TP-LINK®

Embedded Web System User Guide

TL-SG3109

9-port Gigabit Managed Switch

TL-SL3428

24+4G Gigabit Managed Switch

TL-SL3452

48+4G Gigabit Managed Switch

Rev: 1.0

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice. TP-LINK® is a registered trademark of TP-LINK Technologies Co., Ltd. Other brands and product names are trademarks or registered trademarks of their respective holders.

No part of the specifications may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from TP-LINK Technologies Co., Ltd. Copyright © 2006 TP-LINK Technologies Co., Ltd. All rights reserved.

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference.
2) This device must accept any interference received, including interference that may cause undesired operation.

EC DECLARATION OF CONFORMITY (EUROPE)

In compliance with the EMC Directive 89/336/EEC, Low Voltage Directive 73/23/EEC, this product meets the requirements of the following standards:

- EN55022
- EN55024
- EN60950

SAFETY NOTICES

⚠ **Caution:**

Do not use this product near water, for example, in a wet basement or near a swimming pool.

Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

TABLE OF CONTENTS

Preface 1

Guide Overview 1

Intended Audience 2

Section 1. Getting Started 3

1.1 Configuring the device to use TP-Link Embedded Web Interface 3

1.2 Starting the TP-Link Embedded Web Interface 3

1.3 Understanding the TP-Link Embedded Web Interface 4

1.3.1 Device Representation 5

1.3.2 Using the TP-Link Embedded Web Interface Management Buttons 5

1.4 Using Screen and Table Options 6

1.4.1 Adding Configuration Information 6

1.4.2 Modifying Configuration Information 6

1.5 Deleting Configuration Information 6

1.6 Resetting the Device 7

1.7 Logging Off from the Device 7

Section 2. Defining Device Information 8

Section 3. Setting the System Time 9

3.1 Configuring Daylight Savings Time 9

3.2 Configuring SNTP 12

3.2.1 SNTP Overview 12

3.2.1.1 Polling for Unicast Time Information 12

3.2.1.2 Polling for Anycast Time Information 12

3.2.1.3 Polling for Broadcast Time Information 12

3.2.2 Defining SNTP Global Settings 13

3.2.3 Configuring SNTP Authentication 13

3.2.4 Defining SNTP Servers 14

3.2.5 Defining SNTP Interface Settings 15

Section 4. Configuring System Logs 17

4.1 Defining General Log Properties 17

4.2 Viewing Memory Logs 18

4.3 Viewing Flash Logs 18
4.4 Defining System Log Servers 19

Section 5. Configuring Device Security 21

5.1 Configuring Management Security 21
5.1.1 Configuring Authentication Methods 21
5.1.1.1 Defining Access Profiles 21
5.1.1.2 Defining Profile Rules 23
5.1.1.3 Defining Authentication Profiles 24
5.1.1.4 Mapping Authentication Profiles 25
5.1.1.5 Defining TACACS+ Host Settings 27
5.1.1.6 Defining RADIUS Server Settings 28
5.1.2 Configuring Passwords 30
5.1.2.1 Defining Local Users 30
5.1.2.2 Defining Line Passwords 31
5.1.2.3 Defining Enable Passwords 31
5.2 Configuring Network Security 31
5.2.1 Network Security Overview 32
5.2.1.1 Port-Based Authentication 32
5.2.1.2 Advanced Port-Based Authentication 32
5.2.2 Defining Network Authentication Properties 32
5.2.2.1 Defining Port Authentication Properties 33
5.2.2.2 Configuring Multiple Hosts 34
5.2.2.3 Defining Authentication Hosts 35
5.2.3 Configuring Traffic Control 36
5.2.3.1 Managing Port Security 36
5.2.3.2 Enabling Storm Control 37

Section 6. Defining IP Addresses 39

6.1 Defining IP Addressing 39
6.1.1 Defining IP Addresses 39
6.1.2 Defining the Default Gateway 40
6.1.3 Defining DHCP Addresses 40
6.1.4 Defining ARP 41
6.2 Defining Domain Name System 42
6.2.1 Defining DNS Servers 42
6.2.2 Configuring Host Mapping 43

Section 7. Configuring Interfaces 45
7.1 Configuring Ports 45
7.2 Configuring LAGs 47
7.2.1 Defining LAG Members 47
7.2.2 Configuring LACP 48
7.3 Configuring VLANs 49
7.3.1 Defining VLAN Properties 49
7.3.2 Defining VLAN Membership 50
7.3.3 Defining VLAN Interface Settings 51
7.3.4 Configuring GARP 52
7.3.4.1 Defining GARP 52
7.3.5 Defining GVRP 53
Section 8. Defining the Forwarding Database 55
8.1 Configuring Static Addresses 55
8.2 Configuring Dynamic Forwarding Addresses 56
Section 9. Configuring the Spanning Tree Protocol 58
9.1 Configuring the Classic STP 58
9.1.1 Defining STP Properties 58
9.1.2 Defining STP Interface Settings 59
9.2 Configuring the Rapid STP 61
9.3 Configuring the Multiple STP 62
9.3.1 Defining MSTP Properties 62
9.3.2 Configuring MSTP Instances 63
9.3.3 Configuring MSTP VLAN Instances 64
9.3.4 Configuring MSTP Interface Settings 64
Section 10. Configuring Multicast Forwarding 66
10.1 Configuring Multicast Forwarding 66
10.2 Defining Multicast Bridging Groups 67
10.3 Defining Multicast Forward All Parameters 69
Section 11. Configuring SNMP Management 70
11.1 SNMP v1 and v2c 70
11.2 SNMP v3 70
11.3 Defining SNMP Security 70

11.3.1 Defining SNMP Global Parameters 71
11.3.2 Defining SNMP Views........ 71
11.3.3 Defining SNMP Group Profiles........ 72
11.3.4 Defining SNMP Group Members 73
11.3.5 Defining SNMP Communities........ 75
11.3.5.1 SNMP Communities Basic Table 75
11.3.5.2 SNMP Communities Advanced Table........ 75
11.4 Configuring SNMP Notification Settings 76
11.4.1 Defining SNMP Notification Properties 76
11.4.2 Defining Notification Filters 76
11.4.3 Defining Notification Receivers........ 77
11.4.3.1 SNMPv1,2c Notification Recipient 78
11.4.3.2 SNMPv3 Notification Recipient 78

Section 12. Configuring Quality of Service........ 80

12.1 Quality of Service Overview 80
12.1.1 Mapping to Queues 80
12.1.2 QoS Modes........ 81
12.1.2.1 Basic QoS Mode........ 82
12.1.2.2 Advanced QoS Mode 82
12.2 Enabling Quality of Service 82
12.2.1 Enabling Quality of Service 82
12.2.2 Defining Queues........ 83
12.3 Mapping Queues 84
12.3.1 Mapping CoS Values to Queues........ 84
12.3.2 Mapping QoS Values to Queues 84

Section 13. Managing System Files 86

13.1 Downloading System Files........ 86
13.1.1 Download Type 86
13.1.2 Firmware Download........ 87
13.1.3 Configuration Download 87
13.2 Uploading System Files........ 87
13.2.1 Upload Type 87
13.2.2 Software Image Upload 88
13.2.3 Configuration Upload........ 88
13.3 Activating Image Files........ 88

13.4 Copying System Files 88

Section 14. Performing Device Diagnostics 90

14.1 Configuring Port Mirroring 90
14.2 Viewing Integrated Cable Tests 91
14.3 Viewing Optical Transceivers 92

Section 15. Viewing Statistics 93

15.1 Viewing Interface Statistics 93
15.1.1 Viewing Device Interface Statistics 93
15.1.2 Viewing Etherlike Statistics 94
15.1.3 Viewing GVRP Statistics 95
15.1.4 Viewing EAP Statistics 96
15.2 Managing RMON Statistics 96
15.2.1 Viewing RMON Statistics 97
15.2.2 Configuring RMON History 98
15.2.2.1 Defining RMON History Control 98
15.2.2.2 Viewing the RMON History Table 99
15.2.3 Configuring RMON Events 100
15.2.3.1 Defining RMON Events Control 100
15.2.3.2 Viewing the RMON Events Logs 101
15.2.4 Defining RMON Alarms 101

Glossary 104

Preface

The Embedded Web System (EWS) is a network management system. The TP-Link Embedded Web Interface configures, monitors, and troubleshoots network devices from a remote web browser. The TP-Link Embedded Web Interface web pages are easy-to-use and easy-to-navigate. In addition, the TP-Link Embedded Web Inter-face provides real time graphs and RMON statistics to help system administrators monitor network performance.

This preface provides an overview to the TP-Link Embedded Interface User Guide.

This preface includes the following sections:

- Guide Overview
- Intended Audience

Guide Overview

This user guide is divided into the following sections to provide concise information for configuring, and managing the TP-Link device:

Section 1. Getting Started — Provides information about using the EWS, including the TP-Link Embedded Web Interface, management, and information buttons, as well as information about adding, modifying, and deleting devices.

Section 2. Defining Device Information — Provides information about opening the device zoom view, defining general system properties, and enabling Jumbo frames.

Section 3. Setting the System Time — Provides information about configuring system time parameters, includ-ing Daylight Savings Time (DST) and Simple Network Time Protocol (SNTP).

Section 4. Configuring System Logs — Provides information about enabling and defining system logs.

Section 5. Configuring Device Security — Provides information about configuring device security for management security, traffic control, and network security.

Section 7. Configuring Interfaces — Provides information about configuring system interfaces, ports, port groups (LAGs) and protocols (LACP). Provides information about configuring and managing VLANs, including VLAN GARP and VLAN GVRP.

Section 6. Defining IP Addresses — Provides information about defining device IP addresses, ARP, and Domain Name Servers (DNS).

Section 8. Defining the Forwarding Database — Provides information about configuring and managing both static and dynamic MAC addresses.

Section 9. Configuring the Spanning Tree Protocol — Provides information about configuring Spanning Tree Protocol (STP) including the Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP).

Section 10. Configuring Multicast Forwarding — Provides information about Multicast Forwarding.

Section 11. Configuring SNMP Management — Provides information about Simple Network Management Protocol (SNMP) management, including defining SNMP v1,v2c, and v3, SNMP filters and notifications.

Section 12. Configuring Quality of Service — Provides information about configuring Quality of Service parameters on the device.

Section 13. Managing System Files — Provides information about downloading, uploading, and copying system files.

Section 14. Performing Device Diagnostics — Provides information about port mirroring configuration, copper and fiber cables testing, and viewing device health information.

Section 15. Viewing Statistics — Provides information about viewing device statistics, including Remote Monitoring On Network (RMON) statistics, and device history events.

Intended Audience

This guide is intended for network administrators familiar with IT concepts and network terminology.

Section 1. Getting Started

This section provides an introduction to the user interface, and includes the following topics:

- Configuring the device to use TP-Link Embedded Web Interface
- Starting the TP-Link Embedded Web Interface
- Understanding the TP-Link Embedded Web Interface
- Using Screen and Table Options
- Resetting the Device
- Logging Off from the Device

1.1 Configuring the device to use TP-Link Embedded Web Interface

When the device is received, the Embedded Web Interface can not be accessed until the device is properly configured. To use TP-Link Embedded Web Interface, use the console interface to assign an IP address and subnet mask on the default VLAN, and add a super-user with the highest privilege level (15) which is allowed to log onto the device via Embedded Web Interface. Below is an example:

```
console> en
console# config
console(config)# username admin password admin level 15
console(config)# interface vlan 1
console(config-if)# ip address 192.168.1.1 255.255.255.0
console(config-if)# exit
console(config)# exit
console# copy running-config startup-config
01-Jan-2000 01:02:49 %COPY-I-FILECPY: Files Copy - source URL running-config destination URL flash://
startup-config
01-Jan-2000 01:02:50 %COPY-W-TRAP: The copy operation was completed successfully
Copy succeeded
```

The above example uses the following assumptions:

- The user name and password are both "admin"
- The IP address assigned to the default VLAN is 192.168.1.1
- The subnet mask for the network is 255.255.255.0

Once the device is configured as above, you can open the Embedded Web Interface authentication page by typing the URL "http://192.168.1.1/" into the location bar of the web browser. And then use "admin" as both the user name and password to log onto the device.

For more detailed information on how to configure the device via console interface, read "Section 4. Starting and Configuring the Device" in the *TP-Link Installation Guide*.

1.2 Starting the TP-Link Embedded Web Interface

This section contains information on starting the TP-Link Embedded Web interface.

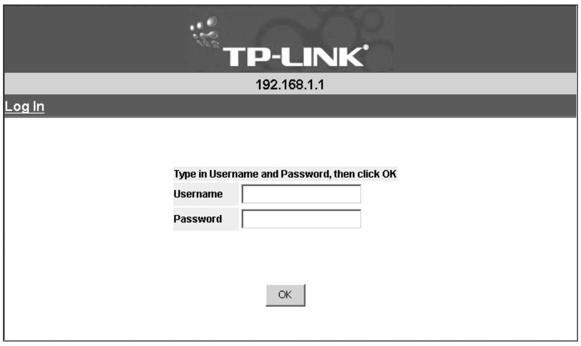
Note:

Disable the popup blocker before beginning device configuration using the EWS.

To access the TP-Link user interface:

1. Open an Internet browser.
2. Ensure that pop-up blockers are disabled. If pop-up blockers are enable, modify, add, and device information messages may not open.
3. Enter the device IP address in the address bar and press Enter. The *Login Page* opens:

Figure 1: Login Page



Type in Username and Password, then click OK

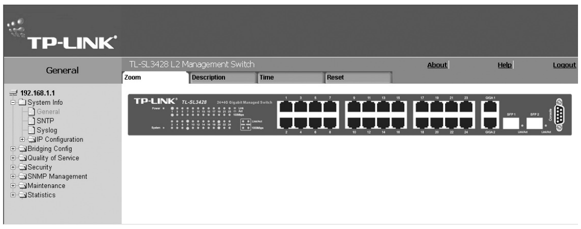
4. Enter your user name and password.

Note:

- Passwords are case sensitive.
- To operate the device, disable all pop-ups with a popup blocker.
- For information on using the CLI to define default passwords, see the *TP-Link CLI Reference Guide*.

5. Click OK. The *TP-Link Embedded Web Interface Home Page* opens:

Figure 2: TP-Link Embedded Web Interface Home Page



The *TP-Link Embedded Web Interface Home Page* contains the following views:

- **Port LED Indicators** — Located at the top of the home page, the port LED indicators provide a visual representation of the ports on the TP-Link front panel.
- **Tab Area** — Located above the LED indicators, the tab area contains a list of the device features and their components.
- **Device View** — Located in the main part of the home page, the device view provides a view of the device, an information or table area, and configuration instructions.

1.3 Understanding the TP-Link Embedded Web Interface

The following table lists the user interface components with their corresponding numbers:

Table 1: Interface Components

View	Description
1 Tree View	Tree View provides easy navigation through the configurable device features. The main branches expand to display the sub-features.
2 Device View	Device View provides information about device ports, current configuration and status, table information, and feature components. Device View also displays other device information and dialog boxes for configuring parameters.
3 Tab Area	The Tab Area enables navigation through the different device features. Click the tabs to view all the components under a specific feature.
4 Zoom View	Provides a graphic of the device on which TP-Link Web Interface runs.
5 TP-Link Web Interface Information Tabs	Provide access to online help, and contain information about the EWS.

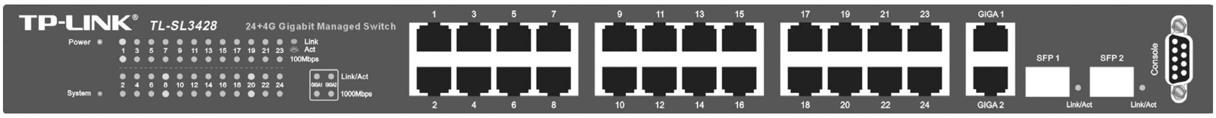
This section provides the following additional information:

- **Device Representation** — Provides an explanation of the TP-Link user interface buttons, including both management buttons and task icons.
- **Using the TP-Link Embedded Web Interface Management Buttons** — Provides instructions for adding, modifying, and deleting configuration parameters.

1.3.1 Device Representation

The *TP-Link Embedded Web Interface Home Page* contains a graphical representation of the device. This representation varies according to the device platform.

Figure 3: Device Representation



Figures in this guide are based on the TL-SL3428 device. The figures captions may differ if another device is used.

