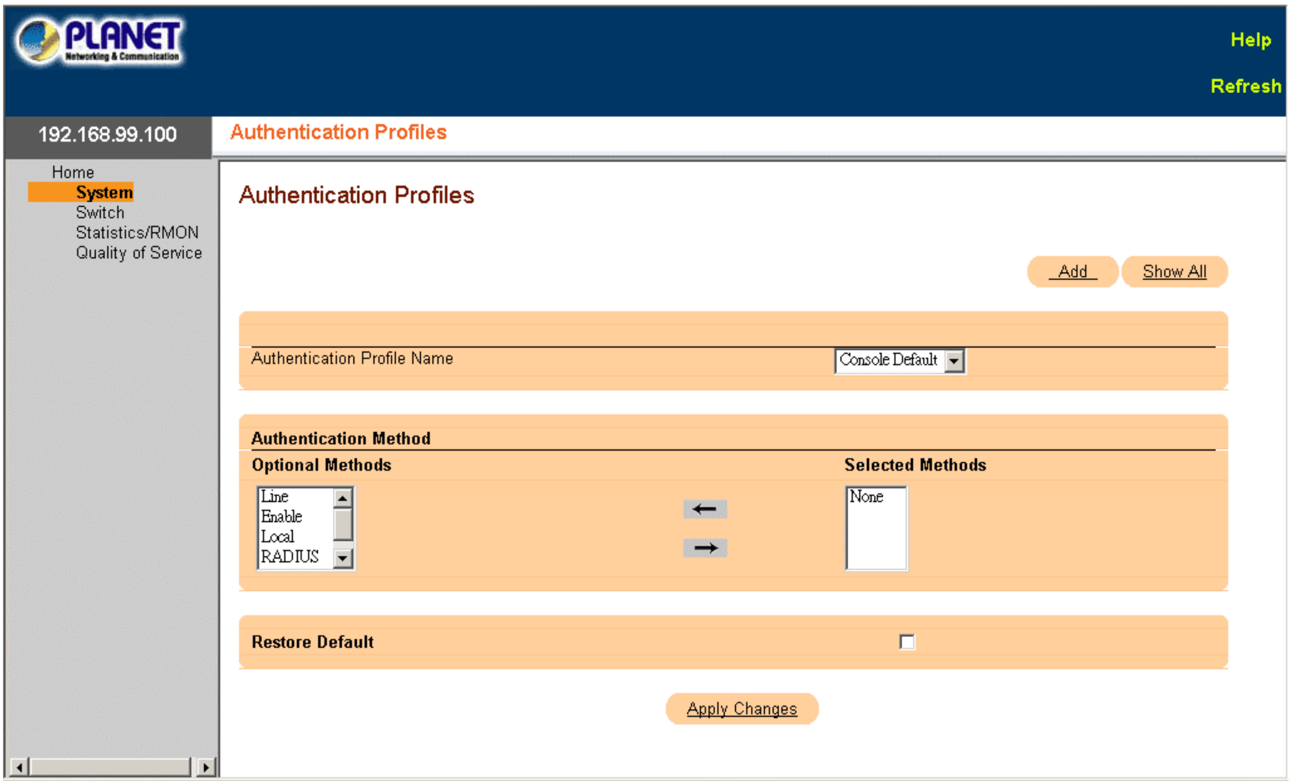
User authentication can also be set to None.

User authentication occurs in the order the methods are selected. For example, if both the Local and RADIUS options are selected, the user is authenticated first locally. If the local user database is empty, the user is then authenticated via the RADIUS server.

If an error occurs during the authentication, the next selected method is used.

To open **Authentication Profile** screen perform the folling:

1. Click System -> Management Security -> Authentication Profile
2. The Authentication Profile screen is displayed as in Figure 3-34.



Authentication Profiles

Authentication Profiles

Authentication Profile Name: Console Default

Authentication Method

Optional Methods: Line, Enable, Local, RADIUS

Selected Methods: None

Restore Default □

Figure 3-34 Authentication Profile screen

The page includes the following fields:

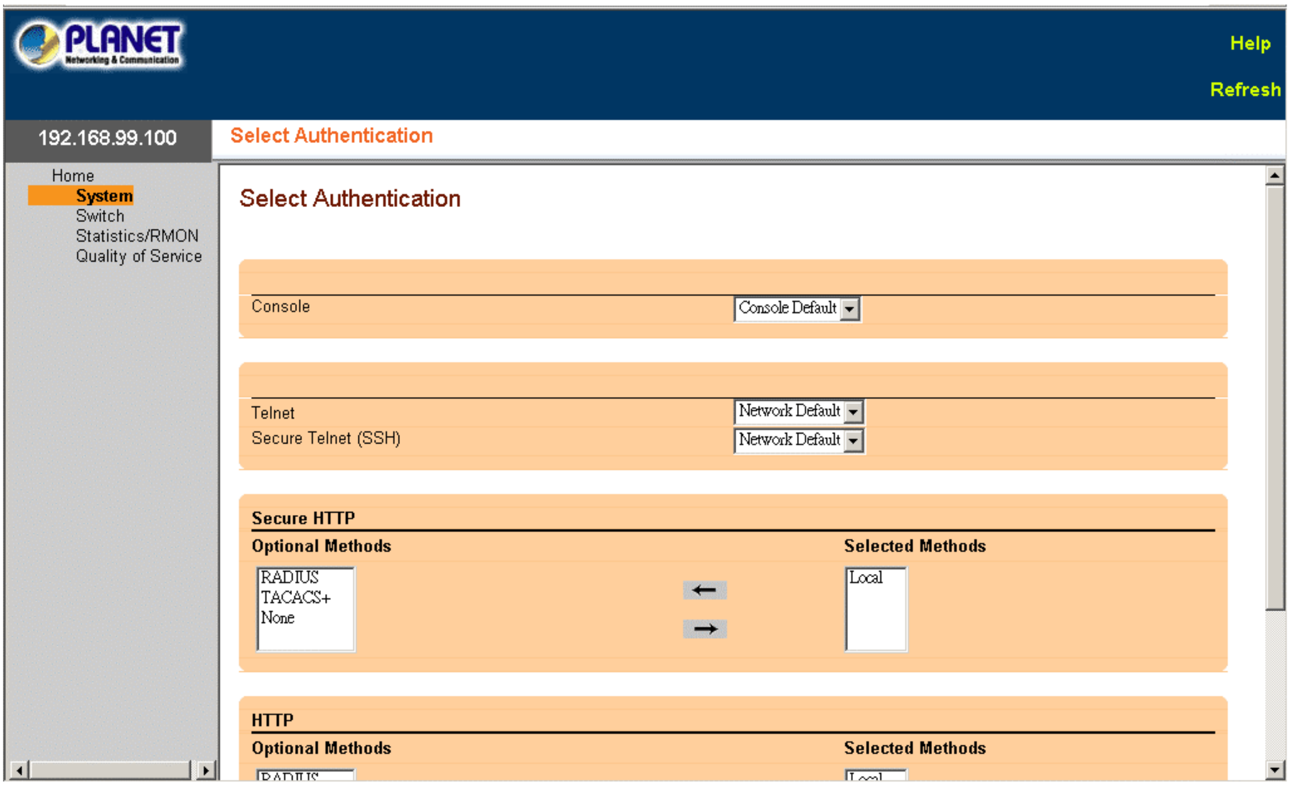
- **Authentication Profile Name --** User-defined authentication profile lists to which user-defined authentication profiles are added. The defaults are Network Default and Console Default.
- **Optional Methods --** User authentication methods. Possible options are:
- **None --** No user authentication occurs.
- **Local --** User authentication occurs at the device level. The device checks the user name and password for authentication.
- **RADIUS --** User authentication occurs at the RADIUS server. For more information, see "Configuring RADIUS Global Parameters."
- **Line --** The line password is used for user authentication.
- **Enable --** The enable password is used for authentication.
- **TACACS+ --** The user authentication occurs at the TACACS+ server.
- **Restore Default--** Restores the default user authentication method on the device.

3.2.2.6.3 Select Authentication

After Authentication Profiles are defined, the Authentication Profiles can be applied to Management Access methods. For example, console users can be authenticated by Authentication Method Lists 1, while Telnet users are authenticated by Authentication Method List 2.

To open **Select Authentication** screen perform the folling:

1. Click System -> Management Security -> Select Authentication
2. The Select Authentication screen is displayed as in Figure 3-35.



Select Authentication

Console: Console Default

Telnet: Network Default

Secure Telnet (SSH): Network Default

Secure HTTP

Optional Methods	Selected Methods
RADIUS TACACS+ None	Local

HTTP

Optional Methods	Selected Methods

Figure 3-35 Select Authentication screen

The page includes the following fields:

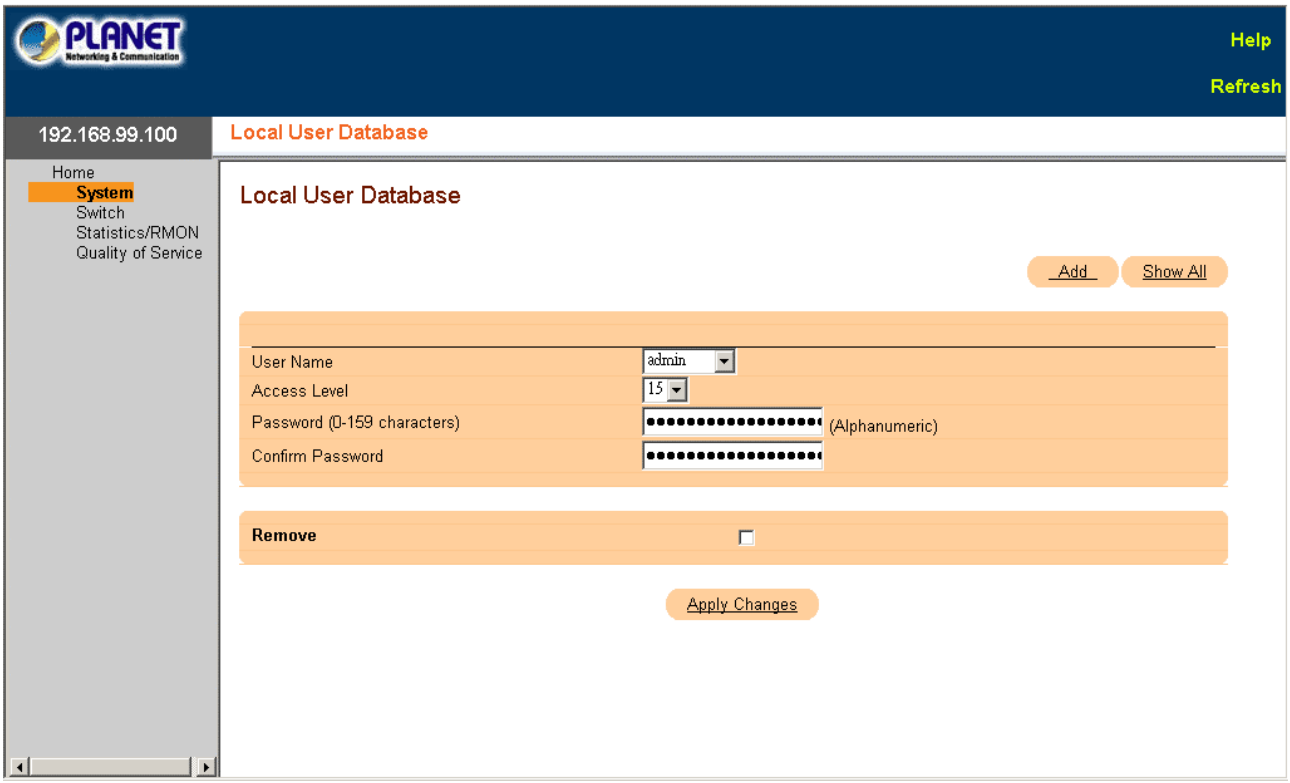
- **Console --** Authentication profiles used to authenticate console users.
- **Telnet --** Authentication profiles used to authenticate Telnet users.
- **Secure Telnet (SSH) --** Authentication profiles used to authenticate Secure Shell (SSH) users. SSH provides clients with secure and encrypted remote connections to a device.
- **HTTP and Secure HTTP --** Authentication method used for HTTP access and Secure HTTP access, respectively. Possible field values are:
- **None --** No authentication method is used for access.
- **Local --** Authentication occurs locally.
- **RADIUS --** Authentication occurs at the RADIUS server.
- **TACACS+ --** Authentication occurs at the TACACS+ server.

3.2.2.6.4 Local User Database

The **Local User Database** page contains fields for defining users, passwords and access levels.

To open **Local User Database** screen perform the folling:

1. Click System -> Management Security -> Local User Database
2. The Local User Database screen is displayed as in Figure 3-36.



Local User Database

User Name	admin
Access Level	15
Password (0-159 characters)	•••••••••••••••••• (Alphanumeric)
Confirm Password	••••••••••••••••••

Remove □

Figure 3-36 Local User Database screen

The page includes the following fields:

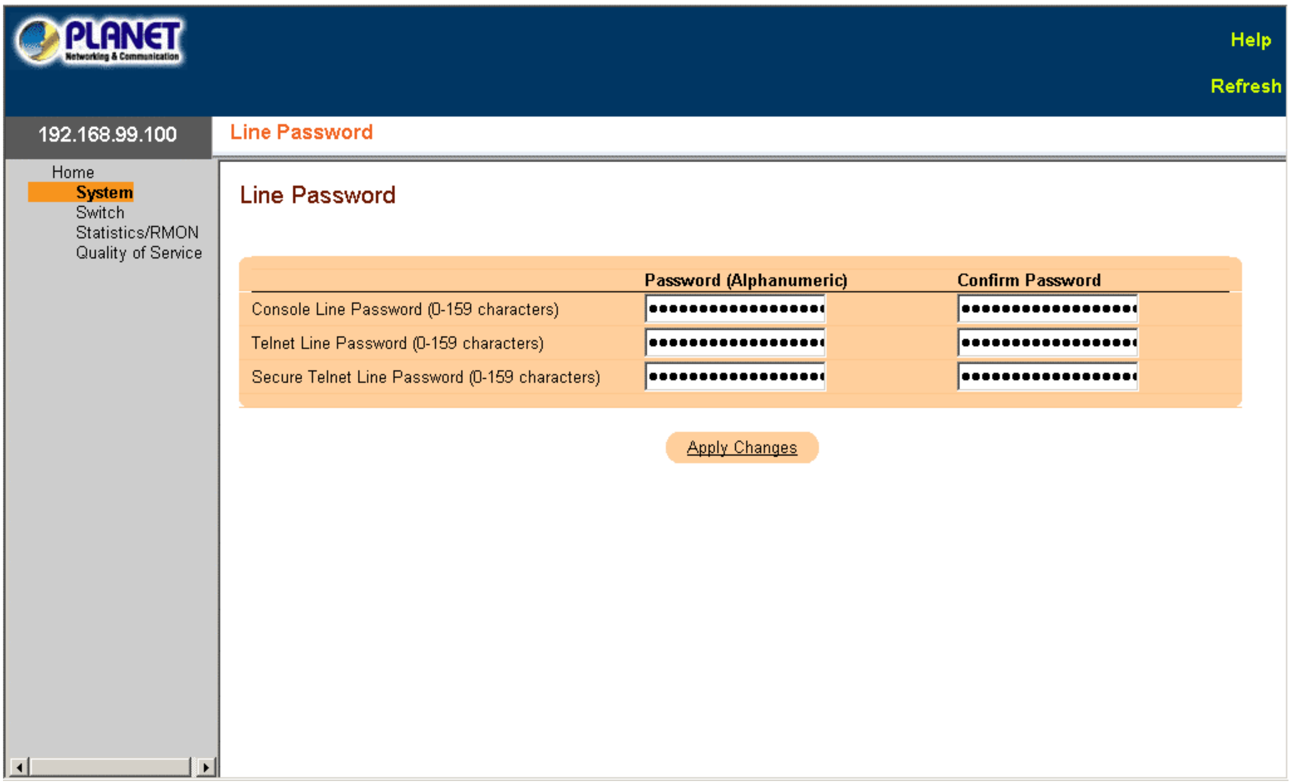
- **User Name --** List of users.
- **Access Level --** User access level. The lowest user access level is 1, and the highest user access level is 15.
- **Password (0-159 Characters) --** User-defined password. Local user database passwords can have a maximum of 159 characters.
- **Confirm Password --** Confirms the user-defined password.
- **Remove --** When selected, removes users from the User Name list.

3.2.2.6.5 Line Password

The **Line Password** page contains fields for defining line passwords for management methods.

To open **Line Password** screen perform the folling:

1. Click System -> Management Security -> Line Password
2. The Line Password screen is displayed as in Figure 3-37.



Line Password

	Password (Alphanumeric)	Confirm Password
Console Line Password (0-159 characters)	••••••••••••••••••	••••••••••••••••••
Telnet Line Password (0-159 characters)	••••••••••••••••••	••••••••••••••••••
Secure Telnet Line Password (0-159 characters)	••••••••••••••••••	••••••••••••••••••

Figure 3-37 Line Password screen

The page includes the following fields:

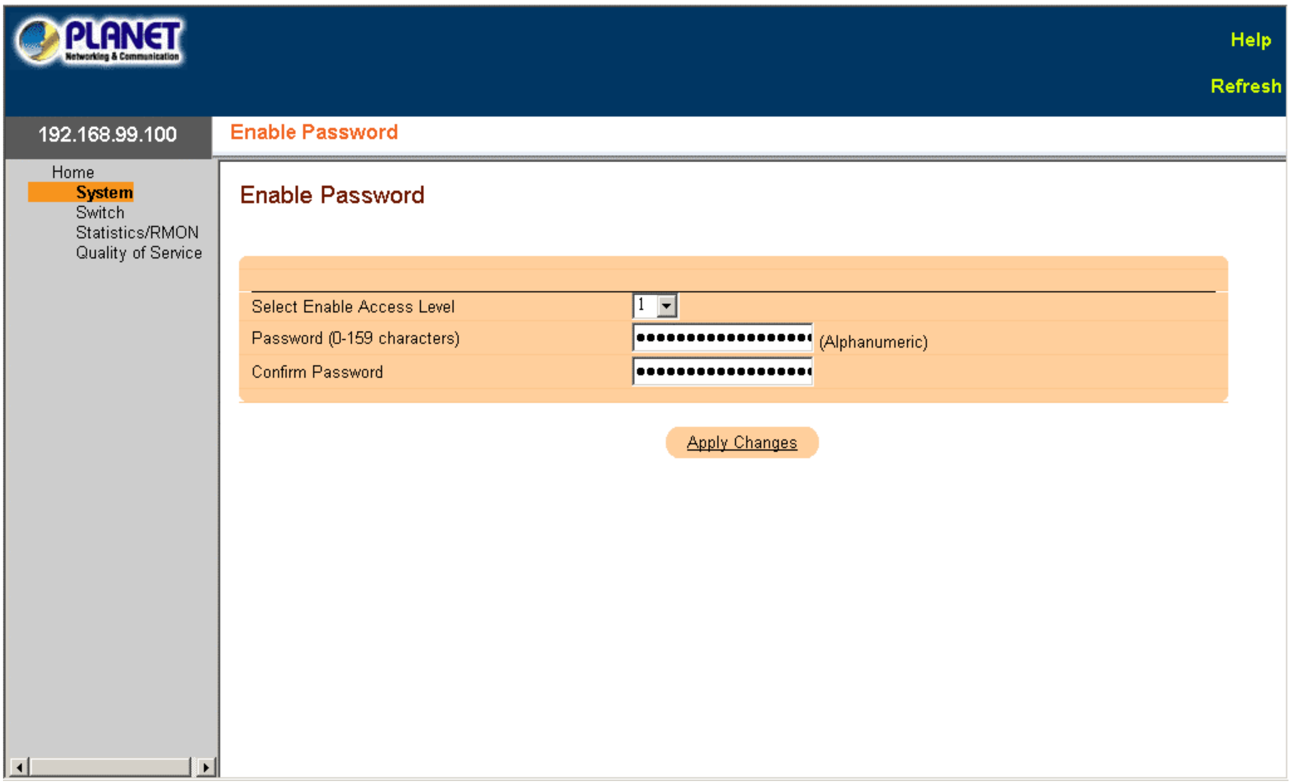
- **Line Password for Console/Telnet/Secure Telnet (0-159 Characters) --** The line password for accessing the device via a console, Telnet, or Secure Telnet session. Passwords can contain a maximum of 159 characters.
- **Confirm Password --** Confirms the new line password. The password appears in the ***** format.

3.2.2.6.6 Enable Password

The **Modify Enable Password** page sets a local password to control access to Normal, Privilege, and Global Configuration.

To open **Enable Password** screen perform the folling:

1. Click System -> Management Security -> Enable Password
2. The Enable Password screen is displayed as in Figure 3-38.



Enable Password

Select Enable Access Level	1	
Password (0-159 characters)	●●●●●●●●●●●●●●●●●●	(Alphanumeric)
Confirm Password	●●●●●●●●●●●●●●●●●●	

Figure 3-38 Enable Password screen

The page includes the following fields:

- **Select Enable Access Level --** Access level associated with the enable password. Possible field values are 1-15.
- **Password (0-159 Characters) --** The currently configured enable password. Enable passwords can contain a maximum of 159 characters.
- **Confirm Password --** Confirms the new enable password. The password appears in the ***** format.

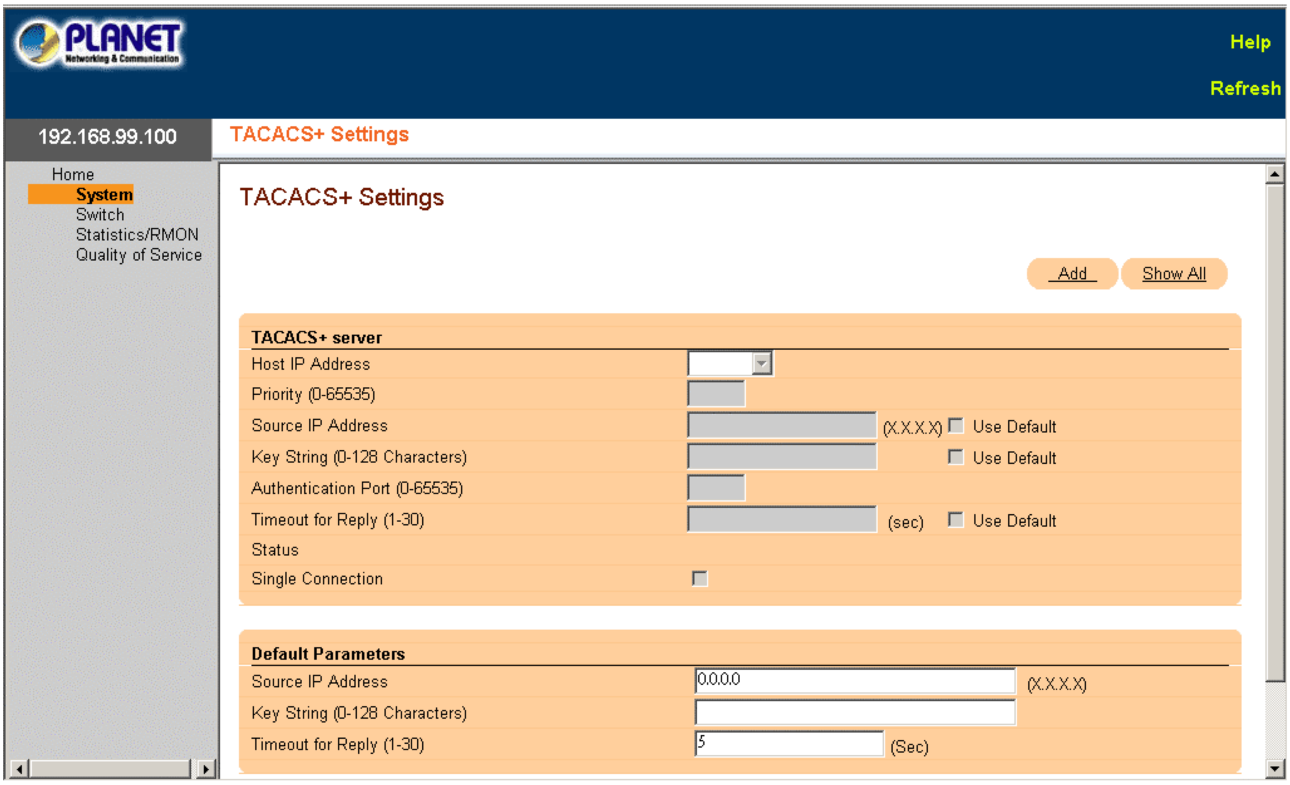
3.2.2.6.7 TACACS+

The devices provide **Terminal Access Controller Access Control System (TACACS+)** client support. TACACS+ provides centralized security for validation of users accessing the device.

TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes.

To open **TACACS+** screen perform the folling:

1. Click System -> Management Security -> TACACS+
2. The TACACS+ screen is displayed as in Figure 3-39.



TACACS+ Settings

TACACS+ server		
Host IP Address		
Priority (0-65535)		
Source IP Address		(X.X.X.X) □ Use Default
Key String (0-128 Characters)		□ Use Default
Authentication Port (0-65535)		
Timeout for Reply (1-30)		(sec) □ Use Default
Status		
Single Connection	□	
Default Parameters		
Source IP Address	0.0.0.0	(X.X.X.X)
Key String (0-128 Characters)		
Timeout for Reply (1-30)	5	(Sec)

Figure 3-39 TACACS+ Settings screen

TACACS+ provides the following services:

- **Authentication --** Provides authentication during login and via user names and user-defined passwords.
- **Authorization --** Performed at login. Once the authentication session is completed, an authorization session starts using the authenticated user name. The TACACS server checks the user privileges.

The TACACS+ protocol ensures network integrity through encrypted protocol exchanges between the device and TACACS+ server.

The TACACS+ Settings page is divided into the following sections:

- **TACACS+ Server Section**
- **Default Parameters Section**

TACACS+ Server Section

The TACACS+ Server section contains the following fields:

- **Host IP Address --** Specifies the TACACS+ server IP address.
- **Priority (0-65535) --** Specifies the order in which the TACACS+ servers are used. The default is 0.
- **Source IP Address --** The device source IP address used for the TACACS+ session between the device and the TACACS+ server.
- **Key String (0-128 Characters) --** Defines the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ server.
- **Authentication Port (0-65535) --** The port number through which the TACACS+ session occurs. The default is port 49.
- **Reply Timeout (1-30) (Sec) --** The amount of time that passes before the connection between the device and the TACACS+ server times out. The field range is 1-30 seconds.
- **Status --** The connection status between the device and the TACACS+ server. The possible field values are:
- **Connected --** There is currently a connection between the device and the TACACS+ server.
- **Not Connected --** There is not currently a connection between the device and the TACACS+ server.

- **Single Connection --** Maintains a single open connection between the device and the TACACS+ server when selected

Default Parameters Section

The TACACS+ default parameters are user-defined defaults. The default settings are applied to newly defined TACACS+ servers. If default values are not defined, the system defaults are applied to the new TACACS+ new servers.

The Default Parameters section contains the following fields:

- **Source IP Address --** The default device source IP address used for the TACACS+ session between the device and the TACACS+ server.
- **Key String (0-128 Characters) --** The default authentication and encryption key for TACACS+ communication between the device and the TACACS+ server.
- **Timeout for Reply (1-30) --** The default time that passes before the connection between the device and the TACACS+ times out.

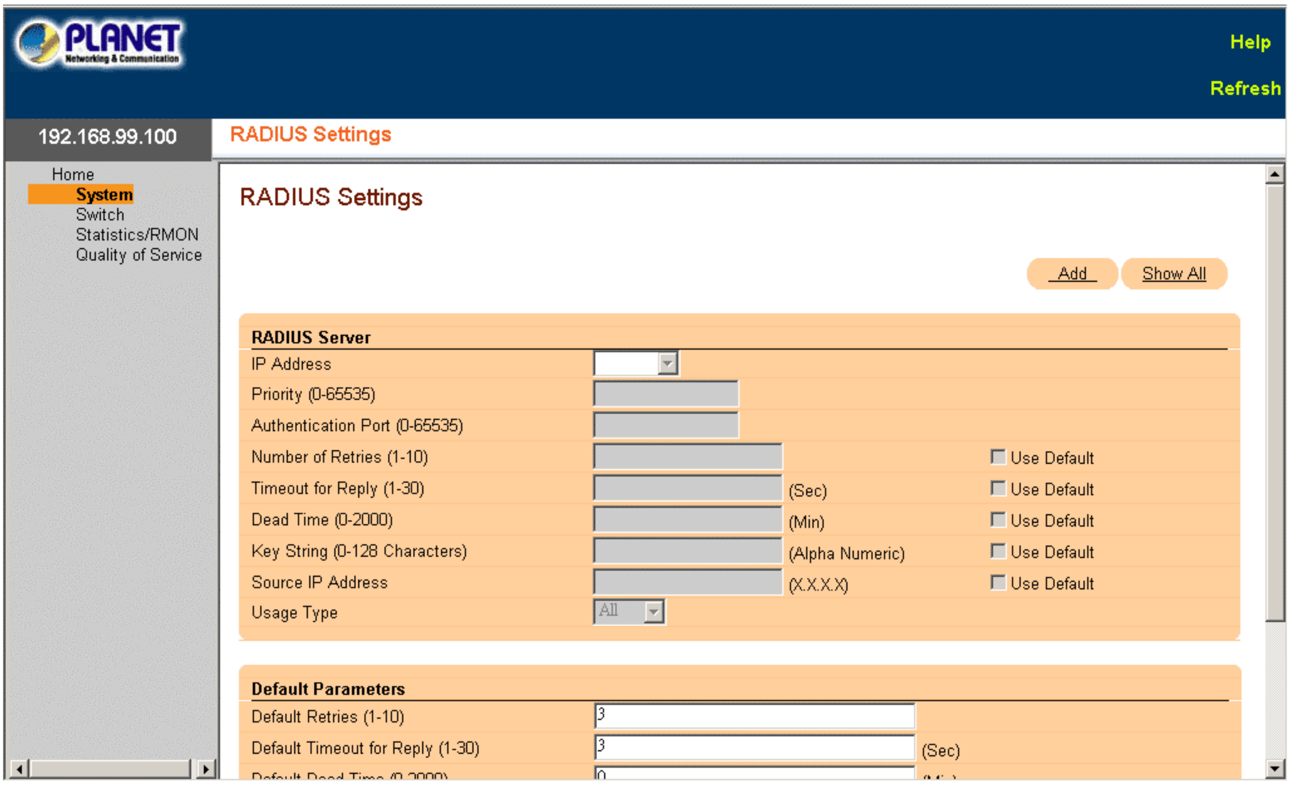
3.2.2.6.8 RADIUS

Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. RADIUS servers provide a centralized authentication method for:

- **Telnet Access**
- **Web Access**
- **Console to Device Access**

To open **RADIUS** screen perform the folling:

1. Click System -> Management Security -> RADIUS
2. The RADIUS screen is displayed as in Figure 3-40.



RADIUS Settings

RADIUS Server

IP Address			
Priority (0-65535)			
Authentication Port (0-65535)			
Number of Retries (1-10)			□ Use Default
Timeout for Reply (1-30)		(Sec)	□ Use Default
Dead Time (0-2000)		(Min)	□ Use Default
Key String (0-128 Characters)		(Alpha Numeric)	□ Use Default
Source IP Address		(X.X.X.X)	□ Use Default
Usage Type	All		

Default Parameters

Default Retries (1-10)	3	
Default Timeout for Reply (1-30)	3	(Sec)
Default Dead Time (0-2000)	0	(Min)

Figure 3-40 RADIUS Settings screen

The RADIUS Settings page is divided into the following sections:

- **RADIUS Server Section**
- **Default Parameters Section**

RADIUS Server Section

The RADIUS Server section contains the following fields:

- **IP Address --** The list of Authentication Server IP addresses.
- **Priority (1-65535) --** The server priority. The possible values are 1-65535, where 1 is the highest value. This is used to configure the order in which servers are queried.
- **Authentication Port --** Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication.
- **Number of Retries (1-10) --** Specifies the number of transmitted requests sent to RADIUS server before a failure occurs. The possible field values are 1 - 10. The default is 3.
- **Timeout for Reply (1-30) --** Specifies the amount of the time in seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. The possible field values are 1 - 30. Three is the default value.
- **Dead Time (0-2000) --** Specifies the amount of time (in seconds) that a RADIUS server is bypassed for service requests. The range is 0-2000.
- **Key String (1-128 Characters) --** The Key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key is encrypted.
- **Source IP Address --** Specifies the source IP address that is used for communication with RADIUS servers.

Default Parameters Section

The following fields set the RADIUS default values:

- **Default Timeout for Reply (1-30) --** Specifies the default amount of the time (in seconds) the device waits for an answer from the RADIUS server before timing out.
- **Default Retries (1-10) --** Specifies the default number of transmitted requests sent to RADIUS server before a failure occurs.
- **Default Dead time (0-2000) --** Specifies the default amount of time (in seconds) that a RADIUS server is bypassed for service requests. The range is 0-2000.
- **Default Key String (1-128 Characters) --** The Default Key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key is encrypted.
- **Source IP Address --** Specifies the source IP address that is used for communication with RADIUS servers.
- **Usage Type --** Specifies the server usage type. Can be one of the following values: login, 802.1x or all. If unspecified, defaults to all.

✍ ***Note:*** If host-specific Timeouts, Retries, or Dead time values are not specified, the Global values (Defaults) are applied to each host.

3.2.2.7 SNMP

Simple Network Management Protocol (SNMP) provides a method for managing network devices. Devices supporting SNMP run a local software (agent).

The SNMP agents maintain a list of variables, which are used to manage the device. The variables are defined in the Management Information Base (MIB). The MIB contains the variables controlled by the agent. The SNMP protocol defines the MIB specification format, as well as the format used to access the information over the network.

Access rights to the SNMP agents are controlled by access strings. To communicate with the device, the Embedded Web Server submits a valid community string for authentication.

The SNMP page contains links to the following topics:

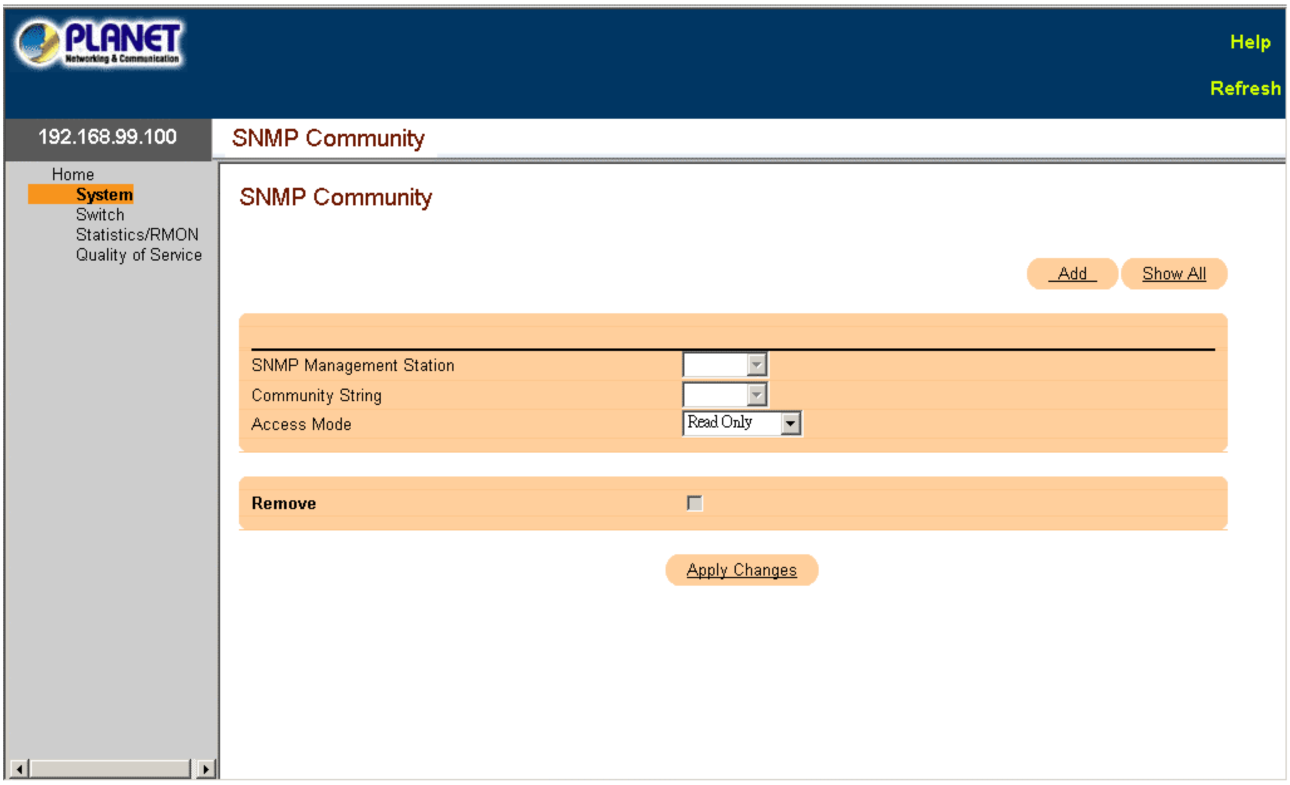
- **Communities**
- **Traps**

3.2.2.7.1 SNMP Communities

Access rights are managed by defining communities in the SNMP Community page. When the community names are changed, access rights are also changed.