1.3.2 Using the TP-Link Embedded Web Interface Management Buttons

Configuration Management buttons and icons provide an easy method of configuring device information, and include the following:

Table 2: TP-Link Web Interface Configuration Management Buttons

Button	Button Name	Description
Back Next	Back/Next	Enables browsing table items.
Clear Logs	Clear Logs	Clears system logs.
Create	Create	Enables creation of configuration entries.
✎	Modify	Modifies configuration settings.
Query	Query	Queries the device table.
Reset	Reset	Resets the device.
Save	Save	Saves the current system configuration.
Submit	Submit	Saves configuration changes to the device.
Test	Test	Performs cable tests.

Table 3: TP-Link Web Interface Information Buttons

Tab	Tab Name	Description
Help	Help	Opens the online help.
Logout	Logout	Opens the Logout page.

1.4 Using Screen and Table Options

The TP-Link Embedded Web Interface contains screens and tables for configuring devices.

This section contains the following topics:

- Adding Configuration Information
- Modifying Configuration Information
- Deleting Configuration Information

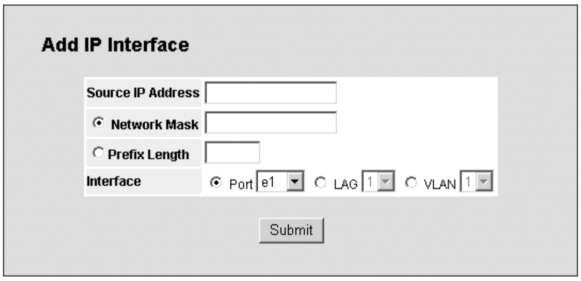
1.4.1 Adding Configuration Information

User-defined information can be added to specific TP-Link Web Interface pages, by opening a new *Add* page.

To add information to tables or TP-Link Web Interface pages:

1. Open an TP-Link Web Interface page.
2. Click Create. An *Add* page opens, for example Add IP Interface Page:

Figure 4: Add IP Interface Page



Add IP Interface

Source IP Address	
● Network Mask	
○ Prefix Length	
Interface	● Port e1 ○ LAG 1 ○ VLAN 1

3. Define the required fields.
4. Click Submit. The configuration information is saved, and the device is updated.

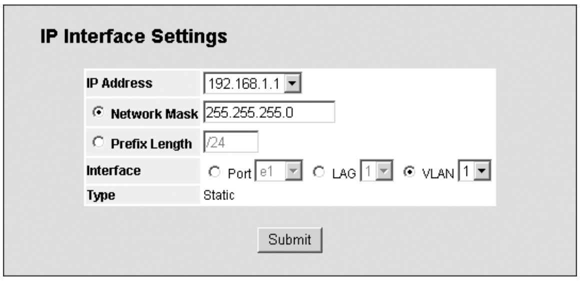
1.4.2 Modifying Configuration Information

User-defined information can be modified in specific TP-Link Web Interface pages, by opening a new *Settings* page.

To modify information in tables or TP-Link Web Interface pages:

1. Open the TP-Link Embedded Web Interface page.
2. Select a table entry.
3. Click ✎ . A Settings page opens, for example the *IP Interface Settings Page*:

Figure 5: IP Interface Settings Page



IP Interface Settings

IP Address	192.168.1.1
● Network Mask	255.255.255.0
○ Prefix Length	/24
Interface	○ Port e1 ○ LAG 1 ● VLAN 1
Type	Static

4. Modify the fields.
5. Click Submit. The settings are saved, and the device is updated.

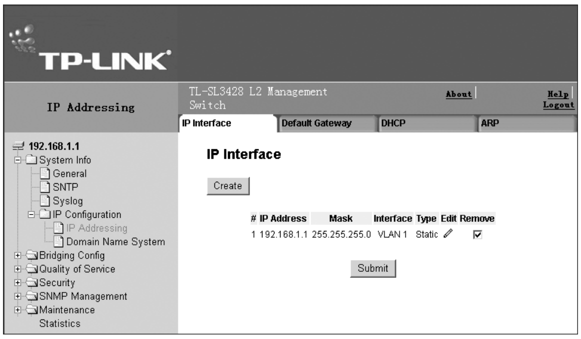
1.5 Deleting Configuration Information

User-defined information can be deleted in specific TP-Link Web Interface pages, using the *Remove* function.

To delete information in tables or TP-Link Web Interface pages:

1. Open the TP-Link Embedded Web Interface page, for example *IP Addressing Page*.

Figure 6: IP Addressing Page



IP Interface

#	IP Address	Mask	Interface	Type	Edit	Remove
1	192.168.1.1	255.255.255.0	VLAN 1	Static	✎	☑

2. Select the *Remove* checkbox in the row of the item to delete.
3. Click Submit. The information is deleted, and the device is updated.

1.6 Resetting the Device

The *Reset* page enables resetting the device from a remote location.

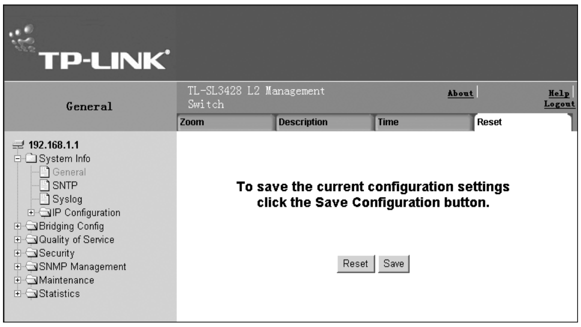
Note:

To prevent the current configuration from being lost, save all changes from the running configuration file to the startup configuration file before resetting the device. For instructions, see *Managing System Files* "Copying System Files" on page 171.

To reset the device:

1. Click **System > General > Reset**. The *Reset Page* opens.

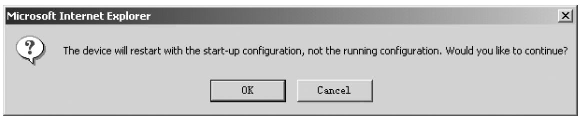
Figure 7: Reset Page



To save the current configuration settings click the Save Configuration button.

2. Click Reset. A confirmation message is displayed.

Figure 8: Reset Confirmation Message



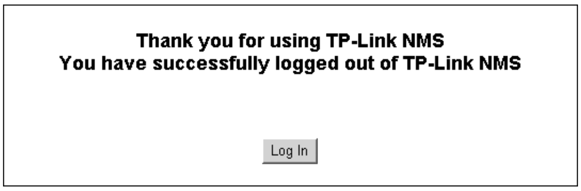
The device will restart with the start-up configuration, not the running configuration. Would you like to continue?

3. Click OK. The device is reset, and a prompt for a user name and password is displayed.
4. Enter a user name and password to reconnect to the web Interface.

1.7 Logging Off from the Device

Click Logout. The *Logout Confirmation Message* is displayed.

Figure 9: Logout Confirmation Message



Thank you for using TP-Link NMS
You have successfully logged out of TP-Link NMS

Section 2. Defining Device Information

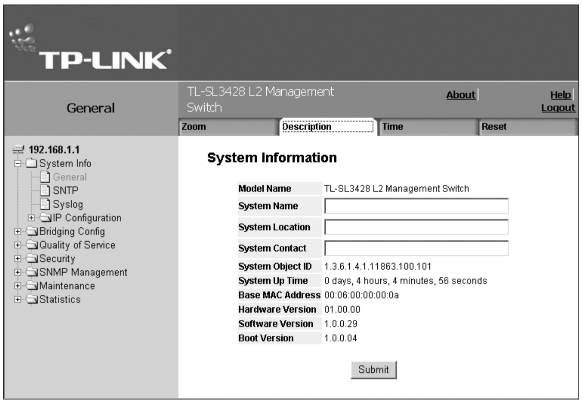
This section contains information for viewing and setting general system information.

The *System Description Page* contains parameters for configuring general device information, including the system name, location, and contact, the system MAC Address, System Object ID, System Up Time, System IP and MAC addresses, and both software and hardware versions.

To view and define the system description:

1. Click **System Info > General > Description**. The *System Description Page* opens:

Figure 10:System Description Page



System Information

Model Name	TL-SL3428 L2 Management Switch
System Name	
System Location	
System Contact	
System Object ID	1.3.6.1.4.1.11863.100.101
System Up Time	0 days, 4 hours, 4 minutes, 56 seconds
Base MAC Address	00:06:00:00:00:0a
Hardware Version	01.00.00
Software Version	1.0.0.29
Boot Version	1.0.0.04

The *System Description Page* contains the following fields:

- **Model Name** — Displays the device model number and name.
- **System Name** — Defines the user-defined device name. The field range is 0-160 characters.
- **System Location** — Defines the location where the system is currently running. The field range is 0-160 characters.
- **System Contact** — Defines the name of the contact person. The field range is 0-160 characters.
- **System Object ID** — Displays the vendor's authoritative identification of the network management sub-system contained in the entity.
- **System Up Time** — Displays the amount of time since the most recent device reset. The system time is displayed in the following format: Days, Hours, Minutes, and Seconds. For example, 41 days, 2 hours, 22 min-utes and 15 seconds.
- **Base MAC Address** — Displays the device MAC address.
- **Hardware Version** — Displays the installed device hardware version number.
- **Software Version** — Displays the installed software version number.
- **Boot Version** — Displays the current boot version running on the device.

2. Define the *System Name, System Location* and *System Contact* fields.
3. Click Submit. The system description is saved and the device is updated.

Section 3. Setting the System Time

This section provides information for configuring system time parameters, including:

- Configuring Daylight Savings Time
- Configuring SNTP

3.1 Configuring Daylight Savings Time

The *System Information Time 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.

The following is a list of Daylight Savings Time start and end times in specific countries:

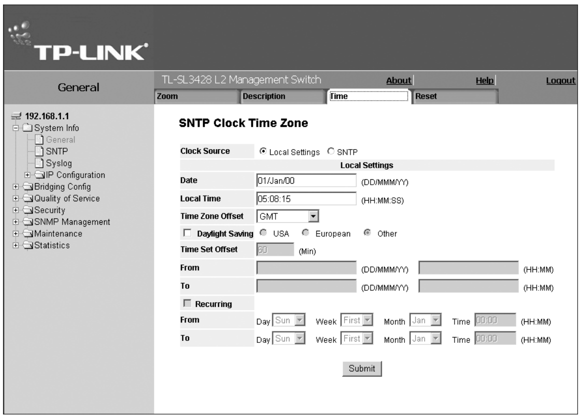
- **Albania** — From the last weekend of March until the last weekend of October.
- **Australia** — From the end of October until the end of March.
- **Australia** - Tasmania — From the beginning of October until the end of March.
- **Armenia** — From the last weekend of March until the last weekend of October.
- **Austria** — From the last weekend of March until the last weekend of October.
- **Bahamas** — From April to October, in conjunction with Daylight Savings Time in the United States.
- **Belarus** — From the last weekend of March until the last weekend of October.
- **Belgium** — From the last weekend of March until the last weekend of October.
- **Brazil** — From the third Sunday in October until the third Saturday in March. During the period of Daylight Saving Time, Brazilian clocks go forward one hour in most of the Brazilian southeast.
- **Chile** — In Easter Island, from March 9 until October 12. In the rest of the country, from the first Sunday in March or after 9th March.
- **China** — China does not use 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** — From the last weekend of March until the last weekend of October.
- **Denmark** — From the last weekend of March until the last weekend of October.
- **Egypt** — From the last Friday in April until the last Thursday in September.
- **Estonia** — From the last weekend of March until the last weekend of October.
- **Finland** — From the last weekend of March until the last weekend of October.
- **France** — From the last weekend of March until the last weekend of October.
- **Germany** — From the last weekend of March until the last weekend of October.
- **Greece** — From the last weekend of March until the last weekend of October.
- **Hungary** — From the last weekend of March until the last weekend of October.
- **India** — India does not use Daylight Saving Time.
- **Iran** — From Farvardin 1 until Mehr 1.
- **Iraq** — From April 1 until October 1.
- **Ireland** — From the last weekend of March until the last weekend of October.
- **Israel** — Varies year-to-year.
- **Italy** — From the last weekend of March until the last weekend of October.
- **Japan** — Japan does not use Daylight Saving Time.
- **ordan** — From the last weekend of March until the last weekend of October.

- **Latvia** — From the last weekend of March until the last weekend of October.
- **Lebanon** — From the last weekend of March until the last weekend of October.
- **Lithuania** — From the last weekend of March until the last weekend of October.
- **Luxembourg** — From the last weekend of March until the last weekend of October.
- **Macedonia** — From the 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** — From the last weekend of March until the last weekend of October.
- **Montenegro** — From the last weekend of March until the last weekend of October.
- **Netherlands** — From the 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 March 15.
- **Norway** — From the last weekend of March until the last weekend of October.
- **Paraguay** — From April 6 until September 7.
- **Poland** — From the last weekend of March until the last weekend of October.
- **Portugal** — From the last weekend of March until the last weekend of October.
- **Romania** — From the last weekend of March until the last weekend of October.
- **Russia** — From the last weekend of March until the last weekend of October.
- **Serbia** — From the last weekend of March until the last weekend of October.
- **Slovak Republic** - From the last weekend of March until the last weekend of October.
- **South Africa** — South Africa does not use Daylight Saving Time.
- **Spain** — From the last weekend of March until the last weekend of October.
- **Sweden** — From the last weekend of March until the last weekend of October.
- **Switzerland** — From the last weekend of March until the last weekend of October.
- **Syria** — From March 31 until October 30.
- **Taiwan** — Taiwan does not use Daylight Saving Time.
- **Turkey** — From the last weekend of March until the last weekend of October.
- **United Kingdom** — From the 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 configure the daylight savings time:

1. Click **System > System Info > General > Time**. The *System Information Time Page* opens:

Figure 11: System Information Time Page



SNTP Clock Time Zone

Clock Source ● Local Settings ○ SNTP

Local Settings

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

Local Time 05:08:15 (HH:MM:SS)

Time Zone Offset GMT

□ Daylight Saving ○ USA ○ European ● Other

Time Set Offset 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)

Submit

The *System Information Time Page* contains the following sections and fields:

- **Clock Source** — The source used to set the system clock. The possible field values are:
  – *None* — Indicates that a clock source is not used. The clock is set locally.
  – *SNTP* — Indicates that the system time is set via an SNTP server.

The *Local Settings* section contains the following fields:

- **Date** — The system date. The field format is Day/Month/Year. For example: 04/May/50 (May 4, 2050).
- **Local Time** — The system time. The field format is HH:MM:SS. For example: 21:15:03.
- **Time Zone Offset** — The hours difference between Greenwich Mean Time (GMT) and local time. For example, the Time Zone Offset for Paris is GMT +1, while the Time Zone Offset for New York is GMT –5.
- **Daylight Savings** — Enables the automatic Daylight Savings Time (DST) on the device based on the device’s location.

The DST can be set according to unique start and end dates for a particular year or as a recurring period for any year. For a specific setting in a particular year, complete the fields in the *Daylight Savings* area; for a recurring setting, complete the fields in the *Recurring* area.

Daylight Savings:

– *USA* — The device switches to DST at 2:00 a.m. on the first Sunday of April, and reverts to standard time at 2:00 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)** — Used for non-USA and European countries to set the amount of time for DST (in minutes). The default time is 60 minutes.
- **From** — Indicates the time that DST begins in countries other than the USA and Europe, in the format Day/Month/Year in one field and HH:MM in another. For example, if DST begins on October 25, 2007 at 5:00 am, the two fields should be set to 25/Oct/07 and 05:00. The possible field values are:

  – *Date* — The date on 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 HH:MM. For example: 05:30.
- **To** — Indicates the time that DST ends in countries other than the USA and Europe, in the format Day/Month/Year in one field and HH:MM in another. For example, if DST ends on March 23, 2008 at midnight, the two fields should be 23/Mar/08 and 00:00. The possible field values are:

  – *Date* — The date on 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 HH:MM. For example: 05:30.

Recurring:

- **Recurring** — Enables user-defined DST for countries in which DST is constant from year to year, other than the USA and Europe.
- **From** — The time that DST begins each year. In the example, DST begins locally every first Sunday in April at midnight. 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** — The time that DST ends each year. In the example, DST ends locally every first Sunday in October at midnight. 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 HH:MM. For example: 05:30.