To open **SNMP Communities** screen perform the folling:

1. Click System -> SNMP -> Communities
2. The SNMP Communities screen is displayed as in Figure 3-41.



SNMP Management Station	
Community String	
Access Mode	Read Only

Remove	□

Figure 3-41 SNMP Communities screen

The page includes the following fields:

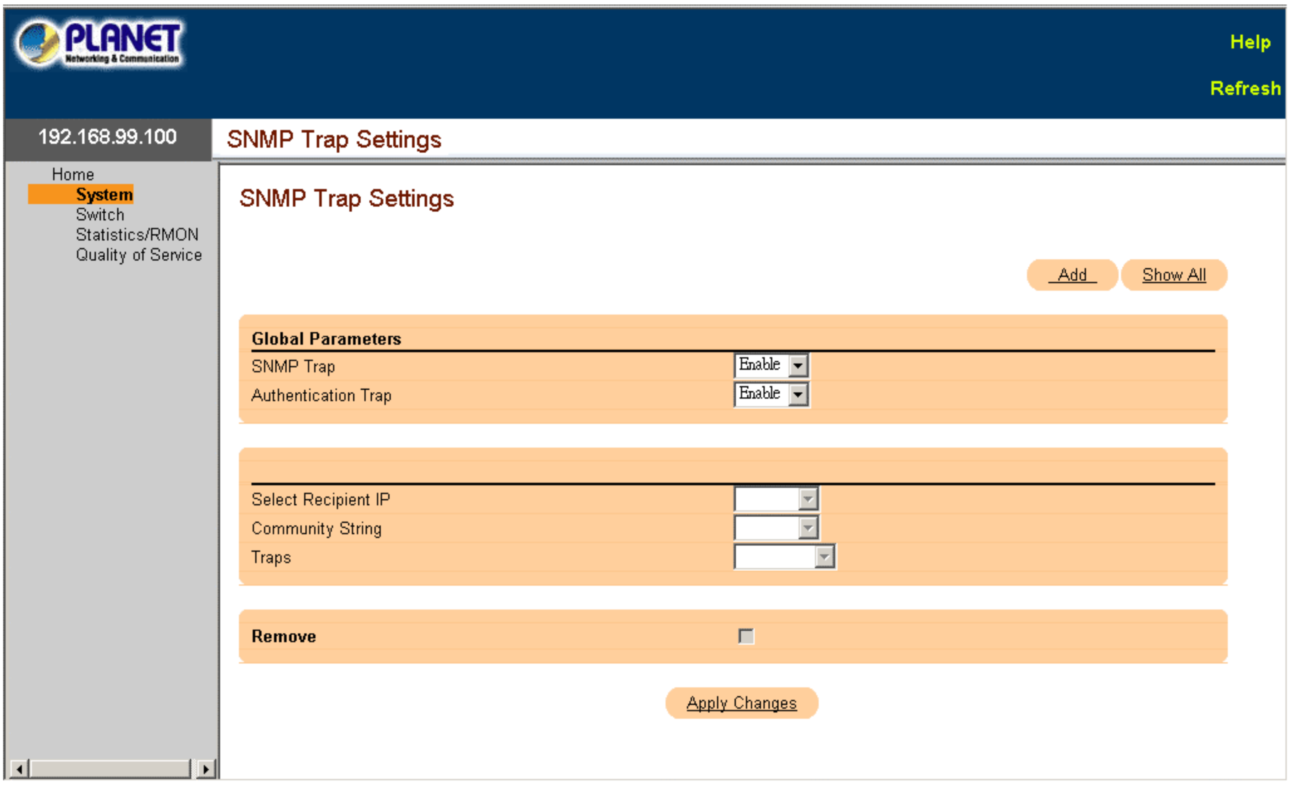
- **SNMP Management Station --** A list of management station IP addresses.
- **Community String --** Functions as a password and used to authenticate the selected management station to the device.
- **Access Mode --** Defines the access rights of the community. The possible field values are:
- **Read Only --** The management access is restricted to read-only, for all MIBs except the community table, for which there is no access.
- **Read Write --** The management access is read-write, for all MIBs except the community table, for which there is no access.
- **SNMP Admin --** The management access is read-write for all MIBs, including the community table.
- **Remove --** Removes a community, when selected.

3.2.2.7.2 SNMP Trap

From the **SNMP Trap** Settings page, the user can enable or disable the device to send SNMP traps or notifications.

To open **SNMP Trap** screen perform the folling:

1. Click System -> SNMP -> Trap
2. The SNMP Trap screen is displayed as in Figure 3-42.



SNMP Trap Settings

Global Parameters

SNMP Trap: Enable

Authentication Trap: Enable

Select Recipient IP:

Community String:

Traps:

Remove □

Figure 3-42 SNMP Trap Settings screen

The page includes the following fields:

- **SNMP Trap --** Enables sending SNMP traps or SNMP notifications from the device to defined trap recipients.
- **Authentication Trap --** Enables sending SNMP traps when authentication failed to define recipients.
- **Select Recipient IP --** Specifies the IP address to whom the traps are sent.
- **Community String --** Identifies the community string of the trap manager.
- **Traps --** Determines the trap type sent to the selected recipient. The possible field values are:
- **SNMP V1 --** SNMP Version 1 traps are sent
- **SNMP V2c --** SNMP Version 2 traps are sent
- **Remove --** Removes Trap Manager Table entries, when selected.

3.2.2.8 File Management

The File Management page contains fields for managing device software, the Image Files, and the Configuration Files. Files can be downloaded from a TFTP server.

The File Management page contains links to the following topics:

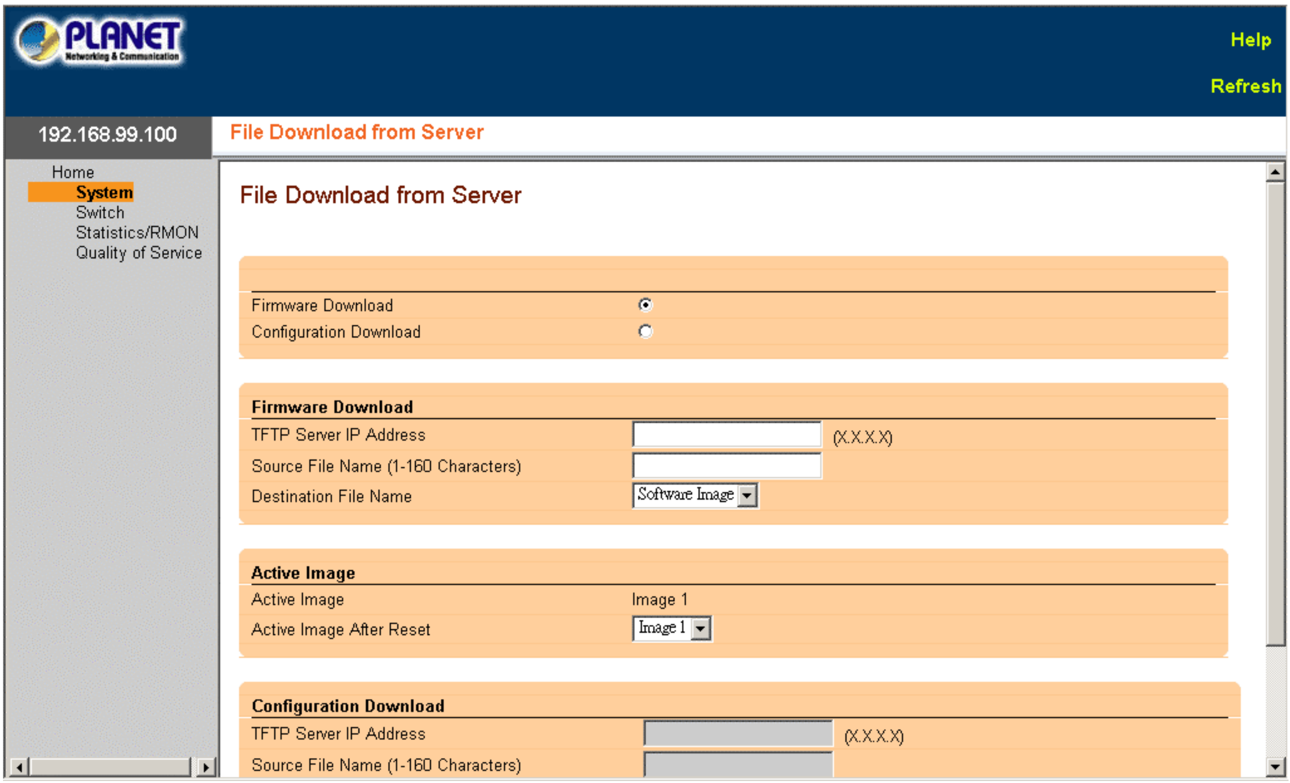
- **File Download**
- **File Upload**
- **Copy Files**

3.2.2.8.1 File Download

The **File Download From Server** page contains fields for downloading system image and Configuration files from the TFTP server to the device.

To open **File Download** screen perform the folling:

1. Click System -> File Management -> File Download
2. The File Download screen is displayed as in Figure 3-43.



File Download from Server

File Download from Server

Firmware Download	●
Configuration Download	○

Firmware Download

TFTP Server IP Address		(X.X.X.X)
Source File Name (1-160 Characters)		
Destination File Name	Software Image ▾	

Active Image

Active Image	Image 1
Active Image After Reset	Image 1 ▾

Configuration Download

TFTP Server IP Address		(X.X.X.X)
Source File Name (1-160 Characters)		

Figure 3-43 File Download screen

The page includes the following fields:

- **Firmware Download --** The Firmware file is downloaded. If Firmware Download is selected, the Configuration Download fields are grayed out.
- **Configuration Download --** The Configuration file is downloaded. If Configuration Download is selected, the Firmware Download fields are grayed out.
- **Firmware Download TFTP Server IP Address --** The TFTP Server IP Address from which files are downloaded.
- **Firmware Download Source File Name --** Specifies the file to be downloaded.
- **Firmware Download Destination File --** The destination file type to which to the file is downloaded. The possible field values are:
  - **Software Image --** Downloads the Image file.
  - **Boot Code --** Downloads the Boot file.
- **Active Image --** The Image file that is currently active.
- **Active Image After Reset --** The Image file that is active after the device is reset.
- **Configuration Download File TFTP Server IP Address --** The TFTP Server IP Address from which the configuration files are downloaded.
- **Configuration Download File Source File Name --** Specifies the configuration files to be downloaded.
- **Configuration Download File Destination --** The destination file to which to the configuration file is downloaded. The possible field values are:
- **Running Configuration --** Downloads commands into the Running Configuration file.
- **Startup Configuration --** Downloads the Startup Configuration file, and overwrites it.
- **Backup Configuration --** Downloads the Backup Configuration file, and overwrites it.

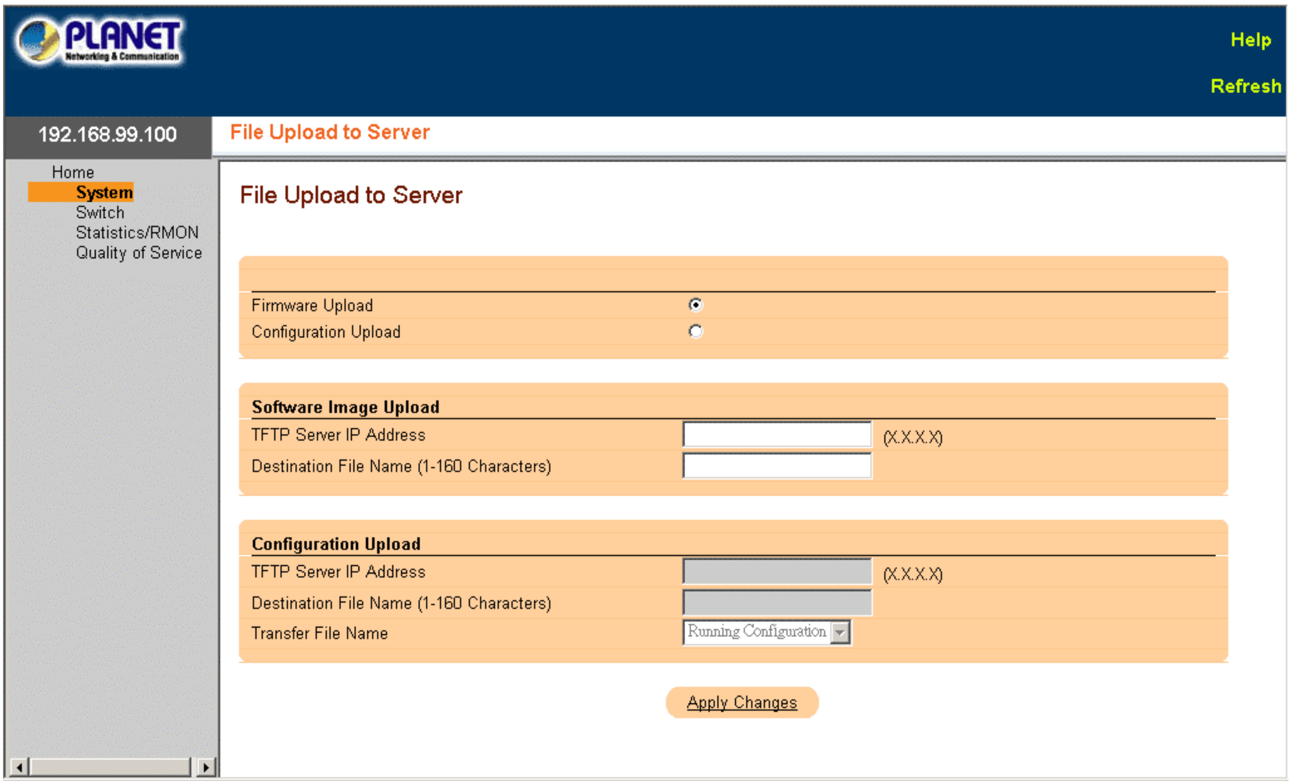
✍ ***Note:*** To activate a selected Image file, reset the device. For information on resetting the device, see "Reset".

3.2.2.8.2 File Upload

The **File Upload to Server** page contains fields for uploading the software from the TFTP server to the device. The Image file can also be uploaded from the File Upload to Server page.

To open **File Upload** screen perform the folling:

1. Click System -> File Management -> File Upload
2. The File Upload screen is displayed as in Figure 3-44.



File Upload to Server

Firmware Upload	●
Configuration Upload	○

Software Image Upload

TFTP Server IP Address		(X.X.X.X)
Destination File Name (1-160 Characters)		

Configuration Upload

TFTP Server IP Address		(X.X.X.X)
Destination File Name (1-160 Characters)		
Transfer File Name	Running Configuration	

Figure 3-44 File Upload Server screen

The page includes the following fields:

- **Firmware Upload --** The Firmware file is uploaded. If Firmware Upload is selected, the Configuration Upload fields are grayed out.
- **Configuration Upload --** The Configuration file is uploaded. If Configuration Upload is selected, the Software Image Upload fields are grayed out.
- **Software Image Upload TFTP Server IP Address --** The TFTP Server IP Address to which the Software Image is uploaded.
- **Software Image Upload Destination --** Specifies the Software Image file path to which the file is uploaded.
- **Configuration Upload TFTP Server IP Address --** The TFTP Server IP Address to which the Configuration file is uploaded.
- **Configuration Upload Destination --** Specifies the Configuration file path to which the file is uploaded.
- **Configuration Upload Transfer file name --** The software file to which the configuration is uploaded. The possible field values are:
- **Running Configuration --** Uploads the Running Configuration file
- **Startup Configuration --** Uploads the Startup Configuration file
- **Backup Configuration --** Uploads the Backup Configurationfile

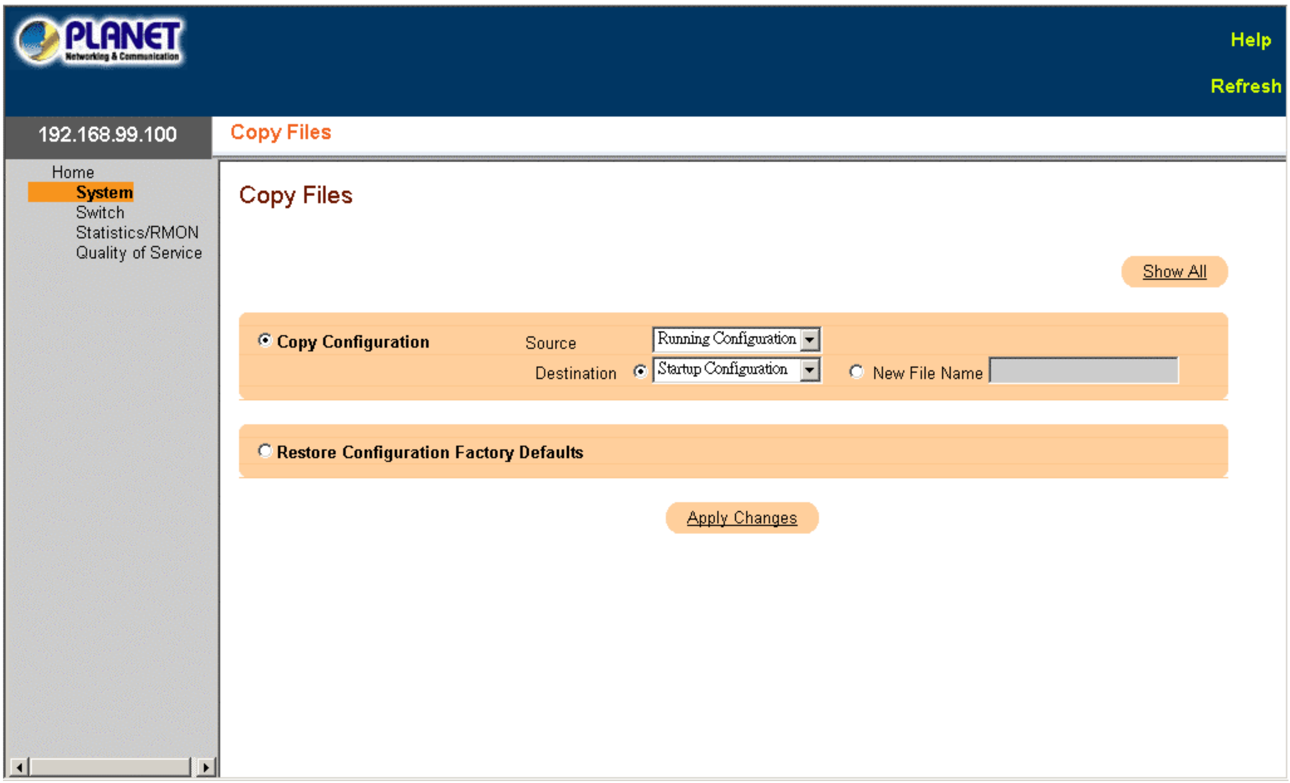
3.2.2.8.3 Copy Files

Files can be copied and deleted from the **Copy Files** page

To open **Copy Files** screen perform the folling:

1. Click System -> File Management -> Copy Files

2. The Copy Files screen is displayed as in Figure 3-45.



Copy Files

● Copy Configuration — Source: Running Configuration

Destination: ● Startup Configuration ○ New File Name

○ Restore Configuration Factory Defaults

Figure 3-45 Copy File screen

The page includes the following fields:

- **Copy Configuration --** When selected, copies either the Running Configuration, Startup Configuration or Backup Configuration files. The possible field values are:
- **Source --** Copies either the Running Configuration, Startup Configuration or Backup Configuration files.
- **Destination --** The file to which the Running Configuration, Startup Configuration or Backup Configuration file is copied.
- **Restore Configuration Factory Defaults --** When selected, specifies that the factory configuration default files should be reset. When unselected, maintains the current configuration settings.

3.2.2.9 Advanced Settings

The the **Advanced Settings** page contains a link for configuring general settings. Use Advanced Settings to set miscellaneous global attributes for the device. The changes to these attributes are applied only after the device is reset.

The Advanced Settings page contains links to the following topics:

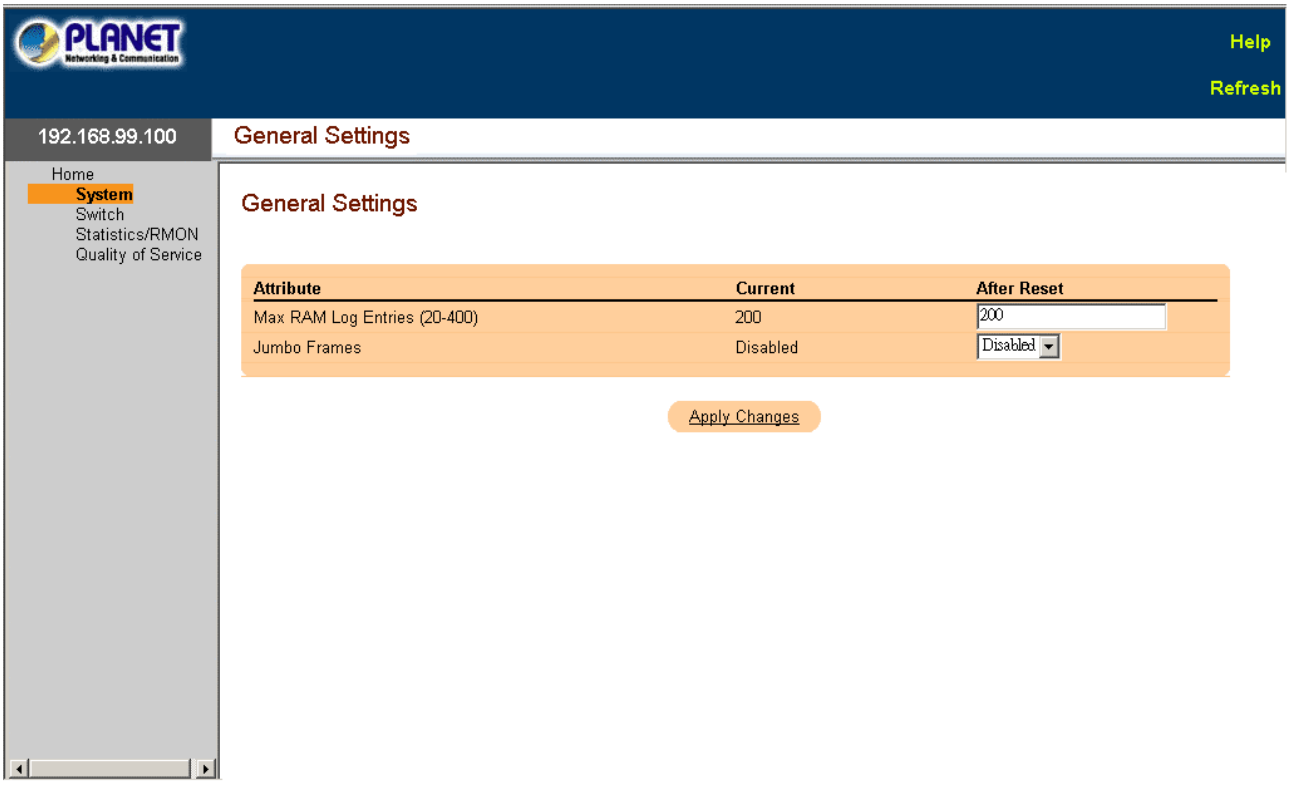
- **General Settings**

3.2.2.9.1 General Settings

The **General Settings** page provides information for defining general device parameters.

To open **Copy Files** screen perform the folling:

1. Click System -> Advanced Settings -> General Settings
2. The General Settings screen is displayed as in Figure 3-46.



General Settings

Attribute	Current	After Reset
Max RAM Log Entries (20-400)	200	200
Jumbo Frames	Disabled	Disabled

Figure 3-46 General Settings screen

The page includes the following fields:

- **Attribute --** The general setting attribute.
- **Current --** The currently configured value.
- **After Reset --** The future (after reset) value. By entering a value in the After Reset column, memory is allocated to the field table.
- **Max RAM Log Entries (20-400) --** The maximum number of RAM Log entries. When the Log entries are full, the log is cleared and the Log file is restarted.
- **Jumbo Frames --** Enables or disables the Jumbo Frames feature. Jumbo Frames enable the transportation of identical data in fewer frames. This ensures less overhead, lower processing time, and fewer interrupts.

3.2.3 Configure Switch Information

This page provides all system operation and general information for configuring network security, ports, Address tables, GARP, VLANs, Spanning Tree, Port Aggregation, and Multicast Support.

The Switch page contains links to the following topics:

- **Network Security**
- **Ports**
- **Address Tables**
- **GARP**
- **Spanning Tree**
- **VLAN**
- **Link Aggregation**
- **Multicast Support**

3.2.3.1 Network Security

The device enables network security through both Access Control Listsand Locked Ports.

The **Network Security** page contains links to the following topics:

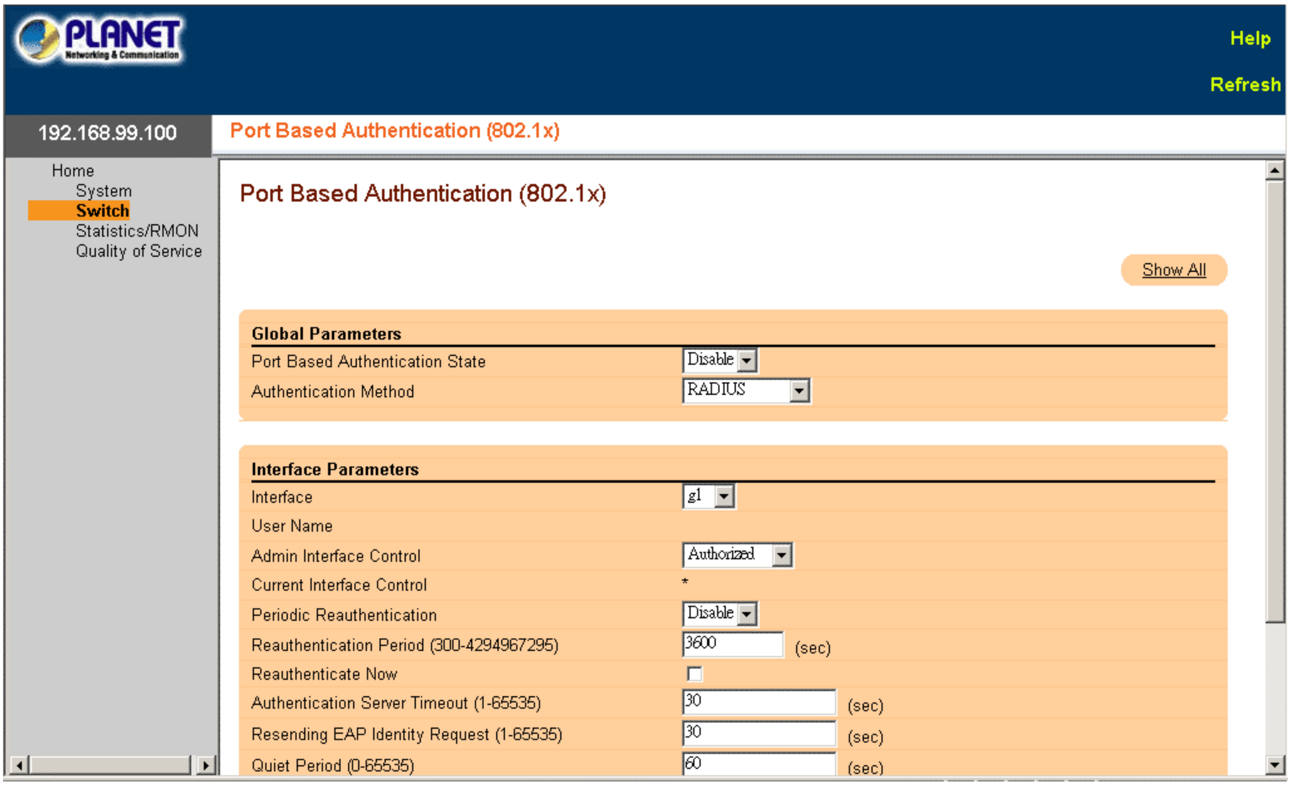
- **Port Based Authentication**
- **Multiple Hosts**
- **Authenticated Users**
- **Port Security**

3.2.3.1.1 Port Base Authentication

The Port Based Authentication page contains fields for configuring port based authentication.

To open **Port Based Authentication** screen perform the folling:

1. Click Switch -> Network Secuity -> Port Based Authentication
2. The Port Based Authentication screen is displayed as in Figure 3-47.



Port Based Authentication (802.1x)

Global Parameters	
Port Based Authentication State	Disable
Authentication Method	RADIUS

Interface Parameters		
Interface	g1	
User Name		
Admin Interface Control	Authorized	
Current Interface Control	*	
Periodic Reauthentication	Disable	
Reauthentication Period (300-4294967295)	3600	(sec)
Reauthenticate Now	□	
Authentication Server Timeout (1-65535)	30	(sec)
Resending EAP Identity Request (1-65535)	30	(sec)
Quiet Period (0-65535)	60	(sec)

Figure 3-47 Port Base Authentication screen

The page includes the following fields:

- **Port Based Authentication State --** Permits port based authentication on the device. The possible field values are:
- Enable -- Enables port based authentication on the device.
- **Disable --** Disables port based authentication on the device.
- **Authentication Method --** The Authentication method used. The possible field values are:
- **None --** No authentication method is used to authenticate the port.
- **RADIUS --** Port authentication is performed via the RADIUS server.
- **RADIUS, None --** Port authentication is performed first via RADIUS server. If the port is not authenticated, then no authentication method is used, and the session is permitted.
- **Interface --** Contains an interface list.
- **User Name --** The user name as configured in the RADIUS server.
- **Admin Interface Control --** Defines the port authorization state. The possible field values are:

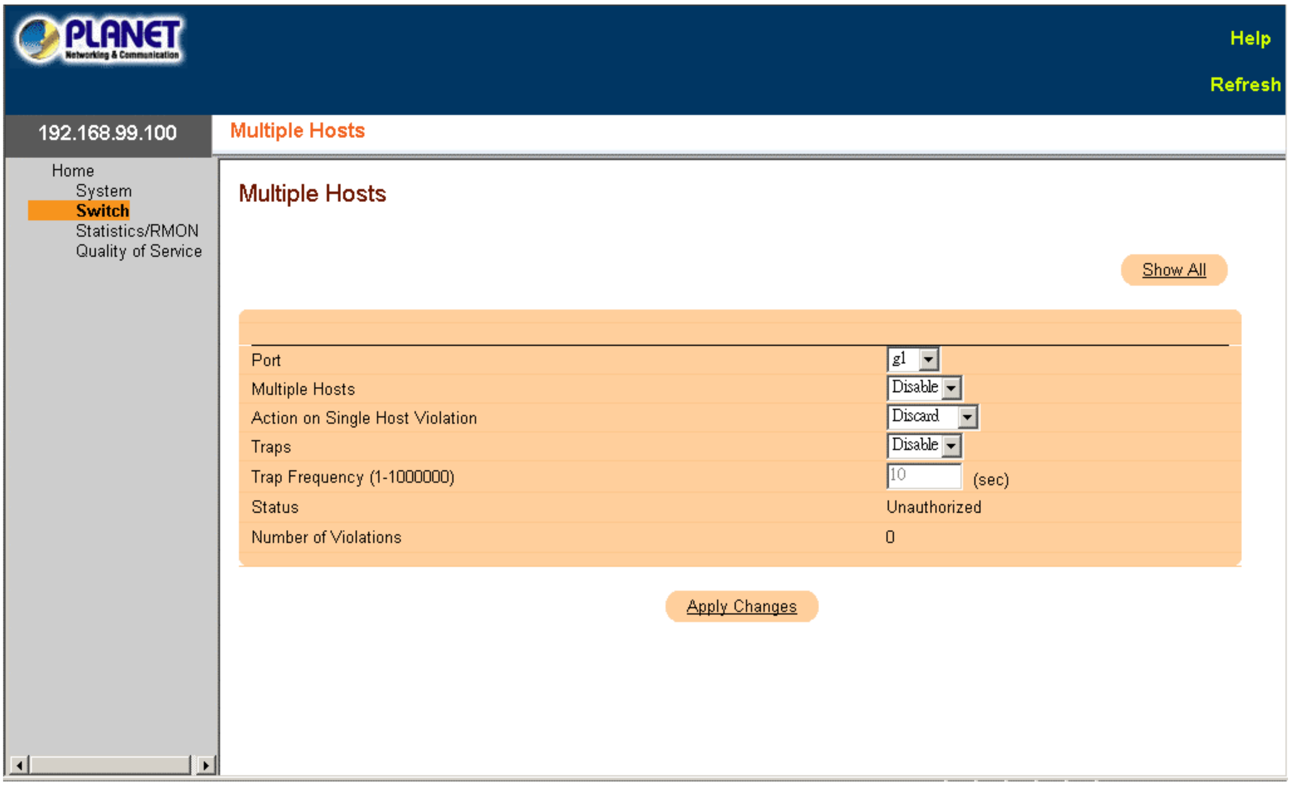
- **Authorized --** Set the interface state to authorized (permit traffic).
- **Unauthorized --** Set the interface state to unauthorized (deny traffic).
- **Auto --** Authorize state is set by the authorization method.
- **Current Interface Control --** The currently configured port authorization state. Asterisk (*) appears for port down.
- **Periodic Reauthentication --** Reauthenticates the selected port periodically, when enabled. The reauthentication period is defined in the Reauthentication Period (300-4294967295) field.
- **Reauthentication Period (300-4294967295) --** Indicate the time span in which the selected port is reauthenticated. The field value is in seconds. The field default is 3600 seconds.
- **Reauthenticate Now --** Permits immediate port reauthentication, when selected.
- **Authentication Server Timeout (1-65535) --** Defines the amount of time that lapses before the device resends a request to the authentication server. The field value is in seconds. The field default is 30 seconds.
- **Resending EAP Identity Request (1-65535) --** Defines the amount of time that lapses before EAP request are resent. The field default is 30 seconds.
- **Quiet Period (0-65535) --** The number of seconds that the device remains in the quiet state following a failed authentication exchange. The possible field range is 0-65535. The field default is 60 seconds.
- **Supplicant Timeout (1-65535) --** The amount of time that lapses before EAP requests are resent to the user. The field value is in seconds. The field default is 30 seconds.
- **Max EAP Requests (1-10) --** The total amount of EAP requests sent. If a response is not received after the defined period, the authentication process is restarted. The field default is 2 retries.

3.2.3.1.2 Multiple Hosts

The **Multiple Hosts** page provides information for defining advanced port based authentication settings for specific ports.

To open **Multiple Hosts** screen perform the folling:

1. Click Switch -> Network Secuity -> Multiple Hosts
2. The Multiple Hosts screen is displayed as in Figure 3-48.



Port	g1
Multiple Hosts	Disable
Action on Single Host Violation	Discard
Traps	Disable
Trap Frequency (1-1000000)	10 (sec)
Status	Unauthorized
Number of Violations	0

Figure 3-48 Multiple Hosts screen

The page includes the following fields:

- **Port --** The port number for which Advanced Port Based Authentication is enabled.

- **Multiple Hosts --** Enables or disables a single host to authorize multiple hosts for system access. This setting must be enabled in order to either disable the ingress-filter, or to use port-lock security on the selected port.
- **Action on Single Host Violation --** Defines the action to be applied to packets arriving in single-host mode, from a host whose MAC address is not the client (supplicant) MAC address. The Action on Single Host Violation field can be defined only if the Multiple Hosts field is defined as Disable. The possible field values are:
- **Permit --** Forwards the packets from an unknown source, however, the MAC address is not learned.
- **Deny --** Discards the packets from any unlearned source. This is the default value.
- **Shutdown --** Discards the packet from any unlearned source and locks the port. Ports remain locked until they are activated, or the device is reset.
- **Traps --** Enables or disables sending traps to the host if a violation occurs.
- **Trap Frequency (1-1000000) (Sec) --** Defines the time period by which traps are sent to the host. The Trap Frequency (1-1000000) field can be defined only if the Multiple Hosts field is defined as Disable. The default is 10 seconds.
- **Status --** The host status. The possible field values are:
- **Unauthorized --** Clents (supplicants) have full port access.
- **Authorized --** Clents (supplicants) have limited port access.
- **No single-host --** Multiple Hosts is enabled.
- **Number of Violations --** The number of packets that arrived on the interface in single-host mode, from a host whose MAC address is not the client (supplicant) MAC address.

3.2.3.1.3 Authentiated Users

The **Authenticated Users** page displays user port access lists.

To open **Authenticated Users** screen perform the folling:

1. Click Switch -> Network Secuity -> Authenticated Users
2. The Authenticated Users screen is displayed as in Figure 3-49.