2. Define the *Date, Local Time* and *Time Zone Offset* fields.

3. To configure the device to automatically switch to DST, select *Daylight Savings* and select either *USA, Euro-pean*, or *Other*. If you select *Other*, you must define its *From* and *To* fields. To configure DST parameters that will recur every year, select *Recurring* and define its *From* and *To* fields.

4. Click Submit. The DST settings are saved, and the device is updated.

3.2 Configuring SNTP

This section contains the following topics:

- SNTP Overview
- Defining SNTP Global Settings
- Configuring SNTP Authentication
- Defining SNTP Servers
- Defining SNTP Interface Settings

3.2.1 SNTP Overview

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. The device operates only as an SNTP client, and cannot provide time services to other systems. The device can poll the following server types for the server time:

- Unicast
- Anycast
- Broadcast

Time sources are established by stratums. Stratums define the accuracy of 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** — A real time clock (such as a GPS system) is used as the time source.
- **Stratum 1** — 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** — 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 client a reply.
- **T4** — The time at which the client received the server's reply.

3.2.1.1 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.

3.2.1.2 Polling for Anycast Time Information

Polling for Anycast information is used when the SNTP 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.

3.2.1.3 Polling for Broadcast Time Information

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

Message Digest 5 (MD5) 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.

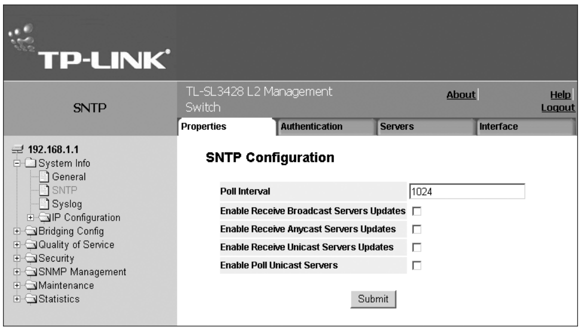
3.2.2 Defining SNTP Global Settings

The *SNTP Properties Page* provides information for defining SNTP parameters globally.

To define the SNTP global parameters:

1. Click **System > System Info > SNTP > Properties**. The *SNTP Properties Page* opens:

Figure 12: SNTP Properties Page



SNTP Configuration

Poll Interval 1024
Enable Receive Broadcast Servers Updates □
Enable Receive Anycast Servers Updates □
Enable Receive Unicast Servers Updates □
Enable Poll Unicast Servers □

The *SNTP Properties Page* contains the following fields:

- **Poll Interval** — Defines the interval (in seconds) at which the SNTP server is polled for Unicast information. The Poll Interval default is 1024 seconds.
- **Enable Receive Broadcast Servers Updates** — Defines whether or not the device monitors the SNTP servers for Broadcast server time information on the selected interfaces. The possible values are:
  – *Enable* — Enables the device to receive Broadcast server updates.
  – *Disable* — Disables the device from receiving Broadcast server updates.
- **Enable Receive Anycast Servers Updates** — Defines whether or not the device polls the SNTP server for Anycast server time information. If both the Enable Receive Anycast Servers Update and the *Enable Receive Broadcast Servers Update* fields are enabled, the system time is set according to the Anycast server time information. The possible values are:
  – *Enable* — Enables the device to receive Anycast server updates.
  – *Disable* — Disables the device from receiving Anycast server updates.
- **Enable Receive Unicast Servers Updates** — Defines whether or not the device polls the SNTP server for Unicast server time information. If the *Enable Receive Broadcast Servers Updates, Enable Receive Anycast Servers Updates*, and *Enable Receive Unicast Servers Updates* fields are all enabled, the system time is set according the Unicast server time information. The possible values are:
  – *Enable* — Enables the device to receive Unicast server updates.
  – *Disable* — Disables the device from receiving Unicast server updates.
- **Enable Poll Unicast Servers** — Defines whether or not the device sends SNTP Unicast forwarding information to the SNTP server. The possible values are:
  – *Enable* — Enables the device to receive Poll Unicast server updates.
  – *Disable* — Disables the device from receiving Poll Unicast server updates.

2. Define the *Poll Interval, Enable Receive Broadcast Servers Update, Enable Receive Anycast Servers Update, Enable Receive Unicast Servers Update*, and *Enable Poll Unicast Servers* fields and select at least one of the Enable fields.

3. Click Submit. The SNTP global settings are defined, and the device is updated.

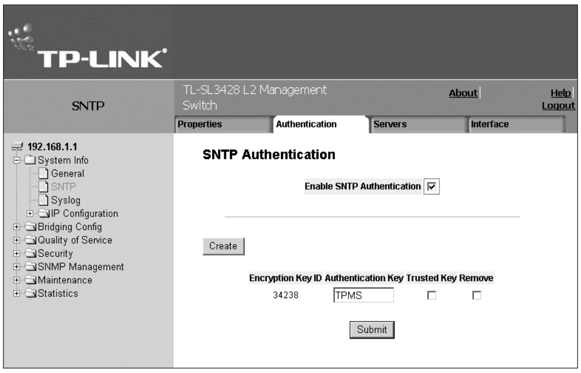
3.2.3 Configuring SNTP Authentication

The *SNTP Authentication Page* enables configuring the SNTP authentication method.

To configure SNTP authentication:

1. Click **System > System Info > SNTP > Authentication**. The *SNTP Authentication Page* opens:

Figure 13: SNTP Authentication Page



SNTP Authentication

Enable SNTP Authentication ☑

Encryption Key ID	Authentication Key	Trusted Key	Remove
34238	TPMS	□	□

The *SNTP Authentication Page* contains the following fields:

- **Enable SNTP Authentication** — Indicates if authenticating an SNTP session between the device and an SNTP server is enabled on the device. The possible field values are:
  – *Checked* — Authenticates SNTP sessions between the device and SNTP server.
  – *Unchecked* — Disables authenticating SNTP sessions between the device and SNTP server.
- **Encryption Key ID** — Indicates if the encryption key identification is used to authenticate the SNTP server and device. The field value is up to 4294967295.
- **Authentication Key** — Indicates the key used for authentication.
- **Trusted Key** — Indicates the encryption key used (Unicast/Anycast) or elected (Broadcast) to authenticate the SNTP server.
- **Remove** — Removes Encryption Key IDs. The possible field values are:
  – *Checked* — Removes the selected Encryption Key ID.
  – *Unchecked* — Maintains the Encryption Key IDs. This is the default value.

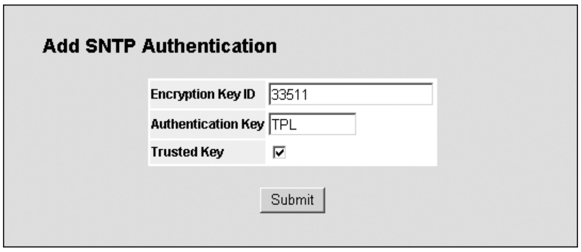
2. Check the *Enable SNTP Authentication* checkbox.

3. Click Submit. SNTP Authentication is defined, and the device is updated.

To define SNTP authentication parameters:

1. Click Create. The *Add SNTP Authentication Page* opens:

Figure 14: Add SNTP Authentication Page



Add SNTP Authentication

Encryption Key ID	33511
Authentication Key	TPL
Trusted Key	☑

2. Define *the Encryption Key ID*, *Authentication Key,* and *Trusted Key fields*.

3. Click Submit. The SNTP Authentication Key is added, and the device is updated.

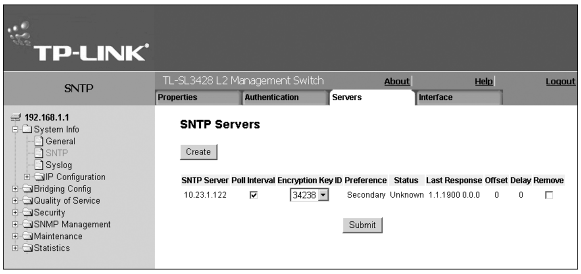
3.2.4 Defining SNTP Servers

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 server traffic.

To define SNTP servers:

1. Click **System > System Info > SNTP > Servers**. The *SNTP Servers Page* opens:

Figure 15: SNTP Servers Page



SNTP Servers

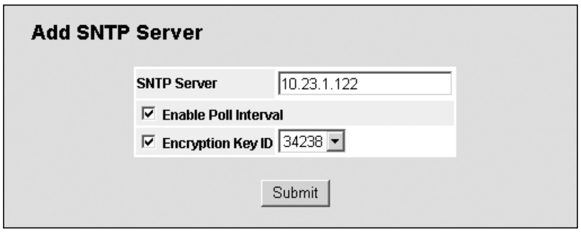
SNTP Server	Poll Interval	Encryption Key ID	Preference	Status	Last Response	Offset	Delay	Remove
10.23.1.122	☑	34238	Secondary	Unknown	1.1.1900 0.0.0	0	0	□

The *SNTP Servers Page* contains the following fields:

- **SNTP Server** — Displays user-defined SNTP server IP addresses. Up to eight SNTP servers can be defined.
- **Poll Interval** — Indicates whether or not the device polls the selected SNTP server for system time information.
- **Encryption Key ID** — Displays the encryption key identification used to communicate between the SNTP server and device. The field range is 1-4294967295.
- **Preference** — Indicates which SNTP server provides the SNTP system time. The possible field values are:
  - *Primary* — Indicates the primary server provides SNTP information.
  - *Secondary* — Indicates the backup server provides SNTP information.
- **Status** — The operating SNTP server status. The possible field values are:
  - *Up* — Indicates the SNTP server is currently operating normally.
  - *Down* — Indicates that a SNTP server is currently not available. For example, the SNTP server is currently not connected or is currently down.
  - *In progress* — Indicates the SNTP server is currently sending or receiving SNTP information.
  - *Unknown* — Indicates the progress of the SNTP information currently being sent is unknown. For example, the device is currently looking for an interface.
- **Last Response** — Displays the last time a response was received from the SNTP server.
- **Offset** — Indicates the time difference between the device local clock and the acquired time from the SNTP server.
- **Delay** — Indicates the amount of time it takes for a device request to reach the SNTP server.
- **Remove** — Removes SNTP servers from the SNTP server list. The possible field values are:
  - *Checked* — Removes the SNTP server.
  - *Unchecked* — Maintains the SNTP server. This is the default value.

2. Click Create. The *Add SNTP Server Page* opens:

Figure 16: Add SNTP Server Page



Add SNTP Server

SNTP Server 10.23.1.122

☑ Enable Poll Interval

☑ Encryption Key ID 34238

3. Define the *SNTP Server, Enable Poll Interval*, and *Encryption Key ID* fields.
4. Click Submit. The SNTP Server is added, and the device is updated.

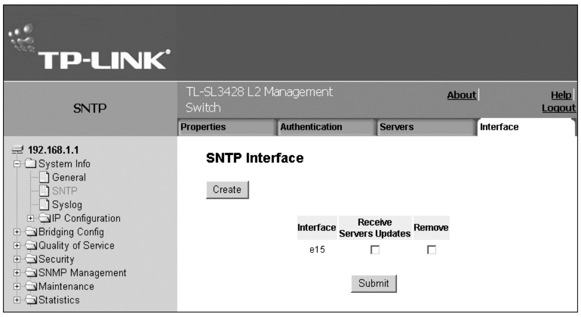
3.2.5 Defining SNTP Interface Settings

The *SNTP Interface Settings Page* contains fields for setting SNTP on different interfaces.

To define SNTP interface settings:

1. Click **System > System Info > SNTP > Interface**. The *SNTP Interface Settings Page* opens:

Figure 17: SNTP Interface Settings Page



SNTP Interface

Interface	Receive Servers Updates	Remove
e15	☐	☐

The *SNTP Interface Settings Page* contains the following fields:

- **Interface** — Indicates the interface on which SNTP can be enabled.

  The possible field values are:

  – *Port* — Indicates the specific port number on which SNTP is enabled.

  – *LAG* — Indicates the specific LAG number on which SNTP is enabled.

  – *VLAN* — Indicates the specific VLAN number on which SNTP is enabled.

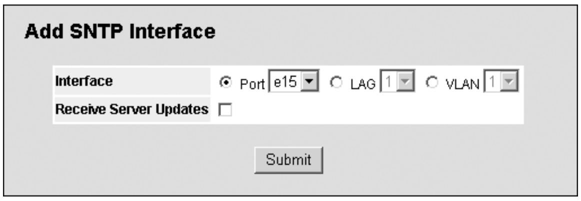
- **Receive Servers Updates** — Enables the server to receive or not receive updates.
- **Remove** — Removes SNTP interfaces.

  – *Checked* — Removes the selected SNTP interface.

  – *Unchecked* — Maintains the defined SNTP interfaces.

2. Click Create. The *Add SNTP Interface Page* opens.

Figure 18: Add SNTP Interface Page



Add SNTP Interface

Interface	● Port e15 ○ LAG 1 ○ VLAN 1
Receive Server Updates	☐

3. Select the *Interface*.
4. Check the *Receive Server Updates* option.
5. Click Submit. The SNTP interface is added, and the device is updated.

Section 4. Configuring System Logs

This section provides information for managing system logs. The system logs enable viewing device events in real time, and recording the events for later usage. System logs record and manage events and report errors and informational messages.

Event messages have a unique format, as per the Syslog protocols recommended message format for all error reporting. For example, Syslog and local device reporting messages are assigned a severity code, and include a message mnemonic, which identifies the source application generating the message. It allows messages to be filtered based on their urgency or relevancy. Each message severity determines the set of event logging devices that are sent per each event message.

The following table lists the log severity levels:

Table 4: System Log Severity Levels

Severity	Level	Message
Emergency	0 (Highest)	The system is not functioning.
Alert	1	The system needs immediate attention.
Critical	2	The system is in a critical state.
Error	3	A system error has occurred.
Warning	4	A system warning has occurred.
Notice	5	The system is functioning properly, but a system notice has occurred.
Informational	6	Provides device information.
Debug	7	Provides detailed information about the log. If a Debug error occurs, contact Customer Tech Support.

This section contains the following topics:

- Defining General Log Properties
- Viewing Memory Logs
- Viewing Flash Logs
- Defining System Log Servers

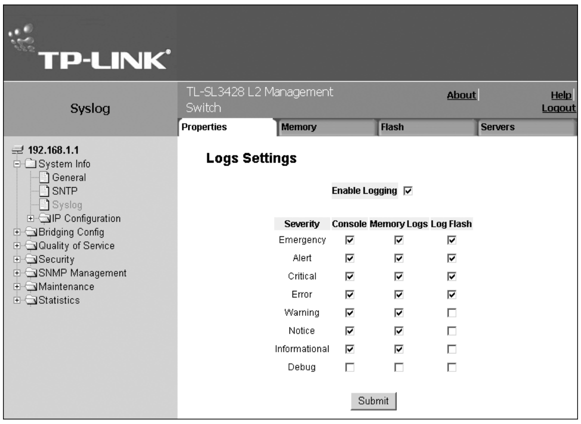
4.1 Defining General Log Properties

The Syslog Properties Page contains fields for defining which events are recorded to which logs. It contains fields for enabling logs globally, and parameters for defining logs. Log messages are listed from the highest severity to the lowest severity level.

To view the system log properties:

1. Click **System > System Info > Syslog > Properties**. The *Syslog Properties Page* opens:

Figure 19: Syslog Properties Page



Logs Settings

Enable Logging ☑

Severity	Console	Memory Logs	Log Flash
Emergency	☑	☑	☑
Alert	☑	☑	☑
Critical	☑	☑	☑
Error	☑	☑	☑
Warning	☑	☑	□
Notice	☑	☑	□
Informational	☑	☑	□
Debug	□	□	□

The *Syslog Properties Page* contains the following fields:

- **Enable Logging** — Indicates if device global logs for Cache, File, and Server Logs are enabled. Console logs are enabled by default. The possible field values are:
  – *Checked* — Enables device logs.
  – *Unchecked* — Disables device logs.
- **Severity** —
  – *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.

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

2. Check the *Enable Logging* option.
3. Check the options for each severity level.

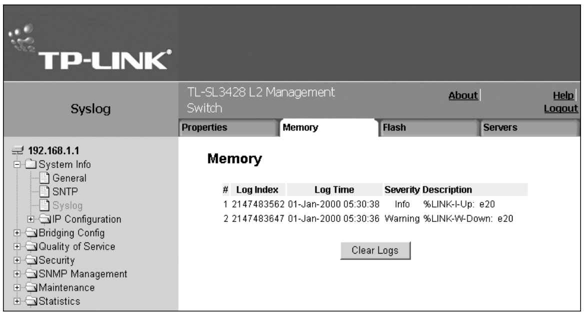
4.2 Viewing Memory Logs

The *Syslog Memory Page* contains all system logs in a chronological order that are saved in RAM (Cache).