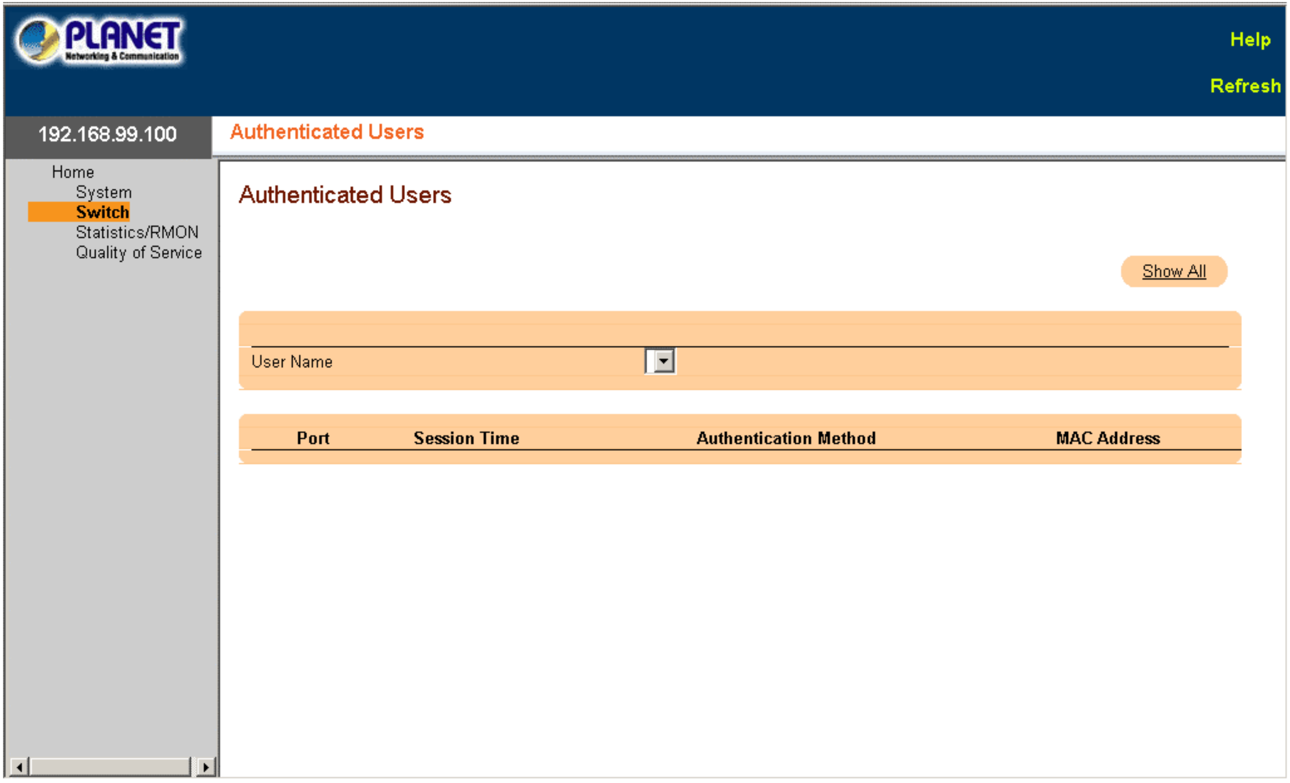


Figure 3-49 Authenitcated Users screen

The page includes the following fields:

- **User Name --** List of users authorized via the RADIUS Server.

- **Port --** The port number(s) used for authentication - per user name.
- **Session Time --** The amount of time the user was logged on to the device. The field format is Day:Hour:Minute:Seconds, for example, 3 days: 2 hours: 4 minutes: 39 seconds.
- **Last Authentication --** The amount of time that has passed since the user was last authenticated. The field format is Day:Hour:Minute:Seconds, for example, 3 days:2 hours: 4 minutes: 39 seconds.
- **Authentication Method --** The method by which the last session was authenticated. The possible field values are:
  - **Remote --** The user was authenticated from a remote server.
  - **None --** The user was not authenticated.
  - **MAC Address --** The client (supplicant) MAC address.

3.2.3.1.4 Port Security

Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. The MAC addresses can be dynamically learned, up to that point, or they can be statically configured. Locked port security monitors both received and learned packets that are received on specific ports. Access to the locked port is limited to users with specific MAC addresses. These addresses are either manually defined on the port, or learned on that port up to the point when it is locked. When a packet is received on a locked port, and the packet □ source MAC address is not tied to that port (either it was learned on a different port, or is unknown to the system), the protection mechanism is invoked, and can provide various options. Unauthorized packets arriving to a locked port are either:

- **Forwarded**
- **Discarded with no trap**
- **Discarded with a trap**
- **The ingress port is disabled**

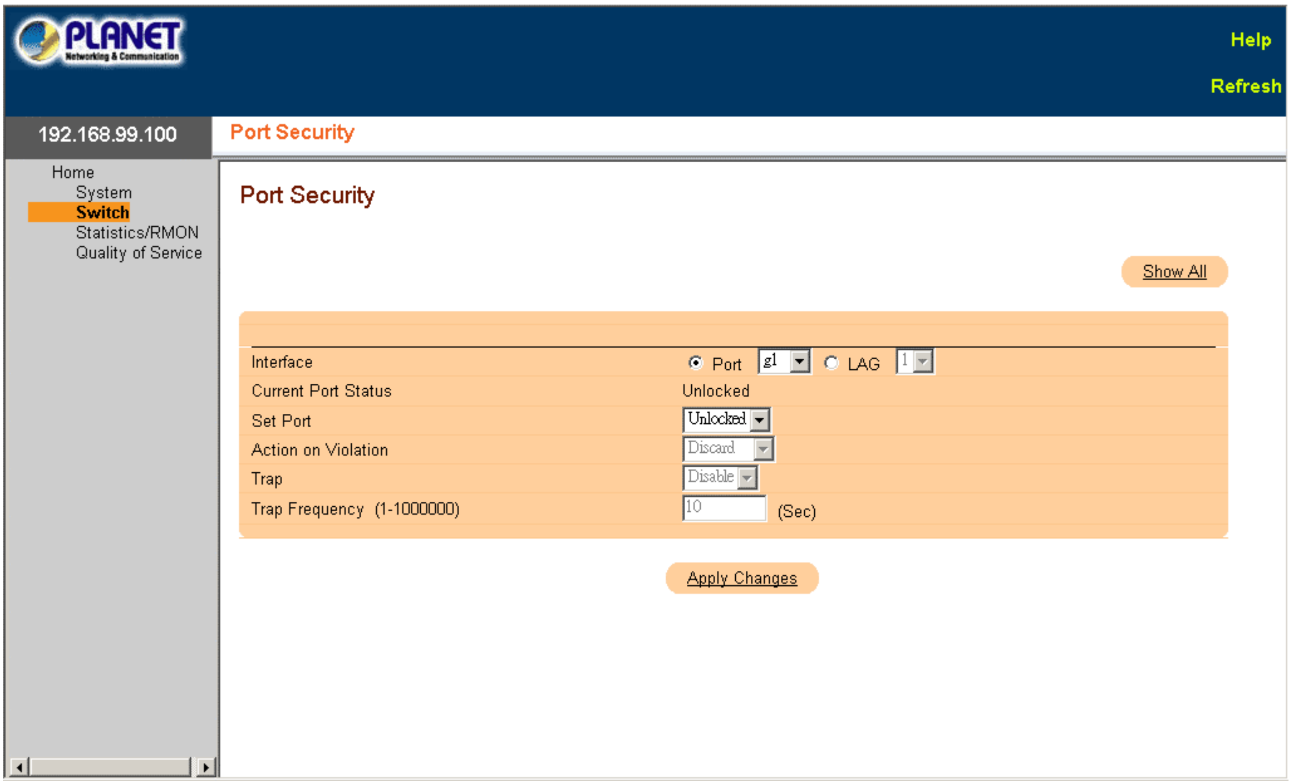
✍ ***Note:*** In order to enable port security, the Multiple Hosts feature must first be enabled on the required port(s).

Locked port security also enables storing a list of MAC addresses in the configuration file. The MAC address list can be restored after the device has been reset.

Disabled ports are activated from the Port Parameters page, see "Port Configuration".

To open **Port Security** screen perform the folling:

1. Click Switch -> Network Secuity -> Port Security
2. The Port Security screen is displayed as in Figure 3-50.



Interface	● Port g1 ○ LAG 1
Current Port Status	Unlocked
Set Port	Unlocked
Action on Violation	Discard
Trap	Disable
Trap Frequency (1-1000000)	10 (Sec)

Figure 3-50 Port Security screen

The page includes the following fields:

- **Interface --** The selected interface type on which Locked Port is enabled.
- **Port --** The selected interface type is a port.
- **LAG --** The selected interface type is a LAG.
- **Current Port Status --** The currently configured Port status.
- **Set Port --** The port is either locked or unlocked. The possible field values are:
  - **Unlocked --** Unlocks Port. This is the default value.
  - **Locked --** Locks Port.
- **Action on Violation --** The action to be applied to packets arriving on a locked port. The possible field values are:
  - **Forward** -- Forwards the packets from an unknown source, however, the MAC address is not learned.
  - **Discard --** Discards the packets from any unlearned source. This is the default value.
  - **Shutdown --** Discards the packet from any unlearned source and locks the port. Port remained locked until they are activated, or the device is reset.
- **Trap --** Enables traps being sent when a packet is received on a locked port.
- **Trap Frequency (1-1000000) --** The amount of time (in seconds) between traps. This field only applies to Locked ports. The default value is 10 seconds.

3.2.3.2 Ports

The **Ports** page contians links to port functionality pages including advanced features,such as Storm Control and Port Mirroring.

The Ports page contains links to the following topics:

- **Port Configuration**
- **LAG Configuration**
- **Storm Control**

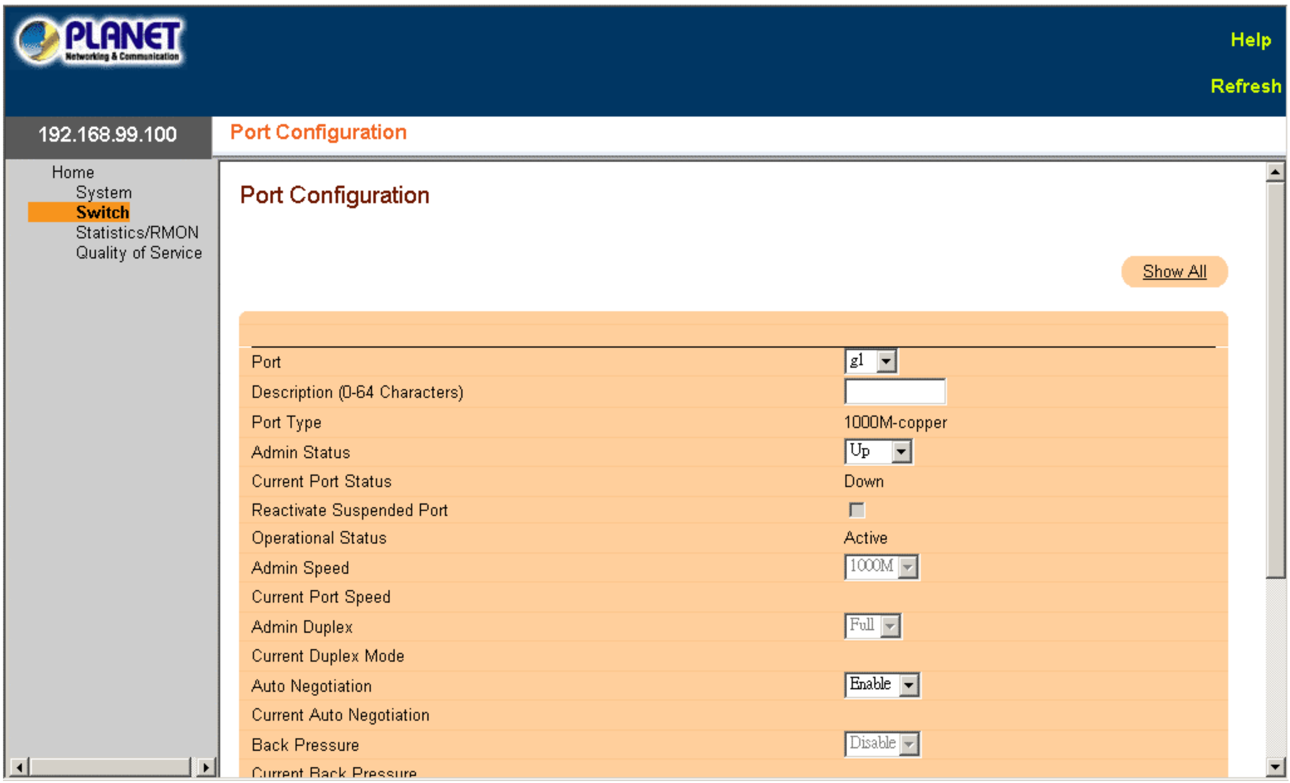
- **Port Mirroring**

3.2.3.2.1 Port Configuration

The **Port Configuration** page contains fields for defining port parameters.

To open **Port Configuration** screen perform the folling:

1. Click Switch -> Ports -> Port Configuration
2. The Port Configuration screen is displayed as in Figure 3-51.



Port Configuration

Port	g1
Description (0-64 Characters)	
Port Type	1000M-copper
Admin Status	Up
Current Port Status	Down
Reactivate Suspended Port	□
Operational Status	Active
Admin Speed	1000M
Current Port Speed	
Admin Duplex	Full
Current Duplex Mode	
Auto Negotiation	Enable
Current Auto Negotiation	
Back Pressure	Disable
Current Back Pressure	

Figure 3-51 Port Configuration screen

The page includes the following fields:

- **Port --** The port number for which port parameters are defined.
- **Description (0-64 Characters) --** A brief interface description, such as Ethernet.
- **Port Type --** The type of port.
- **Admin Status --** Enables or disables traffic forwarding through the port. The new port status is displayed in the Current Port Status field.
- **Current Port Status --** Specifies whether the port is currently operational or non-operational.
- **Re-Activate Port --** Reactivates a port if the port has been disabled through the locked port security option.
- **Operational Status --** The port operational status. Possible field values are:
- **Suspended --** The port is currently active, and is currently not receiving or transmitting traffic.
- **Active --** The port is currently active and is currently receiving and transmitting traffic.
- **Disable --** The port is currently disabled, and is not currently receiving or transmitting traffic.
- **Admin Speed --** The configured rate for the port. The port type determines what speed setting options are available. Admin speed can only be designated when auto negotiation is disabled on the configured port
- **Current Port Speed --** The actual currently configured port speed (bps).
- **Admin Duplex --** The port duplex mode can be either Full or Half. Full indicates that the interface supports transmission between the device and its link partner in both directions simultaneously. Half indicates that the interface supports transmission between the device and the client in only one direction at a time.
- **Current Duplex Mode --** The currently configured port duplex mode.

- **Auto Negotiation --** Enables Auto Negotiation on the port. Auto Negotiation is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode and flow control abilities to its partner.
- **Current Auto Negotiation --** The currently configured Auto Negotiation setting.
- **Back Pressure --** Enables Back Pressure mode on the port. Back Pressure mode is used with Half Duplex mode.
- **Current Back Pressure --** The currently configured Back Pressure setting.
- **Flow Control --** Enables or disables flow control or enables the auto negotiation of flow control on the port. Operates when port is in Full duplex mode.
- **Current Flow Control --** The currently configured Flow Control setting.
- **MDI/MDIX --** Allows the device to decipher between crossed and uncrossed cables. Hubs and switches are deliberately wired opposite the way end stations are wired, so that when a hub or switch is connected to an end station, a straight through Ethernet cable can be used, and the pairs are match up properly. When two hubs/switches are connected to each other, or two end stations are connected to each other, a crossover cable is used ensure that the correct pairs are connected. The possible field values are:
    - **Auto --** Use to automatically detect the cable type.
    - **MDI (Media Dependent Interface) --** Use for end stations.
    - **MDIX (Media Dependent Interface with Crossover) --** Use for hubs and switches.
- **Current MDI/MDIX--** The currently configured device MDI/MDIX settings.
- **LAG --** Specifies if the port is part of a LAG.

3.2.3.2.2 LAG Configuration

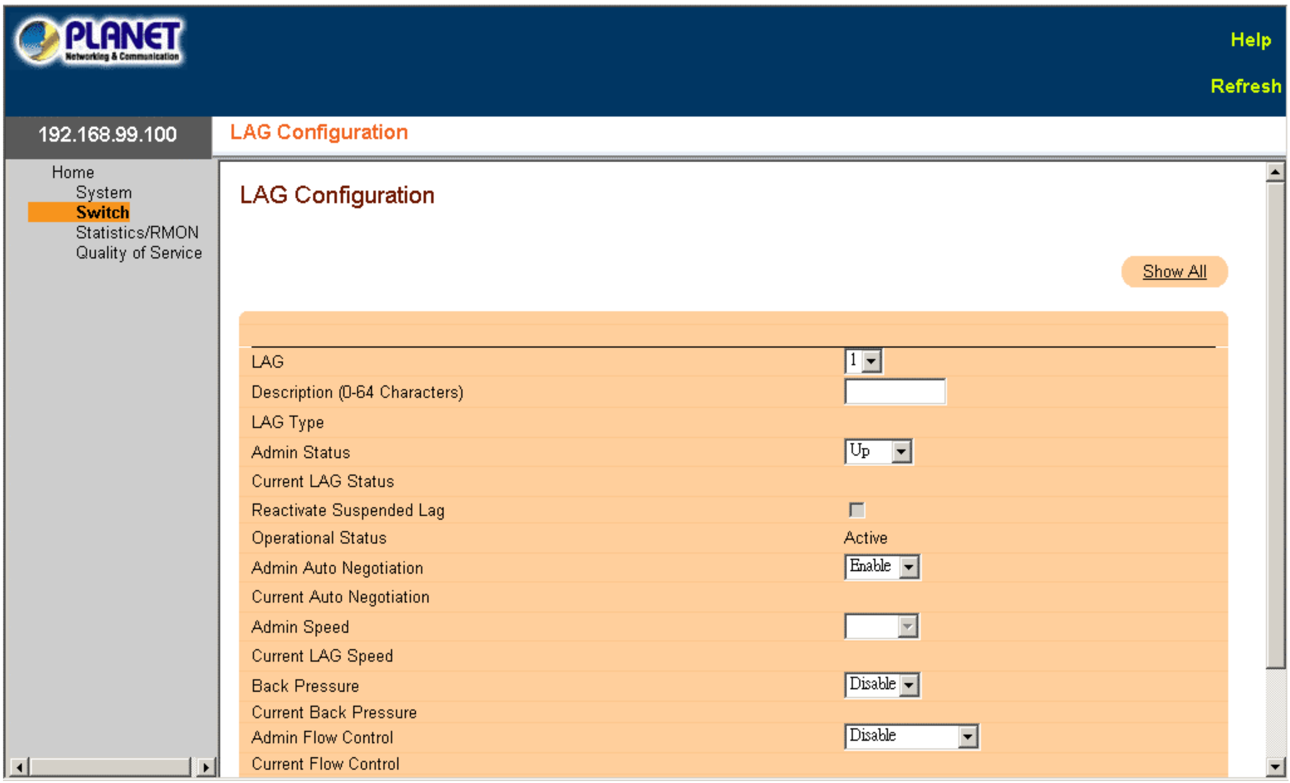
The **LAG Configuration** page contains fields for configuring parameters for configured LAGs. The device supports up to eight ports per LAG, and eight LAGs per system.

For information about Aggregating Ports and assigning ports to LAGs, see Link Aggregation.

✍ ***Note:*** If port configuration is modified while the port is a LAG member, the configuration change is only effective after the port is removed from the LAG.

To open **Port Configuration** screen perform the folling:

1. Click Switch -> Ports -> LAG Configuration
2. The LAG Configuration screen is displayed as in Figure 3-52.



LAG Configuration

LAG	1
Description (0-64 Characters)	
LAG Type	
Admin Status	Up
Current LAG Status	
Reactivate Suspended Lag	□
Operational Status	Active
Admin Auto Negotiation	Enable
Current Auto Negotiation	
Admin Speed	
Current LAG Speed	
Back Pressure	Disable
Current Back Pressure	
Admin Flow Control	Disable
Current Flow Control	

Figure 3-52 LAG Configure screen

The page includes the following fields:

- **LAG --** The LAG number.
- **Description (0-64 Characters) --** Provides a user-defined description of the configured LAG.
- **LAG Type --** The port types that comprise the LAG.
- **Admin Status --** Enables or disables traffic forwarding through the selected LAG.
- **Current LAG Status --** Indicates if the LAG is currently operating.
- **Re-Activate Suspended LAG --** Reactivates a suspended LAG.
- **Operational Status --** Operational status of the LAG.
- **Admin Auto Negotiation --** Enables or disables Auto Negotiation on the LAG. Auto-negotiation is a protocol between two link partners that enables a LAG to advertise its transmission rate, duplex mode and flow control (the flow control default is disabled) abilities to its partner.
- **Current Auto Negotiation --** The currently configured Auto Negotiation setting.
- **Admin Speed --** The speed at which the LAG is operating.
- **Current LAG Speed --** The currently configured speed at which the LAG is operating.
- **Admin Back Pressure --** Enables or disables Back Pressure mode on the LAG. Back Pressure mode is effective on the ports operating in Half Duplex in the LAG.
- **Current Back Pressure --** The currently configured Back Pressure setting.
- **Admin Flow Control --** Enables/disables flow control, or enables the auto negotiation of flow control on the LAG. Flow Control mode is effective on the ports operating in Full Duplex in the LAG.
- **Current Flow Control --** The user-designated flow control setting.

3.2.3.2.3 Storm Control

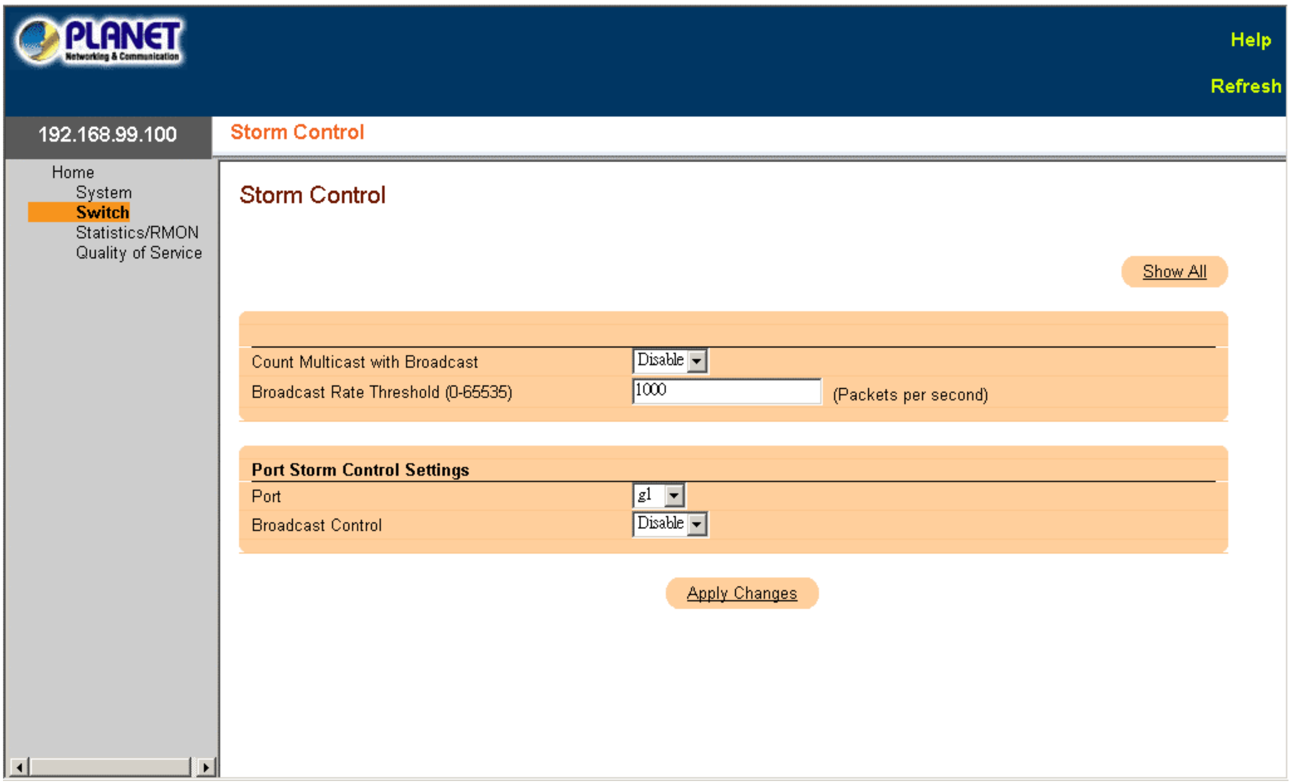
A BroadcastStorm is a result of an excessive amount of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, straining network resources or causing the network to time out.

The system measures the incoming Broadcast and Multicast frame rate separately on each port, and discard frames when the rate exceeds a user-defined rate.

The Storm Control page provides fields for enabling and configuring Storm Control.

To open **Storm Control** screen perform the folling:

1. Click Switch -> Ports -> Strom Control
2. The Storm Control screen is displayed as in Figure 3-53.



Storm Control

Count Multicast with Broadcast: Disable

Broadcast Rate Threshold (0-65535): 1000 (Packets per second)

Port Storm Control Settings

Port: g1

Broadcast Control: Disable

Figure 3-53 Storm Control screen

The page includes the following fields:

- Count Multicast with Broadcast -- Counts Broadcast and Multicast traffic. The possible field values are:
  - Enable -- Counts Broadcast and Multicast traffic.
  - Disable -- Counts only Broadcast traffic.
- Broadcast Rate Threshold (0-65535) -- The maximum rate (packets per second) at which bradcast packets are forwarded. The range is 0-65535. The default value is 1000.
- Port -- The port from which storm control is enabled.
- Broadcast Control -- Enables or disables forwarding broadcast packet types on the device.

3.2.3.2.4 Port Mirroring

Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port.

Port mirroring is configured by selecting a specific port to copy all packets, and different ports from which the packets copied. Before configuring Port Mirroring, note the following:

Before configuring Port Mirroring, note the following:

- Monitored port cannot operate faster than the monitoring port.
- All the RX/TX packets should be monitored to the same port.

The following restrictions apply to ports configured to be destination ports:

- Ports cannot be configured as a source port.
- Ports cannot be a LAG member.
- IP interfaces are not configured on the port.
- GVRP is not enabled on the port.
- The port is not a VLAN member.

- Only one destination port can be defined.

The following restrictions apply to ports configured to be source ports:

- Source Ports cannot be a LAG member.
- Ports cannot be configured as a destination port.
- All packets are transmitted tagged from the destination port.
- Monitored all RX/TX packets to the same port.

✍ **Note:** When a port is set to be a target port for a port-mirroring session, all normal operations on it are suspended. This includes Spanning Tree and LACP.

To open **Port Mirroring** screen perform the folling:

1. Click Switch -> Ports -> Port Mirroring
2. The Port Mirroring screen is displayed as in Figure 3-54.

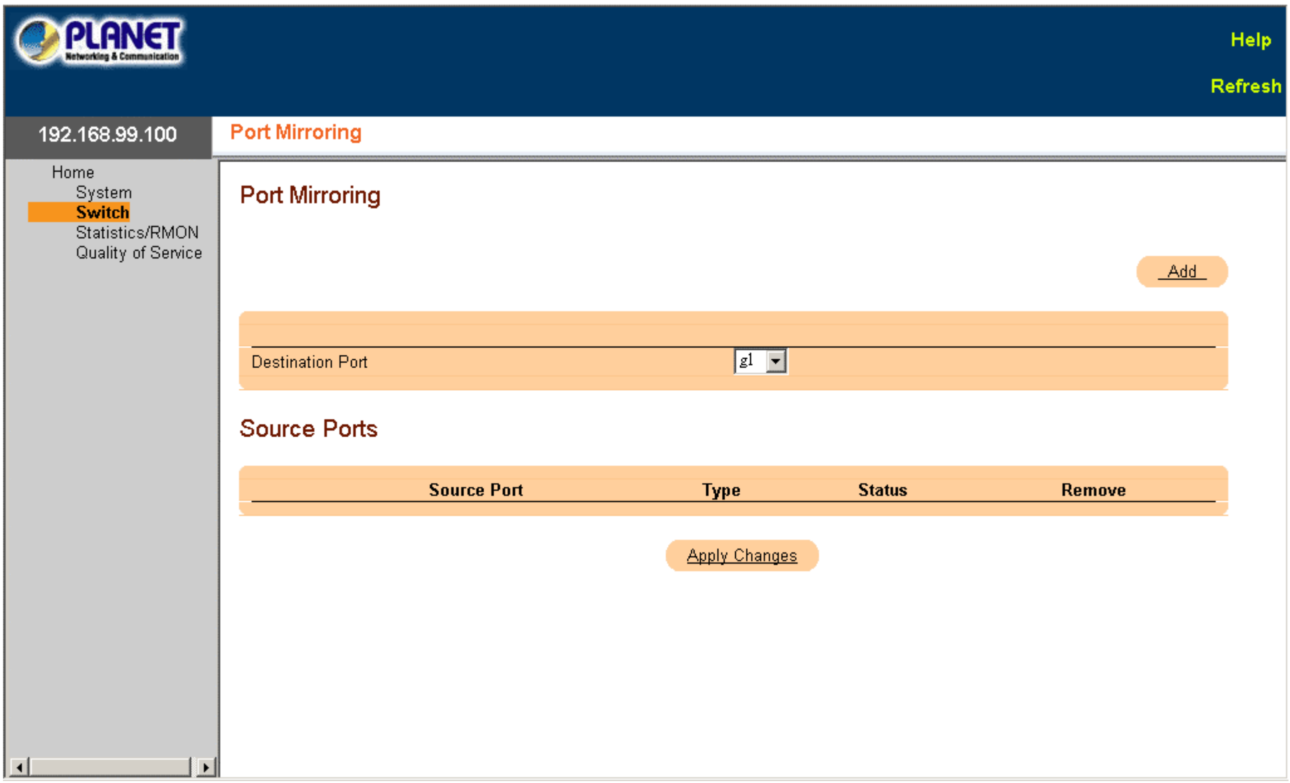


Figure 3-54 Prot Mirroring screen

The page includes the following fields:

- **Destination Port --** The port number to which port traffic is copied.
- **Source Port --** Defines the port number from which port traffic is mirrored.
- **Type --** Indicates if the source port is RX, TX, or both RX and TX.
- **Status --** Indicates if the port is currently monitored (Active) or not monitored (Ready).
- **Remove --** When selected, removes the port mirroring session.

3.2.3.3 Address Table

MAC addresses are stored in either the Static Address or the Dynamic Address databases. A packet addressed to a destination stored in one of the databases is forwarded immediately to the port. The Static and Dynamic Address Tables can be sorted by interface, VLAN, and interface type. MAC addresses are dynamically learned as packets from sources arrive at the device. Addresses are associated with ports by learning the ports from the frame □ source address. Frames addressed to a destination MAC address that is not associated with any port are flooded to all ports of the relevant VLAN. Static addresses are manually configured. In order to prevent the bridging table from overflowing, dynamic MAC addresses, from which no traffic is seen for a certain period, are erased.

The Address Tables page contains links to the following topics:

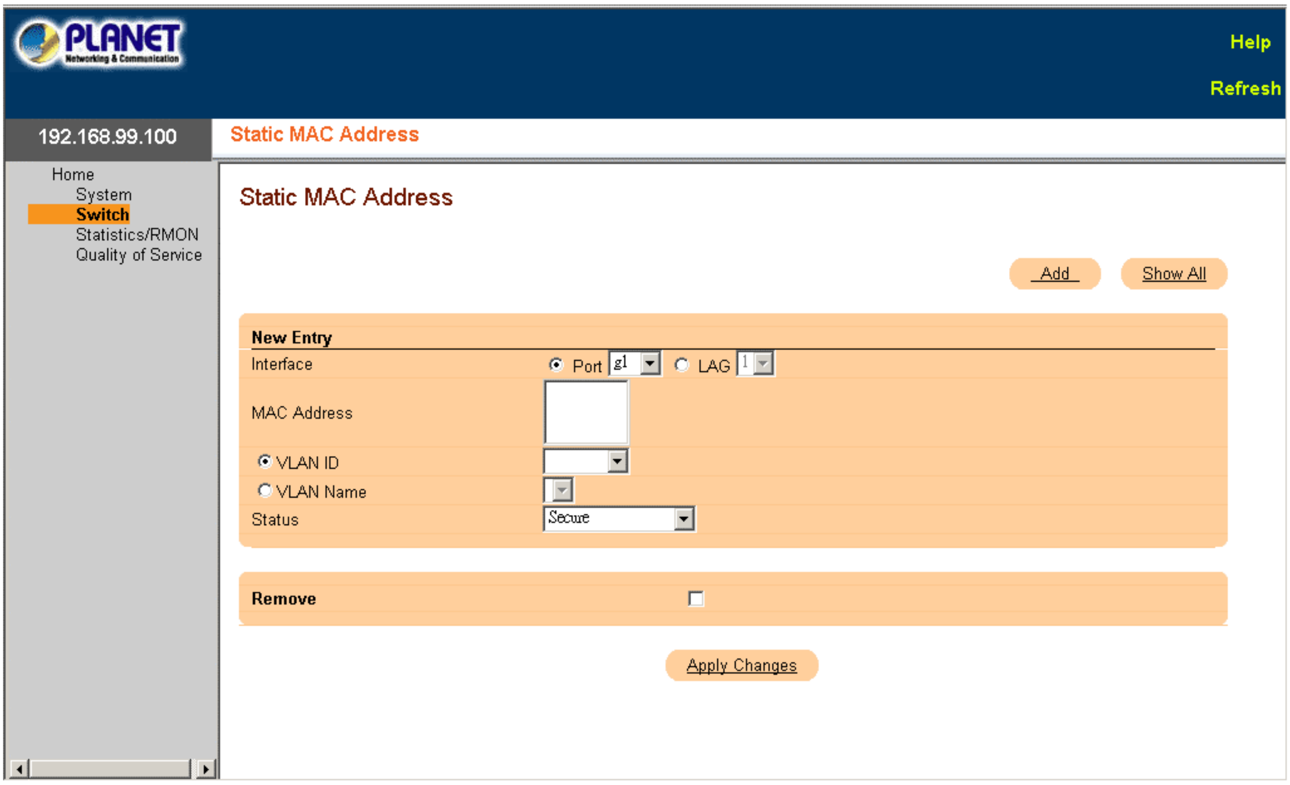
- **Static Address Table**
- **Dynamic Address Table**

3.2.3.3.1 Static Address Table

The Static MAC Address page contains a list of static MAC addresses. Static Address can be added and removed from the Static MAC Address page. In addition, several MAC Addresses can be defined for a single port.

To open **Static Address Table** screen perform the folling:

1. Click Switch -> Address Table -> Static Address Table
2. The Static Address Table screen is displayed as in Figure 3-55.



New Entry

Interface ● Port g1 ○ LAG 1

MAC Address

● VLAN ID

○ VLAN Name

Status Secure

Remove □

Figure 3-55 Static MAC Address screen

The page includes the following fields:

- **Interface --** The specific port or LAG to which the static MAC address is applied.
- **MAC Address --** The MAC address listed in the current static address list.
- **VLAN ID --** The VLAN ID attached to the MAC Address.
- **VLAN Name --** User-defined VLAN name.
- **Status --** MAC address status. Possible values are:
- **Secure --** Guarantees that a locked port MAC address is not deleted.
- **Permanent --** The MAC address is permanent.
- **Delete on Reset --** The MAC address is deleted when the device is reset.

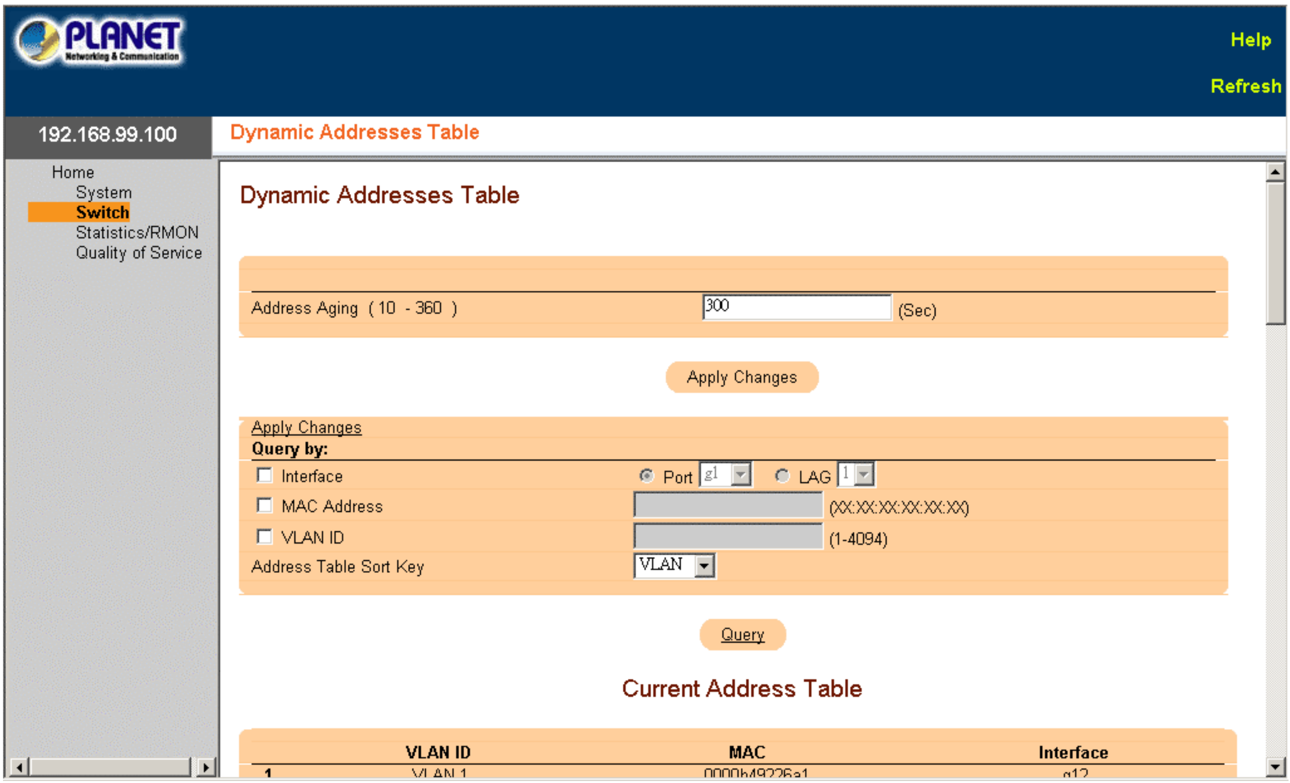
- **Delete on Timeout --** The MAC address is deleted when a timeout occurs.
- **Remove --** When selected, removes the the MAC address from the MAC Address Table.

3.2.3.3.2 Dymanic Address Table

The **Dynamic Address Table** contains fields for querying information in the dynamic address table, including the interface type, MAC addresses, VLAN, and table sorting. Packets forwarded to an address stored in the address table are forwarded directly to those ports. The Dynamic Address Table also contains information about the aging time before a dynamic MAC address is erased, and includes parameters for querying and viewing the Dynamic Address list. The Current Address Table contains dynamic address parameters by which packets are directly forwarded to the ports.

To open **Dynamic Address Table** screen perform the folling:

1. Click Switch -> Address Table -> Dynamic Address Table
2. The Dynamic Address Table screen is displayed as in Figure 3-56.



Dynamic Addresses Table

Address Aging (10 - 360) 300 (Sec)

Apply Changes

Query by:

□ Interface ● Port g1 ○ LAG 1

□ MAC Address (XX:XX:XX:XX:XX:XX)

□ VLAN ID (1-4094)

Address Table Sort Key VLAN

Current Address Table

	VLAN ID	MAC	Interface
1	VLAN 1	0000b49226a1	g12

Figure 3-56 Dymanic Address Table screen

The page includes the following fields:

- **Address Aging (10-360) --** Specifies the amount of time the MAC Address remains in the Dynamic Address Table before it is timed out if no traffic from the source is detected. The default value is 300 seconds.
- **Interface --** Specifies the interface for which the table is queried. There are two interface types from which to select.
- **Port --** Specifies the port numbers for which the table is queried.
- **LAG --** Specifies the LAG for which the table is queried.
- **MAC Address --** Specifies the MAC address for which the table is queried.
- **VLAN ID --** The VLAN ID for which the table is queried.
- **Address Table Sort Key --** Specifies the means by which the Dynamic Address Table is sorted.

3.2.3.4 GARP

Generic Attribute Registration Protocol (GARP) is a general-purpose protocol that registers any network connectivity or membership-style information. GARP defines a set of devices interested in a given network attribute, such as VLAN or Multicast address.

When configuring GARP, ensure the following:

- The leave time must be greater than or equal to three times the join time.
- The leave all time must be greater than the leave time.

Set the same GARP timer values on all Layer 2-connected devices. If the GARP timers are set differently on the Layer 2-connected devices, GARP application does not operate successfully.

The GARP page contains a link to the following topic:

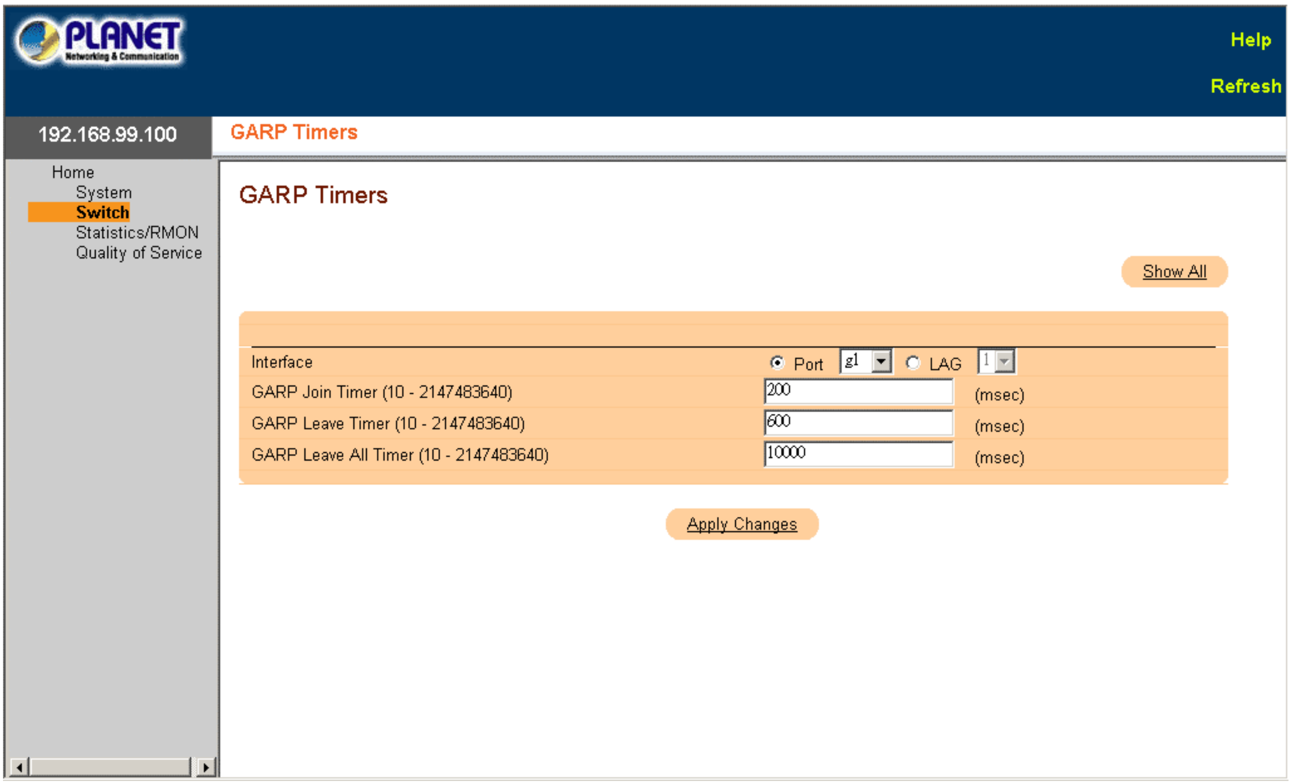
- **GARP Timers**

3.2.3.4.1 GARP Timers

The GARP Timers page contains fields for enabling GARP on the device.

To open **GARP Timer** screen perform the folling:

1. Click Switch -> GARP -> GARP Timer
2. The GARP Timer screen is displayed as in Figure 3-57.



Interface	● Port g1 ○ LAG 1	
GARP Join Timer (10 - 2147483640)	200	(msec)
GARP Leave Timer (10 - 2147483640)	600	(msec)
GARP Leave All Timer (10 - 2147483640)	10000	(msec)

Figure 3-57 GARP Timers screen

The page includes the following fields:

- **Interface --** Determines if enabled on a port or on a LAG.
- **GARP Join Timer (10 - 2147483640) --** Time, in milliseconds, that PDUs are transmitted. The possible field value is 10-2147483640. The default value is 200 msec.
- **GARP Leave Timer (10 - 2147483640) --** Time lapse, in milliseconds, that the device waits before leaving its GARP state. Leave time is activated by a Leave All Time message sent/received, and cancelled by the Join message received. Leave time must be greater than or equal to three times the join time. The possible field value is 0-2147483640. The default value is 600 msec.
- **GARP Leave All Timer (10 - 2147483640) --** Time lapse, in milliseconds, that all devices wait before leaving the GARP state. The leave all time must be greater than the leave time. The possible field value is 0-2147483640. The default value is 10000 msec.

3.2.3.5 Spanning Tree

Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops.

Loops occur when alternate paths exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency.

The devices support the following Spanning Tree protocols:

- **Classic STP --** Provides a single path between end stations, avoiding and eliminating loops. For more information on configuring Classic STP, see "Defining STP Global Settings".
- **Rapid STP --** Detects and uses of network topologies that provide faster spanning tree convergence, without creating forwarding loops. For more information on configuring Rapid STP, see "Configuring Rapid Spanning Tree".

The Spanning Tree page contains links to the following topics:

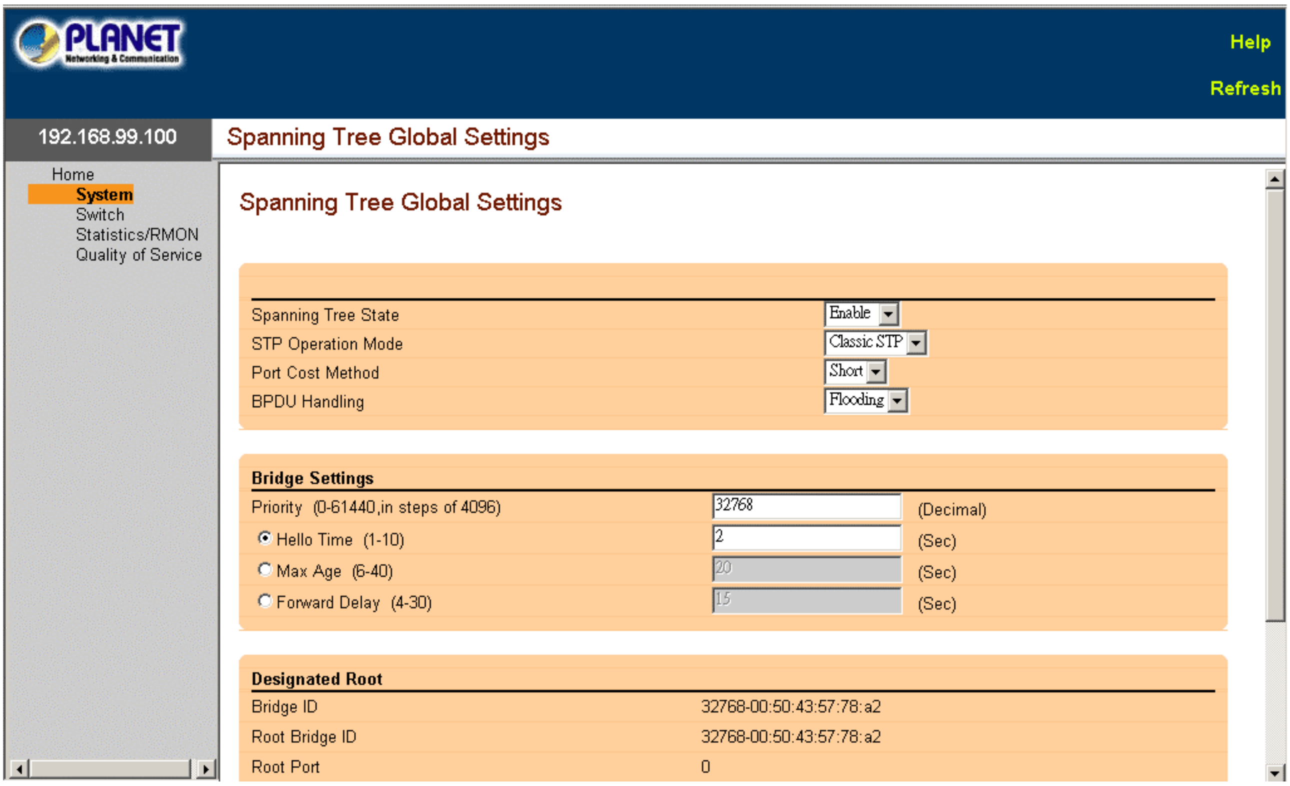
- **Global Settings**
- **STP Port Settings**
- **STP LAG Settings**
- **Rapid Spanning Tree**

3.2.3.5.1 Global Settings

The **STP Global Settings** page contains parameters for enabling and configuring STP operation on the device.

To open **STP Global Settings** screen perform the folling:

1. Click Switch -> Spanning Tree -> Global Settings
2. The STP Global Settings screen is displayed as in Figure 3-58.



Spanning Tree Global Settings

Spanning Tree Global Settings

Spanning Tree State: Enable
STP Operation Mode: Classic STP
Port Cost Method: Short
BPDU Handling: Flooding

Bridge Settings
Priority (0-61440,in steps of 4096): 32768 (Decimal)
● Hello Time (1-10): 2 (Sec)
○ Max Age (6-40): 20 (Sec)
○ Forward Delay (4-30): 15 (Sec)

Designated Root
Bridge ID: 32768-00:50:43:57:78:a2
Root Bridge ID: 32768-00:50:43:57:78:a2
Root Port: 0

Figure 3-58 Spanning Tree Global Settings screen

The page includes the following fields:

- **Spanning Tree State --** Enables or disables Spanning Tree on the device. The possible field values are:
- **Enable --** Enables Spanning Tree
- **Disable --** Disables Spanning Tree
- **STP Operation Mode --** The STP mode by which STP is enabled on the device. The possible field values are:
  - **Classic STP --** Enables Classic STP on the device. This is the default value.
  - **Rapid STP --** Enables Rapid STP on the device.

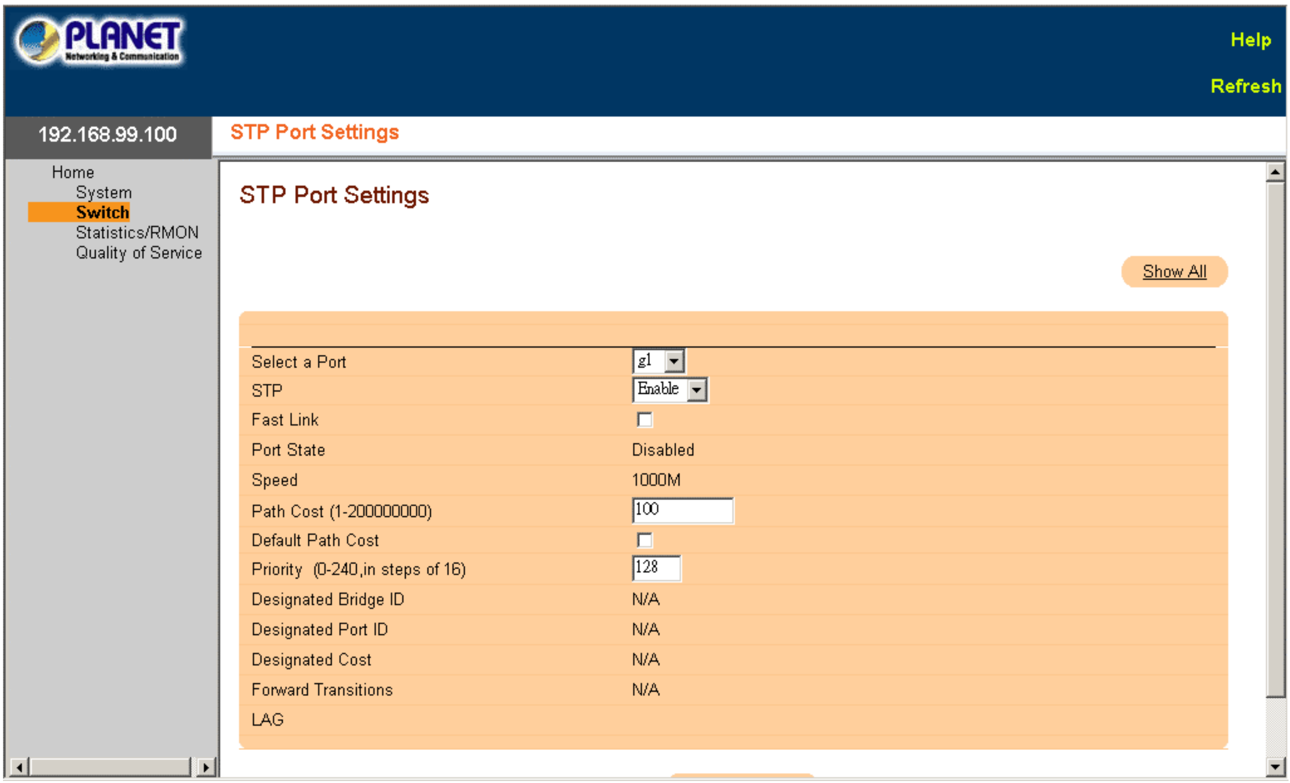
- **Port Cost Method --** Determines the Spanning Tree default path cost method. The possible field values are:
- **Short --** Specifies 1 through 65535 range for port path costs. This is the default value.
- **Long --** Specifies 1 through 200000000 range for port path costs.
- **BPDU Handling --** Determines how BPDU packets are managed when STP is disabled on the port/ device. BPDUs are used to transmit spanning tree information. The possible field values are:
  - **Filtering --** Filters BPDU packets when spanning tree is disabled on an interface.
  - **Flooding --** Floods BPDU packets when spanning tree is disabled on an interface. This is the default value.
- **Priority (0-61440, in steps of 4096) --** Specifies the bridge priority value. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the Root Bridge. The default value is 32768. The bridge priority value is provided in increments of 4096 (4K increments). For example, 0, 4096, 8192, etc.
- **Hello Time (1-10) --** Specifies the device Hello Time. The Hello Time indicates the amount of time in seconds a root bridge waits between configuration messages. The default is 2 seconds.
- **Max Age (6-40) --** Specifies the device Maximum Age Time. The Maximum Age Time indicates the amount of time in seconds a bridge waits before sending configuration messages. The default max age is 20 seconds.
- **Forward Delay (4-30) --** Specifies the device forward delay time. The Forward Delay Time indicates the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. The default is 15 seconds.
- **Bridge ID --** Identifies the Bridge priority and MAC address.
- **Root Bridge ID --** Identifies the Root Bridge priority and MAC address.
- **Root Port --** The port number that offers the lowest cost path from this bridge to the Root Bridge. It is significant when the Bridge is not the Root. The default is zero.
- **Root Path Cost --** The cost of the path from this bridge to the root.
- **Topology Changes Counts --** Specifies the total amount of STP state changes that have occurred since the last reboot.
- **Last Topology Change --** The amount of time that has elapsed since the bridge was initialized or reset, and the last topographic change occurred. The time is displayed in a day hour minute second format. For eample 41 days, 2 hours, 22 minutes and 15 seconds

3.2.3.5.2 STP Port Settings

The STP Port Settings page contains fields for assigning STP properties to individual ports.

To open **STP Port Settings** screen perform the folling:

1. Click Switch -> Spanning Tree -> STP Port Settings
2. The STP Port Settings screen is displayed as in Figure 3-59.



STP Port Settings

Select a Port	g1
STP	Enable
Fast Link	□
Port State	Disabled
Speed	1000M
Path Cost (1-200000000)	100
Default Path Cost	□
Priority (0-240,in steps of 16)	128
Designated Bridge ID	N/A
Designated Port ID	N/A
Designated Cost	N/A
Forward Transitions	N/A
LAG	

Figure 3-59 STP Port Settings screen

The page includes the following fields:

- **Select a Port --** Port on which STP is enabled.
- **STP --** Enables or disables STP on the port.
- **Fast Link --** When selected, enables Fast Link mode for the port. If Fast Link mode is enabled for a port, the Port State is automatically placed in the Forwarding state when the port link is up. Fast Link mode optimizes the time it takes for the STP protocol to converge. STP convergence can take 30-60 seconds in large networks.
- **Port State --** The current port STP state. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:
- **Disabled --** The port link is currently down.
- **Blocking --** The port is currently blocked and cannot be used to forward traffic or learn MAC addresses. Blocking is displayed when Classic STP is enabled.
- **Listening --** The port is currently in the listening mode. The port cannot forward traffic nor can it learn MAC addresses.
- **Learning --** The port is currently in the learning mode. The port cannot forward traffic however it can learn new MAC addresses.
- **Forwarding --** The port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Speed --** Speed at which the port is operating.
- **Path Cost (1-200000000) --** The port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path being rerouted.
- **Default Path Cost --** The default path cost of the port is automatically set by the port speed and the default path cost method. The default values for long path costs are:
    - Ethernet - 2000000
    - Fast Ethernet - 200000
    - Gigabit Ethernet - 20000

    The default values for short path costs (short path costs are the default) are:

        - Ethernet - 100
        - Fast Ethernet - 19

- Gigabit Ethernet - 4

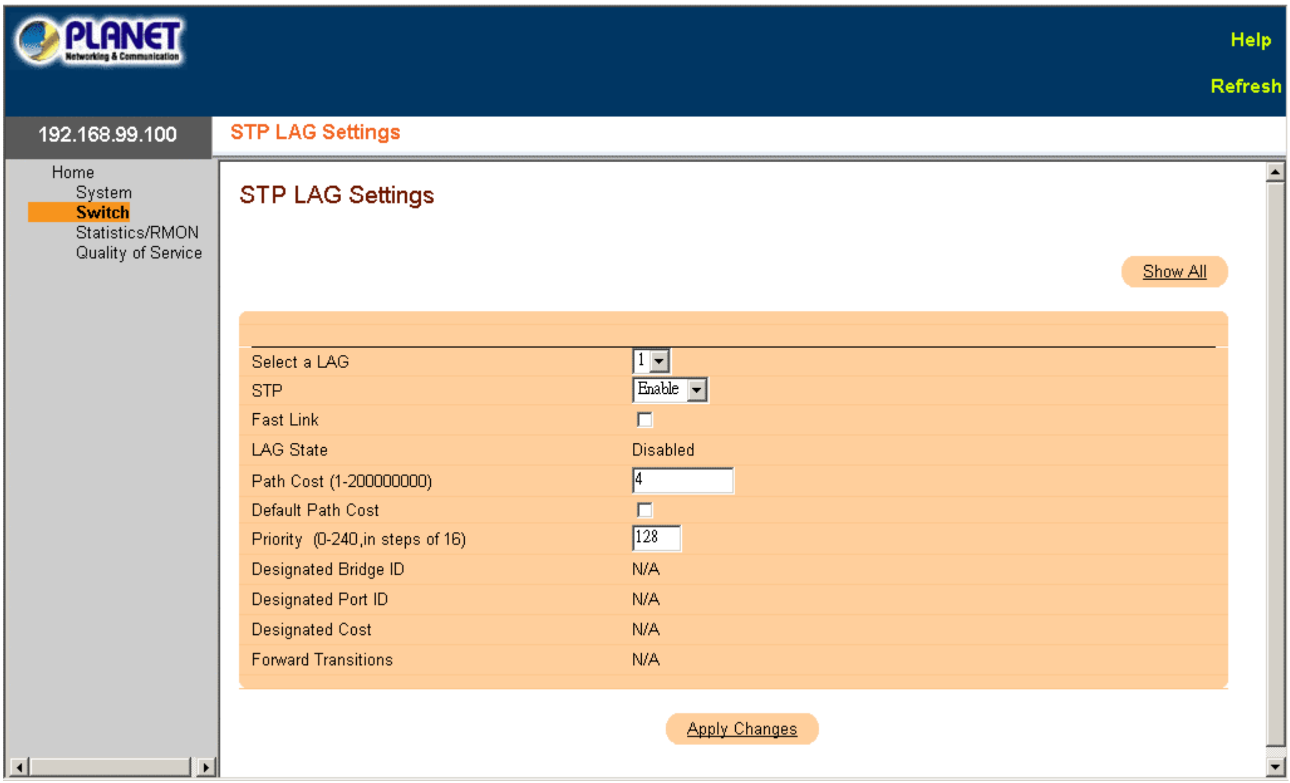
- **Priority (0-240, in steps of 16) --** Priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop. The priority value is between 0-240. The priority value is provided in increments of 16.
- **Designated Bridge ID --** The bridge priority and the MAC Address of the designated bridge.
- **Designated Port ID--** The selected port□ priority and interface.
- **Designated Cost --** Cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
- **Forward Transitions --** Number of times the port has changed from the Blocking state to the Forwarding state.
- **LAG --** The LAG to which the port is attached.

3.2.3.5.3 STP LAG Settings

The **STP LAG Settings** page contains fields for assigning STP aggregating port parameters.

To open **STP LAG Settings** screen perform the folling:

1. Click Switch -> Spanning Tree -> STP LAG Settings
2. The STP LAG Settings screen is displayed as in Figure 3-60



STP LAG Settings

Select a LAG	1
STP	Enable
Fast Link	□
LAG State	Disabled
Path Cost (1-200000000)	4
Default Path Cost	□
Priority (0-240,in steps of 16)	128
Designated Bridge ID	N/A
Designated Port ID	N/A
Designated Cost	N/A
Forward Transitions	N/A

Figure 3-60 STP LAG Settings

The page includes the following fields:

- **Select a LAG --** The user-defined LAG. For more information, see "Defining LAG Membership".
- **STP --** Enables or disables STP on the LAG.
- **Fast Link --** Enables Fast Link mode for the LAG. If Fast Link mode is enabled for a LAG, the LAG State is automatically placed in the Forwarding state when the LAG is up. Fast Link mode optimizes the time it takes for the STP protocol to converge. STP convergence can take 30-60 seconds in large networks.
- **LAG State --** Current STP state of a LAG. If enabled, the LAG state determines what forwarding action is taken on traffic. If the bridge discovers a malfunctioning LAG, the LAG is placed in the Broken state. Possible LAG states are:
  - **Disabled --** The LAG link is currently down.
  - **Blocking --** The LAG is blocked and cannot be used to forward traffic or learn MAC addresses.

- **Listening --** The LAG is in the listening mode and cannot forward traffic or learn MAC addresses.
- **Learning --** The LAG is in the learning mode and cannot forward traffic, but it can learn new MAC addresses.
- **Forwarding --** The LAG is currently in the forwarding mode, and it can forward traffic and learn new MAC addresses.
- **Broken --** The LAG is currently malfunctioning and cannot be used for forwarding traffic.

- **Path Cost (1-200000000) --** Amount the LAG contributes to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path being rerouted. The path cost has a value of 1 to 200000000. If the path cost method is short, the LAG cost default value is 4. If the path cost method is long, the LAG cost default value is 20000.
- **Default Path Cost --** When selected, the LAG path cost returns to its default value.
- **Priority (0-240, in steps of 16) --** Priority value of the LAG. The priority value influences the LAG choice when a bridge has two looped ports. The priority value is between 0-240, in increments of 16.
- **Designated Bridge ID --** The bridge priority and the MAC Address of the designated bridge.
- **Designated Port ID --** The port priority and interface number of the designated port.
- **Designated Cost --** The cost of the designated bridge.
- **Forward Transitions --** Number of times the LAG State has changed from the Blocking state to a Forwarding state.

3.2.3.5.4 Rapid Spanning Tree

While Classic Spanning Tree guarantees preventing L2 forwarding loops in a general network topology, convergence can take up to 30-60 seconds. The convergence time is considered too long for many applications. When network topology allows, faster convergence may be possible. The **Rapid Spanning Tree Protocol (RSTP)** detects and uses of network topologies that provide faster convergence of the spanning tree, without creating forwarding loops.

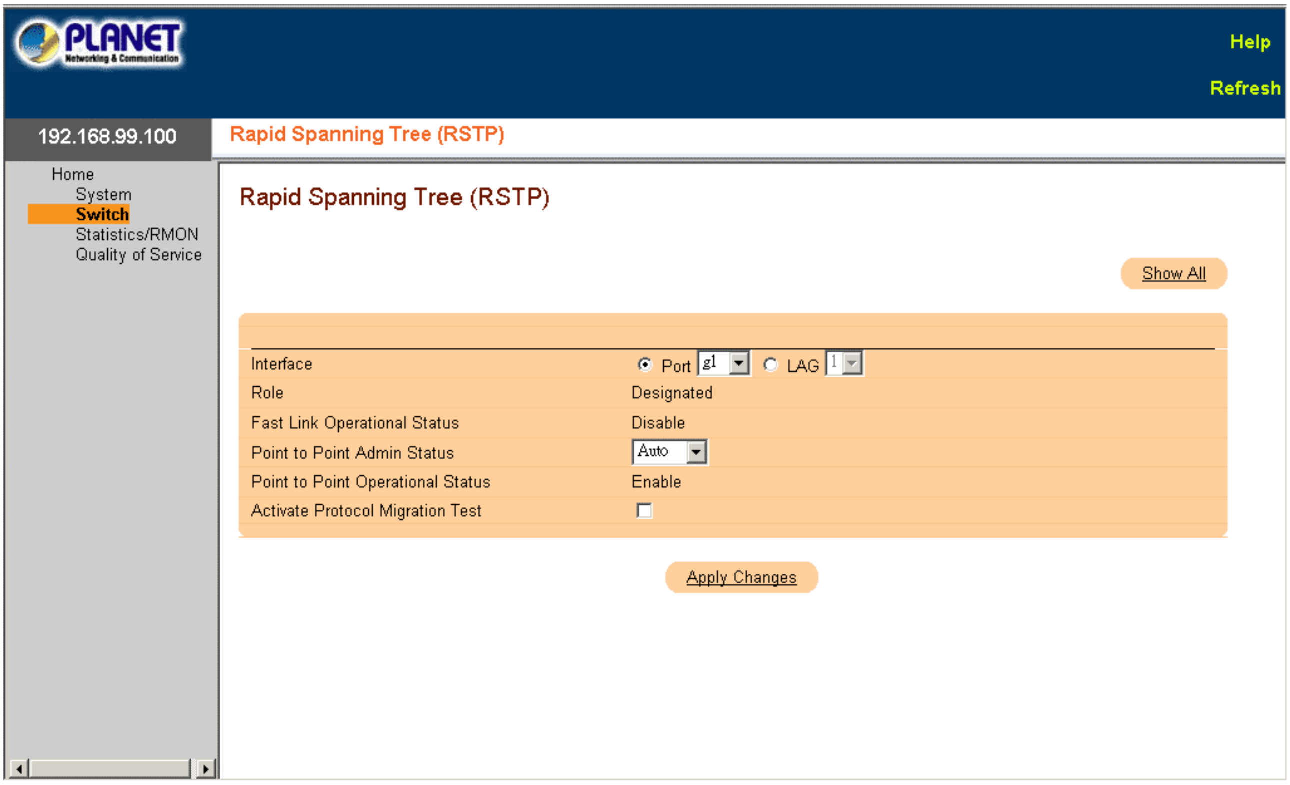
RSTP has the following different port states:

- Disabled
- Learning
- Discarding
- Forwarding

Rapid Spanning Tree is enabled on the STP Global Settings page.

To open **Rapid Spanning Tree** screen perform the folling:

1. Click Switch -> Spanning Tree -> Rapid Spanning Tree
2. The Rapid Spanning Tree screen is displayed as in Figure 3-61



Rapid Spanning Tree (RSTP)

Interface	● Port g1 ○ LAG 1
Role	Designated
Fast Link Operational Status	Disable
Point to Point Admin Status	Auto
Point to Point Operational Status	Enable
Activate Protocol Migration Test	□

Figure 3-61 Rapid Spanning Tree screen

The page includes the following fields:

- **Interface --** Port or LAG on which Rapid STP is enabled.
- **Role --** The port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:
    - **Root --** Provides the lowest cost path to forward packets to root device.
    - **Designated --** The port or LAG via which the designated device is attached to the LAN.
    - **Alternate --** Provides an alternate path to the root device from the root interface.
    - **Backup --** Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
    - **Disabled --** The port is not participating in the Spanning Tree (the port link is down).
- **Fast Link Operational Status --** Indicates if Fast Link is enabled or disabled for the port or LAG. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state.
- **Point-to-Point Admin Status --** Enables or disables the device to establish a point-to-point link, or specifies for the device to automatically establish a point-to-point link.
- To establish communications over a point-to-point link, the originating PPP first sends Link Control Protocol (LCP) packets to configure and test the data link. After a link is established and optional facilities are negotiated as needed by the LCP, the originating PPP sends Network Control Protocols (NCP) packets to select and configure one or more network layer protocols. When each of the chosen network layer protocols has been configured, packets from each network layer protocol can be sent over the link. The link remains configured for communications until explicit LCP or NCP packets close the link, or until some external event occurs.
- **Point-to-Point Operational Status --** The Point-to-Point operating state. This is the actual device port link type.
- **Activate Protocol Migrational Test --** When selected, enables PPP sending Link Control Protocol (LCP) packets to configure and test the data link. It may differ from the administrative state.

3.2.3.6 VLAN

VLANs are logical subgroups of a Local Area Network (LAN) created via software rather than defining a hardware solution. VLANs combine user stations and network devices into a single domain regardless of the physical LAN segment to which they are attached. VLANs allow network traffic to flow more efficiently within subgroups. VLANs managed through software reduces the amount of time in which network changes are implemented.

VLANs have no minimum number of ports, and can be created per device or any other logical connection combination, as VLANs are software based and not defined by physical attributes.

VLANs function at Layer 2. Since VLANs isolate traffic within the VLAN, a Layer 3 router functioning router is needed to allows traffic flow between VLANs. Layer 3 routers identify segments and coordinate with VLANs. VLANs are broadcast and Multicast domains. Broadcast and Multicast traffic is transmitted only in the VLAN in which the traffic is generated.

VLAN tagging provides a method of transferring VLAN information between VLAN groups. VLAN tagging attaches a tag to packet headers. The VLAN tag indicates to which VLAN the packet belongs. VLAN tags are attached to the packet by either the end station or by the network device. VLAN tags also contains VLAN network priority information. Combining VLANs and GVRP enables the automatic dispersal of VLAN information.

The VLAN page contains links to the following topics:

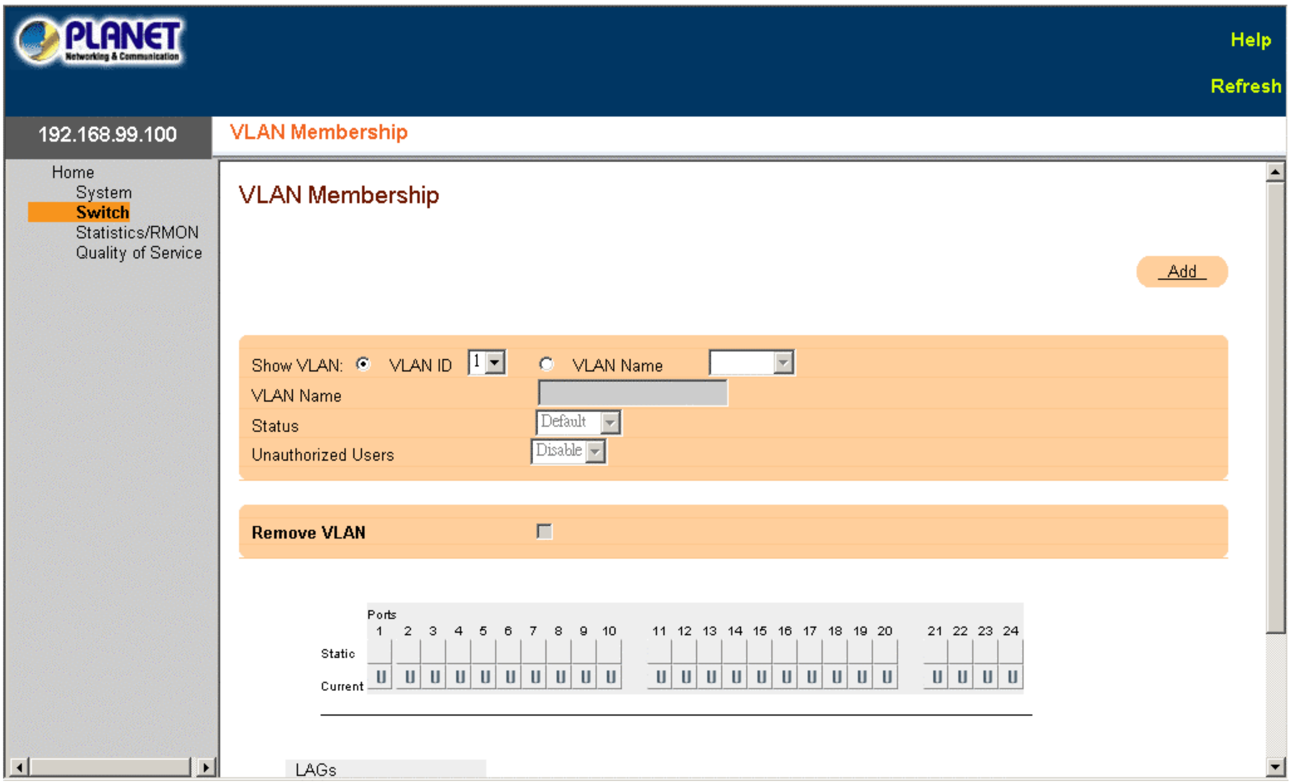
- **VLAN Membership**
- **Port Settings**
- **LAG Settings**
- **Protocol Group**
- **Protocol Port Table**
- **GVRP Parameters**

3.2.3.6.1 VLAN Membership

The **VLAN Membership** page contains fields for defining VLAN groups. The device supports the mapping of 4094 VLAN IDs to 256 VLANs. All ports must have a defined PVID. If no other value is configured the default VLAN PVID is used. VLAN number 1 is the default VLAN, and cannot be deleted from the system.