To view memory logs:

1. Click **System > System Info > Syslog > Memory**. The S*yslog Memory Page* opens:

Figure 20: Syslog Memory Page



Memory

#	Log Index	Log Time	Severity	Description
1	2147483562	01-Jan-2000 05:30:38	Info	%LINK-I-Up: e20
2	2147483647	01-Jan-2000 05:30:36	Warning	%LINK-W-Down: e20

The *Syslog Memory Page* contains the following fields:

- **Log Index** — Lists the log number.
- **Log Time** — Lists the date and time that the log was entered.
- **Severity** — Lists the severity of the event for which the log was entered.
- **Description** — Lists the event description.

2. To clear all logs, click Clear Logs.
3. Click OK. All log items are removed from the table, and the device is updated.

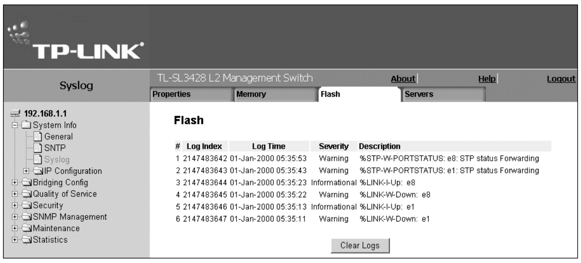
4.3 Viewing Flash Logs

The Syslog Flash Page contains information about log entries saved to the log file in Flash, including the time the log was generated, the log severity, and a description of the log message. The message log is available after reboot.

To view Flash memory logs:

1. Click **System > System Info > Syslog > Flash**. The *Syslog Flash Page* opens:

Figure 21: Syslog Flash Page



Flash

#	Log Index	Log Time	Severity	Description
1	2147483642	01-Jan-2000 05:35:53	Warning	%STP-W-PORTSTATUS: e8: STP status Forwarding
2	2147483643	01-Jan-2000 05:35:43	Warning	%STP-W-PORTSTATUS: e1: STP status Forwarding
3	2147483644	01-Jan-2000 05:35:23	Informational	%LINK-I-Up: e8
4	2147483645	01-Jan-2000 05:35:22	Warning	%LINK-W-Down: e8
5	2147483646	01-Jan-2000 05:35:13	Informational	%LINK-I-Up: e1
6	2147483647	01-Jan-2000 05:35:11	Warning	%LINK-W-Down: e1

The *Syslog Flash Page* contains the following information:

- **Log Index** — Lists the log index number.
- **Log Time** — Lists the date and time that the log was entered.
- **Severity** — Lists the severity of the event for which the log was created in Flash memory.
- **Description** — Lists the event description.

2. To remove current Flash memory logs, click Clear Logs.
3. Click OK. Logs are removed from the table.

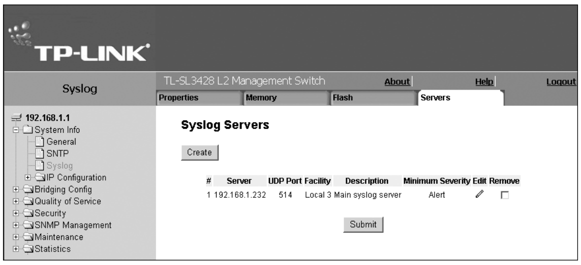
4.4 Defining System Log Servers

The *Syslog Servers Page* contains information for viewing and configuring the remote log servers. New log servers can be defined, and the log severity sent to each server.

To define Syslog servers:

1. Click **System > System Info > Syslog > Servers**. The *Syslog Servers Page* opens:

Figure 22: Syslog Servers Page



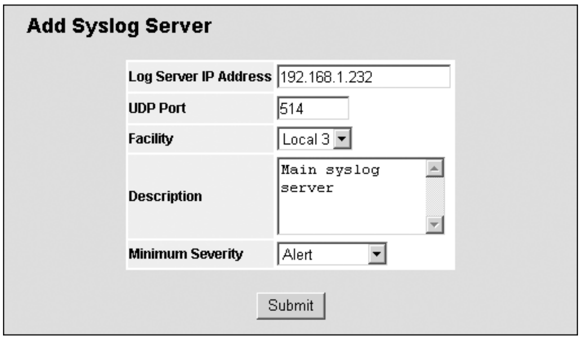
Syslog Servers

#	Server	UDP Port	Facility	Description	Minimum Severity	Edit	Remove
1	192.168.1.232	514	Local 3	Main syslog server	Alert	✎	□

The *Syslog Servers Page* list the server parameters and contains the following fields:

- **Server** — Specifies the server to which logs can be sent.
- **UDP Port** — Defines the UDP port to which the server logs are sent. The possible range is 1 - 65535. The default value is 514.
- **Port-Facility** — Defines an 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 is overridden. All applications defined for a device utilize the same facility on a server. The field default is Local 7. The possible field values are Local 0 - Local 7.
- **Description** — Provides a user-defined server description.
- **Minimum Severity** — Indicates the minimum severity from which logs are sent to the server. For example, if Notice is selected, all logs with a severity level of Notice and higher are sent to the remote server.
- **Remove** — Deletes the currently selected server from the Servers list. The possible field values are:
  – *Checked* — Removes the selected server from the Syslog Properties Page. Once removed, logs are no longer sent to the removed server.
  – *Unchecked* — Maintains the remote servers.

2. Click Create. The *Add Syslog Server Page* opens.



Add Syslog Server

Log Server IP Address	192.168.1.232
UDP Port	514
Facility	Local 3
Description	Main syslog server
Minimum Severity	Alert

Figure 23: Add Syslog Server Page

3. Define the *IP Address, UDP Port, Facility, Description*, and *Minimum Severity* fields.

4. Click Submit. The Log server is defined and the device is updated.

Section 5. Configuring Device Security

This section describes pages that contain fields for setting security parameters for ports, device management methods, users, and server security for the TP-Link device.

This section contains the following topics:

- Configuring Management Security
- Configuring Network Security

5.1 Configuring Management Security

This section provides information for configuring device management security.

This section includes the following topics:

- Configuring Authentication Methods
- Configuring Passwords

5.1.1 Configuring Authentication Methods

This section provides information for configuring device authentication methods.

This section includes the following topics:

- Defining Access Profiles
- Defining Profile Rules
- Defining Authentication Profiles
- Mapping Authentication Profiles
- Defining TACACS+ Host Settings
- Defining RADIUS Server Settings

5.1.1.1 Defining Access Profiles

Access profiles are profiles and rules for accessing the device. Access to management functions can be limited to user groups. User groups are defined for interfaces according to IP addresses or IP subnets. Access profiles contain management methods for accessing and managing the device. The device management methods include:

- All
- Telnet
- Secure Telnet (SSH)
- HTTP

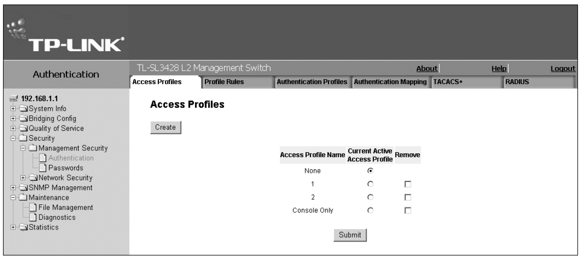
Management access to different management methods may differ between user groups. For example, User Group 1 can access the switch module only via an HTTPS session, while User Group 2 can access the switch module via both HTTPS and Telnet sessions. The Access Profile Page contains the currently configured access profiles and their activity status.

Assigning an access profile to an interface denies access via other interfaces. If an access profile is assigned to any interface, the device can be accessed by all interfaces.

To configure access profiles:

1. Click **System > Management Security > Authentication > Access Profiles**. The *Access Profile Page* opens:

Figure 24: Access Profile Page



Access Profiles

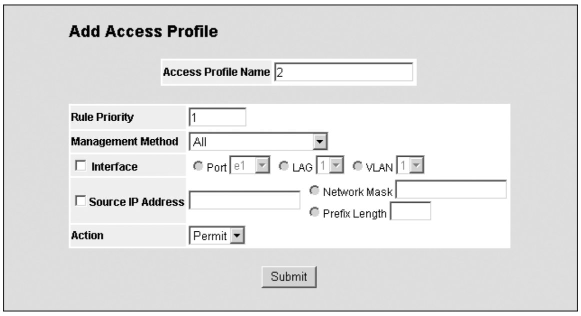
Access Profile Name	Current Active Access Profile	Remove
None	●	
1	○	□
2	○	□
Console Only	○	□

The *Access Profile Page* contains the following fields:

- **Access Profile Name** — Defines the access profile name. The access profile name can contain up to 32 characters.
- **Active Profile** — Defines the access profile currently active.
- **Remove** — Removes the selected access profile. The possible field values are:
  – *Checked* — Removes the selected access profile. Access Profiles cannot be removed when Active.
  – *Unchecked* — Maintains the access profiles.
- **Disable Active Profile** — Disables the active access profile. The possible field values are:
  – *Checked* — Disables the active access profiles.
  – *Unchecked* — Indicates the access profile is currently active. This is the default value.

2. Click Create. The *Add Access Profile Page* opens:

Figure 25: Add Access Profile Page



Add Access Profile

Access Profile Name: 2

Rule Priority: 1

Management Method: All

□ Interface: ○ Port e1 ○ LAG 1 ○ VLAN 1

□ Source IP Address: ○ Network Mask ○ Prefix Length

Action: Permit

In addition to the fields in the *Access Profile Page*, the *Add Access Profile Page* contains the following fields:

- **Access Profile Name** — Defines a new access profile name.
- **Rule Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. 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 Page*.
- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
  – *All* — Assigns all management methods to the rule.
  – *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  – *Secure Telnet (SSH)* — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  – *HTTP* — Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
  – *Secure HTTP (HTTPS)* — Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
  – *SNMP* — Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.
- **Interface** — Defines the interface on which the access profile is defined. The possible field values are:
  – *Port* — Specifies the port on which the access profile is defined.
  – *LAG* — Specifies the LAG on which the access profile is defined.
  – *VLAN* — Specifies the VLAN on which the access profile is defined.
  – *Source IP Address* — Defines the interface source IP address to which the access profile applies. The *Source IP Address* field is valid for a subnetwork.
  – *Network Mask* — Defines the network mask of the source IP address.

– *Prefix Length* — Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.

- **Action** —Defines the action attached to the access rule. The possible field values are:
  – *Permit* — Permits access to the device.
  – *Deny* — Denies access to the device. This is the default.

3. Click Submit. The access profile is saved and the device is updated.

5.1.1.2 Defining Profile Rules

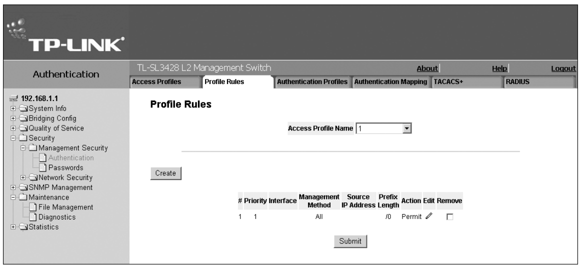
Access profiles can contain up to 128 rules that determine which users can manage the switch module, and by which methods. Users can also be blocked from accessing the device. Rules are composed of filters including:

- Rule Priority
- Interface
- Management Method
- IP Address
- Prefix Length
- Forwarding Action

To define profile rules:

1. Click **System > Management Security > Authentication > Profile Rules**. The *Profile Rules Page* opens:

Figure 26: Profile Rules Page



Profile Rules

Access Profile Name: 1

#	Priority	Interface	Management Method	Source IP Address	Prefix Length	Action	Edit	Remove
1	1		All		/0	Permit	✎	□

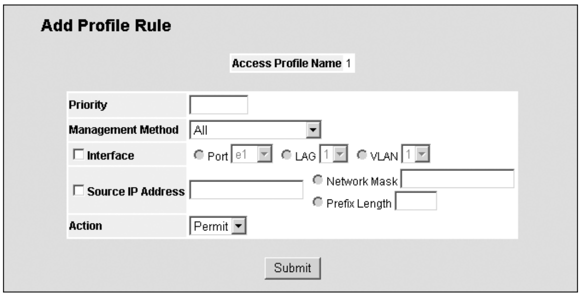
The *Profile Rules Page* contains the following fields:

- **Access Profile Name** — Displays the access profile to which the rule is attached.
- **Priority** — Defines the rule priority. When the packet is matched to a rule, user groups are either granted permission or denied device management access. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis.
- **Interface** — Indicates the interface type to which the rule applies. The possible field values are:
  – *Port* — Attaches the rule to the selected port.
  – *LAG* — Attaches the rule to the selected LAG.
  – *VLAN* — Attaches the rule to the selected VLAN.
- **Management Method** — Defines the management method for which the rule is defined. Users with this access profile can access the device using the management method selected. The possible field values are:
  – *All* — Assigns all management methods to the rule.
  – *Telnet* — Assigns Telnet access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  – *Secure Telnet (SSH)* — Assigns SSH access to the rule. If selected, users accessing the device using Telnet meeting access profile criteria are permitted or denied access to the device.
  – *HTTP* — Assigns HTTP access to the rule. If selected, users accessing the device using HTTP meeting access profile criteria are permitted or denied access to the device.
  – *Secure HTTP (HTTPS)* — Assigns HTTPS access to the rule. If selected, users accessing the device using HTTPS meeting access profile criteria are permitted or denied access to the device.
  – *SNMP* — Assigns SNMP access to the rule. If selected, users accessing the device using SNMP meeting access profile criteria are permitted or denied access to the device.
- **Source IP Address** — Defines the interface source IP address to which the rule applies.

- **Prefix Length** — Defines the number of bits that comprise the source IP address prefix, or the network mask of the source IP address.
- **Action** — Defines the action attached to the rule. The possible field values are:
  – *Permit* — Permits access to the device.
  – *Deny* — Denies access to the device. This is the default.
- **Remove** — Removes rules from the selected access profiles. The possible field values are:
  – *Checked* — Removes the selected rule from the access profile.
  – *Unchecked* — Maintains the rules attached to the access profile.

2. Click Create. The Add *Profile Rule Page* opens:

Figure 27: Add Profile Rule Page



Add Profile Rule

Access Profile Name 1

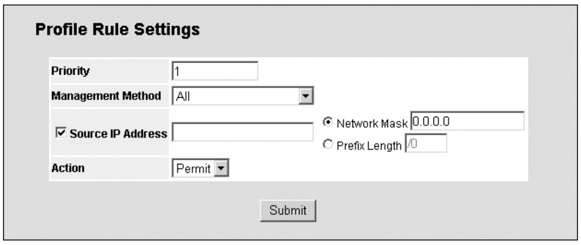
Priority	
Management Method	All
□ Interface	○ Port e1 ○ LAG 1 ○ VLAN 1
□ Source IP Address	○ Network Mask ○ Prefix Length
Action	Permit

3. Define the fields.
4. Click Submit. The profile rule is added to the access profile, and the device is updated.

To modify a Profile Rule:

1. Click **Security > Management Security > Authentication > Access Profile**. The *Access Profile Page* opens.
2. Click ✎ . The *Profile Rule Settings Page* opens:

Figure 28: Profile Rule Settings Page



Profile Rule Settings

Priority	1
Management Method	All
☑ Source IP Address	● Network Mask 0.0.0.0 ○ Prefix Length /0
Action	Permit

3. Modify the fields.
4. Click Submit. The profile rule is modified, and the device is updated.

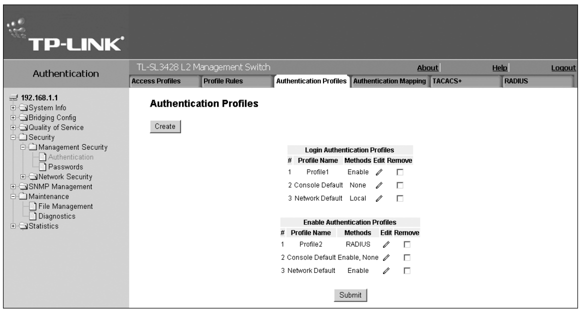
5.1.1.3 Defining Authentication Profiles

Authentication profiles allow network administrators to assign authentication methods for user authentication. User authentication can be performed either locally or on an external server. User authentication occurs in the order the methods are selected. If the first authentication method is not available, the next selected method is used. For example, if the selected authentication methods are RADIUS and Local, and the RADIUS server is not available, then the user is authenticated locally.

To define Authentication profiles:

1. Click **System > Management Security > Authentication > Authentication Profiles**. The *Authentication Profiles Page* opens:

Figure 29: Authentication Profiles Page



Authentication Profiles

Login Authentication Profiles

#	Profile Name	Methods	Edit	Remove
1	Profile1	Enable	✎	□
2	Console Default	None	✎	□
3	Network Default	Local	✎	□

Enable Authentication Profiles

#	Profile Name	Methods	Edit	Remove
1	Profile2	RADIUS	✎	□
2	Console Default	Enable, None	✎	□
3	Network Default	Enable	✎	□

The *Authentication Profiles Page* provides the following tables:

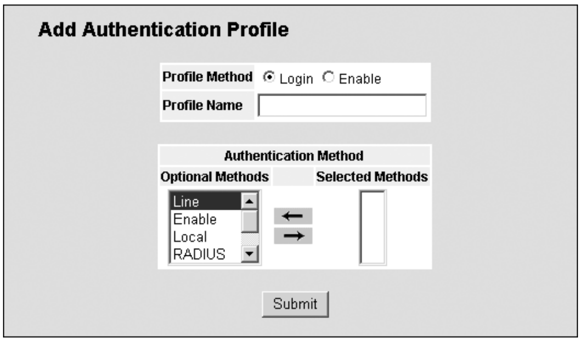
- Login Authentication Profiles
- Enable Authentication Profiles

Each of the tables contains the following fields:

- **Profile Name** — Contains a list of user-defined authentication profile lists to which user-defined authentication profiles are added.
- **Methods** — Defines the user authentication methods. The possible field values are:
  – *None* — Assigns no authentication method to the authentication profile.
  – *Local* — Authenticates the user at the device level. The device checks the user name and password for authentication.
  – *RADIUS* — Authenticates the user at the RADIUS server. For more information, see *Defining RADIUS Server Settings.*
  – *Line* — Authenticates the user using a line password.
  – *Enable* — Authenticates the user using an enable password.
- **Remove** — Removes the selected authentication profile. The possible field values are:
  – *Checked* — Removes the selected authentication profile.
  – *Unchecked* — Maintains the authentication profiles.

2. Click Create. The *Add Authentication Profile Page* opens.

Figure 30: Add Authentication Profile Page



Add Authentication Profile

Profile Method ● Login ○ Enable
Profile Name

Authentication Method

Optional Methods		Selected Methods
Line Enable Local RADIUS	← →	

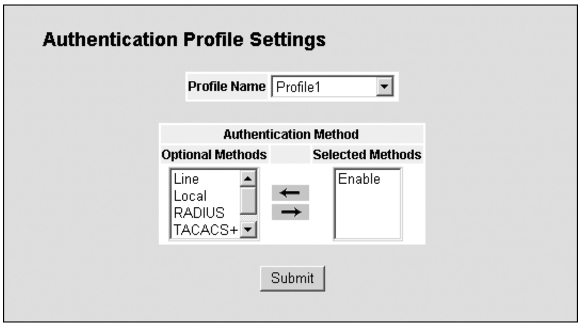
Submit

3. Define the *Profile Method and enter the Profile Name* fields.
4. Select the Authentication Method using the move arrow →.
5. Click Submit. The authentication profile is defined, and the device is updated.

To modify an authentication profile:

1. Click **System > Management Security > Authentication > Authentication Profiles**. The *Authentication Profiles Page* opens.
2. Click ✎ . The *Authentication Profile Settings Page* opens:

Figure 31: Authentication Profile Settings Page



Authentication Profile Settings

Profile Name Profile1

Authentication Method

Optional Methods		Selected Methods
Line Local RADIUS TACACS+	← →	Enable

Submit

3. Select the Authentication Method using the move arrow →.
4. Click Submit. The authentication method is selected, and the device is updated.

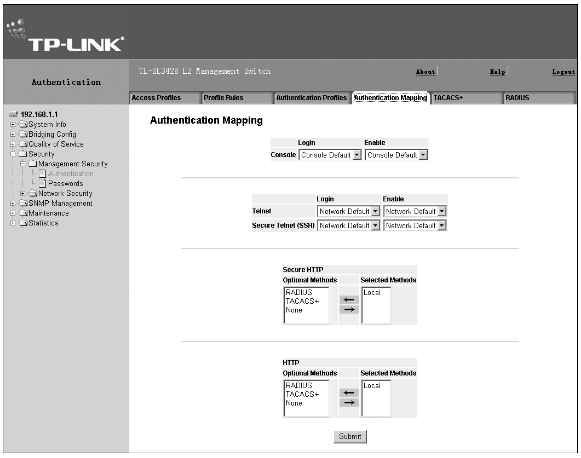
5.1.1.4 Mapping Authentication Profiles

After authentication profiles are defined, they can be applied to management access methods. For example, console users can be authenticated by Authentication Profile List 1, while Telnet users are authenticated by Authentication Method List 2. Authentication methods are selected using arrows. The order in which the methods are selected is the order by which the authentication methods are used.

To map authentication methods:

1. Click **System > Management Security > Authentication > Authentication Mapping**. The *Authentication Mapping Page* opens:

Figure 32: Authentication Mapping Page



Authentication Mapping

	Login	Enable
Console	Console Default	Console Default

	Login	Enable
Telnet	Network Default	Network Default
Secure Telnet (SSH)	Network Default	Network Default

Secure HTTP

Optional Methods	Selected Methods
RADIUS TACACS+ None	Local

HTTP

Optional Methods	Selected Methods
RADIUS TACACS+ None	Local

The *Authentication Mapping Page* contains the following fields:

- **Console** — Indicates that authentication profiles are used to authenticate console users.
- **Telnet** — Indicates that authentication profiles are used to authenticate Telnet users.
- **Secure Telnet (SSH)** — Indicates that authentication profiles are used to authenticate Secure Shell (SSH) users. SSH provides clients secure and encrypted remote connections to a device.
- **Secure HTTP** — Indicates that authentication methods are used for Secure HTTP access. Possible field values are:

  – *None* — Indicates that no authentication method is used for access.

  – *Local* — Indicates that authentication occurs locally.

  – *RADIUS* — Indicates that authentication occurs at the RADIUS server.

  – *Line* — Indicates that authentication uses a line password.

  – *Enable* — Indicates that authentication uses an Enable password.

  – *Local, RADIUS* — Indicates that authentication first occurs locally. If authentication cannot be verified locally, the RADIUS server authenticates the management method. If the RADIUS server cannot authenticate the management method, the session is blocked.

  – *RADIUS, Local* — Indicates that authentication first occurs at the RADIUS server. If authentication cannot be verified at the RADIUS server, the session is authenticated locally. If the session cannot be authenticated locally, the session is blocked.

  – *Local, RADIUS, None* — Indicates that authentication first occurs locally. If authentication cannot be verified locally, the RADIUS server authenticates the management method. If the RADIUS server cannot authenticate the management method, the session is permitted.

  – *RADIUS, Local, None* — Indicates that authentication first occurs at the RADIUS server. If authentication cannot be verified at the RADIUS server, the session is authenticated locally. If the session cannot be authenticated locally, the session is permitted.
- **HTTP** — Indicates that authentication methods are used for HTTP access. Possible field values are:

  – *None* — Indicates that no authentication method is used for access.

  – *Local* — Indicates that authentication occurs locally.

  – *RADIUS* — Indicates that authentication occurs at the RADIUS server.

  – *Line* — Indicates that authentication uses a line password.

  – *Enable* — Indicates that authentication uses an Enable password.

  – *Local, RADIUS* — Indicates that authentication first occurs locally. If authentication cannot be verified locally, the RADIUS server authenticates the management method. If the RADIUS server cannot authenticate the management method, the session is blocked.

  – *RADIUS, Local* — Indicates that authentication first occurs at the RADIUS server. If authentication cannot be verified at the RADIUS server, the session is authenticated locally. If the session cannot be authenticated locally, the session is blocked.

  – *Local, RADIUS, None* — Indicates that authentication first occurs locally. If authentication cannot be verified locally, the RADIUS server authenticates the management method. If the RADIUS server cannot authenticate the management method, the session is permitted.

  – *RADIUS, Local, None* — Indicates that authentication first occurs at the RADIUS server. If authentication cannot be verified at the RADIUS server, the session is authenticated locally. If the session cannot be authenticated locally, the session is permitted.

2. Define the *Console, Telnet*, and *Secure Telnet (SSH)* fields.
3. Map the authentication method in the *Secure HTTP* selection box.
4. Map the authentication method in the *HTTP* selection box.
5. Click Submit. The authentication mapping is saved, and the device is updated.

5.1.1.5 Defining TACACS+ Host Settings

Terminal Access Controller Access Control System (TACACS+) provides centralized security user access validation. The system supports up-to 4 TACACS+ servers.

TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. 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+ protocol ensures network integrity through encrypted protocol exchanges between the client and TACACS+ server.

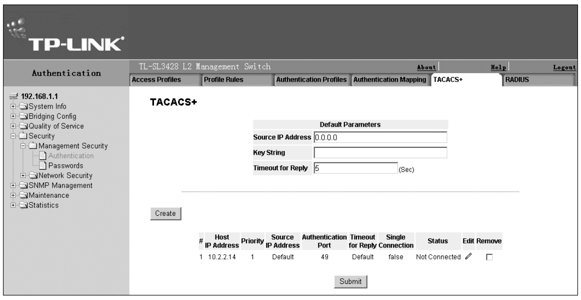
Note:

The TACACS+ default parameters are user-assigned 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+ servers.

To define TACACS+ authentication settings:

1. Click **Security > Management Security > Authentication > TACACS+**. The *TACACS+ Page* opens:

Figure 33: TACACS+ Page



TACACS+

Default Parameters	
Source IP Address	0.0.0.0
Key String	
Timeout for Reply	5 (Sec)

#	Host IP Address	Priority	Source IP Address	Authentication Port	Timeout for Reply	Single Connection	Status	Edit	Remove
1	10.2.2.14	1	Default	49	Default	false	Not Connected	✎	□

The ***Default Parameters*** section contains the following fields:

- **Source IP Address** — Defines the default device source IP address used for the TACACS+ session between the device and the TACACS+ server.
- **Key String (1-128 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.
- **Timeout for Reply** — Defines the default time that passes before the connection between the device and the TACACS+ times out. The default is 5.

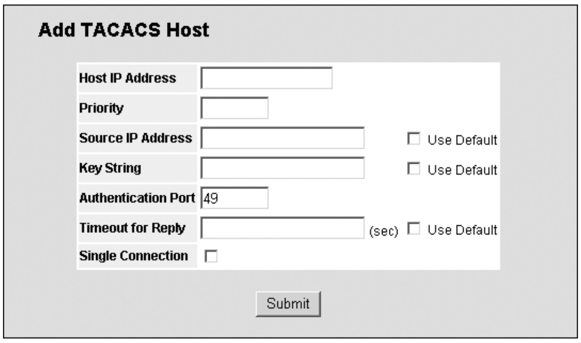
The *TACACS+ Page* also contains the following fields:

- **Host IP Address** — Defines the TACACS+ Server IP address.
- **Priority** — Defines the order in which the TACACS+ servers are used. The field range is 0-65535. The default is 0.
- **Source IP Address** — Defines the device source IP address used for the TACACS+ session between the device and the TACACS+ server.
- **Authentication Port (0-65535)** — Defines the port number via which the TACACS+ session occurs. The default port is port 49.

- **Timeout for Reply** — Defines the amount of time in seconds that passes before the connection between the device and the TACACS+ times out. The field range is 1-1000 seconds.
- **Single Connection** — Maintains a single open connection between the device and the TACACS+ server. The possible field values are:
  – *Checked* — Enables a single connection.
  – *Unchecked* — Disables a single connection.
- **Status** — Indicates the connection status between the device and the TACACS+ server. The possible field values are:
  – *Connected* — Indicates there is currently a connection between the device and the TACACS+ server.
  – *Not Connected* — Indicates there is not currently a connection between the device and the TACACS+ server.
- **Remove** — Removes TACACS+ server. The possible field values are:
  – *Checked* — Removes the selected TACACS+ server.
  – *Unchecked* — Maintains the TACACS+ servers.

2. Click Create. The *Add TACACS+ Host Page* opens:

Figure 34: Add TACACS+ Host Page



Add TACACS Host

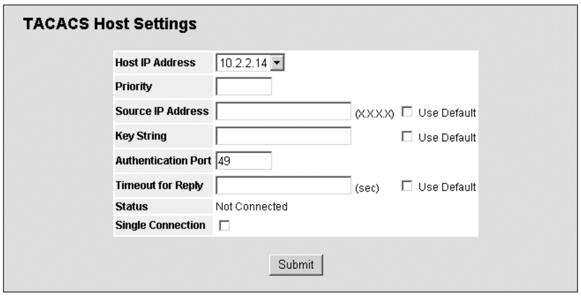
Host IP Address		
Priority		
Source IP Address		□ Use Default
Key String		□ Use Default
Authentication Port	49	
Timeout for Reply	(sec)	□ Use Default
Single Connection	□	

3. Define the fields.
4. Click Submit. The TACACS+ server is defined, and the device is updated.

To modify the TACACS+ server settings:

1. Click **Security > Management Security >Authentication > TACACS+**. The *TACACS+ Page* opens.
2. Select TACACS+ server entry.
3. Click ✎ . The *TACACS+ Host Settings Page* opens.

Figure 35: TACACS+ Host Settings Page



TACACS Host Settings

Host IP Address	10.2.2.14	
Priority		
Source IP Address	(X.X.X.X)	□ Use Default
Key String		□ Use Default
Authentication Port	49	
Timeout for Reply	(sec)	□ Use Default
Status	Not Connected	
Single Connection	□	

4. Modify the fields.
5. Click Submit. The TACACS+ host settings are saved, and the device is updated.

5.1.1.6 Defining RADIUS Server Settings

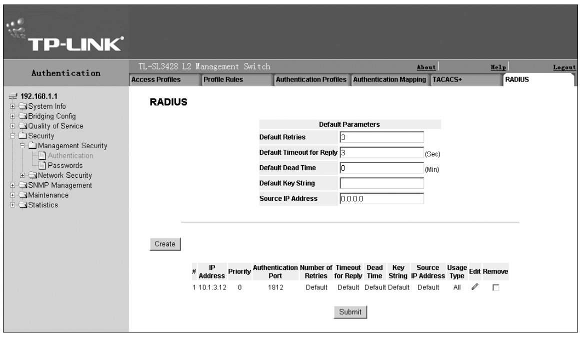
Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. RADIUS servers provide a centralized authentication method for web access.

The default parameters are user-defined, and are applied to newly defined RADIUS servers. If new default parameters are not defined, the system default values are applied to newly defined RADIUS servers.

To configure RADIUS servers:

1. Click **System > Management Security > Authentication > Radius**. The *Radius Page* opens:

Figure 36: Radius Page



RADIUS

Default Parameters	
Default Retries	3
Default Timeout for Reply	3 (Sec)
Default Dead Time	0 (Min)
Default Key String	
Source IP Address	0.0.0.0

#	IP Address	Priority	Authentication Port	Number of Retries	Timeout for Reply	Dead Time	Key String	Source IP Address	Usage Type	Edit	Remove
1	10.1.3.12	0	1812	Default	Default	Default	Default	Default	All	✎	□

The *Default Parameters section of the Radius Page* contains the following fields:

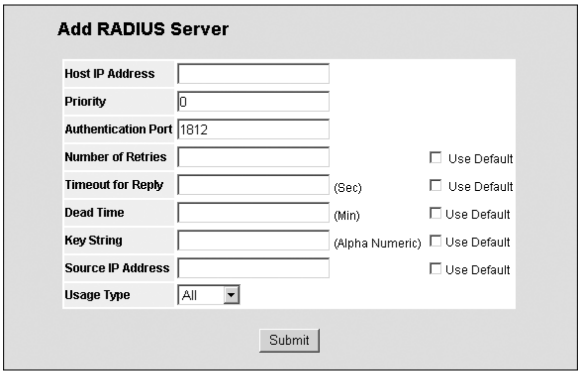
- **Retries** — Defines the number of transmitted requests sent to the RADIUS server before a failure occurs. Possible field values are 1-10. The default value is 3.
- **Timeout for Reply** — Defines the amount of time (in seconds) the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. Possible field values are 1-30. The default value is 3.
- **Dead Time** — Defines the default amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. The default value is 0.
- **Key String** — Defines the default key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS encryption.
- **Source IP Address** — Defines the default IP address of a device accessing the RADIUS server.