To open **VLAN Membership** screen perform the folling:

1. Click Switch -> VLAN -> VLAN Membership
2. The VLAN Membership screen is displayed as in Figure 3-62



VLAN Membership

Show VLAN: ● VLAN ID 1 ○ VLAN Name

VLAN Name

Status Default

Unauthorized Users Disable

Remove VLAN □

	Ports 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Static																								
Current	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U

LAGs

Figure 3-62 VLAN Membership screen

The VLAN Membership page is divided into the following sections:

- **VLAN Membership Configuration**
- **VLAN Port Membership Table**

VLAN Membership Configuration

The VLAN Membership section contains parameters for assigning VLAN membership to ports. The section contains the following fields:

- **Show VLAN --** Lists and displays specific VLAN information according to VLAN ID or VLAN name.
- **VLAN Name --** The user-defined VLAN name.
- **Status --** The VLAN type. Possible values are:
- **Dynamic --** The VLAN was dynamically created through GVRP.
- **Static --** The VLAN is user-defined.
- **Default --** The VLAN is the default VLAN.
- **Unauthorized Users --** Enables or disables unauthorized users from accessing a VLAN.
- **Remove VLAN --** When selected, removes the VLAN from the VLAN Membership Table.

VLAN Port Membership Table

The VLAN Port Membership Table contains a Port Table for assigning ports to VLANs. Ports are assigned VLAN membership by toggling through the Port Control settings. Ports can have the following values:

Port Control	Definition
T	The interface Is a member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.
U	The interface is a VLAN member. Packets forwarded by the interface are untagged.
F	The interface is denied membership to a VLAN.
Blank	The interface is not a VLAN member. Packets associated with the interface are not forwarded.

✍ **Note:** Ports which are LAG members are not displayed in the VLAN Port Membership Table.

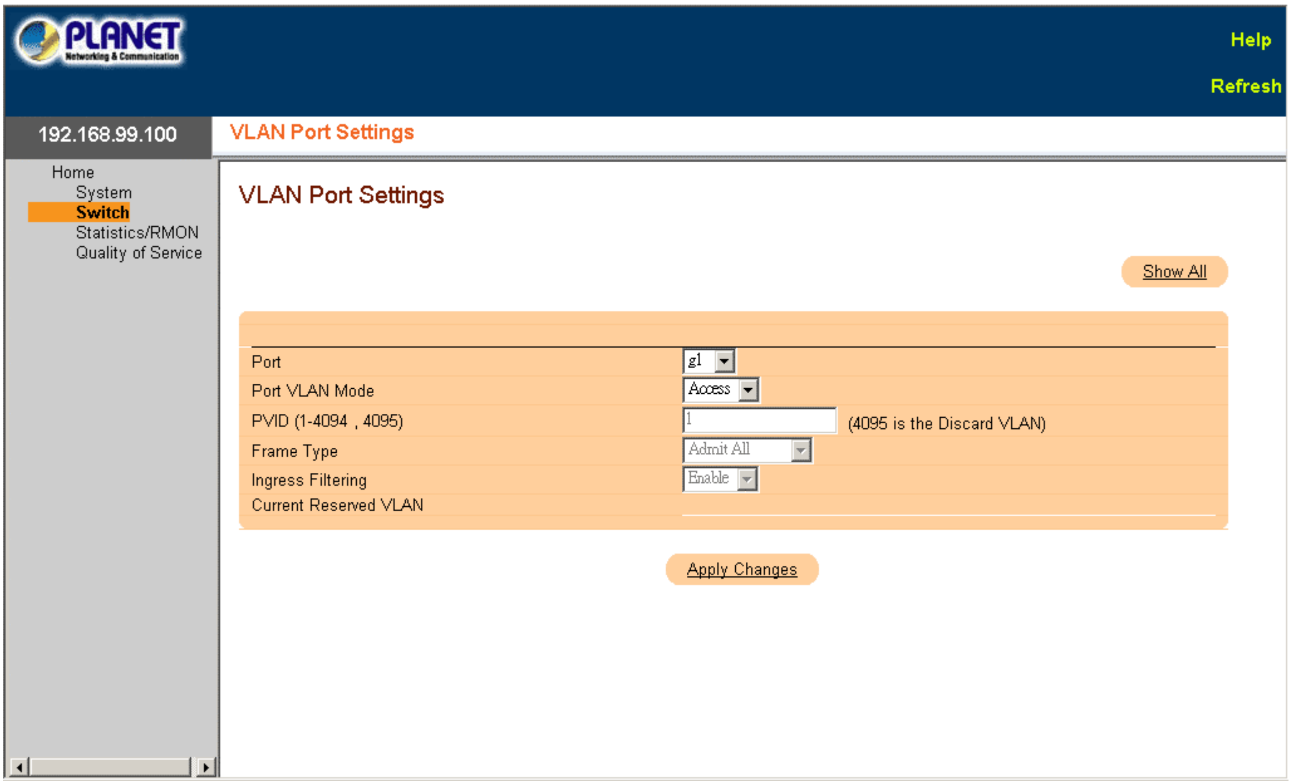
The VLAN Port Membership Table displays the ports and the ports states, as well as LAGs.

3.2.3.6.2 VLAN Port Settings

The **VLAN Port Settings** page contains fields for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the VLAN Port Settings page. All untagged packets arriving to the device are tagged by the ports PVID.

To open **VLAN Membership** screen perform the folling:

1. Click Switch -> VLAN -> VLAN Port Settings
2. The VLAN Port Settings screen is displayed as in Figure 3-63



VLAN Port Settings

Port	g1
Port VLAN Mode	Access
PVID (1-4094 , 4095)	1 (4095 is the Discard VLAN)
Frame Type	Admit All
Ingress Filtering	Enable
Current Reserved VLAN	

Figure 3-63 VLAN Port Settings screen

The page includes the following fields:

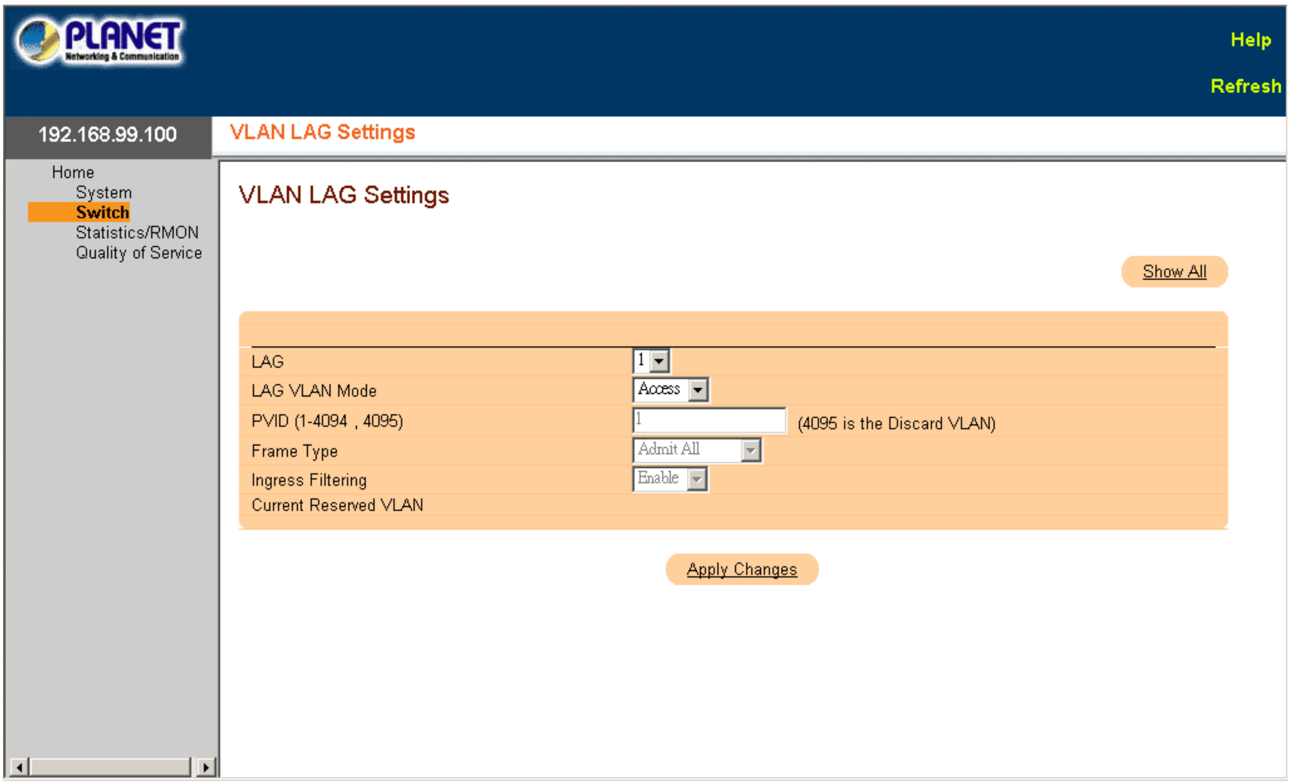
- **Port --** The port number included in the VLAN.
- **Port VLAN Mode --** The port mode. Possible values are:
- **General --** The port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).
- **Access --** The port belongs to a single untagged VLAN. When a port is in Access mode, the packet types which are accepted on the port cannot be designated. Ingress filtering cannot be enabled/disabled on an access port.
- **Trunk --** The port belongs to VLANs in which all ports are tagged (except for one port that can be untagged).
- **PVID --** Assigns a VLAN ID to untagged packets. The possible values are 1-4094. VLAN 4095 is defined as per standard and industry practice as the discard VLAN. Packets classified to the Discard VLAN are dropped.
- **Frame Type --** Packet type accepted on the port. Possible values are:
- **Admit Tag Only --** Only tagged packets are accepted on the port.
- **Admit All --** Both tagged and untagged packets are accepted on the port.
- **Ingress Filtering --** Enables or disables Ingress filtering on the port. Ingress filtering discards packets that are destined to VLANs of which the specific port is not a member.
- **Current Reserve VLAN --** The VLAN currently designated as the reserved VLAN.
- **Reserve VLAN for Internal Use --** The VLAN that is designated as the reserved VLAN after the device is reset.

3.2.3.6.3 VLAN LAG Settings

The **VLAN LAG Setting** page provides parameters for managing LAGs that are part of a VLAN. VLANs can either be composed of individual ports or of LAGs. Untagged packets entering the device are tagged with the LAGs ID specified by the PVID.

To open **VLAN LAG Settings** screen perform the folling:

1. Click Switch -> VLAN -> LAG Settings
2. The VLAN LAG Settings screen is displayed as in Figure 3-64



VLAN LAG Settings

LAG	1
LAG VLAN Mode	Access
PVID (1-4094 , 4095)	1 (4095 is the Discard VLAN)
Frame Type	Admit All
Ingress Filtering	Enable
Current Reserved VLAN	

Figure 3-64 VLAN LAG Settings

The page includes the following fields:

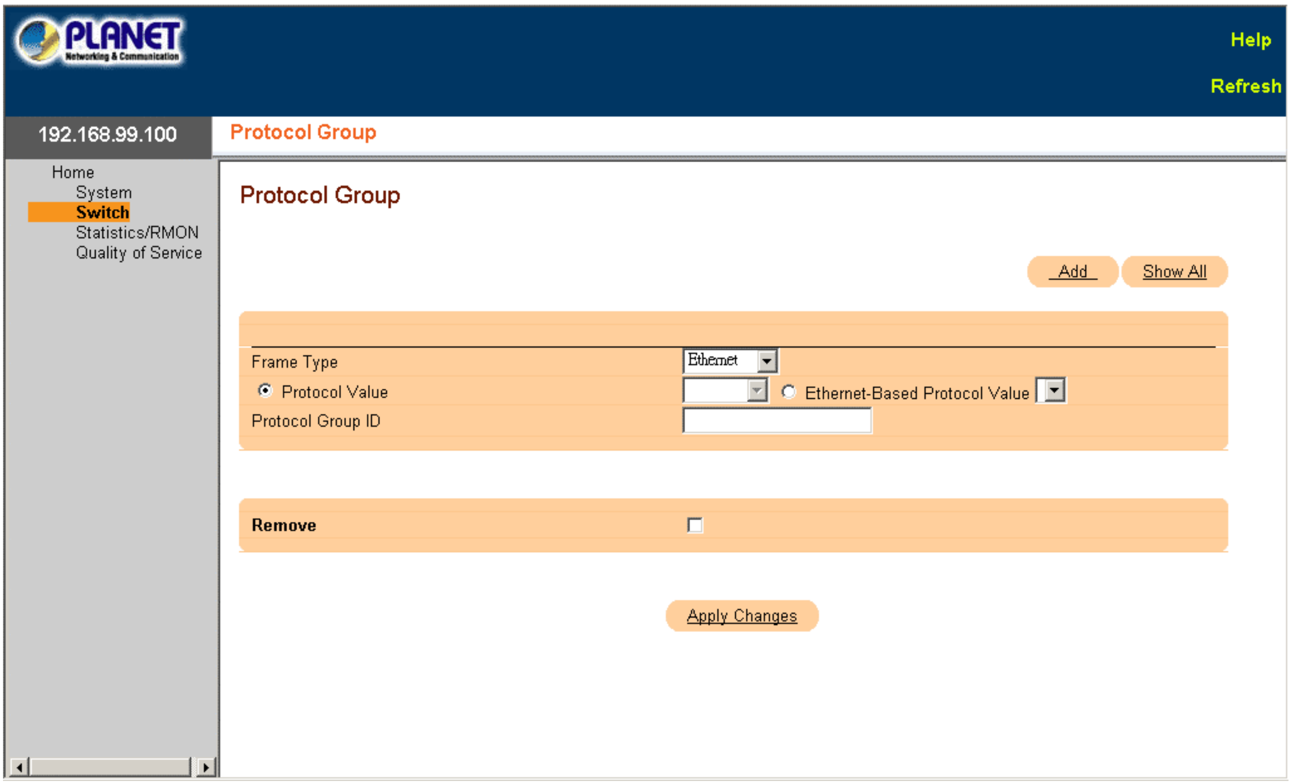
- **LAG --** The LAG number included in the VLAN.
- **LAG VLAN Mode --** The LAG VLAN mode. Possible values are:
- **General --** The LAG belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).
- **Access --** The LAG belongs to a single, untagged VLAN.
- **Trunk --** The LAG belongs to VLANs in which all ports are tagged (except for an optional single native VLAN).
- **PVID --** Assigns a VLAN ID to untagged packets. The possible field values are 1-4095. VLAN 4095 is defined as per standard and industry practice, as the discard VLAN. Packets classified to this VLAN are dropped.
- **Frame Type --** Packet type accepted by the LAG. Possible values are:
- **Admit Tag Only --** Only tagged packets are accepted by the LAG.
- **Admit All --** Tagged and untagged packets are both accepted by the LAG.
- **Ingress Filtering --** Enables or disables Ingress filtering by the LAG. Ingress filtering discards packets that are destined to VLANs of which the specific LAG is not a member.
- **Current Reserve VLAN --** The VLAN currently designated by the system as the reserved VLAN.
- **Reserve VLAN for Internal Use --** The VLAN selected by the user to be the reserved VLAN if not in use by the system.

3.2.3.6.4 Portocol Group

The **Protocol Group** page provides parameters for configuring frame types to specific protocol groups.

To open **VLAN Membership** screen perform the folling:

1. Click Switch -> VLAN -> VLAN Port Settings
2. The VLAN Port Settings screen is displayed as in Figure 3-64



Protocol Group

Frame Type	Ethernet
● Protocol Value	○ Ethernet-Based Protocol Value
Protocol Group ID	

Remove	□

Figure 3-64 Protocol Group screen

The page includes the following fields:

Frame Type -- The packet type. Possible field values are Ethernet, RFC1042, and LLC Other.

Protocol Value -- User-defined protocol name.

Ethernet-Based Protocol Value -- The Ethernet protocol group type. The possible field values are IP, IPX and IPV6.

Protocol Group ID -- The VLAN Group ID number.

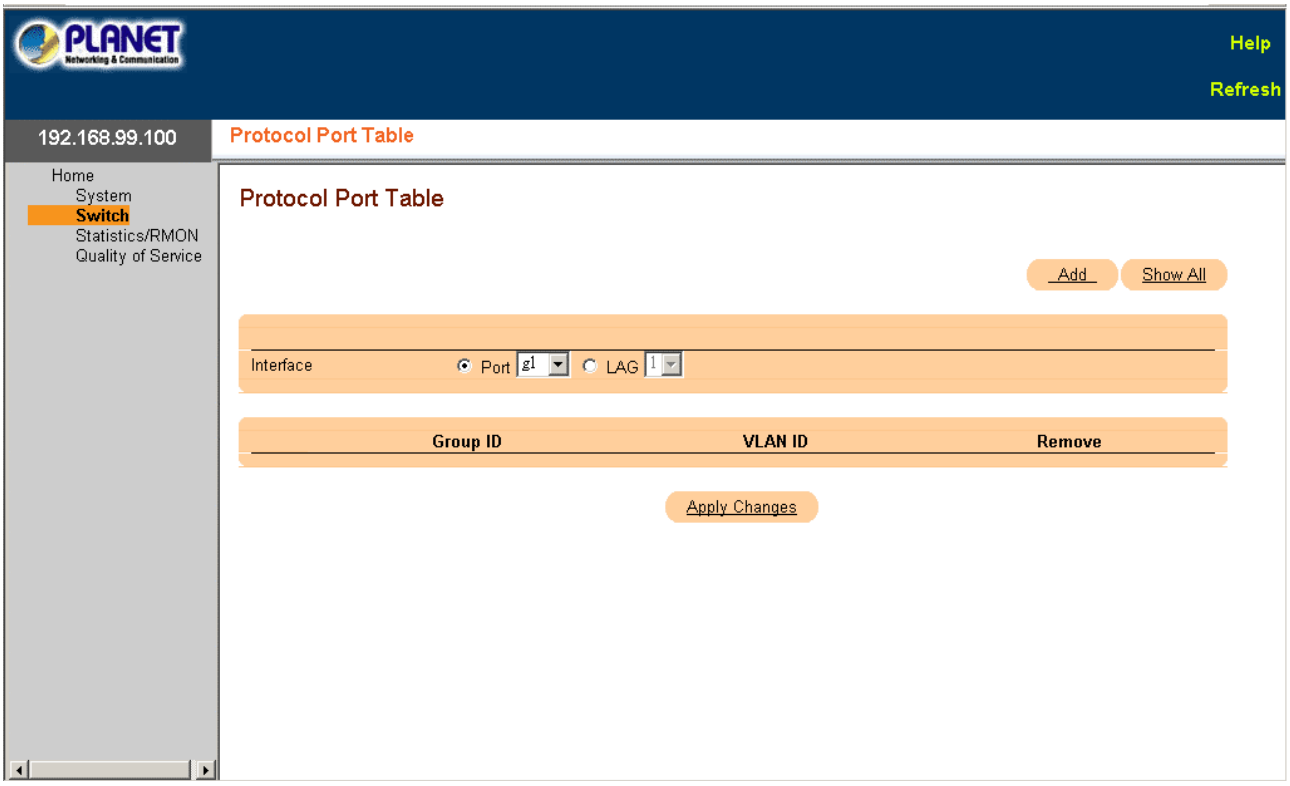
Remove -- When selected, removes frame-to-protocol group mapping, if the protocol group to be removed is not configured on this protocol port.

3.2.3.6.5 Protocol Port Table

The **Protocol Port** page adds interfaces to Protocol groups.

To open **Protocol Port** screen perform the folling:

1. Click Switch -> VLAN -> Protocol Port
2. The Protocol Port Settings screen is displayed as in Figure 3-65



Interface ● Port g1 ○ LAG 1

Group ID	VLAN ID	Remove

Figure 3-65 Protocol Port Table screen

The page includes the following fields:

- **Interface --** Port or LAG number added to a protocol group.
- **Group ID --** Protocol group ID to which the interface is added. Protocol group IDs are defined in the Protocol Group Table.
- **VLAN ID (1-4095) --** Attaches the interface to a user-defined VLAN ID. The VLAN ID is defined on the Create a New VLAN page. Protocol ports can either be attached to a VLAN ID or a VLAN name.

✍ ***Note:*** VLAN 4095 is the discard VLAN.

✍ ***Note:*** Protocol ports can be defined only on ports that are defined as General in the VLAN Port Membership Table page.

3.2.3.6.6 GVRP Parameters

GARP VLAN Registration Protocol (GVRP) is specifically provided for automatic distribution of VLAN membership information among VLAN-aware bridges. GVRP allows VLAN-aware bridges to automatically learn VLANs to bridge ports mapping, without having to individually configure each bridge and register VLAN membership.

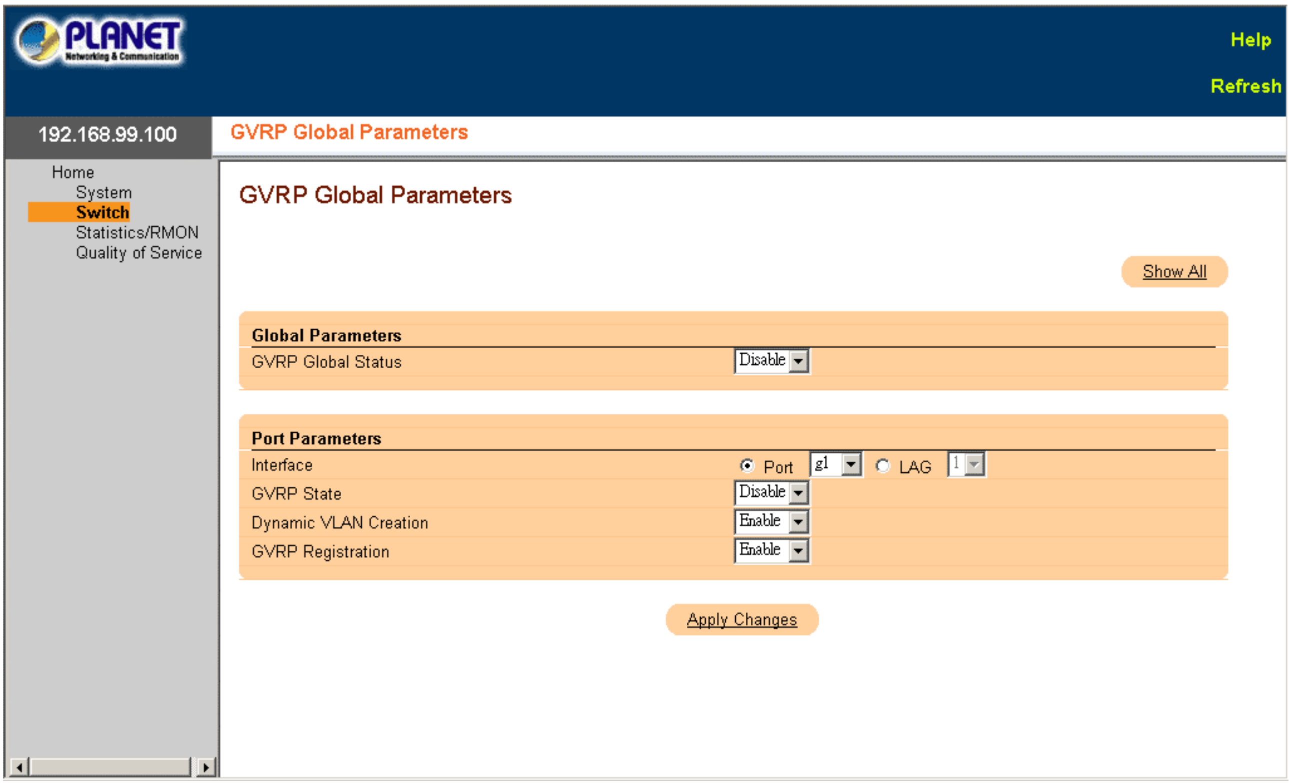
To ensure the correct operation of the GVRP protocol, it is advised to set the maximum number of GVRP VLANs equal to a value which significantly exceeds the sum of:

- The number of all static VLANs both currently configured and expected to be configured.
- The number of all dynamic VLANs participating in GVRP, both currently configured (initial number of dynamic GVRP VLANs is 128) and expected to be configured.

The GVRP Global Parameters page enables GVRP globally. GVRP can also be enabled on a per-interface basis.

To open **GVRP Parameters** screen perform the folling:

1. Click Switch -> VLAN -> GVRP Parameters
2. The GVRP Parameters screen is displayed as in Figure 3-66



GVRP Global Parameters

Global Parameters	
GVRP Global Status	Disable

Port Parameters	
Interface	● Port g1 ○ LAG 1
GVRP State	Disable
Dynamic VLAN Creation	Enable
GVRP Registration	Enable

Figure 3-66 GVRP Global Parameters screen

The page includes the following fields:

- GVRP Global Status -- Enables or disables GVRP on the device. GVRP is disabled by default.
- Interface -- The port or LAG for which GVRP is enabled.
- GVRP State -- Enables or disables GVRP on an interface.
- Dynamic VLAN Creation -- Enables or disables VLAN creation through GVRP.
- GVRP Registration -- The GVRP Registration status.

3.2.3.7 Link Agreegation

Port Aggregation optimizes port usage by linking a group of ports together to form a single Link Aggregated Groups (LAGs). Port Aggregation multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy. The device supports up to eight LAGs per system, and eight ports per LAG per device.

Each LAG is composed of ports of the same speed, set to full-duplex operations. Ports in a LAG, can be of different media types (UTP/Fiber, or different fiber types), provided they operate at the same speed.

Aggregated Links can be assigned manually or automatically by enabling Link Aggregation Control Protocol (LACP) on the relevant links. The device provides LAG Load Balancing based on both source MAC addresses and destination MAC addresses.

Aggregated Links are treated by the system as a single logical port. Specifically, the Aggregated Link has similar port attributes to a non-aggregated port, including auto-negotiation, speed, Duplex setting, etc.

The device supports both static LAGs and Link Aggregation Control Protocol (LACP) LAGs. LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.

The following guidelines should be followed when adding ports to a LAG:

- There is no Layer 3 interface defined on the port.
- The port does not belong to any VLAN.
- The port does not belong to any other LAG.
- The port is not a mirrored port.
- The port's 802.1p priority is equal to LAGs 802.1p priority.

- QoS Trust is not disabled on the port.
- GVRP is not enabled.

✍ **Note:** Ports can be configured as LACP ports only if the ports are not part of a previously configured LAG.

The device uses a hash function to determine which frames are carried on which aggregated-link member. The hash function statistically load-balances the aggregated link members. The device considers an Aggregated Link as a single logical port.

Each Aggregated Link has an Aggregated Link Port Type, including Gigabit Ethernet ports. Ports can be added to an Aggregated Link only if they are the same port type. When ports are removed from an Aggregated Links, the ports revert to the original port settings.

The Link Aggregation page contains links to the following topics:

- **LACP Parameters**
- **LAG Membership**

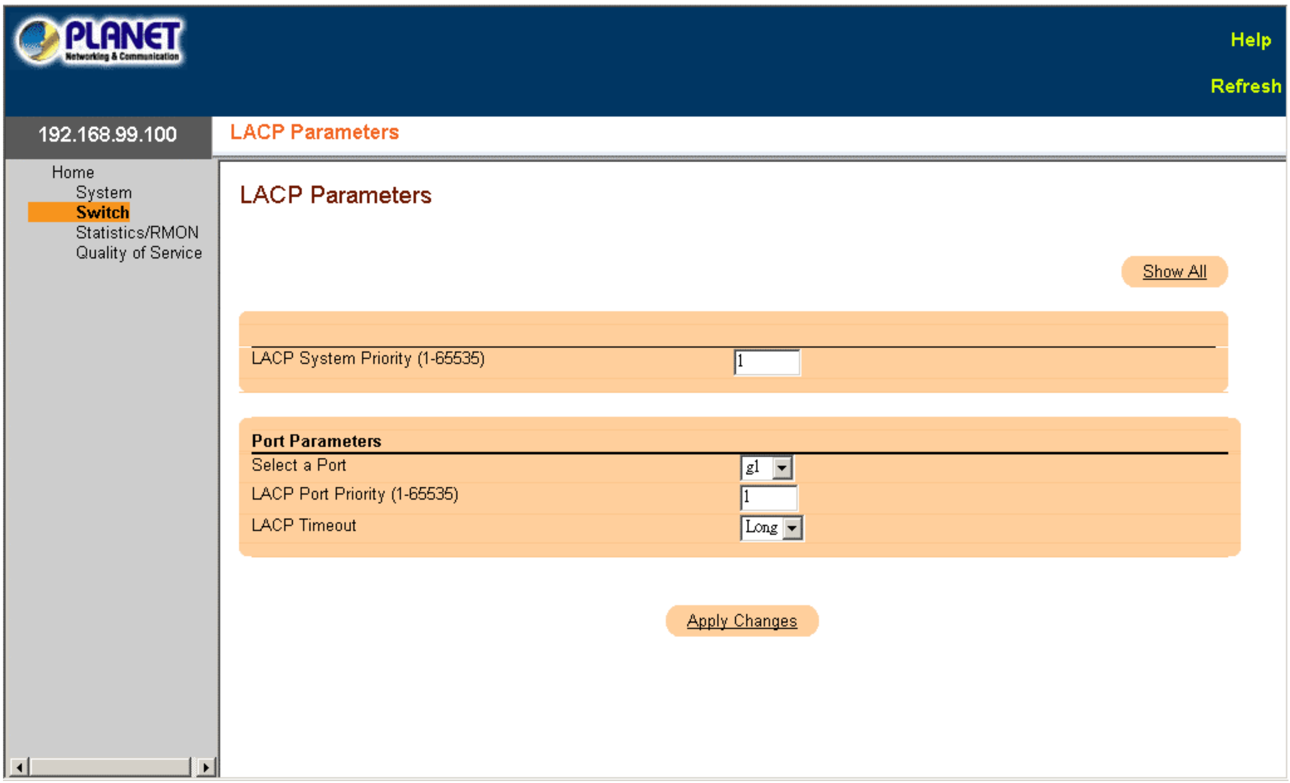
3.2.3.7.1 LACP Parameters

The LACP Parameters page contains fields for configuring LACP LAGs. Aggregate ports can be linked into link-aggregation port-groups. Each group is comprised of ports with the same speed.

Aggregated Links can be manually setup or automatically established by enabling Link Aggregation Control Protocol (LACP) on the relevant links.

To open **LACP Parameters** screen perform the folling:

1. Click Switch -> Link Agreegation -> LACP Parameters
2. The LACP Parameters screen is displayed as in Figure 3-67



LACP System Priority (1-65535) 1

Port Parameters

Select a Port g1

LACP Port Priority (1-65535) 1

LACP Timeout Long

Figure 3-67 LACP Parameters

The page includes the following fields:

- **LACP System Priority (1-65535) --** The LACP priority value for global settings. The possible range is 1- 65535. The default value is 1.
- **Select a Port --** The port number to which timeout and priority values are assigned.

- **LACP Port Priority (1-65535) --** LACP priority value for the port.
- **LACP Timeout --** Administrative LACP timeout. The possible field values are:
- **Short --** Specifies a short timeout value.
- **Long --** Specifies a long timeout value.

3.2.3.7.2 LAG Membership

The **LAG Membership** page contains fields for assigning ports to LAGs. LAGs can include up to 8 ports.When a port is added to a LAG, the port acquires the LAG□ properties. If the port cannot be configured with the LAG properties, a trap is generated and the port operates with its default settings.

The LAG Membership page contains fields for assigning ports to LAGs.

To open **LAG Membership** screen perform the folling:

1. Click Switch -> Link Agreegation -> LAG Membership
2. The LAG Membership screen is displayed as in Figure 3-68

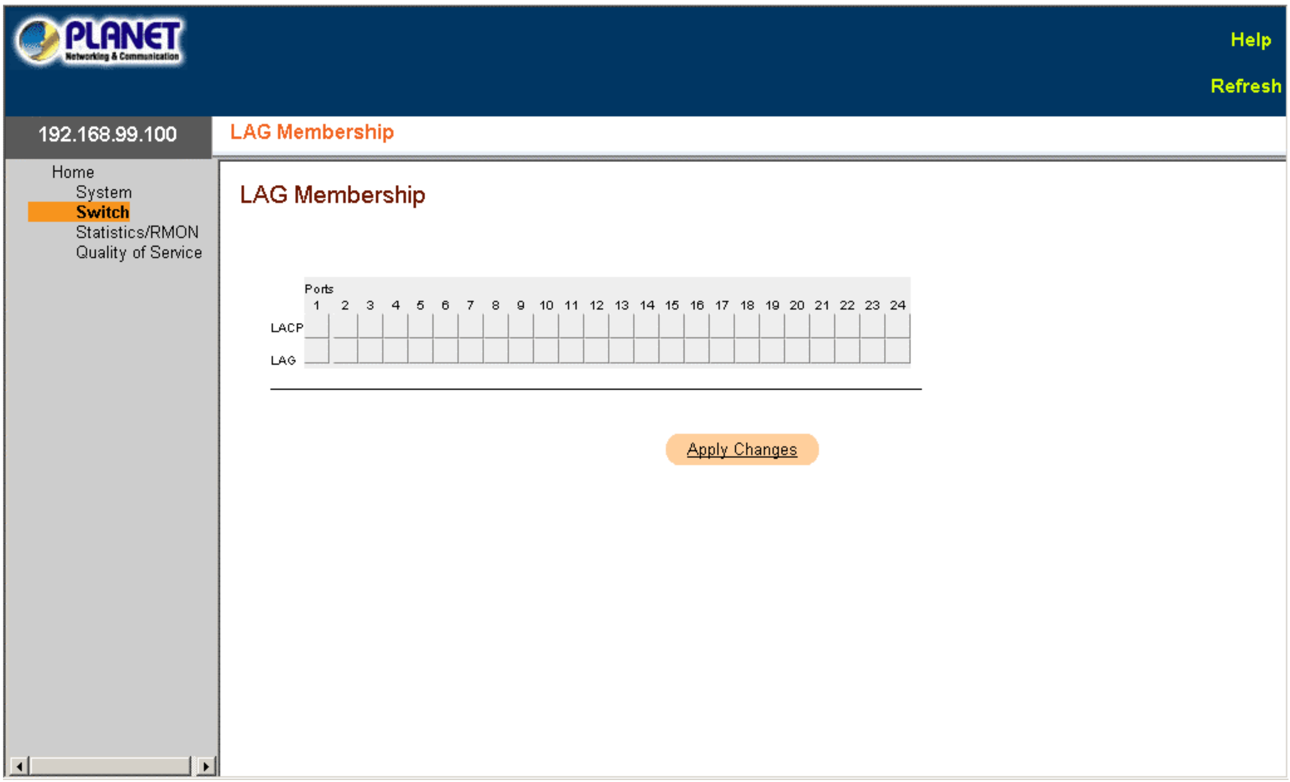


Figure 3-68 LAG Membership screen

The page includes the following fields:

- **LACP --** Aggregates the port to a LAG, using LACP.
- **LAG --** Adds a port to a LAG, and indicates the specific LAG to which the port belongs.

Configuring a Port to a LAG or LACP

1. Open the LAG Membership page.
2. In the LAG row (the second row), toggle the button to a specific number to aggregate or remove the port to that LAG number.
3. In the LACP row (the first row), toggle the button under the port number to assign either the LACP or the static LAG.
4. Click Apply Changes.

The port is added to the LAG or LACP, and the device is updated.

3.2.3.8 Multicast Support

Multicast forwarding allows a single packet to be forwarded to multiple destinations. L2 Multicast service is based on L2 switch receiving a single packet addressed to a specific Multicast address. Multicast forwarding creates copies of the packet, and transmits the packets to the relevant ports.

The device supports:

- **Forwarding L2 Multicast Packets --** Enabled by default, and not configurable.

✍ ***Note:*** The system supports Multicast filtering for 320 Multicast groups.

- **Filtering L2 Multicast Packets --** Enables forwarding of Layer 2 packets to interfaces. If Multicast filtering is disabled, Multicast packets are flooded to all relevant ports.