The *Radius Page* also contains the following fields:

- **IP Address** — Lists the RADIUS server IP addresses.
- **Priority** — Displays the RADIUS server priority. The possible values are 1-65535, where 1 is the highest value. The RADIUS server priority is used to configure the server query order.
- **Authentication Port** — Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.
- **Number of Retries** — Defines the number of transmitted requests sent to the RADIUS server before a failure occurs. The possible field values are 1-10. Three is the default value.
- **Timeout for Reply** — Defines the amount of 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** — Defines the amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. The default is 0 minutes.
- **Source IP Address** — Defines the source IP address that is used for communication with RADIUS servers.
- **Usage Type** — Specifies the RADIUS server authentication type. The default value is All. The possible field values are:
  - – *Log in* — Indicates the RADIUS server is used for authenticating user name and passwords.
  - – *802.1X* — Indicates the RADIUS server is used for 802.1X authentication.
  - – *All* — Indicates the RADIUS server is used for authenticating user names and passwords, and 802.1X port authentication.
- **Remove** — Removes a RADIUS server. The possible field values are:
  - – *Checked* — Removes the selected RADIUS server.
  - – *Unchecked* — Maintains the RADIUS servers. This is the default value.

2. Click Create. The *Add Radius Server Page* opens:

Figure 37: Add Radius Server Page



Add RADIUS Server

Host IP Address			
Priority	0		
Authentication Port	1812		
Number of Retries			□ Use Default
Timeout for Reply		(Sec)	□ Use Default
Dead Time		(Min)	□ Use Default
Key String		(Alpha Numeric)	□ Use Default
Source IP Address			□ Use Default
Usage Type	All ▾		

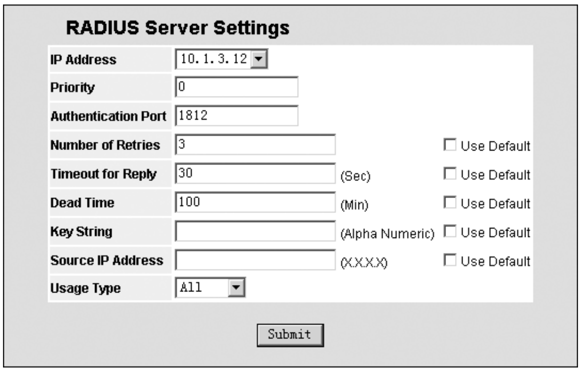
3. Define the fields.

4. Click Submit. The RADIUS server is added, and the device is updated.

To modify RADIUS server settings:

1. Click ✎ . The *RADIUS Server Settings Page* opens:

Figure 38: RADIUS Server Settings Page



RADIUS Server Settings

IP Address	10.1.3.12 ▾		
Priority	0		
Authentication Port	1812		
Number of Retries	3		□ Use Default
Timeout for Reply	30	(Sec)	□ Use Default
Dead Time	100	(Min)	□ Use Default
Key String		(Alpha Numeric)	□ Use Default
Source IP Address		(X.X.X.X)	□ Use Default
Usage Type	All ▾		

2. Modify the fields.

3. Click Submit. The RADIUS server settings are saved, and the device is updated.

5.1.2 Configuring Passwords

This section contains information for defining device passwords, and includes the following topics.

- Defining Local Users
- Defining Line Passwords
- Defining Enable Passwords

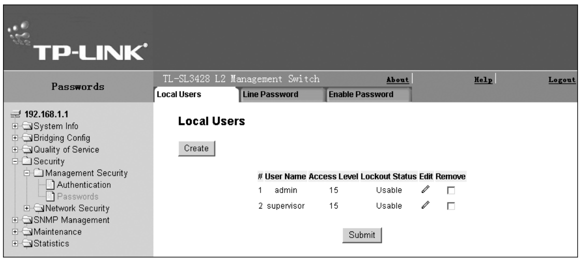
5.1.2.1 Defining Local Users

Network administrators can define users, passwords, and access levels for users using the *Local Users Page*.

To define local users:

1. Click **System > Management Security > Passwords > Local Users**. The *Local Users Page* opens:

Figure 39: Local Users Page



Local Users

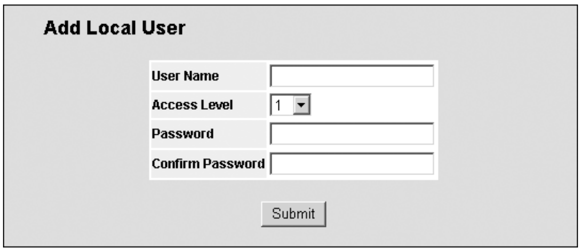
#	User Name	Access Level	Lockout Status	Edit	Remove
1	admin	15	Usable	✎	□
2	supervisor	15	Usable	✎	□

The *Local Users Page* contains the following fields:

- **User Name** — Displays the user name.
- **Access Level** — Displays the user access level. The lowest user access level is 1 and the highest is 15. Users with access level 15 are Privileged Users.
- **Reactivate User** — Changes the user status to active.
- **Remove** — Removes the user from the User Name list. The possible field values are:
  – *Checked* — Removes the selected local user.
  – *Unchecked* — Maintains the local users.

2. Click Create. The *Add Local User Page* opens:

Figure 40: Add Local User Page



Add Local User

User Name	
Access Level	1 ▾
Password	
Confirm Password	

In addition to the fields in the *Local Users Page*, the *Add Local User Page* contains the following fields:

- **Password** — Defines the local user password. Local user passwords can contain up to 159 characters.
- **Confirm Password** — Verifies the password.

3. Define the fields.

4. Click Submit. The Local User password is saved, and the device is updated.

5.1.2.2 Defining Line Passwords

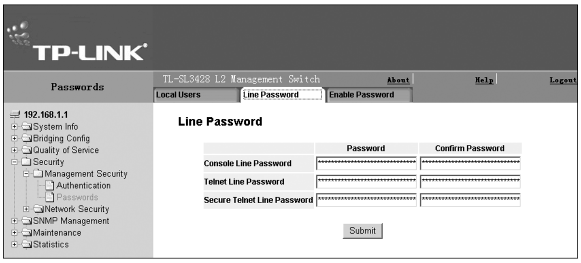
Network administrators can define line passwords in the *Line Password Page*. After the line password is defined, a management method is assigned to the password. The device can be accessed using the following methods:

- Console Passwords
- Telnet Passwords
- Secure Telnet Passwords

To configure line passwords:

1. Click **System > Management Security > Passwords > Line Password**. The *Line Password Page* opens:

Figure 41: Line Password Page



Line Password

	Password	Confirm Password
Console Line Password	******************************	******************************
Telnet Line Password	******************************	******************************
Secure Telnet Line Password	******************************	******************************

The *Line Password Page* contains the following fields:

- **Console Line Password** — Defines the line password for accessing the device via a Console session. Passwords can contain a maximum of 159 characters.
- **Telnet Line Password** — Defines the line password for accessing the device via a Telnet session. Passwords can contain a maximum of 159 characters.
- **Secure Telnet Line Password** — Defines the line password for accessing the device via a secure Telnet session. Passwords can contain a maximum of 159 characters.
- **Confirm Password** — Confirms the new line password. The password appears in the ***** format.

2. Define the *Console Line Password, Telnet Line Password*, and *Secure Telnet Line Password* fields.
3. Redefine the *Confirm Password* field for each of the passwords defined in the previous steps to verify the passwords.
4. Click Submit. Line password is configured and device is updated.

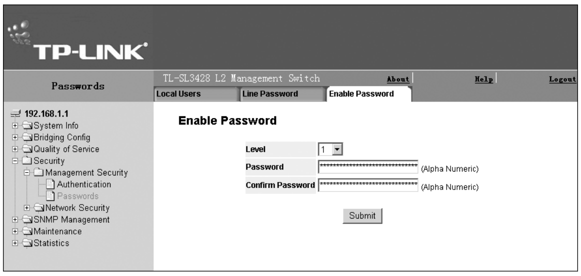
5.1.2.3 Defining Enable Passwords

The *Enable Password Page* sets a local password for a particular access level.

To enable passwords:

1. Click **System > Management Security > Passwords > Enable Password**. The *Enable Password Page* opens:

Figure 42: Enable Password Page



Enable Password

Level	1	
Password	******************************	(Alpha Numeric)
Confirm Password	******************************	(Alpha Numeric)

The *Enable Password Page* contains the following fields:

- **Enable Access Level** — Defines the access level associated with the enable password. Possible field val-ues are 1-15.
- **Password** — Defines the enable password.
- **Confirm Password** — Confirms the new enable password. The password appears in the ***** format.

2. Configure the fields and click Submit.The password is enabled and the device is updated.

5.2 Configuring Network Security

Network security manages both access control lists and locked ports. This section contains the following topics:

- Network Security Overview
- Defining Network Authentication Properties
- Configuring Traffic Control

5.2.1 Network Security Overview

This section provides an overview of network security and contains the following topics:

- Port-Based Authentication
- Advanced Port-Based Authentication

5.2.1.1 Port-Based Authentication

Port-based authentication authenticates users on a per-port basis via an external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the RADIUS server using the *Extensible Authentication Protocol* (EAP). Port-based authentication includes:

- **Authenticators** — Specifies the device port which is authenticated before permitting system access.
- **Supplicants** — Specifies the host connected to the authenticated port requesting to access the system ser-vices.
- **Authentication Server** — Specifies the server that performs the authentication on behalf of the authenticator, and indicates whether the supplicant is authorized to access system services.

Port-based authentication creates two access states:

- **Controlled Access** — Permits communication between the supplicant and the system, if the supplicant is authorized.
- **Uncontrolled Access** — Permits uncontrolled communication regardless of the port state.

The device currently supports port-based authentication via RADIUS servers.

5.2.1.2 Advanced Port-Based Authentication

Advanced port-based authentication enables multiple hosts to be attached to a single port. Advanced port-based authentication requires only one host to be authorized for all hosts to have system access. If the port is unautho-rized, all attached hosts are denied access to the network.

Advanced port-based authentication also enables user-based authentication. Specific VLANs in the device are always available, even if specific ports attached to the VLAN are unauthorized. For example, Voice over IP does not require authentication, while data traffic requires authentication. VLANs for which authorization is not required can be defined. Unauthenticated VLANs are available to users, even if the ports attached to the VLAN are defined as authorized.

Advanced port-based authentication is implemented in the following modes:

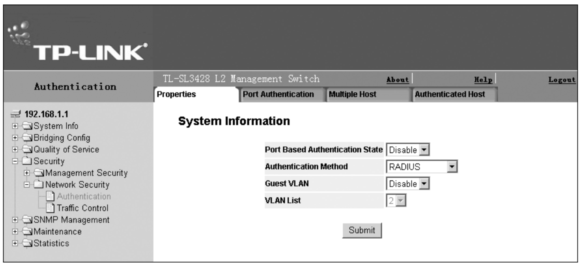
- **Single Host Mode** — Allows port access only to the authorized host.
- **Multiple Host Mode** — Multiple hosts can be attached to a single port. Only one host must be authorized for all hosts to access the network. If the host authentication fails, or an EAPOL-logoff message is received, all attached clients are denied access to the network.
- **Guest VLANs** — Provides limited network access to authorized ports. If a port is denied network access via port-based authorization, but the Guest VLAN is enabled, the port receives limited network access. For example, a network administrator can use Guest VLANs to deny network access via port-based authentication, but grant Internet access to unauthorized users.
- **Unauthenticated VLANS** — Are available to users, even if the ports attached to the VLAN are defined as unauthorized.

5.2.2 Defining Network Authentication Properties

The *Network Security Authentication Properties Page* allows network managers to configure network authentication parameters. In addition, Guest VLANs are enabled from the *Network Security Authentication Properties Page*.

To define the network authentication properties:

1. Click **System > Network Security > Authentication > Properties**. The *Network Security Authentication Properties Page* opens:



System Information

Port Based Authentication State: Disable
Authentication Method: RADIUS
Guest VLAN: Disable
VLAN List: 2

Figure 43: Network Security Authentication Properties Page

The *Network Security Authentication Properties Page* contains the following fields:

- **Port-Based Authentication State** — Indicates if Port Authentication is enabled 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** — Specifies the authentication method used for port authentication. The possible field values are:
  – *None* — Indicates that no authentication method is used to authenticate the port.
  – *RADIUS* — Provides port authentication using the RADIUS server.
  – *RADIUS, None* — Provides port authentication, first using the RADIUS server. If the port is not authenticated, then no authentication method is used, and the session is permitted.
- **Guest VLAN** — Specifies whether the Guest VLAN is enabled on the device. The possible field values are:
  – *Enable* — Enables using a Guest VLAN for unauthorized ports. If a Guest VLAN is enabled, the unauthorized port automatically joins the VLAN selected in the VLAN List field.
  – *Disable* — Disables port-based authentication on the device. This is the default.
- **Guest VLAN ID** — Contains a list of VLANs. The Guest VLAN is selected from the VLAN list.

2. Enable the *Port-Based Authentication, and define the Authentication Method, enable Guest VLAN, and select the Guest VLAN ID*.

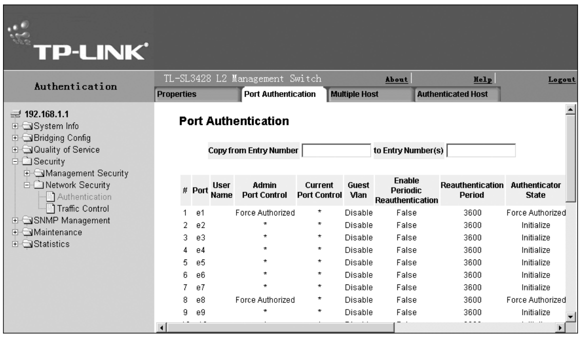
3. Click Submit. The network security authentication properties are saved, and the device is updated.

5.2.2.1 Defining Port Authentication Properties

The *Port Authentication Page* allows network managers to configure port-based authentication global parameters.

To define the port-based authentication global properties:

1. Click **System > Network Security > Authentication > Port Authentication**. The *Port Authentication Page* opens:



Port Authentication

Copy from Entry Number:
to Entry Number(s):

#	Port	User Name	Admin Port Control	Current Port Control	Guest Vlan	Enable Periodic Reauthentication	Reauthentication Period	Authenticator State
1	e1		Force Authorized	*	Disable	False	3600	Force Authorized
2	e2		*	*	Disable	False	3600	Initialize
3	e3		*	*	Disable	False	3600	Initialize
4	e4		*	*	Disable	False	3600	Initialize
5	e5		*	*	Disable	False	3600	Initialize
6	e6		*	*	Disable	False	3600	Initialize
7	e7		*	*	Disable	False	3600	Initialize
8	e8		Force Authorized	*	Disable	False	3600	Force Authorized
9	e9		*	*	Disable	False	3600	Initialize

Figure 44: Port Authentication Page

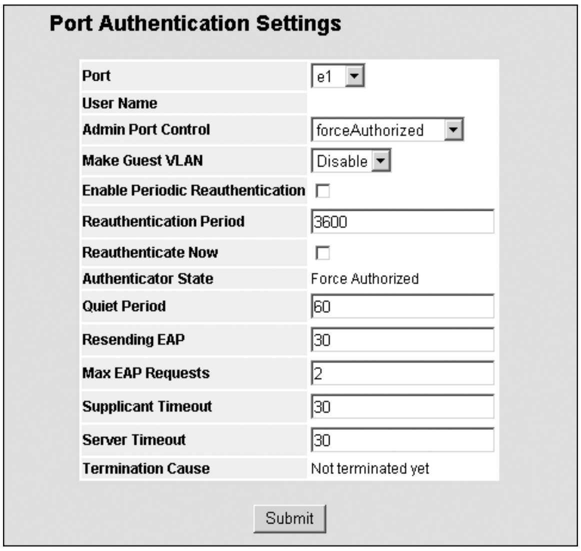
The *Port Authentication Page* contains the following fields:

- **Copy from Entry Number** — Copies port authentication information from the selected port.
- **to Entry Number(s)** — Copies port authentication information to the selected port.
- **Port** — Displays a list of interfaces on which port-based authentication is enabled.
- **User Name** — Displays the supplicant user name.