The Multicast Support page contains links to the following topics:

- **Global Parameters**
- **Bridge Multicast Group**
- **Bridge Multicast Forward All**
- **IGMP Snooping**

3.2.3.8.1 Global Parameters

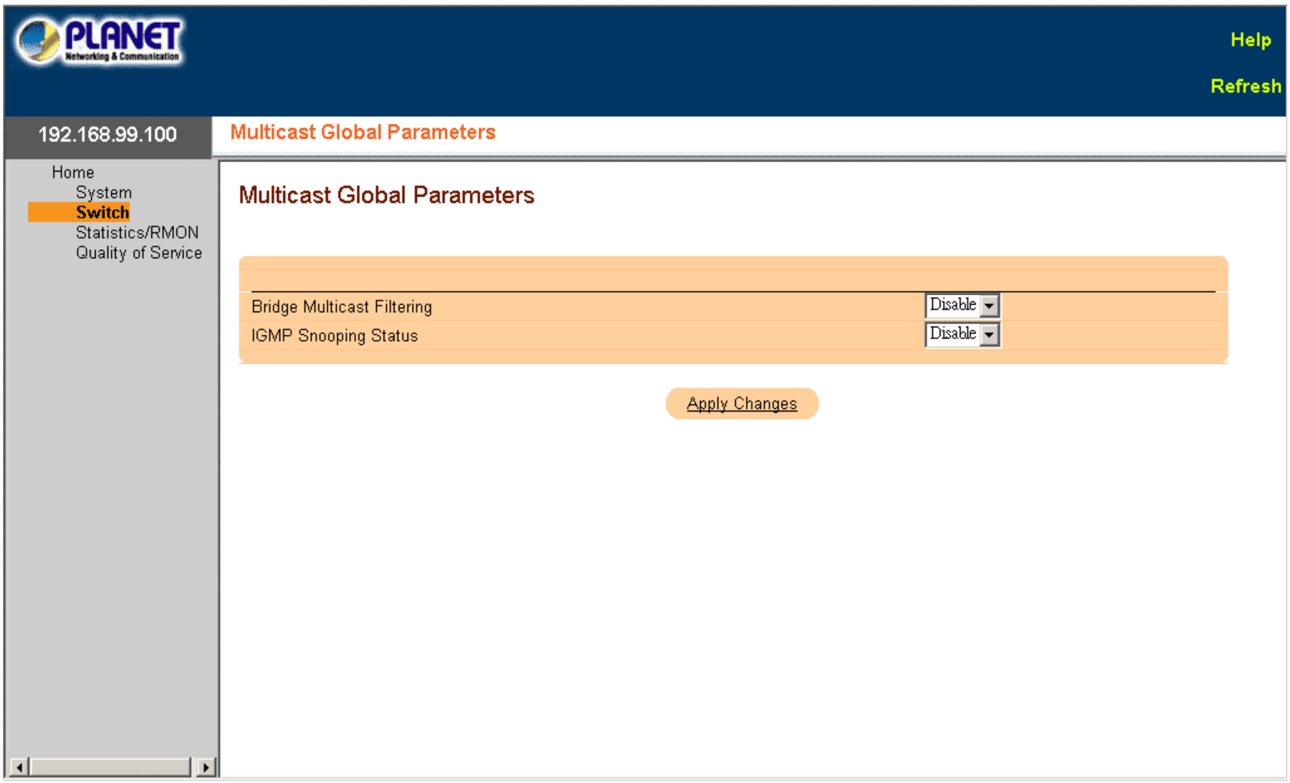
Layer 2 switching forwards Multicast packets to all relevant VLAN ports by default, treating the packet as a Multicast transmission. While this is functional, in the sense that all relevant ports/nodes receive a copy of the frame, it is potentially wasteful as ports/nodes may receive irrelevant frames only needed by a subset of the ports of that VLAN. Multicast forwarding filters enable forwarding of Layer 2 packets to port subsets, defined in the Multicast filter database.

When IGMP snooping is enabled globally, the switching ASIC is programmed to forward all IGMP packets to the CPU. The CPU analyzes the incoming packets and determines which ports are to join which Multicast groups, which ports have Multicast routers generating IGMP queries, and what routing protocols are forwarding packets and Multicast traffic. Ports requesting to join a specific Multicast group issues an IGMP report specifying that Multicast group. This results in the creation of the Multicast filtering database.

The Multicast Global Parameters page contains fields for enabling IGMP Snooping on the device.

To open **Global Parameters** screen perform the folling:

1. Click Switch -> Multicast Support -> Global Parameter
2. The Global Parameter screen is displayed as in Figure 3-69



Multicast Global Parameters

Bridge Multicast Filtering: Disable

IGMP Snooping Status: Disable

Figure 3-69 Multicast Global Parameters

The page includes the following fields:

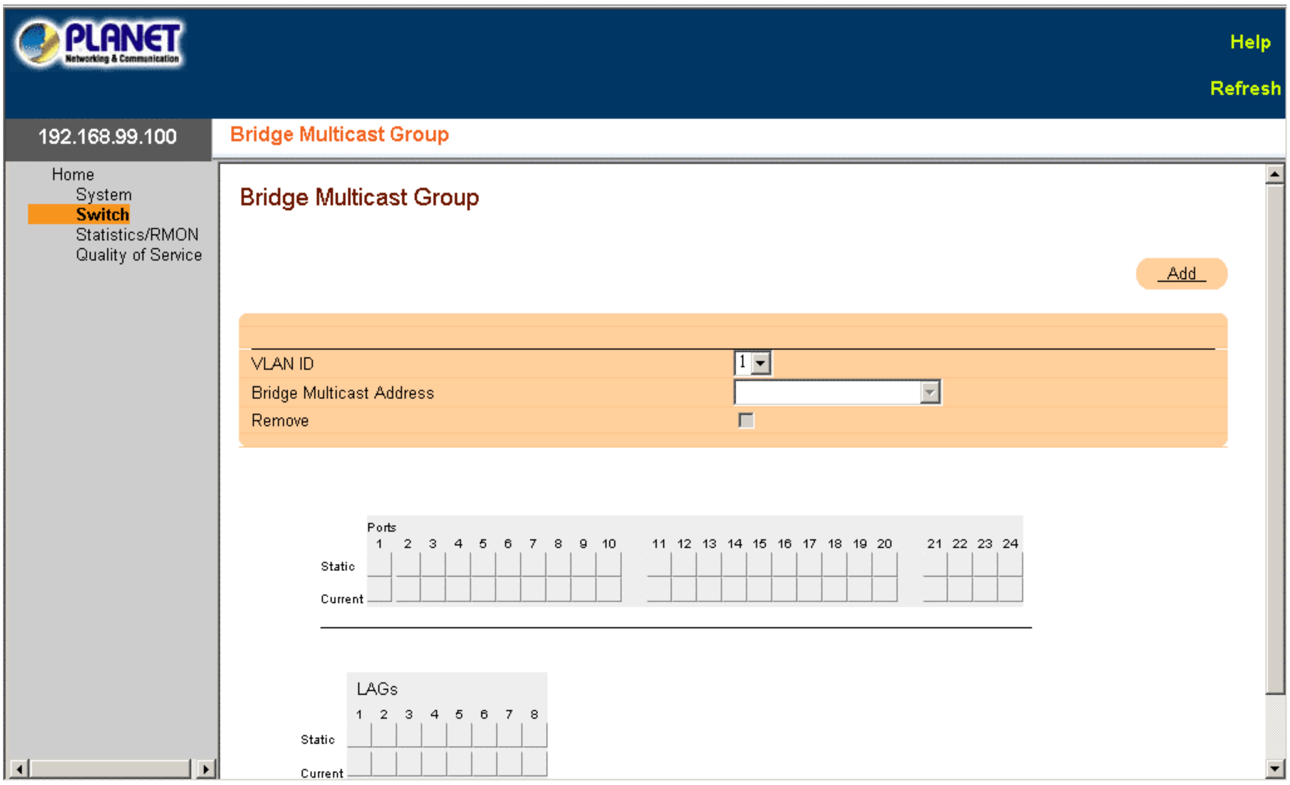
- **Bridge Multicast Filtering --** Enables or disables bridge Multicast filtering. Disabled is the default value. IGMP Snooping can be enabled only if Bridge Multicast Filtering is enabled.
- **IGMP Snooping Status --** Enables or disables IGMP Snooping on the device. Disabled is the default value.

3.2.3.8.2 Bridge Multicast Group

The Bridge Multicast Group page displays the ports and LAGs attached to the Multicast service group in the Ports and LAGs tables. The Port and LAG tables also reflect the manner in which the port or LAGs joined the Multicast group. Ports can be added either to existing groups or to new Multicast service groups. The Bridge Multicast Group page permits new Multicast service groups to be created. The Bridge Multicast Group page also assigns ports to a specific Multicast service address group.

To open **Bridge Multicast Group** screen perform the folling:

1. Click Switch -> Multicast Support -> Bridge Multicast Group
2. The Bridge Multicast Group screen is displayed as in Figure 3-70



Bridge Multicast Group

Bridge Multicast Group

VLAN ID 1

Bridge Multicast Address

Remove □

Figure 3-70 Bridge Multicast Group screen

The page includes the following fields:

- **VLAN ID --** Identifies a VLAN and contains information about the Multicast group address.
- **Bridge Multicast Address --** Identifies the Multicast group MAC address/IP address.
- **Remove --** When selected, removes a Bridge Multicast address.
- **Ports --** Port that can be added to a Multicast service.
- **LAGs --** LAGs that can be added to a Multicast service.

The following table contains the IGMP port and LAG members management settings:

Port Control	Definition
D	The port/LAG has joined the Multicast group dynamically in the Current Row.
S	Attaches the port to the Multicast group as static member in the Static Row.The port/LAG has joined the Multicast group statically in the Current Row.
F	Forbidden.
Blank	The port is not attached to a Multicast group.

Adding Bridge Multicast Addresses

1. Click Add. The Add Bridge Multicast Group page opens.
2. Define the VLAN ID and New Bridge Multicast Address fields.
3. Toggle a port to S to join the port to the selected Multicast group.
4. Toggle a port to F to forbid adding specific Multicast addresses to a specific port.
5. Click Apply Changes.

The bridge Multicast address is assigned to the Multicast group, and the device is updated.

Defining Ports to Receive Multicast Service

1. Define the VLAN ID and the Bridge Multicast Address fields.

2. Toggle a port to S to join the port to the selected Multicast group.

3. Toggle a port to F to forbid adding specific Multicast addresses to a specific port.

4. Click Apply Changes.

The port is assigned to the Multicast group, and the device is updated.

Assigning LAGs to Receive Multicast Service

1. Define the VLAN ID and the Bridge Multicast Address fields.

2. Toggle the LAG to S to join the LAG to the selected Multicast group.

3. Toggle the LAG to F to forbid adding specific Multicast addresses to a specific LAG.

4. Click Apply Changes.

The LAG is assigned to the Multicast group, and the device is updated.

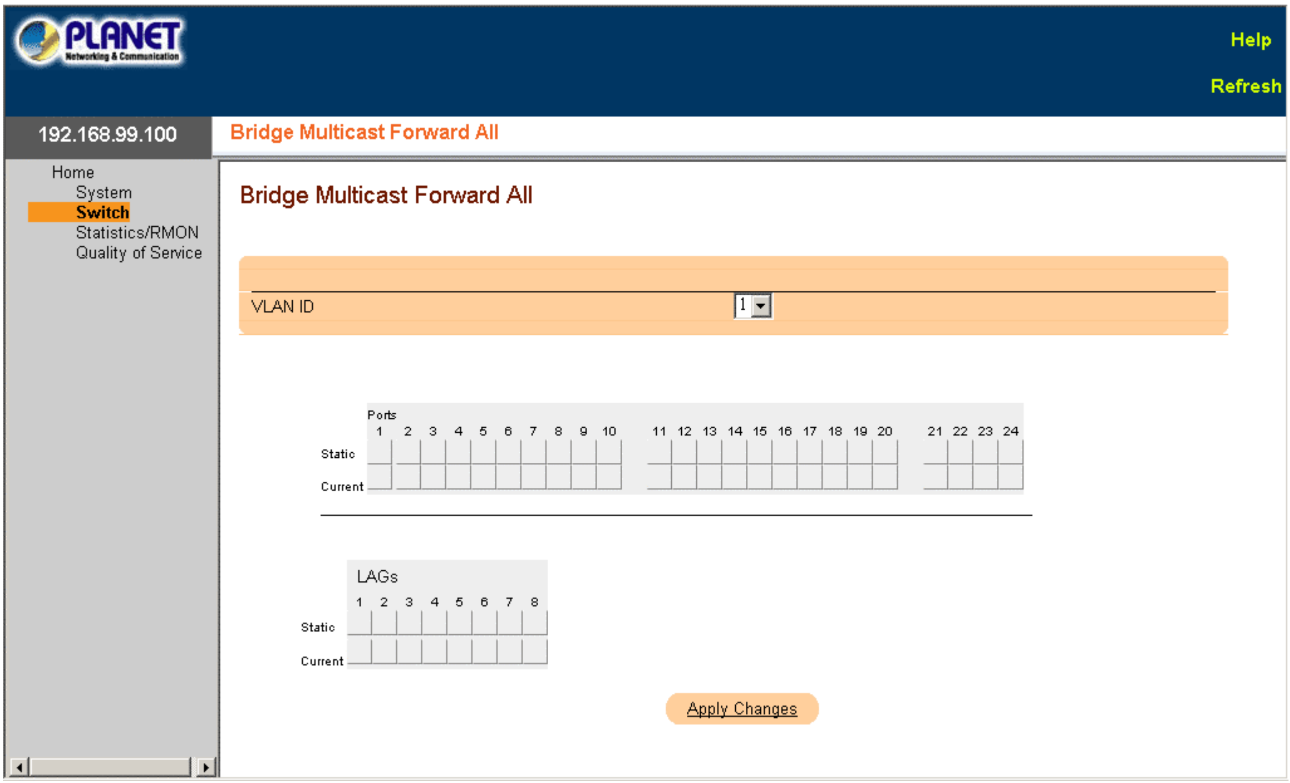
3.2.3.8.3 Bridge Multicast Forward All

The Bridge Multicast Forward All page contains fields for attaching ports or LAGs to a device that is attached to a neighboring Multicast router/switch. Once IGMP Snooping is enabled, Multicast packets are forwarded to the appropriate port or VLAN.

To open **Bridge Multicast Forward All** screen perform the folling:

1. Click Switch -> Multicast Support -> Bridge Multicast Forward All

2. The Bridge Multicast Forward All screen is displayed as in Figure 3-71



VLAN ID 1

Figure 3-71 Bridge Multicast Forward All

The page includes the following fields:

- **VLAN ID --** Identifies a VLAN.
- **Ports --** Ports that can be added to a Multicast service.
- **LAGs --** LAGs that can be added to a Multicast service.

The following table contains the settings for managing router and port settings.

Port Control	Definition
D	Attaches the port to the Multicast router or switch as a dynamic port.
S	Attaches the port to the Multicast router or switch as a static port.
F	Forbidden.
Blank	The port is not attached to a Multicast router or switch.

Attaching a Port to a Multicast Router or Switch

1. Define the VLAN ID field.
2. Select a port in the Ports table, and assign the port a value.
3. Click Apply Changes.

The port is attached to the Multicast router or switch.

Attaching a LAG to a Multicast Router or Switch

1. Define the VLAN ID field.
2. Select a port in the LAGs table, and assign the LAG a value.
3. Click Apply Changes.

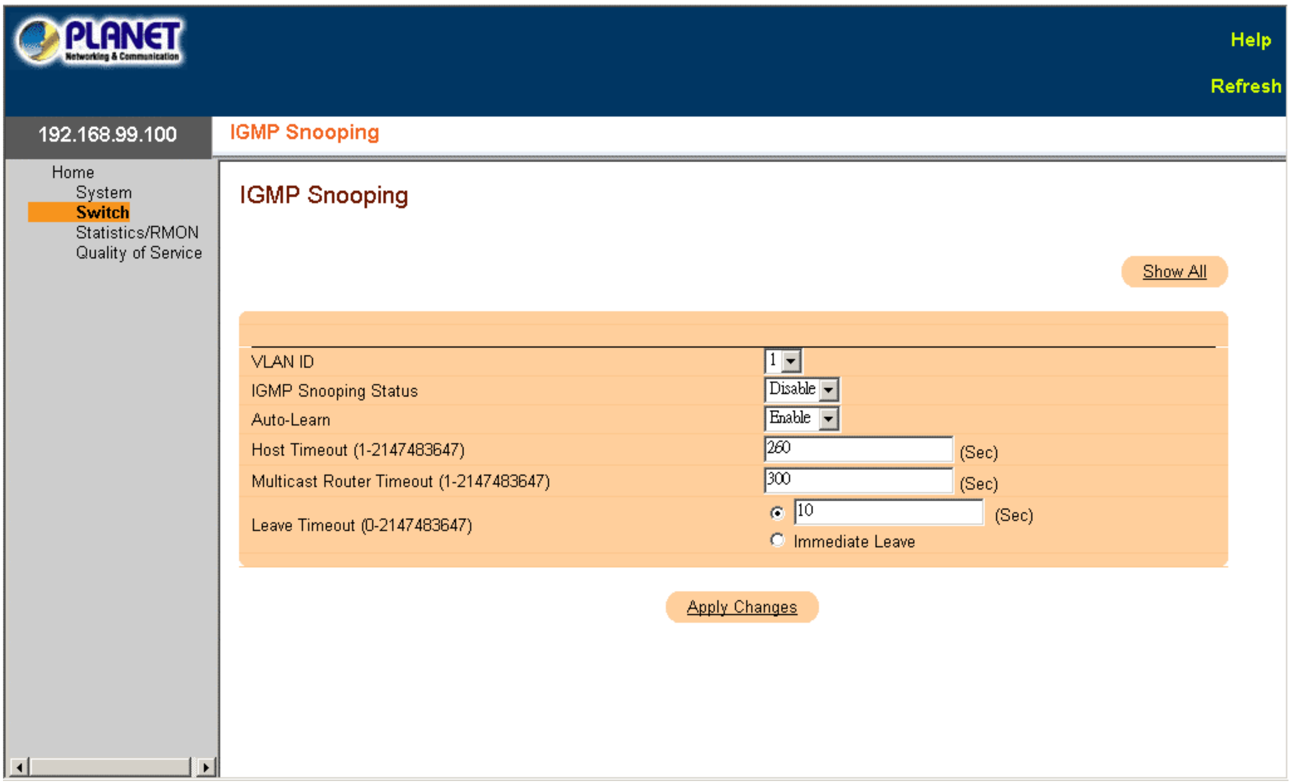
The LAG is attached to the Multicast router or switch.

3.2.3.8.4 IGMP Snooping

The **IGMP Snooping** page contains fields for adding IGMP members.

To open **IGMP Snooping** screen perform the folling:

1. Click Switch -> Multicast Support -> IGMP Snooping
2. The IGMP Snooping screen is displayed as in Figure 3-72



IGMP Snooping

VLAN ID	1
IGMP Snooping Status	Disable
Auto-Learn	Enable
Host Timeout (1-2147483647)	260 (Sec)
Multicast Router Timeout (1-2147483647)	300 (Sec)
Leave Timeout (0-2147483647)	● 10 (Sec) ○ Immediate Leave

Figure 3-72 IGMP Snooping screen

The page includes the following fields:

- **VLAN ID --** Specifies the VLAN ID.
- **IGMP Snooping Status --** Enables or disables IGMP snooping on the VLAN.
- **Auto Learn --** Enables or disables Auto Learn on the device.
- **Host Timeout (1-2147483647) --** Time before an IGMP snooping entry is aged out. The default time is 260 seconds.
- **Multicast Router Timeout (1-2147483647) --** Time before aging out a Multicast router entry. The default value is 300 seconds.
- **Leave Timeout (0-2147483647) --** Time, in seconds, after a port leave message is received before the entry is aged out. User-defined enables a user-definable timeout period, and Immediate Leave specifies an immediate timeout period. The default timeout is 10 seconds.

3.2.4 View Statistics/RMON Information

The Statistic pages contains links to device information for interface, GVRP, etherlike, RMON, and device utilization.

✍ ***Note:*** CLI commands are not available for all the Statistics pages.

The Statistics/RMON page contains links to the following topics:

- **Table Views**
- **RMON**
- **Charts**

3.2.4.1 Table Views

The Table Views page contains links for displaying statistics in a chart form.

The Table Views page contains links to the following topics:

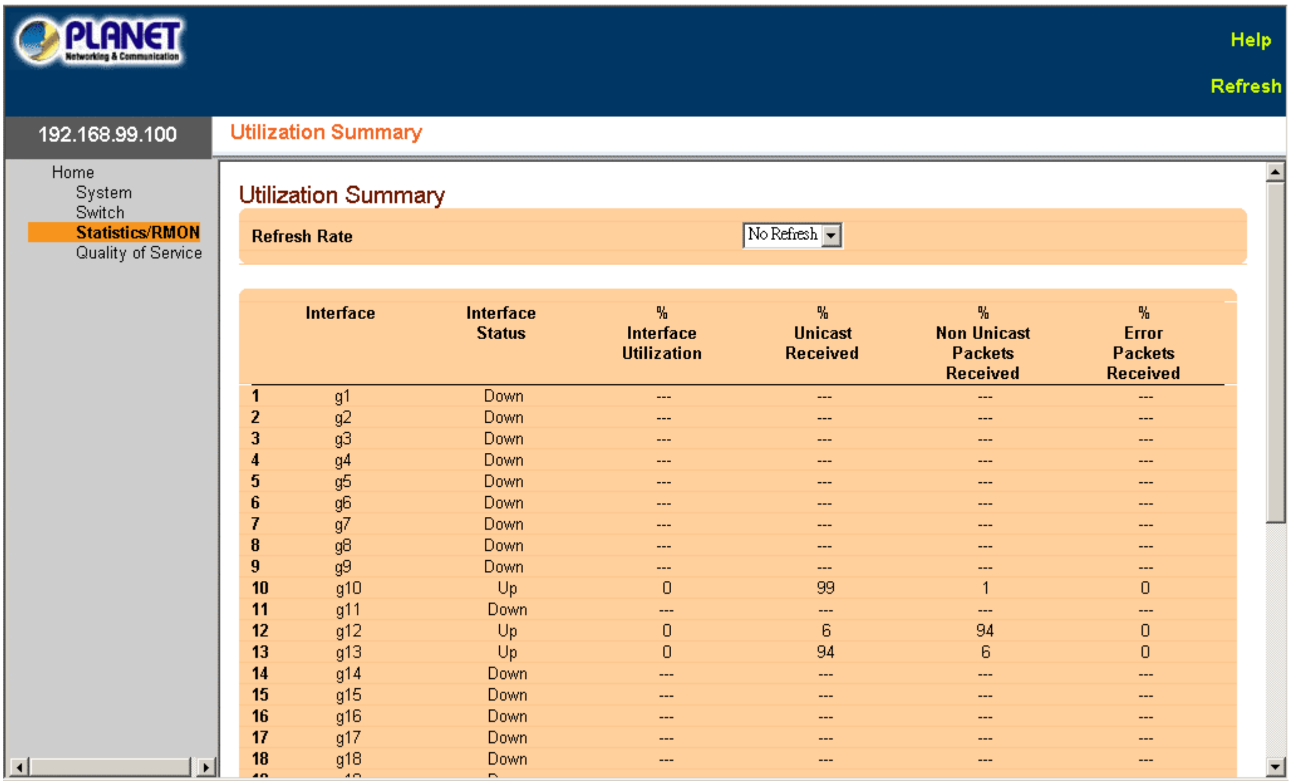
- **Utilization Summary**
- **Counter Summary**
- **Interface Statistics**
- **Etherlike Statistics**
- **GVRP Statistics**
- **EAP Statistics**

3.2.4.1.1 Utilization Summary

The **Utilization Summary** page contains statistics for interface utilization.

To open **Utilization Summary** screen perform the folling:

1. Click Statics/RMON -> Table Views -> Utilization Summary
2. The Utilization Summary screen is displayed as in Figure 3-73



Utilization Summary

Refresh Rate: No Refresh

	Interface	Interface Status	% Interface Utilization	% Unicast Received	% Non Unicast Packets Received	% Error Packets Received
1	g1	Down	---	---	---	---
2	g2	Down	---	---	---	---
3	g3	Down	---	---	---	---
4	g4	Down	---	---	---	---
5	g5	Down	---	---	---	---
6	g6	Down	---	---	---	---
7	g7	Down	---	---	---	---
8	g8	Down	---	---	---	---
9	g9	Down	---	---	---	---
10	g10	Up	0	99	1	0
11	g11	Down	---	---	---	---
12	g12	Up	0	6	94	0
13	g13	Up	0	94	6	0
14	g14	Down	---	---	---	---
15	g15	Down	---	---	---	---
16	g16	Down	---	---	---	---
17	g17	Down	---	---	---	---
18	g18	Down	---	---	---	---

Figure 3-73 Utilization Summary screen

The page includes the following fields:

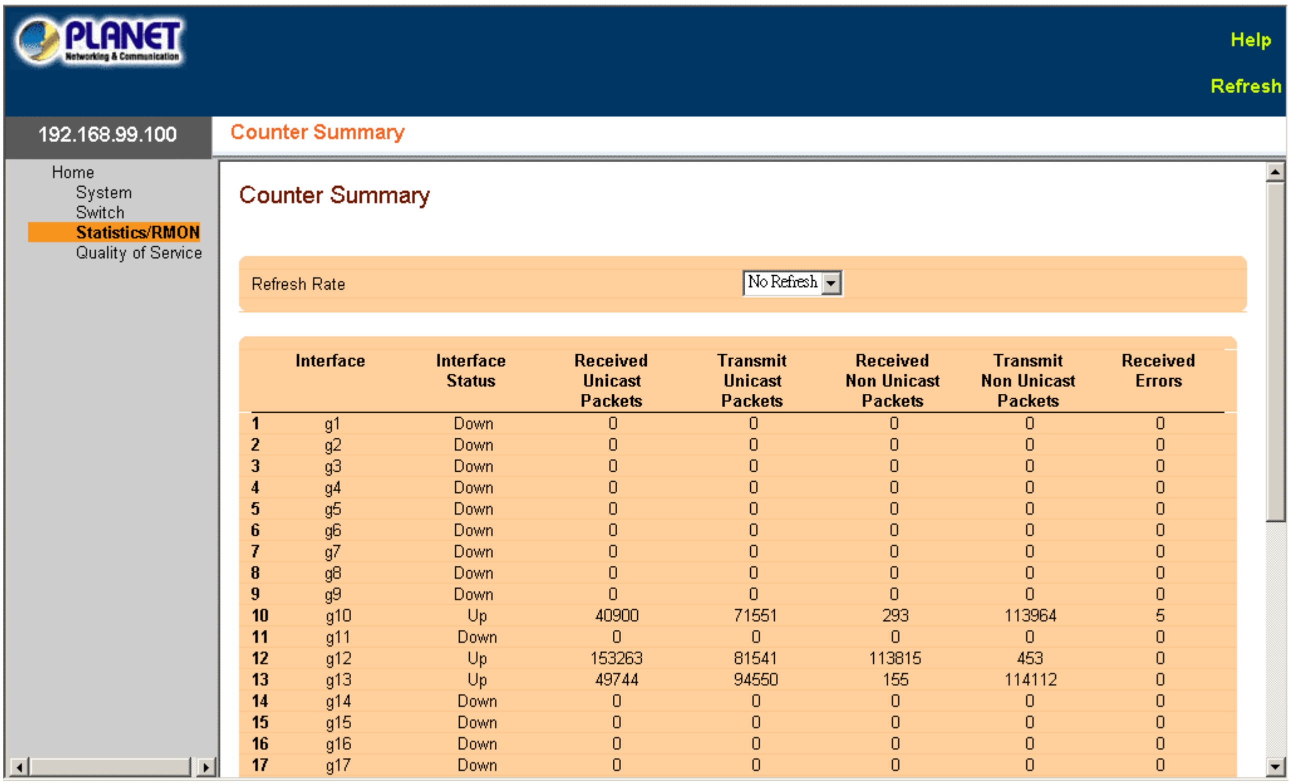
- **Refresh Rate --** The amount of time that passes before the interface statistics are refreshed.
- **Interface --** The interface number.
- **Interface Status --** Status of the interface.
- **Interface Utilization --** Network interface utilization percentage based on the duplex mode of the interface. The range of this reading is from 0 to 200%. The maximum reading of 200% for a full duplex connection indicates that 100% of bandwidth of incoming and outgoing connections is used by the traffic travelling through the interface. The maximum reading for a half duplex connection is 100%.
- **Unicast Received --** Percentage of Unicast packets received on the interface.
- **Non Unicast Packets Received --** Percentage of non-Unicast packets received on the interface.
- **Error Packets Received --** Number packets with errors received on the interface.
- **Global System LAG --** Current LAG/trunk performance.

3.2.4.1.2 Counter Summary

The **Counter Summary** page contains statistics for port utilization in numeric sums as opposed to percentages.

To open **Counter Summary** screen perform the folling:

1. Click Statics/RMON -> Table Views -> Counter Summary
2. The Counter Summary screen is displayed as in Figure 3-74



Counter Summary

Refresh Rate: No Refresh

	Interface	Interface Status	Received Unicast Packets	Transmit Unicast Packets	Received Non Unicast Packets	Transmit Non Unicast Packets	Received Errors
1	g1	Down	0	0	0	0	0
2	g2	Down	0	0	0	0	0
3	g3	Down	0	0	0	0	0
4	g4	Down	0	0	0	0	0
5	g5	Down	0	0	0	0	0
6	g6	Down	0	0	0	0	0
7	g7	Down	0	0	0	0	0
8	g8	Down	0	0	0	0	0
9	g9	Down	0	0	0	0	0
10	g10	Up	40900	71551	293	113964	5
11	g11	Down	0	0	0	0	0
12	g12	Up	153263	81541	113815	453	0
13	g13	Up	49744	94550	155	114112	0
14	g14	Down	0	0	0	0	0
15	g15	Down	0	0	0	0	0
16	g16	Down	0	0	0	0	0
17	g17	Down	0	0	0	0	0

Figure 3-74 Counter Summary screen

The page includes the following fields:

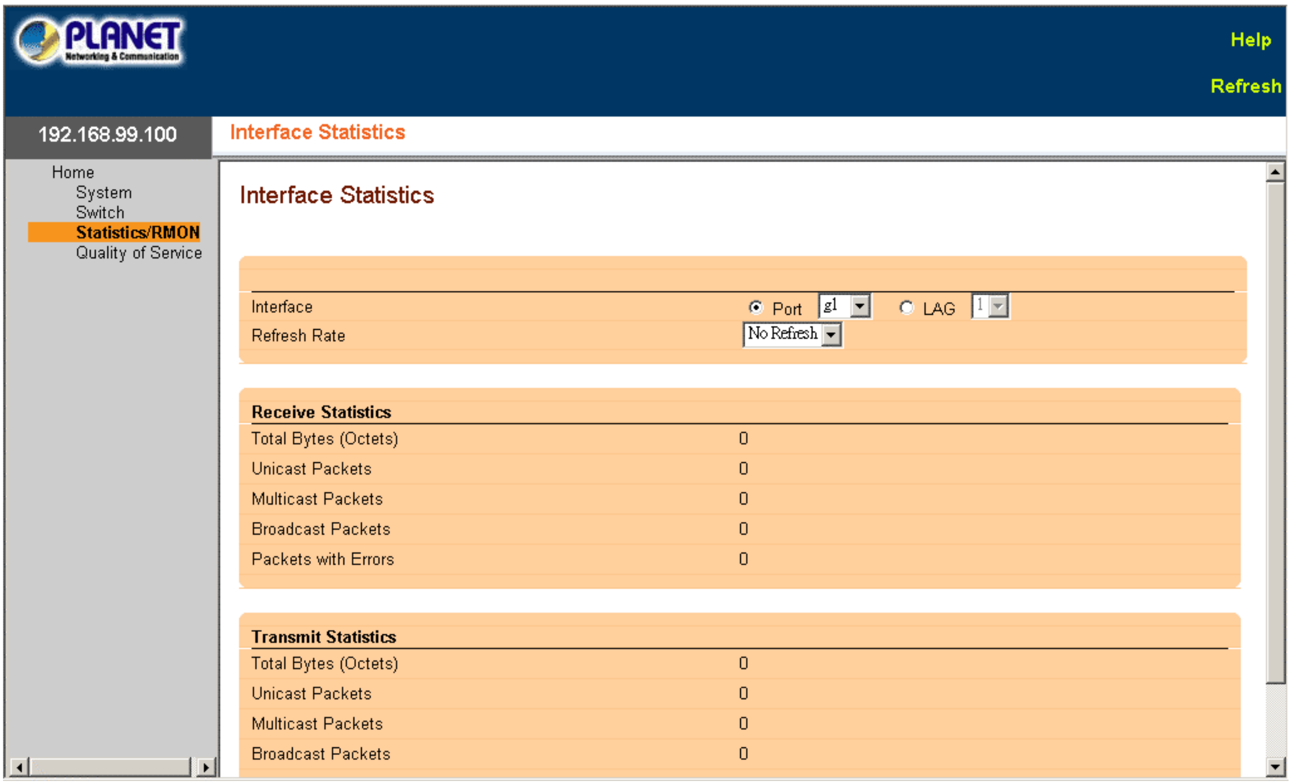
- **Refresh Rate --** The amount of time that passes before the interface statistics are refreshed.
- **Interface --** The interface number.
- **Interface Status --** The interface status.
- **Received Unicast Packets --** Number of received Unicast packets on the interface.
- **Received Non Unicast Packets --** Number of received non-Unicast packets on the interface.
- **Transmit Unicast Packets --** Number of transmitted Unicast packets from the interface.
- **Transmit Non Unicast Packets --** Number of transmitted non-Unicast packets from the interface.
- **Received Errors --** The number of error packets received on the interface.
- **Global System LAG --** Current LAG/trunk performance.

3.2.4.1.3 Interface Statistics

The Interface Statistics page contains statistics for both received and transmitted packets. The fields for both received and transmitted packets are identical.

To open **Interface Statistics** screen perform the folling:

1. Click Statics/RMON -> Table Views -> Interface Statistics
2. The Interface Statistics screen is displayed as in Figure 3-75



Interface Statistics

Interface	● Port g1 ○ LAG 1
Refresh Rate	No Refresh

Receive Statistics	
Total Bytes (Octets)	0
Unicast Packets	0
Multicast Packets	0
Broadcast Packets	0
Packets with Errors	0

Transmit Statistics	
Total Bytes (Octets)	0
Unicast Packets	0
Multicast Packets	0
Broadcast Packets	0

Figure 3-75 Interface Statistics

The Interface Statistics page is divided into the following sections:

- **Statistics Selection**
- **Receive Statistics**
- **Transmit Statistics**

Statistics Selection

The Statistics Selection section contains the following fields:

- **Interface --** Specifies whether statistics are displayed for a port or LAG.
- **Refresh Rate --** Number of time that passes before the interface statistics are refreshed.

Receive Statistics

The Receive Statistics section contains the following fields:

- **Total Bytes (Octets) --** Number of octets received on the selected interface.
- **Unicast Packets --** Number of Unicast packets received on the selected interface.
- **Multicast Packets --** Number of Multicast packets received on the selected interface.
- **Broadcast Packets --** Number of Broadcast packets received on the selected interface.
- P**ackets with Errors --** Number of error packets received on the selected interface.

Transmit Statistics

The Transmit Statistics section contains the following fields:

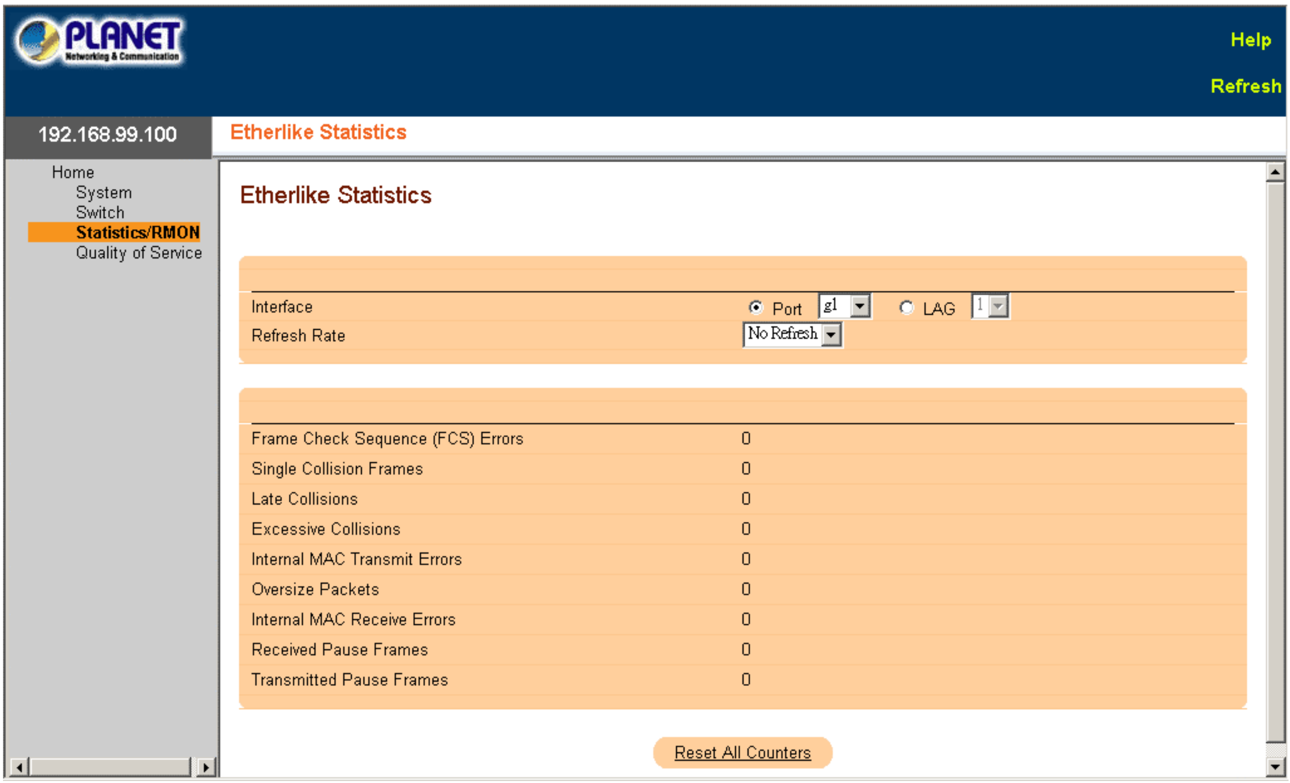
- **Total Bytes (Octets) --** Number of octets transmitted on the selected interface.
- **Unicast Packets --** Number of Unicast packets transmitted on the selected interface.
- **Multicast Packets --** Number of Multicast packets transmitted on the selected interface.
- **Broadcast Packets --** Number of Broadcast packets transmitted on the selected interface.
- **Packets with Errors --** Number of error packets transmitted on the selected interface.

3.2.4.1.4 Etherlink Statistics

The **Etherlike Statistics** page contains interface statistics.

To open **Etherlink Statistics** screen perform the folling:

1. Click Statics/RMON -> Table Views -> Etherlink Statistics
2. The Etherlink Statistics screen is displayed as in Figure 3-76



Etherlike Statistics

Etherlike Statistics

Interface	● Port g1 ○ LAG 1
Refresh Rate	No Refresh

Frame Check Sequence (FCS) Errors	0
Single Collision Frames	0
Late Collisions	0
Excessive Collisions	0
Internal MAC Transmit Errors	0
Oversize Packets	0
Internal MAC Receive Errors	0
Received Pause Frames	0
Transmitted Pause Frames	0

Figure 3-76 Etherlink Statistics screen

The page includes the following fields:

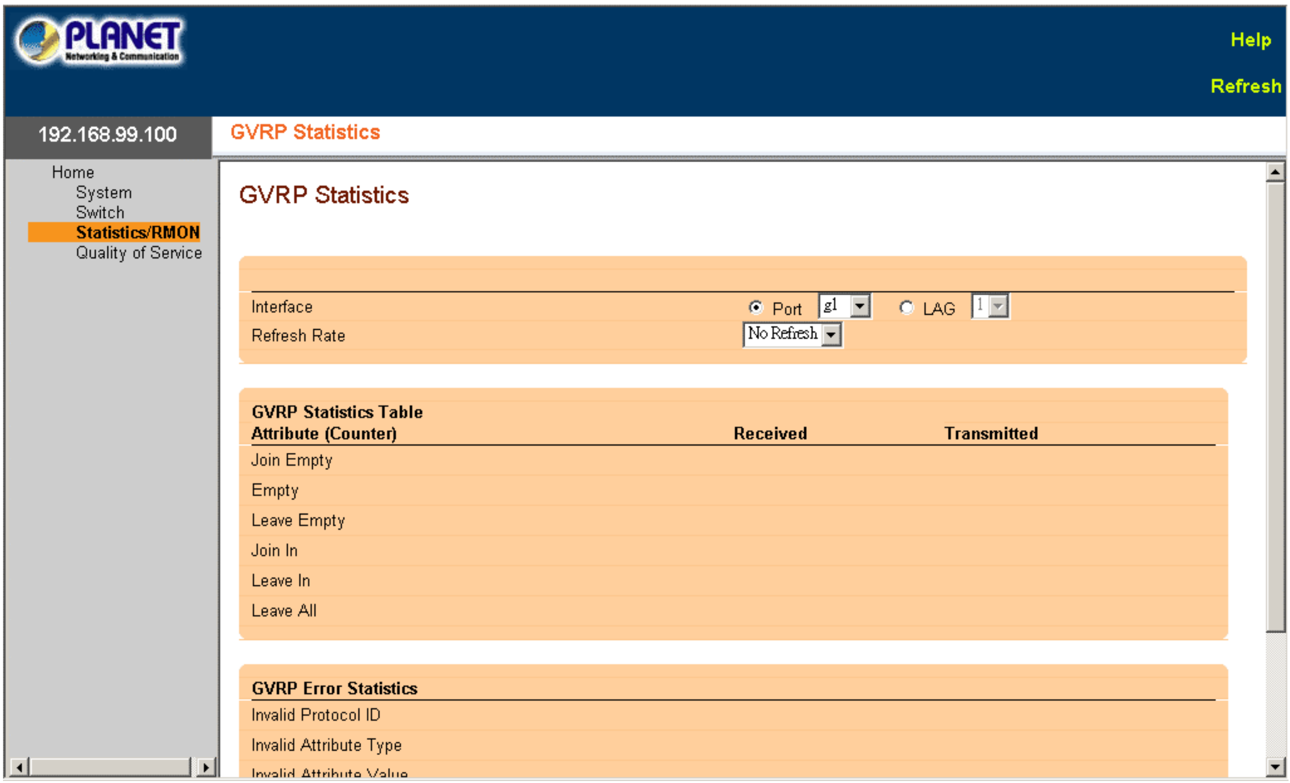
- **Interface --** Specifies whether statistics are displayed for a port or LAG.
- **Refresh Rate --** Amount of time that passes before the interface statistics are refreshed.
- **Frame Check Sequence (FCS) Errors --** Number of FCS errors received on the selected interface.
- **Single Collision Frames --** Number of single collision frames received on the selected interface.
- **Multiple Collision Frames --** Number of multiple collisions frames received on the selected interface.
- **Single Quality Error (SQE) Test Errors --** Number of SQE test errors received on the selected interface.
- **Deferred Transmissions --** Number of deferred transmissions on the selected interface.
- **Late Collisions --** Number of late collisions received on the selected interface.
- **Excessive Collisions --** Number of excessive collisions received on the selected interface.
- **Internal MAC Transmit Errors --** Number of internal MAC transmit errors on the selected interface.
- **Carrier Sense Errors --** Number of carrier sense errors on the selected interface.
- **Oversize Packets --** Number of oversized packet errors on the selected interface.
- **Internal MAC Receive Errors --** Number of internal MAC received errors on the selected interface.
- **Single Quality Errors (SQE) Test Errors --** The amount of SQE test errors received on the selected interface.
- **Receive Pause Frames --** Number of received paused frames on the selected interface.
- **Transmitted Paused Frames --** The number of Pause Frames transmitted from the selected interface.

3.2.4.1.5 GVRP Statistics

The **GVRP Statistics** page contains device statistics for GVRP.

To open **GVRP Statistics** screen perform the folling:

1. Click Statics/RMON -> Table Views -> GVRP Statistics
2. The GVRP Statistics screen is displayed as in Figure 3-77



GVRP Statistics

Interface ● Port g1 ○ LAG 1

Refresh Rate No Refresh

GVRP Statistics Table

Attribute (Counter)	Received	Transmitted
Join Empty		
Empty		
Leave Empty		
Join In		
Leave In		
Leave All		

GVRP Error Statistics

Invalid Protocol ID

Invalid Attribute Type

Invalid Attribute Value

Figure 3-76 GVRP Statistics screen

The Interface Statistics page is divided into the following sections:

- **Statistics Selection**
- **GVRP Statistics Table Attribute (Counter)**
- **GVRP Error Statistics**

Statistics Selection

- **Interface --** Specifies whether statistics are displayed for a port or LAG.
- **Refresh Rate --** Amount of time that passes before the interface statistics are refreshed.

GVRP Statistics Table Attribute (Counter)

- **Join Empty --** Device GVRP Join Empty statistics.
- **Empty --** Device GVRP Empty statistics.
- **Leave Empty --** Device GVRP Leave Empty statistics.
- **Join In --** Device GVRP Join In statistics.
- **Leave In --** Device GVRP Leave In statistics.
- **Leave All --** Device GVRP Leave all statistics.

GVRP Error Statistics

- **Invalid Protocol ID --** Device GVRP Invalid Protocol ID statistics.

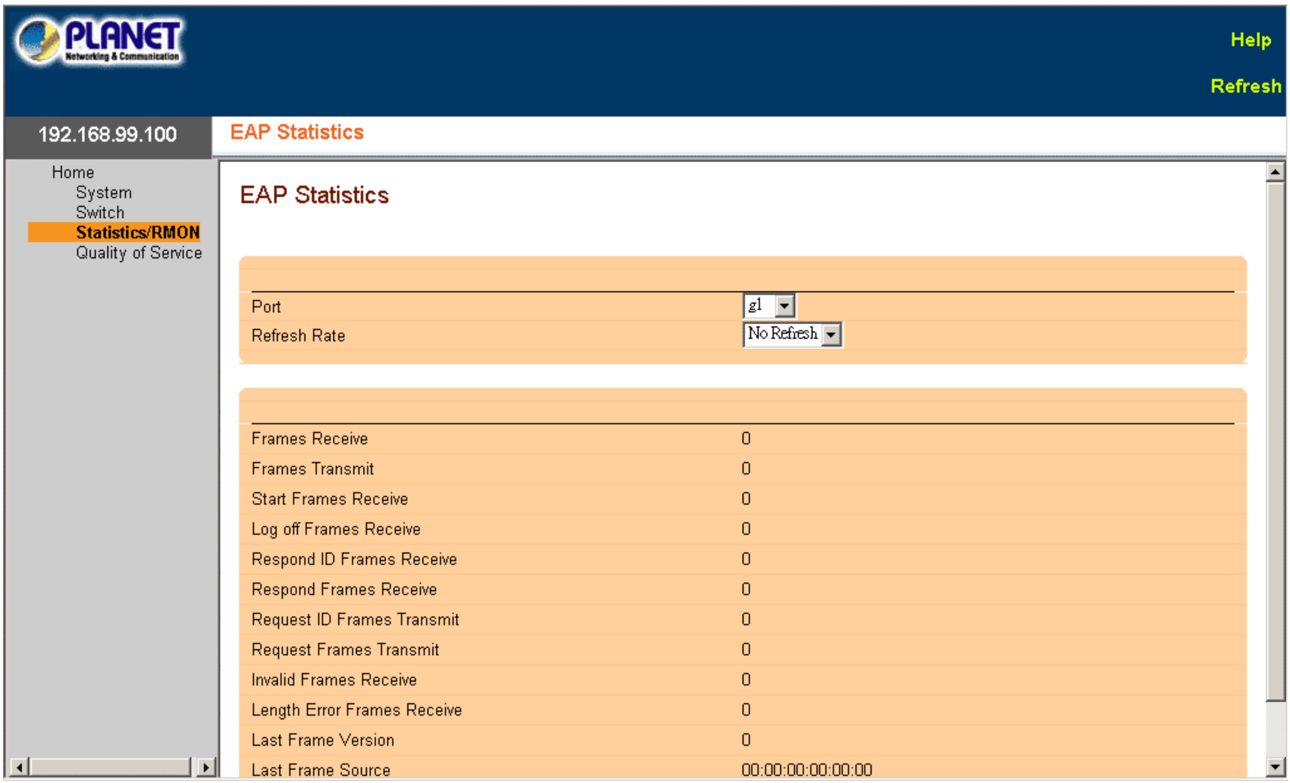
- **Invalid Attribute Type --** Device GVRP Invalid Attribute ID statistics.
- **Invalid Attribute Value --** Device GVRP Invalid Attribute Value statistics.
- **Invalid Attribute Length --** Device GVRP Invalid Attribute Length statistics.
- **Invalid Events --** Device GVRP Invalid Events statistics.

3.2.4.1.6 EAP Statistics

The **EAP Statistics** page contains information about EAP packets received on a specific port. For more information about EAP, see "Port Based Authentication (802.1x)".

To open **EAP Statistics** screen perform the folling:

1. Click Statics/RMON -> Table Views -> EAP Statistics
2. The EAP Statistics screen is displayed as in Figure 3-78



EAP Statistics

Port	g1
Refresh Rate	No Refresh

Frames Receive	0
Frames Transmit	0
Start Frames Receive	0
Log off Frames Receive	0
Respond ID Frames Receive	0
Respond Frames Receive	0
Request ID Frames Transmit	0
Request Frames Transmit	0
Invalid Frames Receive	0
Length Error Frames Receive	0
Last Frame Version	0
Last Frame Source	00:00:00:00:00:00

Figure 3-78 EAP Statistics screen

The page includes the following fields:

- **Port --** The port which is polled for statistics.
- **Refresh Rate --** Amount of time that passes before the interface statistics are refreshed.
- **Frames Receive --** The number of valid EAPOL frames received on the port.
- **Frames Transmit --** The number of EAPOL frames transmitted via the port.
- **Start Frames Receive --** The number of EAPOL Start frames received on the port.
- **Log off Frames Receive --** The number of EAPOL Logoff frames that have been received on the port.
- **Respond ID Frames Receive --** The number of EAP Resp/Id frames that have been received on the port.
- **Respond Frames Receive --** The number of valid EAP Response frames received on the port.
- **Request ID Frames Transmit --** The number of EAP Requested ID frames transmitted via the port.
- **Request Frames Transmit --** The number of EAP Request frames transmitted via the port.
- **Invalid Frames Receive --** The number of unrecognized EAPOL frames received on this port.
- **Length Error Frames Receive --** The number of EAPOL frames with an invalid Packet Body Length received on this port.

- **Last Frame Version --** The protocol version number attached to the most recently received EAPOL frame.
- **Last Frame Source --** The source MAC address attached to the most recently received EAPOL frame.

3.2.4.2 RMON

Remote Monitoring (RMON) allows network managers to view network information from a remote location.

The page includes the following fields:

The RMON page contains links to the following topics:

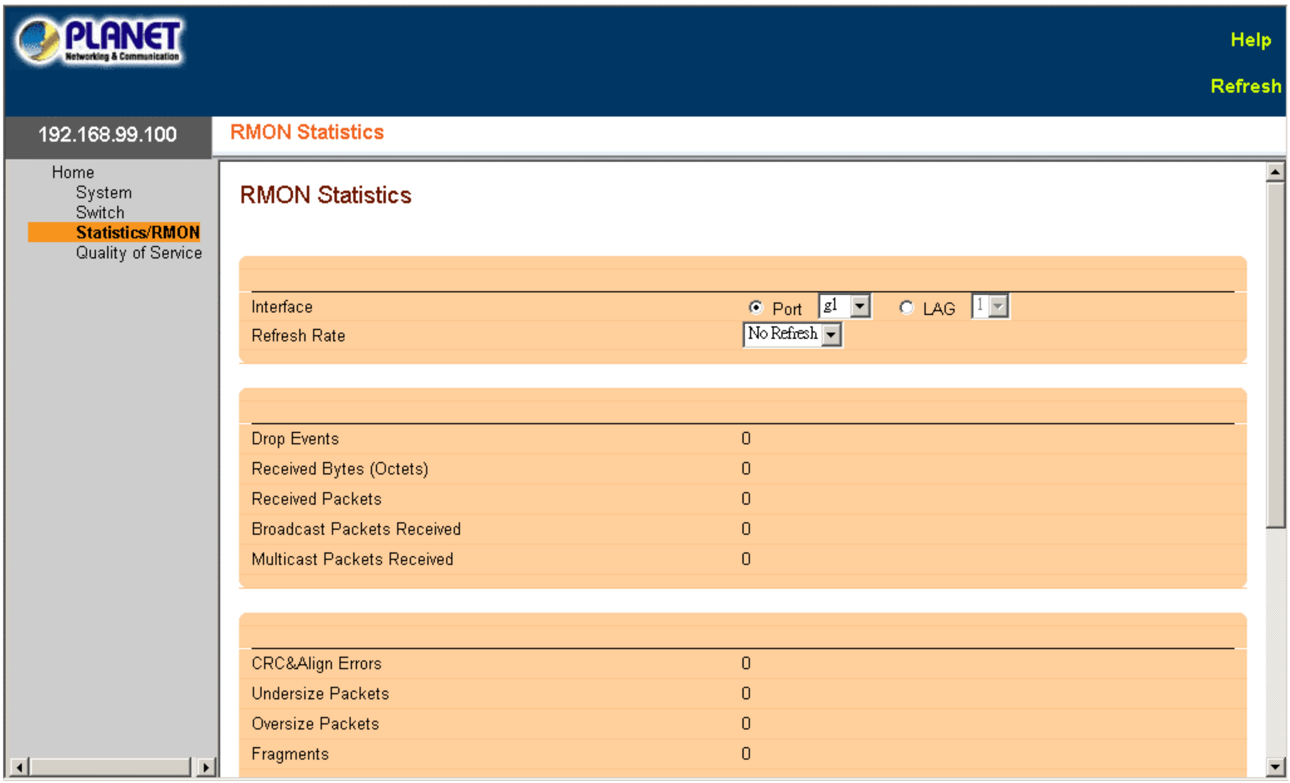
- **Statistics**
- **History Control**
- **History Table**
- **Events Control**
- **Events Log**
- **Alarms**

3.2.4.2.1 RMON Statistics

The **RMON Statistics Group** page contains fields for viewing information about device utilization and errors that occurred on the device.

To open **EAP Statistics** screen perform the folling:

1. Click Statics/RMON -> RMON -> Statistics
2. The Statistics screen is displayed as in Figure 3-79



RMON Statistics

Interface ● Port g1 ○ LAG 1
Refresh Rate No Refresh

Drop Events 0
Received Bytes (Octets) 0
Received Packets 0
Broadcast Packets Received 0
Multicast Packets Received 0

CRC&Align Errors 0
Undersize Packets 0
Oversize Packets 0
Fragments 0

Figure 3-79 RMON Statistics screen

The page includes the following fields:

- **Interface --** Specifies the port or LAG for which statistics are displayed.
- **Refresh Rate --** Amount of time that passes before the statistics are refreshed.
- **Drop Events --** Number of dropped events that have occurred on the interface since the device was last refreshed.

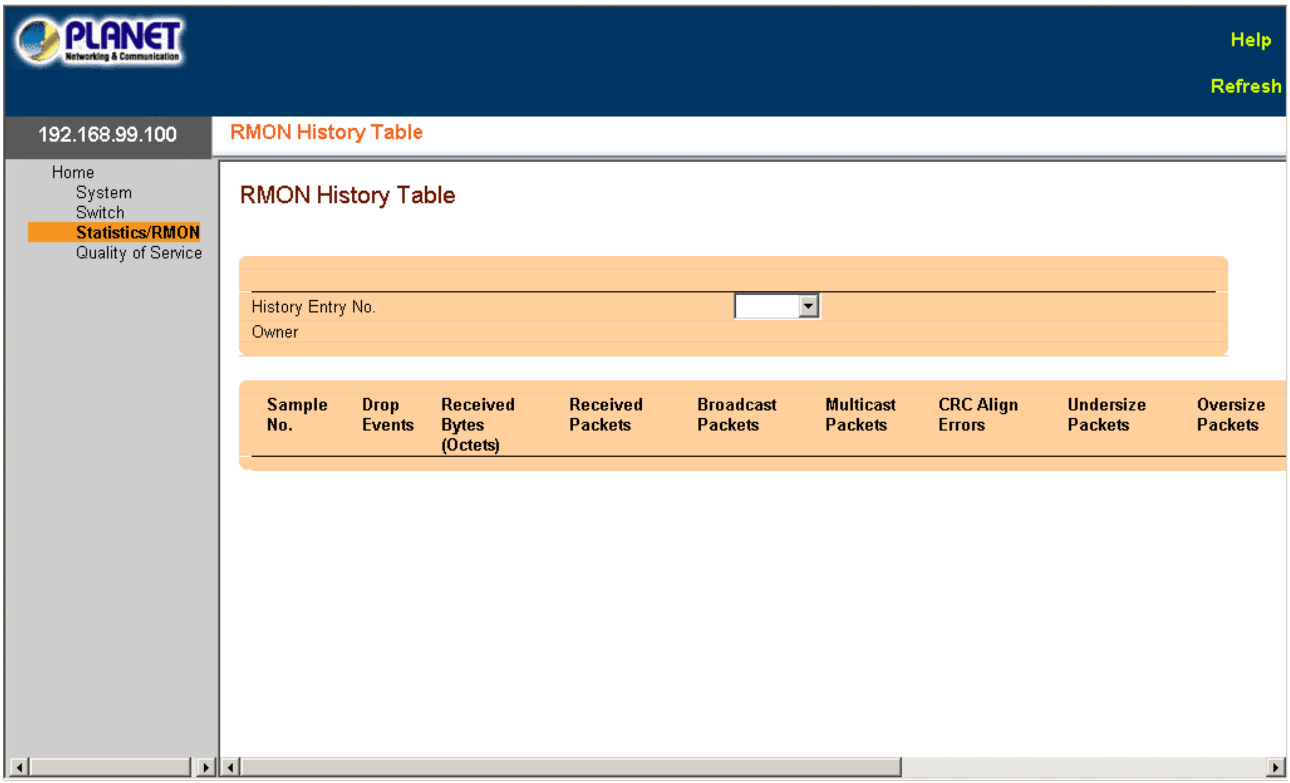
- **Received Bytes (Octets) --** Number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.
- **Received Packets --** Number of packets received on the interface, including bad packets, Multicast and broadcast packets, since the device was last refreshed.
- **Broadcast Packets Received --** Number of good broadcast packets received on the interface since the device was last refreshed. This number does not include Multicast packets.
- **Multicast Packets Received --** Number of good Multicast packets received on the interface since the device was last refreshed.
- **CRC & Align Errors --** Number of CRC and Align errors that have occurred on the interface since the device was last refreshed.
- **Undersize Packets --** Number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.
- **Oversize Packets --** Number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.
- **Fragments --** Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.
- **Jabbers --** The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). The allowed range to detect jabber is between 20 ms and 150 ms.
- **Collisions --** Number of collisions received on the interface since the device was last refreshed

3.2.4.2.2 RMON History Control

The **RMON History Control** page contains information about samples of data taken from ports. For example, the samples may include interface definitions or polling periods.

To open **RMON History Control** screen perform the folling:

1. Click Statics/RMON -> RMON -> History Control
2. The RMON History Control screen is displayed as in Figure 3-80



RMON History Table

History Entry No.	
Owner	

Sample No.	Drop Events	Received Bytes (Octets)	Received Packets	Broadcast Packets	Multicast Packets	CRC Align Errors	Undersize Packets	Oversize Packets

Figure 3-80 RMON History Control screen

The page includes the following fields:

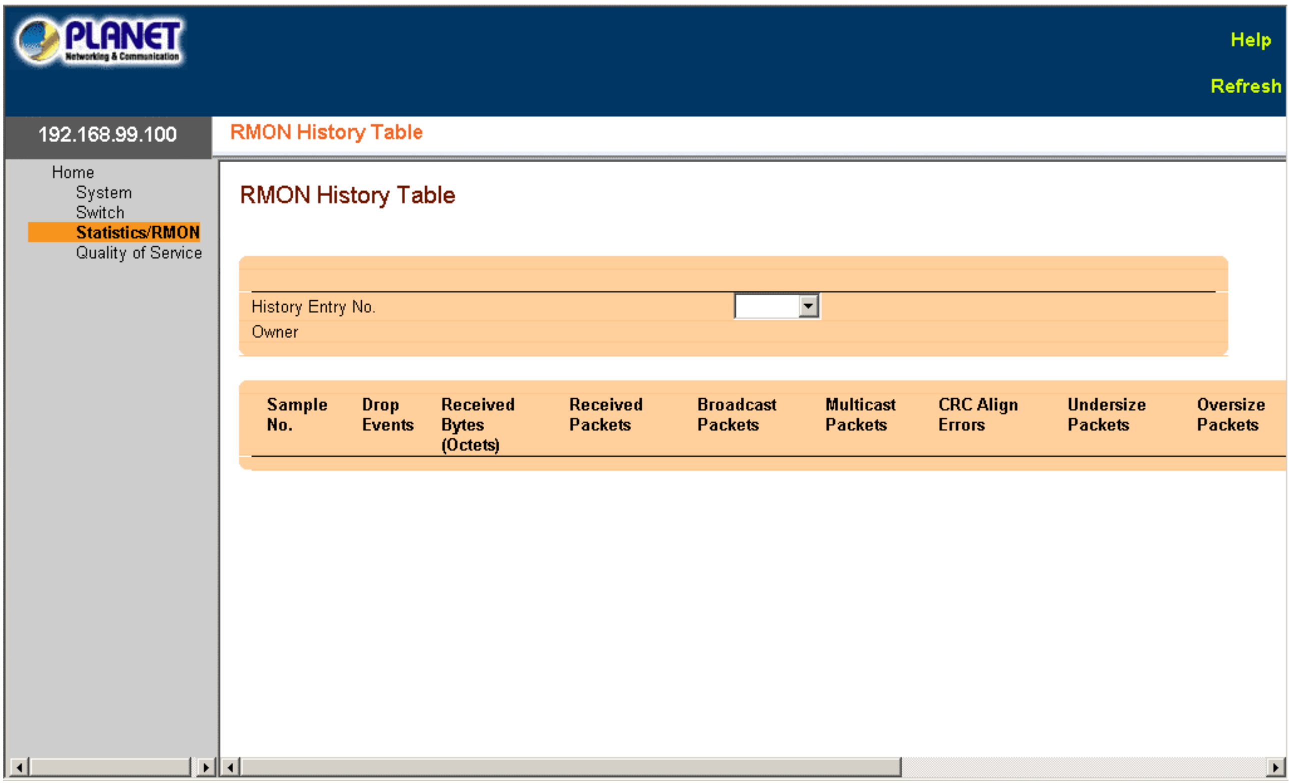
- **History Entry No. --** Entry number for the History Control Table page.
- **Source Interface --** Port or LAG from which the history samples were taken.
- **Owner (0-20 characters) --** RMON station or user that requested the RMON information.
- **Max No. of Samples to Keep (1-65535) --** Number of samples to be saved. The default value is 50.
- **Current No. of Samples in List --** The current number of samples taken.
- **Sampling Interval (1-3600) --** Indicates in seconds the time that samples are taken from the ports. The possible values are 1-3600 seconds. The default is 1800 seconds (30 minutes).
- **Remove --** When selected, removes the History Control Table entry.

3.2.4.2.3 RMON History Table

The **RMON History Table** contains interface specific statistical network samplings. Each table entry represents all counter values compiled during a single sample.

To open **RMON History Control** screen perform the folling:

1. Click Statics/RMON -> RMON -> History Table
2. The RMON History Table screen is displayed as in Figure 3-81



RMON History Table

History Entry No.	
Owner	

Sample No.	Drop Events	Received Bytes (Octets)	Received Packets	Broadcast Packets	Multicast Packets	CRC Align Errors	Undersize Packets	Oversize Packets

Figure 3-82 RMON History Table screen

The page includes the following fields:

- **Sample No. --** The specific sample the information in the table reflects.
- **Drop Events --** The number of dropped packets due to lack of network resources during the sampling interval. This may not represent the exact number of dropped packets, but rather the number of times dropped packets were detected.
- **Received Bytes (Octets) --** The number of data octets, including bad packets, received on the network.
- **Received Packets --** The number of packets received during the sampling interval.
- **Broadcast Packets --** The number of good broadcast packets received during the sampling interval.
- **Multicast Packets --** The number of good Multicast packets received during the sampling interval.
- **CRC Align Errors --** The number of packets received during the sampling session with a length of 64-1518 octets, a bad Frame Check Sequence (FCS), and with an integral number of octets, or a bad FCS with a non-integral number.

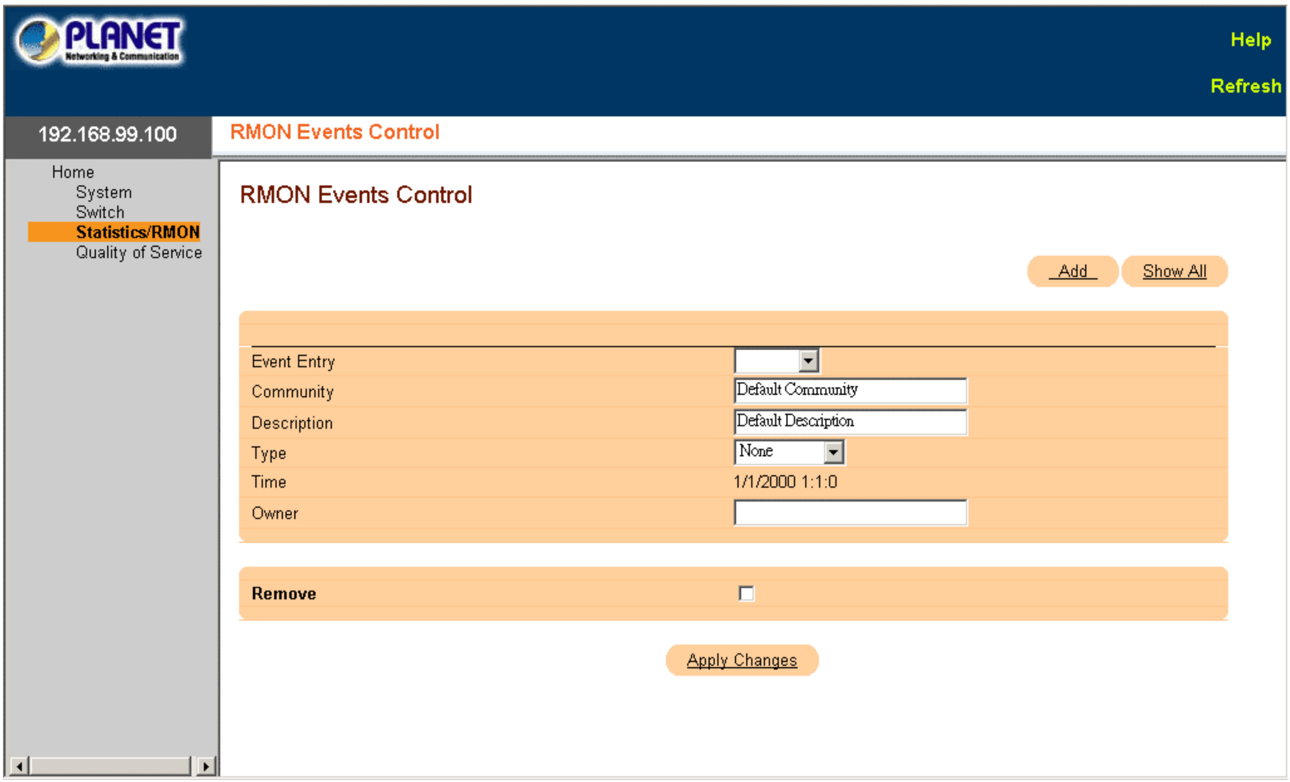
- **Undersize Packets --** The number of packets received less than 64 octets long during the sampling session.
- **Oversize Packets --** The number of packets received more than 1518 octets long during the sampling session.
- **Fragments --** The number of packets received less than 64 octets long and had a FCS during the sampling session.
- **Jabbers --** The number of packets received more than 1518 octets long and had a FCS during the sampling session.
- **Collisions --** Estimates the total number of packet collisions that occurred during the sampling session. Collisions are detected when repeater ports detects two or more stations transmit simultaneously.
- **Utilization --** Estimates the main physical layer network usage on an interface during the session sampling. The value is reflected in hundredths of a percent.

3.2.4.2.4 RMON Events Control

The **RMON Events Control** page contains fields for defining RMON events.

To open **RMON History Control** screen perform the folling:

1. Click Statics/RMON -> RMON -> Events Control
2. The RMON Events Control screen is displayed as in Figure 3-82



RMON Events Control

Event Entry	
Community	Default Community
Description	Default Description
Type	None
Time	1/1/2000 1:1:0
Owner	

Remove □

Figure 3-82 RMON Events Control screen

The page includes the following fields:

- **Event Entry --** The event.
- **Community --** Community to which the event belongs.
- **Description --** User-defined event description.
- **Type --** Describes the event type. Possible values are:
- **Log --** Event type is a log entry.
- **Trap --** Event type is a trap.
- **Log and Trap --** Event type is both a log entry and a trap.
- None -- There is no event.

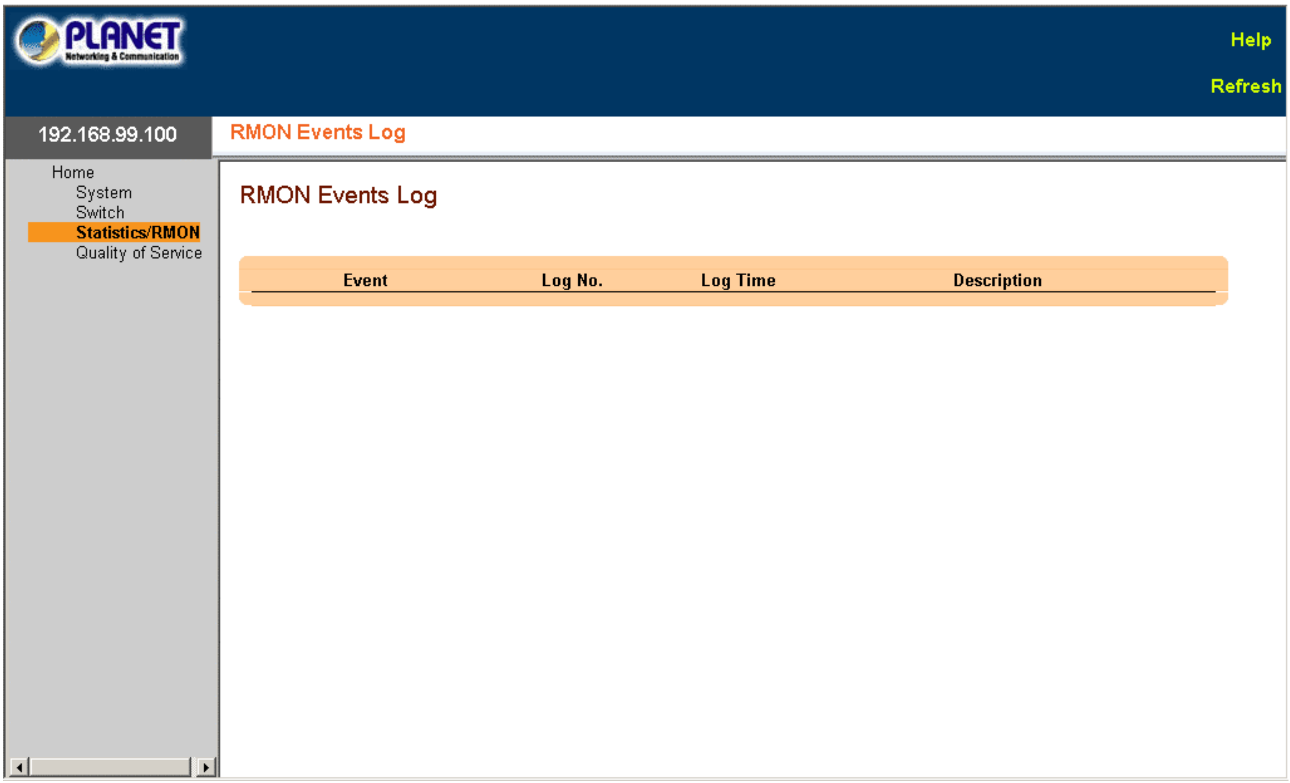
- **Time --** Time when the event occurred for example 29 March 2004 at 11:00am is displayed as 29/03/2004 11:00:00.
- **Owner --** The device or user that defined the event.
- **Remove --** When selected, removes the event from the RMON Events Table.

3.2.4.2.5 RMON Events Log

The **RMON Events Log** page contains a list of RMON events.

To open **RMON Event Log** screen perform the folling:

1. Click Statics/RMON -> RMON -> Events Log
2. The RMON Events Log screen is displayed as in Figure 3-83



RMON Events Log

Event	Log No.	Log Time	Description

Figure 3-83 RMON Event Log screen

The page includes the following fields:

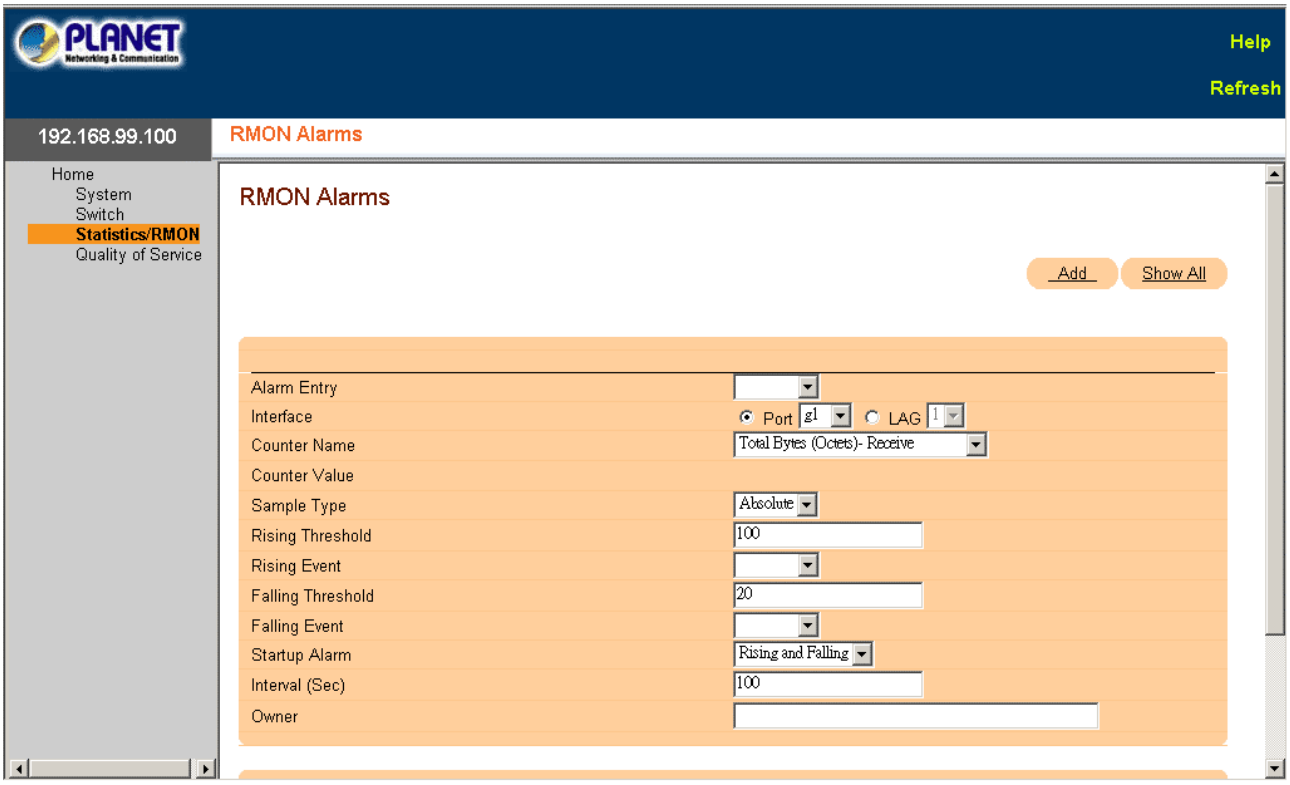
- **Event --** The RMON Events Log entry number.
- **Log No.--** The log number.
- **Log Time --** Time when the log entry was entered.
- **Description --** Describes the log entry.