- **Current Port Control** — Displays the current port authorization state. The possible field values are:
  – *Auto* — Enables port-based authentication on the device. The interface moves between an authorized or unauthorized state based on the authentication exchange between the device and the client.
  – *Authorized* — Indicates the interface is in an authorized state without being authenticated. The interface re-sends and receives normal traffic without client port-based authentication.
  – *Unauthorized* — Denies the selected interface system access by moving the interface into unauthorized state. The device cannot provide authentication services to the client through the interface.
- **Enable Periodic Reauthentication** — Permits immediate port reauthentication. The possible field values are:
  – *Enable* — Enables immediate port reauthentication. This is the default value.
  – *Disable* — Disables port reauthentication.
- **Reauthentication Period** — Displays the time span (in seconds) in which the selected port is reauthenticated. The field default is 3600 seconds.
- **Authenticator State** — Displays the current authenticator state.
- **Quiet Period** — Displays 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.
- **Resending EAP** — Defines the amount of time (in seconds) that lapses before EAP requests are resent. The field default is 30 seconds.
- **Max EAP Requests** — Displays 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.
- **Supplicant Timeout** — Displays the amount of time (in seconds) that lapses before EAP requests are resent to the supplicant. The field default is 30 seconds.
- **Server Timeout** — Displays the amount of time (in seconds) that lapses before the device re-sends a request to the authentication server. The field default is 30 seconds.
- **Termination Cause** — Indicates the reason for which the port authentication was terminated.

2. Click ✎ . The *Port Authentication Settings Page* opens:

Figure 45: Port Authentication Settings Page



Port Authentication Settings

Port	e1
User Name	
Admin Port Control	forceAuthorized
Make Guest VLAN	Disable
Enable Periodic Reauthentication	□
Reauthentication Period	3600
Reauthenticate Now	□
Authenticator State	Force Authorized
Quiet Period	60
Resending EAP	30
Max EAP Requests	2
Supplicant Timeout	30
Server Timeout	30
Termination Cause	Not terminated yet

3. Define the fields.
4. Check "Reauthenticate Now" to immediately reauthenticate the selected port when submitting.
5. Click Submit. The port authentication settings are saved, and the device is updated.

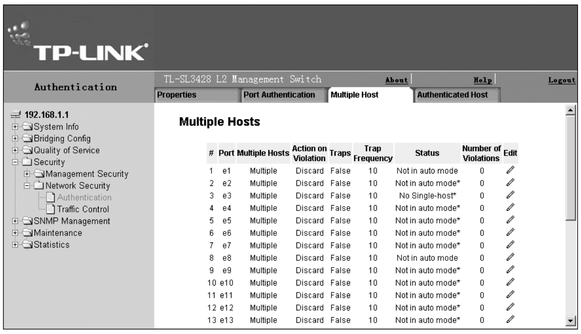
5.2.2.2 Configuring Multiple Hosts

The *Multiple Hosts Page* allows network managers to configure advanced port-based authentication settings for specific ports and VLANs. For more information on advanced port-based authentication, see *Advanced Port-Based Authentication*.

To define the network authentication global properties:

1. Click **System > Network Security > Authentication > Multiple Hosts**. The *Multiple Hosts Page* opens:

Figure 46: Multiple Hosts Page



Multiple Hosts

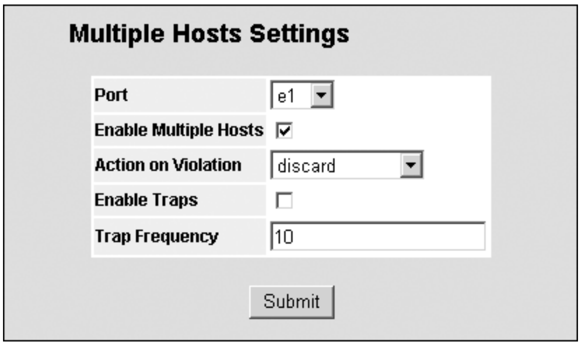
#	Port	Multiple Hosts	Action on Violation	Traps	Trap Frequency	Status	Number of Violations	Edit
1	e1	Multiple	Discard	False	10	Not in auto mode	0	✎
2	e2	Multiple	Discard	False	10	Not in auto mode*	0	✎
3	e3	Multiple	Discard	False	10	No Single-host*	0	✎
4	e4	Multiple	Discard	False	10	Not in auto mode*	0	✎
5	e5	Multiple	Discard	False	10	Not in auto mode*	0	✎
6	e6	Multiple	Discard	False	10	Not in auto mode*	0	✎
7	e7	Multiple	Discard	False	10	Not in auto mode*	0	✎
8	e8	Multiple	Discard	False	10	Not in auto mode	0	✎
9	e9	Multiple	Discard	False	10	Not in auto mode*	0	✎
10	e10	Multiple	Discard	False	10	Not in auto mode*	0	✎
11	e11	Multiple	Discard	False	10	Not in auto mode*	0	✎
12	e12	Multiple	Discard	False	10	Not in auto mode*	0	✎
13	e13	Multiple	Discard	False	10	Not in auto mode*	0	✎

The *Multiple Hosts Page* contains the following fields:

- **Port** — Displays the port number for which advanced port-based authentication is enabled.
- **Multiple Hosts** — Indicates whether multiple hosts are enabled. Multiple hosts must be enabled in order to either disable the ingress-filter, or to use port-lock security on the selected port. The possible field values are:
  - *Multiple* — Multiple hosts are enabled.
  - *Disable* — Multiple hosts are disabled.
- **Action on Violation** — Defines the action to be applied to packets arriving in single-host mode, from a host whose MAC address is not the supplicant MAC address. The possible field values are:
  - *Forward* — Forwards the packet.
  - *Discard* — Discards the packets. This is the default value.
  - *Shutdown* — Discards the packets and shuts down the port. The port remains shut down until reactivated, or until the device is reset.
- **Traps** — Indicates if traps are enabled for Multiple Hosts. The possible field values are:
  - *True* — Indicates that traps are enabled for Multiple hosts.
  - *False* — Indicates that traps are disabled for Multiple hosts.
- **Trap Frequency** — Defines the time period by which traps are sent to the host. The Trap Frequency (1-1000000) field can be defined only if multiple hosts are disabled. The default is 10 seconds.
- **Status** — Indicates the host status. If there is an asterisk (*), the port is either not linked or is down. The possible field values are:
  - *Unauthorized* — Indicates that either the port control is Force Unauthorized and the port link is down, or the port control is Auto but a client has not been authenticated via the port.
  - *Not in Auto Mode* — Indicates that the port control is Forced Authorized, and clients have full port access.
  - *Single-host Lock* — Indicates that the port control is Auto and a single client has been authenticated via the port.
  - *No Single Host* — Indicates that Multiple Host is enabled.
- **Number of Violations** — Indicates the number of packets that arrived on the interface in single-host mode, from a host whose MAC address is not the supplicant MAC address.

2. Click ✎ . The *Multiple Host Settings Page* opens:

Figure 47: Multiple Host Settings Page



Multiple Hosts Settings

Port	e1
Enable Multiple Hosts	☑
Action on Violation	discard
Enable Traps	□
Trap Frequency	10

3. Define the fields.

4. Click Submit. The multiple host settings are saved, and the device is updated.

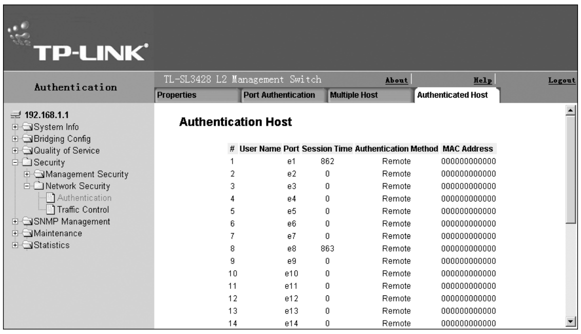
5.2.2.3 Defining Authentication Hosts

The *Authenticated Hosts Page* contains a list of authenticated users.

To define authenticated users:

1. Click **System > Network Security > Authentication > Authenticated Hosts**. The *Authenticated Hosts Page* opens:

Figure 48: Authenticated Hosts Page



Authentication Host

#	User Name	Port	Session Time	Authentication Method	MAC Address
1		e1	862	Remote	000000000000
2		e2	0	Remote	000000000000
3		e3	0	Remote	000000000000
4		e4	0	Remote	000000000000
5		e5	0	Remote	000000000000
6		e6	0	Remote	000000000000
7		e7	0	Remote	000000000000
8		e8	863	Remote	000000000000
9		e9	0	Remote	000000000000
10		e10	0	Remote	000000000000
11		e11	0	Remote	000000000000
12		e12	0	Remote	000000000000
13		e13	0	Remote	000000000000
14		e14	0	Remote	000000000000

The *Authenticated Hosts Page* contains the following fields:

- **User Name** — Lists the supplicants that were authenticated, and are permitted on each port.
- **Port** — Displays the port number.
- ***Session Time*** — Displays the amount of time (in seconds) the supplicant was logged on the port.
- **Authentication Method** — Displays the method by which the last session was authenticated. The possible field values are:
  - *Remote* — 802.1x authentication is not used on this port (port is forced-authorized).
  - *None* — The supplicant was not authenticated.
  - *RADIUS* — The supplicant was authenticated by a RADIUS server.
- **MAC Address** — Displays the supplicant MAC address.

5.2.3 Configuring Traffic Control

This section contains information for managing both port security and storm control, and includes the following topics:

- Managing Port Security
- Enabling Storm Control

5.2.3.1 Managing 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 or 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 TP-Link source MAC address is not tied to that port (either it was learned on a different port, or it is unknown to the system), the protection mechanism is invoked, and can provide various options.

Unauthorized packets arriving at a locked port are either:

- Forwarded
- Discarded with no trap
- Discarded with a trap
- Shuts down the port

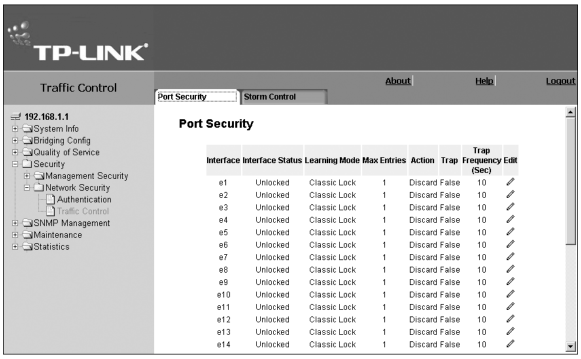
Locked port security also enables storing a list of MAC addresses in the configuration file. The MAC address list can be restored after the device has been reset.

Disabled ports are activated from the *Port Security Page*.

To view port security parameters:

1. Click **System > Network Security > Traffic Control > Port Security**. The *Port Security Page* opens:

Figure 49: Port Security Page



Port Security

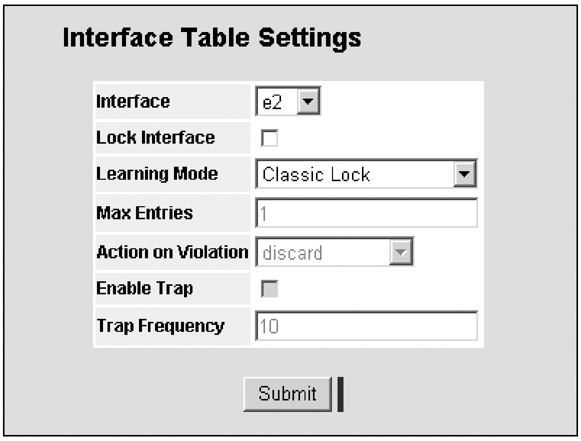
Interface	Interface Status	Learning Mode	Max Entries	Action	Trap	Trap Frequency (Sec)	Edit
e1	Unlocked	Classic Lock	1	Discard	False	10	✎
e2	Unlocked	Classic Lock	1	Discard	False	10	✎
e3	Unlocked	Classic Lock	1	Discard	False	10	✎
e4	Unlocked	Classic Lock	1	Discard	False	10	✎
e5	Unlocked	Classic Lock	1	Discard	False	10	✎
e6	Unlocked	Classic Lock	1	Discard	False	10	✎
e7	Unlocked	Classic Lock	1	Discard	False	10	✎
e8	Unlocked	Classic Lock	1	Discard	False	10	✎
e9	Unlocked	Classic Lock	1	Discard	False	10	✎
e10	Unlocked	Classic Lock	1	Discard	False	10	✎
e11	Unlocked	Classic Lock	1	Discard	False	10	✎
e12	Unlocked	Classic Lock	1	Discard	False	10	✎
e13	Unlocked	Classic Lock	1	Discard	False	10	✎
e14	Unlocked	Classic Lock	1	Discard	False	10	✎

The *Port Security Page* contains the following fields:

- **Interface** — Displays the *Port* or *LAG* name.
- **Interface Status** — Indicates the host status. The possible field values are:
  - – *Unauthorized* — Indicates that the port control is Force Unauthorized, the port link is down or the port control is Auto, but a client has not been authenticated via the port.
  - – *Not in Auto Mode* — Indicates that the port control is Forced Authorized, and clients have full port access.
  - – *Single-host Lock* — Indicates that the port control is Auto and a single client has been authenticated via the port.
- **Learning Mode** — Defines the locked port type. The Learning Mode field is enabled only if Locked is selected in the Set Port field.The possible field values are:
  - – *Classic Lock* — Locks the port using the classic lock mechanism. The port is immediately locked, regardless of the number of addresses that have already been learned.
  - – *Limited Dynamic Lock* — Locks the port by deleting the current dynamic MAC addresses associated with the port. The port learns up to the maximum addresses allowed on the port. Both relearning and aging MAC addresses are enabled.
- **Max Entries** — Specifies the number of MAC address that can be learned on the port. The Max Entries field is enabled only if Locked is selected in the Set Port field. In addition, the Limited Dynamic Lock mode is selected. The default is 1.
- **Action** — Indicates the action to be applied to packets arriving on a locked port. The possible field values are:
  - – *Forward* — Forwards packets from an unknown source without learning the MAC address.
  - – *Discard* — Discards packets from any unlearned source. This is the default value.
  - – *Shutdown* — Discards packets from any unlearned source and shuts down the port. The port remains shut down until reactivated, or until the device is reset.
- **Trap** — Enables traps when a packet is received on a locked port. The possible field values are:
  - – Checked — Enables traps.
  - – Unchecked — Disables traps.
- **Trap Frequency (Sec.)** — The amount of time (in seconds) between traps. The default value is 10 seconds To modify port security:

1. Click ✎ . The *Port Security Settings Page* opens:

Figure 50: Port Security Settings Page



Interface Table Settings

Interface	e2
Lock Interface	□
Learning Mode	Classic Lock
Max Entries	1
Action on Violation	discard
Enable Trap	□
Trap Frequency	10

2. Modify port security settings fields.
3. Click Submit. The port security settings are saved, and the device is updated.

5.2.3.2 Enabling Storm Control

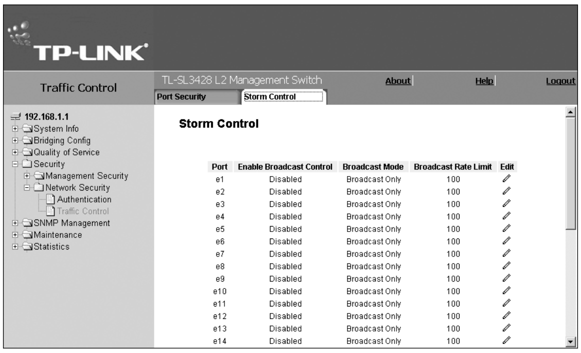
Storm control limits the amount of Multicast and Broadcast frames accepted and forwarded by the device. When Layer 2 frames are forwarded, Broadcast, and Multicast frames are flooded to all ports on the relevant VLAN. This occupies bandwidth, and loads all nodes on all ports.

A Broadcast Storm 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. Storm control is enabled for all Gigabit ports by defining the packet type and the rate the packets are transmitted. The system measures the incoming Broadcast and Multicast frame rates separately on each port, and discards the frames when the rate exceeds a user-defined rate. The *Storm Control Page* provides fields for configuring broadcast storm control.