3.2.4.2.6 RMON Alarms

The **RMON Alarms** page contains fields for setting network alarms. Network alarms occur when a network problem, or event, is detected. Rising and falling thresholds generate events.

To open **RMON Event Log** screen perform the folling:

1. Click Statics/RMON -> RMON -> Alarms
2. The Alarms screen is displayed as in Figure 3-84



RMON Alarms

Alarm Entry	
Interface	● Port g1 ○ LAG 1
Counter Name	Total Bytes (Octets)- Receive
Counter Value	
Sample Type	Absolute
Rising Threshold	100
Rising Event	
Falling Threshold	20
Falling Event	
Startup Alarm	Rising and Falling
Interval (Sec)	100
Owner	

Figure 3-84 RMON Alarm screen

The page includes the following fields:

- **Alarm Entry --** Indicates a specific alarm.
- **Interface --** The interface for which RMON statistics are displayed.
- **Counter Name --** The selected MIB variable.
- **Counter Value --** B class=cBold origTag="Bold" cs="Bold"> The value of the selected MIB variable.
- **Sample Type --** Specifies the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:
- **Delta --** Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.
- **Absolute --** Compares the values directly with the thresholds at the end of the sampling interval.
- **Rising Threshold --** The rising counter value that triggers the rising threshold alarm. The rising threshold is presented on top of the graph bars. Each monitored variable is designated a color.
- **Rising /Falling Event --** The mechanism in which the alarms are reported -- LOG, TRAP, or a combination of both. When LOG is selected, there is no saving mechanism either in the device or in the management system. However, if the device is not being reset, it remains in the device LOG table. If TRAP is selected, an SNMP trap is generated and reported via the trap□ general mechanism. The TRAP can be saved using the same mechanism.
- **Falling Threshold --** The falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on the bottom of the graph bars. Each monitored variable is designated a color.
- **Startup Alarm --** The trigger that activates the alarm generation. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.
- **Interval (sec) --** Alarm interval time.
- **Owner --** Device or user that defined the alarm.
- **Remove --** When selected, removes an RMON Alarm.

3.2.4.3 Charts

The Chart page contains links for displaying statistics in a chart form.

The Chart page contains links to the following topics:

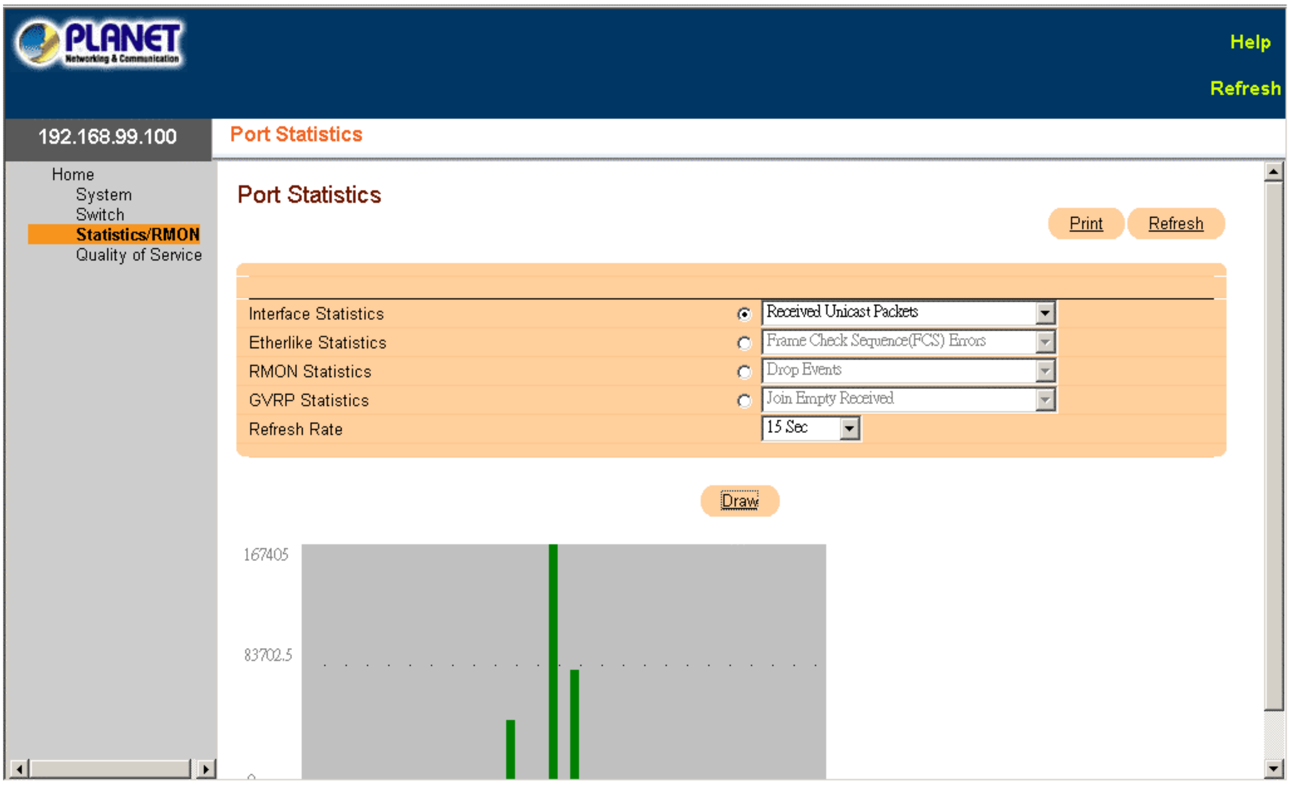
- **Ports**
- **LAGs**

3.2.4.3.1 Ports

The **Port Statistics** page contains fields for opening statistics in a chart form for port elements.

To open **Port Statistics** screen perform the folling:

1. Click Statics/RMON -> Charts -> Ports
2. The Ports Statistics screen is displayed as in Figure 3-85



Port Statistics

Interface Statistics	●	Received Unicast Packets
Etherlike Statistics	○	Frame Check Sequence(FCS) Errors
RMON Statistics	○	Drop Events
GVRP Statistics	○	Join Empty Received
Refresh Rate		15 Sec

Figure 3-85 Port Statistics screen

The page includes the following fields:

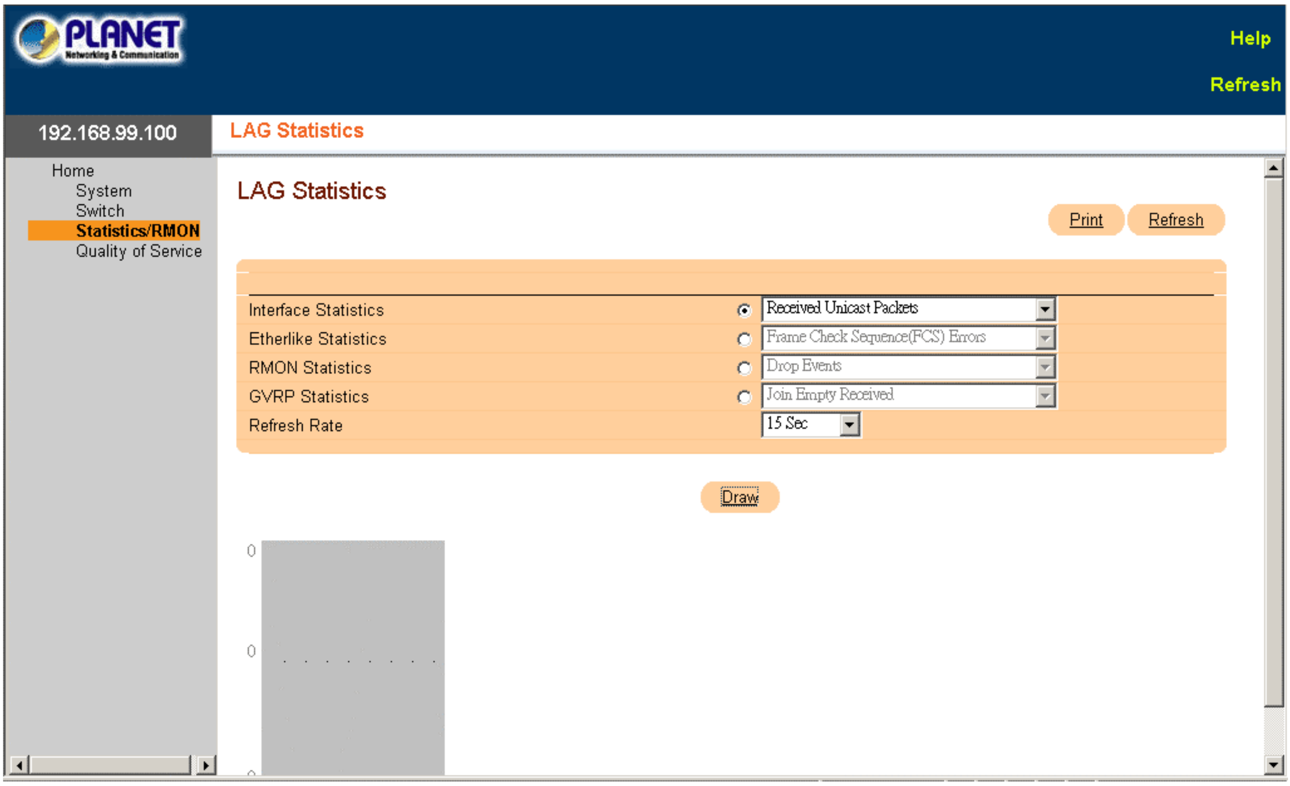
- **Interface Statistics --** Selects the type of interface statistics to open.
- **Etherlike Statistics --** Selects the type of Etherlike statistics to open.
- **RMON Statistics --** Selects the type of RMON statistics to open.
- **GVRP Statistics --** Selects the GVRP statistics type to open.
- **Refresh Rate --** Amount of time that passes before the statistics are refreshed.

3.2.4.3.2 LAG Statistics

The **LAG Statistics** page contains fields for opening statistics in a chart form for LAGs.

To open **Port Statistics** screen perform the folling:

1. Click Statics/RMON -> Charts -> LAGS
2. The LAG Statistics screen is displayed as in Figure 3-86



LAG Statistics

Interface Statistics	●	Received Unicast Packets
Etherlike Statistics	○	Frame Check Sequence(FCS) Errors
RMON Statistics	○	Drop Events
GVRP Statistics	○	Join Empty Received
Refresh Rate		15 Sec

Figure 3-86 LAG Statistics screen

The page includes the following fields:

- **Interface Statistics --** Selects the type of interface statistics to open.
- **Etherlike Statistics --** Selects the type of Etherlike statistics to open.
- **RMON Statistics --** Selects the type of RMON statistics to open.
- **GVRP Statistics --** Selects the type of GVRP statistics to open.
- **Refresh Rate --** Amount of time that passes before the statistics are refreshed.

3.2.4 Configure Quality of Service

This Quality of Service provides information for defining and configuring Quality of Service (QoS) parameters.

The Quality of Service page contains links to the following topics:

- **QoS Global Parameters**

3.2.4.1 Qos Global Parameters

Class of Service global parameters are set from the CoS Global Parameter pages.

The CoS Global Parameters page contains links to the following topics:

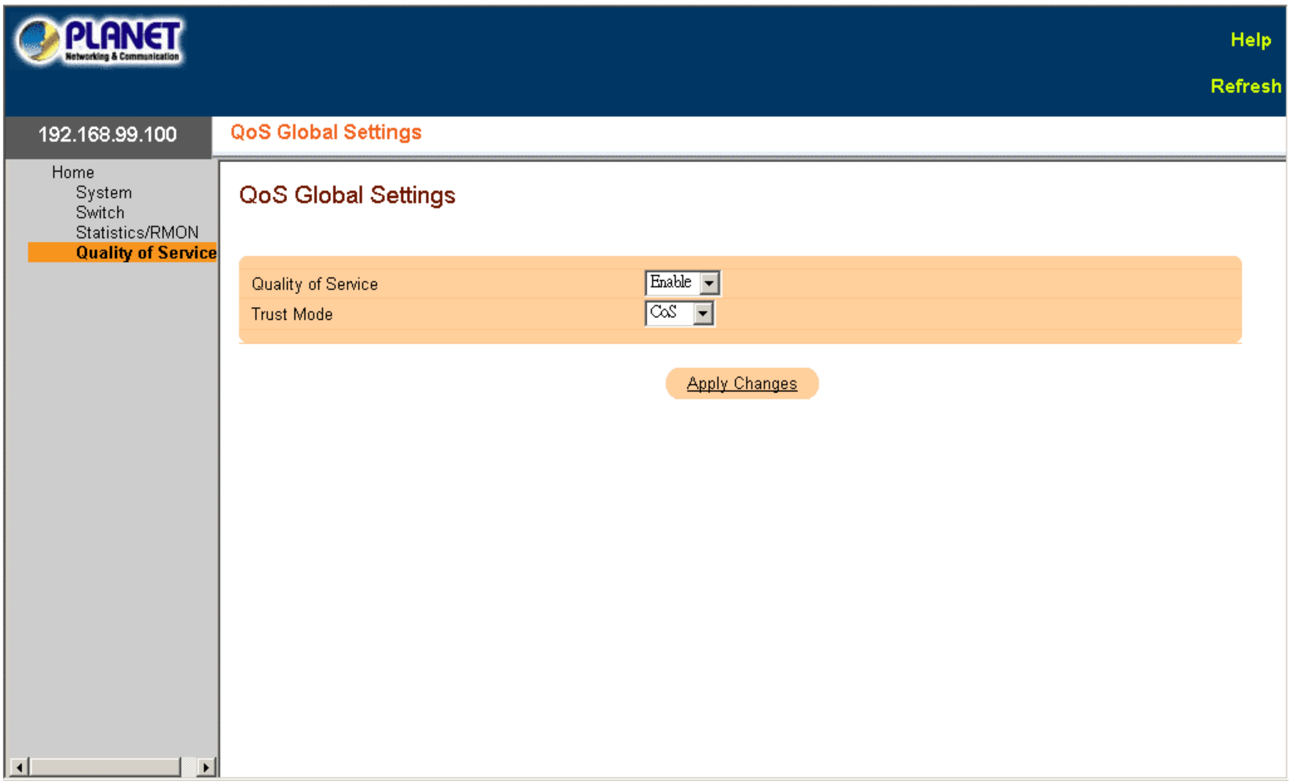
- **QoS Settings**
- **Interface Settings**
- **Queue Settings**
- **CoS to Queue**
- **DSCP to Queue**

3.2.4.1.1 QoS Settings

The **QoS Global Settings** page contains fields for enabling or disabling QoS. In addition, the Trust mode can be selected. The Trust mode relies on predefined fields within the packet to determine the output queue.

To open **QoS Settings** screen perform the folling:

1. Click Quality of Service -> QoS Global Parameters -> QoS Settings
2. The QoS Settings screen is displayed as in Figure 3-87



QoS Global Settings

QoS Global Settings

Quality of Service	Enable
Trust Mode	CoS

Apply Changes

Figure 3-87 QoS Global Settings screen

The page includes the following fields:

- **Quality of Service --** Enables or disables managing network traffic using Quality of Service.
- **Trust Mode --** Determines which packet fields to use for classifying packets entering the device. When no rules are defined the traffic containing the predefined packet field (CoS or DSCP) is mapped according to the relevant trust modes table. Traffic not containing a predefined packet field is mapped to best effort. The possible Trust Mode field values are:
- **CoS --** The output queue assignment is determined by the IEEE802.1p VLAN priority tag (VPT) or by the default VPT assigned to a port.
- **DSCP --** The output queue assignment is determined by the DSCP field.

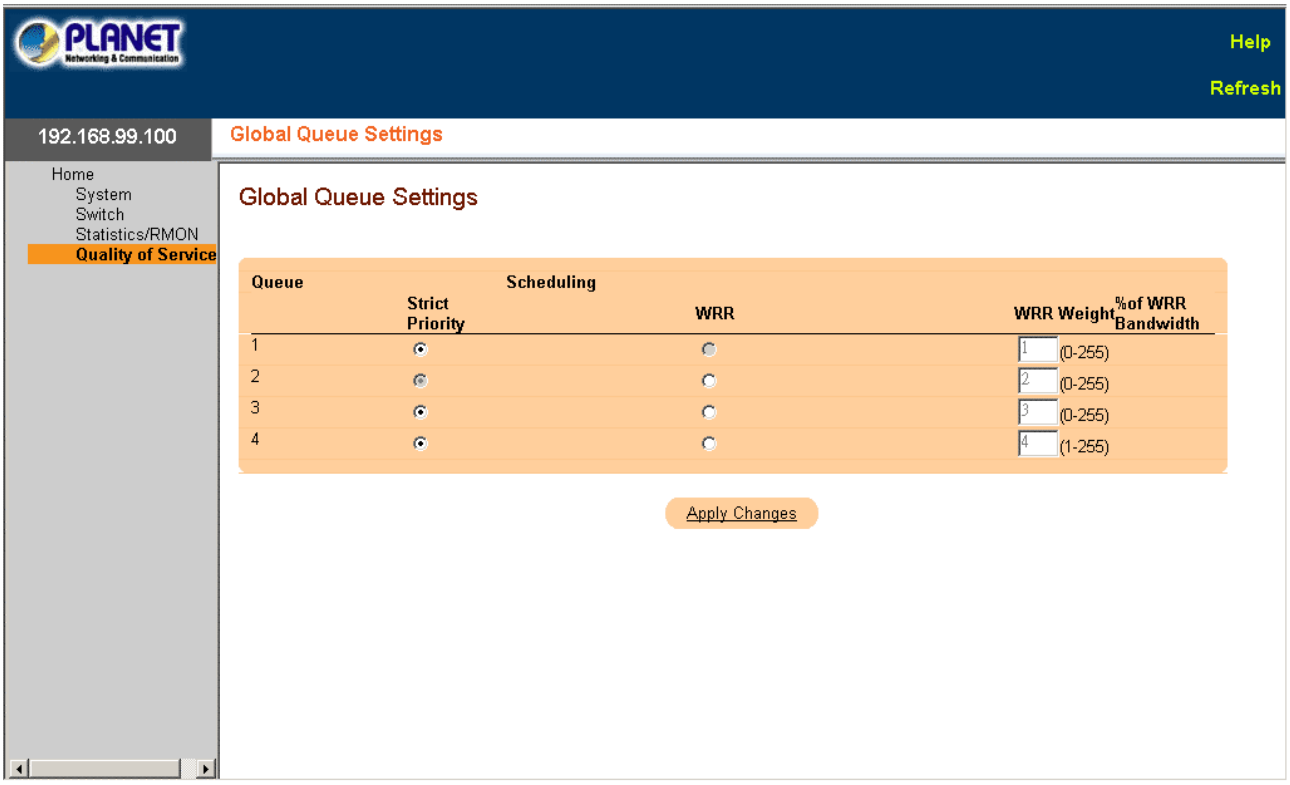
✍ ***Note:*** The interface Trust settings overrides the global Trust setting.

3.2.4.1.2 Queue Settings

The **Global Queue Setting** page contains fields for configuring the scheduling method by which the queues are maintained.

To open **Queue Settings** screen perform the folling:

1. Click Quality of Service -> QoS Global Parameters -> Queue Settings
2. The Queue Settings screen is displayed as in Figure 3-88



Global Queue Settings

Queue	Scheduling			
	Strict Priority	WRR	WRR Weight	%of WRR Bandwidth
1	●	○	1 (0-255)	
2	●	○	2 (0-255)	
3	●	○	3 (0-255)	
4	●	○	4 (1-255)	

Figure 3-88 Global Queue Settings screen

The page includes the following fields:

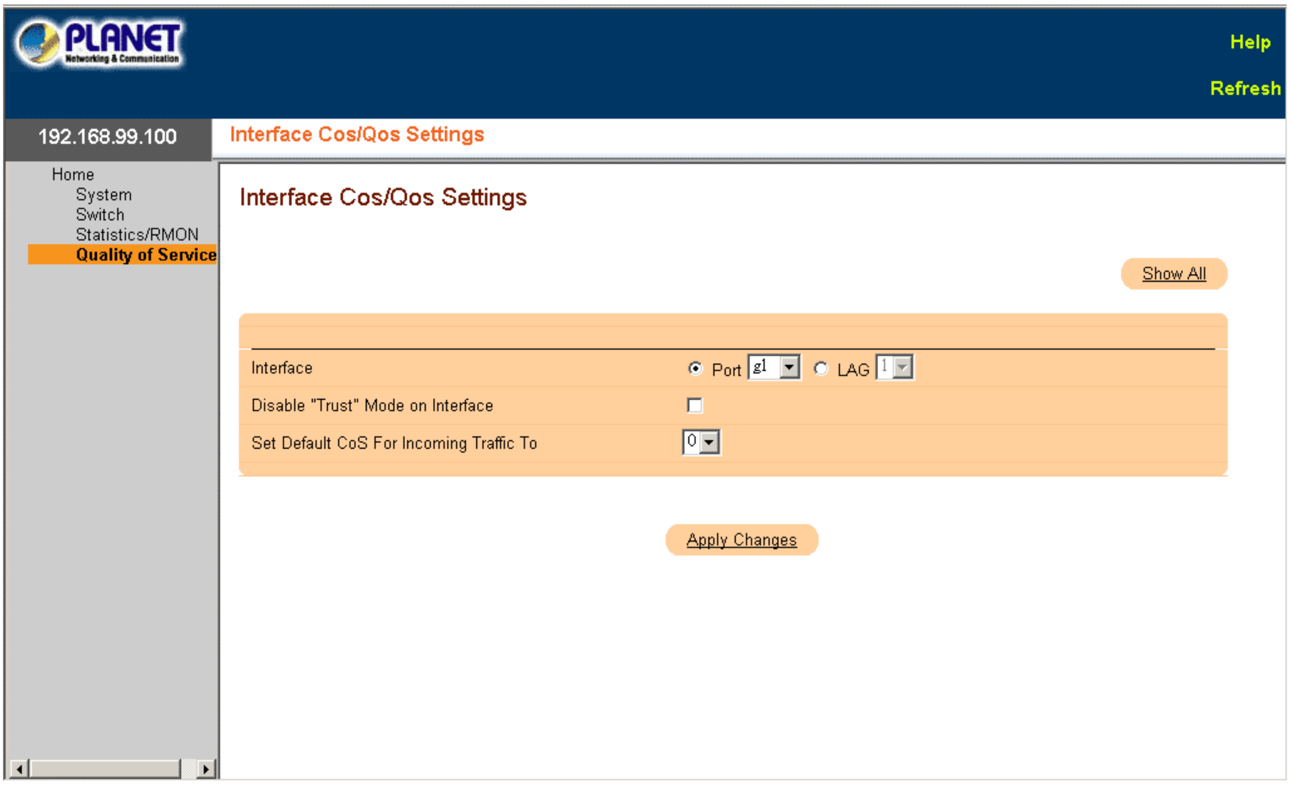
- **Queues --** The Queue number.
- **Strict Priority --** Specifies if traffic scheduling is based strictly on the queue priority. The default is enabled.
- **WRR --** Specifies if traffic scheduling is based on the Weighted Round Robin (WRR) weights to egress queues

3.2.4.1.3 Interface Settings

The **Interface Settings** page contains fields for defining, per interface, if the selected Trust mode is to be activated. The default priority for incoming untagged packets is also selected in the Interface Settings page.

To open **Interface Settings** screen perform the folling:

1. Click Quality of Service -> QoS Global Parameters -> Interface Settings
2. The Interface Settings screen is displayed as in Figure 3-89



Interface Cos/Qos Settings

Interface	● Port g1 ○ LAG 1
Disable "Trust" Mode on Interface	□
Set Default CoS For Incoming Traffic To	0

Figure 3-89 Interface Cos/Qos Settings screen

The page contains the following areas:

- **Interface Setting**
- **Queue Settings**

Interface Settings Area

The Interface Settings area includes the following fields:

- **Interface --** The specific port, LAG to configure:
- **Disable "Trust" Mode on Interface --** Disables Trust values on the device. For more information on Trust settings, see "Configuring Global CoS Settings".
- **Set Default CoS For Incoming Traffic To --** Sets the default CoS tag value untagged packets. The CoS tag values are 0-7. The default value is 0.

Queue Settings Area

The Queue Settings area includes the following fields:

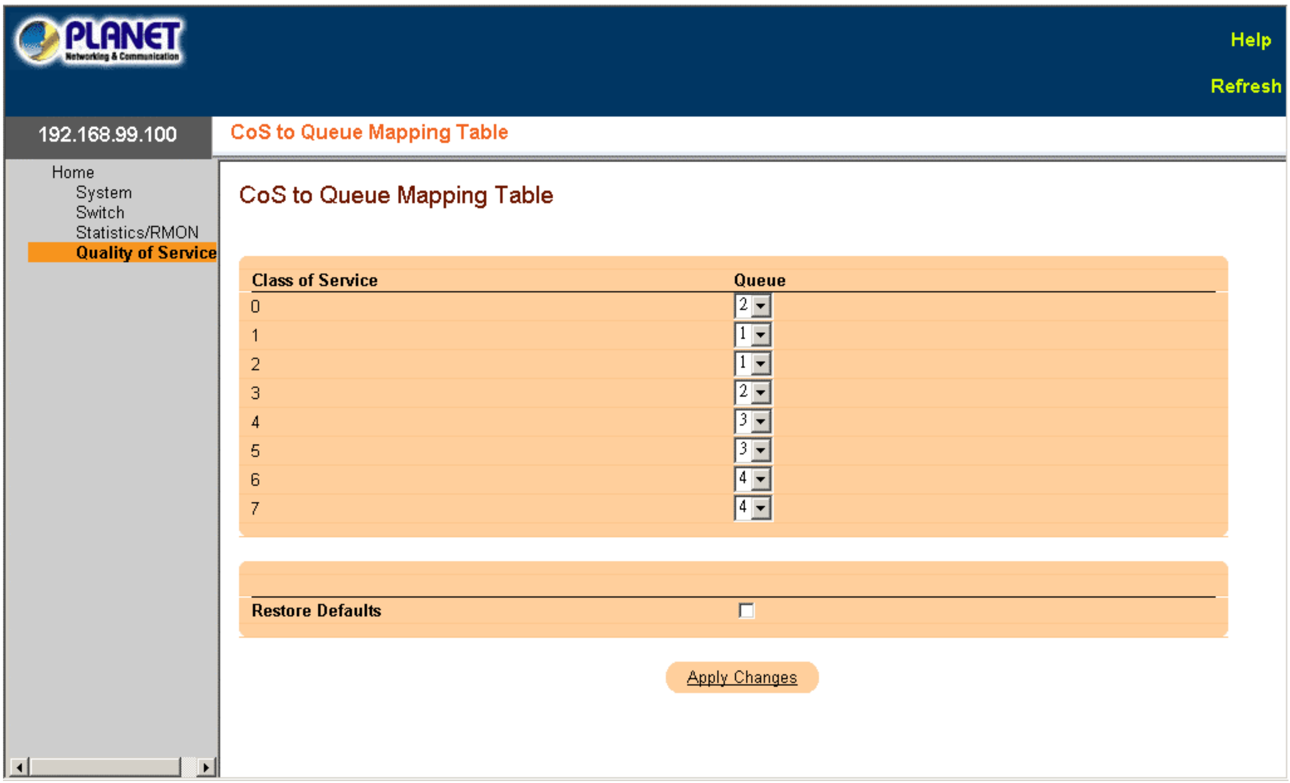
- **Interface --** The specific port or LAG to configure:
- **Disable "Trust" Mode on Interface --** Disables Trust values on the device. For more information on Trust settings, see "Configuring Global CoS Settings".
- **Set Default CoS For Incoming Traffic To --** Sets the default CoS tag value untagged packets. The CoS tag values are 0-7. The default value is 0.
- **Queue --** The queue number.
- **Queue Mode --** Indicates whether the queue is Strict Priority or WRR. This is defined in the Queue Settings screen. Queue 4 has the highest priority and queue 1 the lowest priority. Therefore, if queue 1 is defined as Strict Priority, all other queues are automatically defined as Strict Priority.
- **Weight (6-255) --** Assigns WRR weights to queues. This field is enabled only for queues in WRR queue mode.
- **% of WRR Bandwidth --** The percentage translation of the weight defined in the Weight (6-255) field.

3.2.4.1.4 CoS to Queue Mapping Table

The **CoS to Queue Mapping Table** page contains fields for classifying CoS settings to traffic queues.

To open **CoS to Queue Mapping Table** screen perform the folling:

1. Click Quality of Service -> QoS Global Parameters -> CoS to Queue
2. The CoS to Queue Mapping Table screen is displayed as in Figure 3-90



CoS to Queue Mapping Table

Class of Service	Queue
0	2
1	1
2	1
3	2
4	3
5	3
6	4
7	4

Restore Defaults □

Figure 3-90 CoS to Queue Mapping Table

The page includes the following fields:

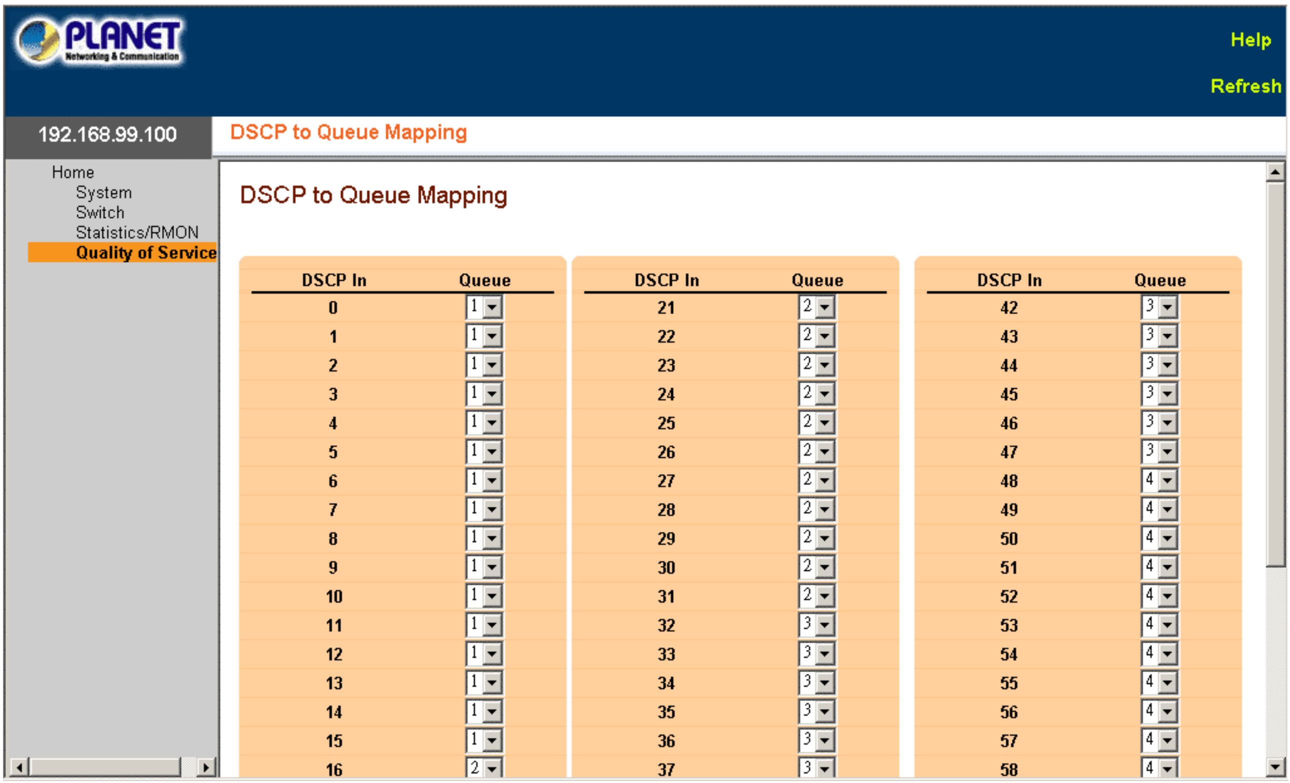
- **Class of Service --** Specifies the CoS priority tag values, where zero is the lowest and 7 is the highest.
- **Queue --** The traffic forwarding queue to which the CoS priority is mapped. Four traffic priority queues are supported.
- **Restore Defaults --** Restores the device factory defaults for mapping CoS values to a forwarding queue

3.2.4.1.5 DSCP to Queue Mapping

The **DSCP Mapping** page provides fields for defining output queue to specific DSCP fields.

To open **CoS to Queue Mapping Table** screen perform the folling:

1. Click Quality of Service -> QoS Global Parameters -> DSCP to Queue
2. The DSCP to Queue Mapping Table screen is displayed as in Figure 3-91



DSCP to Queue Mapping

DSCP to Queue Mapping

DSCP In	Queue	DSCP In	Queue	DSCP In	Queue
0	1	21	2	42	3
1	1	22	2	43	3
2	1	23	2	44	3
3	1	24	2	45	3
4	1	25	2	46	3
5	1	26	2	47	3
6	1	27	2	48	4
7	1	28	2	49	4
8	1	29	2	50	4
9	1	30	2	51	4
10	1	31	2	52	4
11	1	32	3	53	4
12	1	33	3	54	4
13	1	34	3	55	4
14	1	35	3	56	4
15	1	36	3	57	4
16	2	37	3	58	4

Figure 3-91 DSCP to Queue Mapping

The page includes the following fields:

- **DSCP In --** The values of the DSCP field within the incoming packet.
- **Queue --** The queue to which packets with the specific DSCP value is assigned. The values are 1-4, where one is the lowest value and four is the highest.

4. SWITCH OPERATION

4.1 Address Table

The Switch is implemented with an address table. This address table composed of many entries. Each entry is used to store the address information of some node in network, including MAC address, port no, etc. This information comes from the learning process of Ethernet Switch.

4.2 Learning

When one packet comes in from any port, the Switch will record the source address, port no. And the other related information in address table. This information will be used to decide either forwarding or filtering for future packets.

4.3 Forwarding & Filtering

When one packet comes from some port of the Ethernet Switching, it will also check the destination address besides the source address learning. The Ethernet Switching will lookup the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, which this packet comes in. And these ports will transmit this packet to the network it connected. If found, and the destination address is located at different port from this packet comes in, the Ethernet Switching will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port with this packet comes in, then this packet will be filtered. Thereby increase the network throughput and availability.

4.4 Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques. A Store-and-Forward Ethernet Switching stores the incoming frame in an internal buffer, do the complete error checking before transmission. Therefore, no error packets occurrence, it is the best choice when a network needs efficiency and stability.

The Ethernet Switch scans the destination address from the packet-header, searches the routing table provided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. However, the switch is most commonly used to segment existing hubs, which nearly always improves overall performance. An Ethernet Switching can be easily configured in any Ethernet network environment to significantly boost bandwidth using conventional cabling and adapters.

Due to the learning function of the Ethernet switching, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines the network traffic to its respective domain, reducing the overall load on the network.

The Switch performs "Store and forward" therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

4.5 Auto-Negotiation

The STP ports on the Switch have built-in “Auto-negotiation” function. This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detect the modes and speeds at the second of both device is connected and capable of, both 10Base-T and 100Base-TX devices can connect with the port in either Half- or Full-Duplex mode. 1000Base-T can be only connected in Full-duplex mode.

APPENDIX A

A.1 Switch‵s RJ-45 Pin Assignments

1000Mbps, 1000Base T

Contact	MDI	MDI-X
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

A.2 10/100Mbps, 10/100Base-TX

Contact	MDI	MDI-X
1	1	3
2	2	6
3	3	1
6	6	2

APPENDIX B

B.1 System Default configuration.

The following file is the factory default settings of WGSW-24010. Once you have to reset your WGSW-24010 configuration to default values, please upload the file to replace the running/startup/backup configuration.

```
no spanning-tree
interface range ethernet all
flowcontrol auto
exit
interface range ethernet all
mdix auto
exit
interface vlan 1
ip address 192.168.0.100 255.255.255.0
exit
management access-list Web_Mgt
permit vlan 1 service http
exit
username admin password 21232f297a57a5a743894a0e4a801fc3 level 15 encrypted
username guest password d41d8cd98f00b204e9800998ecf8427e  encrypted
snmp-server community public
```