To enable storm control for a port:

1. Click **System > Network Security > Traffic Control > Storm Control**. The *Storm Control Page* opens:

Figure 51: Storm Control Page



Storm Control

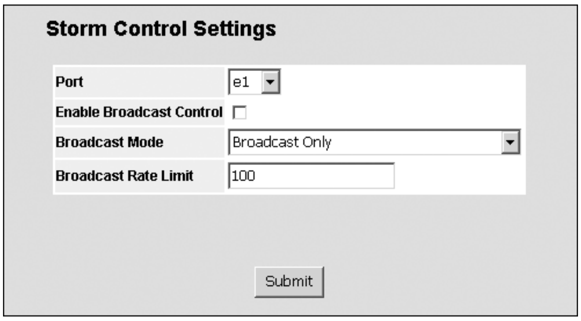
Port	Enable Broadcast Control	Broadcast Mode	Broadcast Rate Limit	Edit
e1	Disabled	Broadcast Only	100	✎
e2	Disabled	Broadcast Only	100	✎
e3	Disabled	Broadcast Only	100	✎
e4	Disabled	Broadcast Only	100	✎
e5	Disabled	Broadcast Only	100	✎
e6	Disabled	Broadcast Only	100	✎
e7	Disabled	Broadcast Only	100	✎
e8	Disabled	Broadcast Only	100	✎
e9	Disabled	Broadcast Only	100	✎
e10	Disabled	Broadcast Only	100	✎
e11	Disabled	Broadcast Only	100	✎
e12	Disabled	Broadcast Only	100	✎
e13	Disabled	Broadcast Only	100	✎
e14	Disabled	Broadcast Only	100	✎

The *Storm Control Page* contains the following fields:

- **Port** — Indicates the type of storm control which is enabled on the selected port. The possible field values are:
  – *U, cast B, cast M* — tbd
  – *B, cast M, cast* — tbd
  – *B, cast* — tbd
- **Enable Broadcast Control** — Indicates if forwarding Broadcast packet types on the interface.
- **Broadcast Mode** — Specifies the Broadcast mode currently enabled on the device. The possible field values are:
  – *Unknown Unicast, Multicast & Broadcast* — Counts Unicast, Multicast, and Broadcast traffic.
  – *Multicast & Broadcast* — Counts both Broadcast and Multicast traffic together.
  – *SOHO Broadcast* — Counts only the Broadcast traffic.
- **Broadcast Rate Threshold** — Indicates the maximum rate (kilobytes per second) at which unknown packets are forwarded. The range is 0-1,000,000. The default value is zero. All values are rounded to the nearest 64 Kbps. If the field value is under 64 Kbps, the value is rounded up to 64 Kbps, with the exception of the value zero.

2. Click ✎ next to the port to configure. The *Storm Control Settings Page* opens:

Figure 52: Storm Control Settings Page



Storm Control Settings

Port	e1
Enable Broadcast Control	□
Broadcast Mode	Broadcast Only
Broadcast Rate Limit	100

3. Select the *Port Storm Control Settings*.
4. Click *Enable Broadcast Control*, and define the *Rate Threshold*.
5. Click Submit. Storm control is enabled on the device for the selected port.

Section 6. Defining IP Addresses

This section provides information for defining IP addresses on the device using DHCP and ARP. In addition, this section contains parameters for defining device default gateways, and Domain Name Servers.

This section contains the following topics:

- Defining IP Addressing
- Defining Domain Name System

6.1 Defining IP Addressing

This section provides information for assigning interface and default gateway IP addresses, and defining ARP and DHCP parameters for the interfaces.

This section contains the following topics:

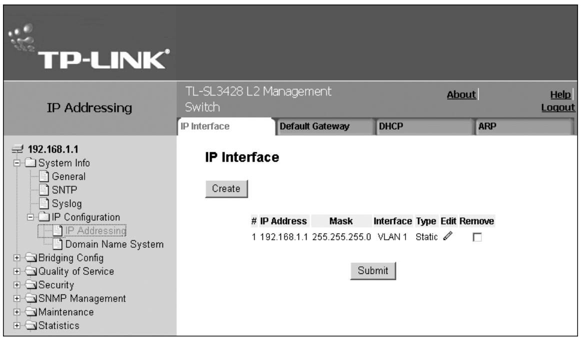
- Defining IP Addresses
- Defining the Default Gateway
- Defining DHCP Addresses
- Defining ARP

6.1.1 Defining IP Addresses

The IP Interface Page contains fields for assigning IP addresses. 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.

1. Click **System > System Info > IP Configuration > IP Addressing**. The *IP Interface Page* opens:

Figure 53: IP Interface Page



IP Interface

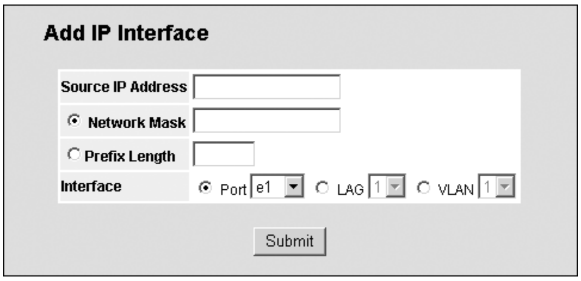
#	IP Address	Mask	Interface	Type	Edit	Remove
1	192.168.1.1	255.255.255.0	VLAN 1	Static	✎	□

The *IP Interface Page* contains the following fields:

- **IP Address** — Displays the currently configured IP address.
- **Mask** — Displays the currently configured IP address mask.
- **Interface** — Displays the interface used to manage the device.
- **Dynamic** — Indicates that the IP address is dynamically created.
- **Static** — Indicates the IP address is a static IP address.
- **Remove** — Removes the selected IP address from the interface. The possible field values are:
  – *Checked* — Removes the IP address from the interface.
  – *Unchecked* — Maintains the IP address assigned to the Interface.

2. Click Create. The *Add IP Interface Page* opens:

Figure 54: Add IP Interface Page



Add IP Interface

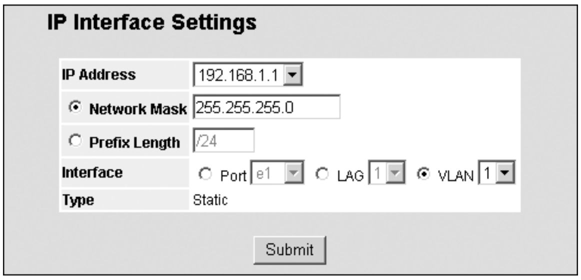
Source IP Address	
● Network Mask	
○ Prefix Length	
Interface	● Port e1 ○ LAG 1 ○ VLAN 1

3. Define the *IP Address, Network Mask, Prefix Length* and *Interface* (Port, LAG or VLAN).
4. Click Submit. The new interface is added and the device is updated.

To modify IP interface settings:

1. Click **System > System Info > IP Configuration > IP Addressing**. The *IP Interface Page* opens.
2. Click . The *IP Interface Settings Page* opens:

Figure 55: IP Interface Settings Page



IP Interface Settings

IP Address	192.168.1.1
● Network Mask	255.255.255.0
○ Prefix Length	/24
Interface	○ Port e1 ○ LAG 1 ● VLAN 1
Type	Static

3. Modify the *IP Address and Interface* fields.
4. Click Submit. The interface is modified and the device is updated.

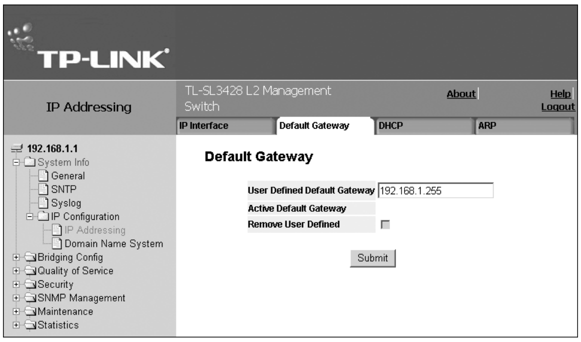
6.1.2 Defining the Default Gateway

Packets are forwarded to the default IP when frames are sent to a remote network via the default gateway. The configured IP address must belong to the same subnet of one of the IP interfaces.

To define a default gateway for the system:

1. Click **System > System Info > IP Configuration > IP Addressing > Default Gateway**. The *Default Gateway Page* opens:

Figure 56: Default Gateway Page



Default Gateway

User Defined Default Gateway	192.168.1.255
Active Default Gateway	
Remove User Defined	□

The *Default Gateway Page* contains the following fields:

- **User Defined Default Gateway** — Indicates the name of the current default gateway.
- **Active Default Gateway** — Indicates if the current default gateway is defined as active.
- **Remove** — Removes the defined default gateway.

2. Enter the name of the *User Defined Default Gateway*.
3. Click Submit. The gateway is saved and the device is updated.

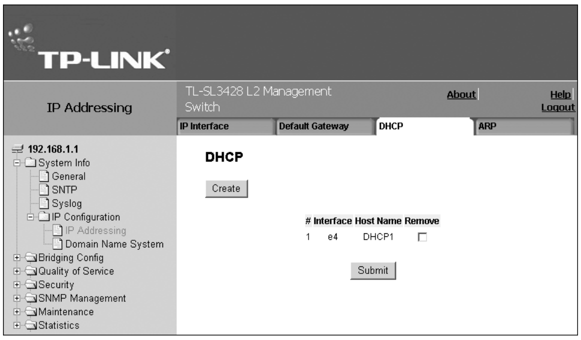
6.1.3 Defining DHCP Addresses

The Dynamic Host Configuration Protocol (DHCP) assigns dynamic IP addresses to devices on a network. DHCP ensures that network devices can have a different IP address every time the device connects to the network.

To define DHCP addressing:

1. Click **System > System Info > IP Configuration > IP Addressing > DHCP**. The *DHCP Page* opens:

Figure 57: DHCP Page



DHCP

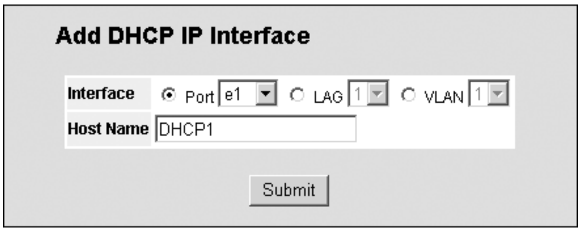
#	Interface	Host Name	Remove
1	e4	DHCP1	□

The *DHCP Page* contains the following fields:

- Interface — Displays the IP address of the interface which is connected to the DHCP server.
- **Host Name** — Displays the system name.
- **Remove** — Removes DHCP interfaces. The possible field values are:
  - *Checked* — Removes the selected DHCP interface.
  - *Unchecked* — Maintains the DHCP interfaces.

2. Click Create. The *Add IP Interface Page* page opens:

Figure 58: Add IP Interface Page



Add DHCP IP Interface

Interface	● Port e1 ○ LAG 1 ○ VLAN 1
Host Name	DHCP1

3. Select the *Interface* (Port, LAG or VLAN).
4. Enter the *Host Name*.
5. Click Submit. The new interface is added to DHCP, and the device is updated.

To remove the DHCP definition:

- Click the *Remove* checkbox. The current DHCP definition is removed and system information is updated.

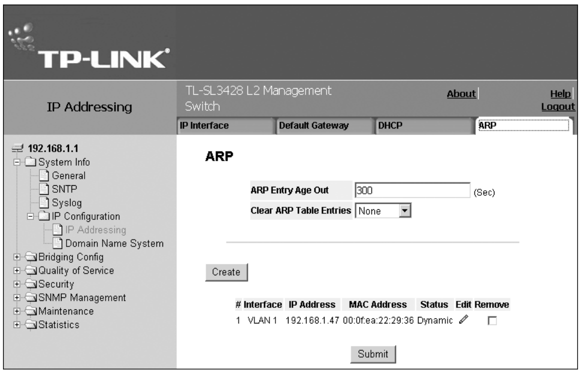
6.1.4 Defining ARP

The Address Resolution Protocol (ARP) converts IP addresses into physical addresses, and maps the IP address to a MAC address. ARP allows a host to communicate with other hosts only when the IP address of its neighbors is known.

To define ARP:

1. Click **System > System Info > IP Configuration > IP Addressing > ARP**. The *ARP Page* opens:

Figure 59: ARP Page



ARP

ARP Entry Age Out	300 (Sec)
Clear ARP Table Entries	None

#	Interface	IP Address	MAC Address	Status	Edit	Remove
1	VLAN 1	192.168.1.47	00:0f:ea:22:29:36	Dynamic	✎	□

The *ARP Page* contains the following fields:

- **ARP Entry Age Out** — Specifies the amount of time (in seconds) that passes between ARP Table entry. requests. Following the ARP Entry Age period, the entry is deleted from the table. The range is 1 - 40000000. The default value is 60000 seconds.
- **Clear ARP Table Entries** — Specifies the types of ARP entries that are cleared. The possible values are:
  - *None* — Maintains the ARP entries.
  - *All* — Clears all ARP entries.
  - *Dynamic* — Clears only dynamic ARP entries.
  - *Static* — Clears only static ARP entries.
- **Interface** — Displays the interface type for ARP parameters. The possible field values are:
  - *Port* — Indicates the port for which ARP parameters are defined.
  - *LAG* — Indicates the LAG for which ARP parameters are defined.
  - *VLAN* — Indicates the VLAN for which ARP parameters are defined.

- **IP Address** - Indicates the station IP address, which is associated with the MAC address filled in below.
- **MAC Address** - Displays the station MAC address, which is associated in the ARP table with the IP address.
- **Status** - Displays the ARP table entry type. Possible field values are:

  – *Dynamic* — Indicates the ARP entry is learned dynamically.

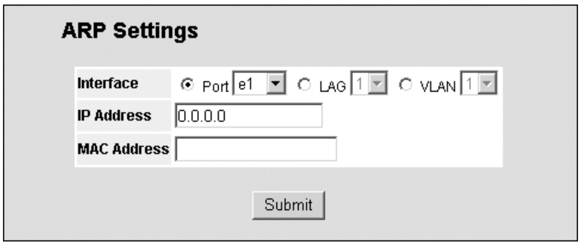
  – *Static* — Indicates the ARP entry is a static entry.
- **Remove** — Removes a specific ARP entry. The possible field values are:

  – *Checked* — Removes the selected ARP entries.

  – *Unchecked* - Maintains the current ARP entries.

2. Define the *ARP Entry Age Out* parameter.
3. Define the *Clear ARP Table Entries* parameter.
4. Click Create. The *Add ARP Entry Page* opens:

Figure 60: Add ARP Entry Page



ARP Settings

Interface	● Port e1 ○ LAG 1 ○ VLAN 1
IP Address	0.0.0.0
MAC Address	

5. Select the *Interface* (Port, LAG or VLAN).
6. Define the IP Address and the MAC Address.
7. Click Submit. The new entry is added to ARP, and the device is updated.

6.2 Defining 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 into 192.87.56.2. DNS servers maintain databases of domain names and their corresponding IP addresses.

This section contains the following topics:

- Defining DNS Servers
- Configuring Host Mapping

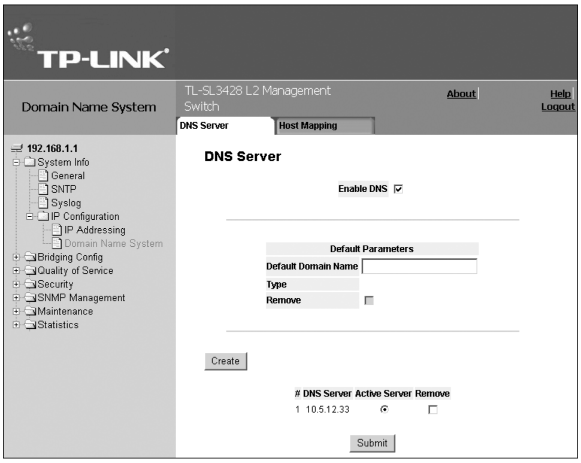
6.2.1 Defining DNS Servers

The DNS Server Page contains fields for enabling and activating specific DNS servers.

To enable DNS and define the DNS server:

1. Click **System > System Info > IP Configuration > Domain Name System**. The *DNS Server Page* opens:

Figure 61: DNS Server Page



DNS Server

Enable DNS ☑

Default Parameters	
Default Domain Name	
Type	
Remove	□

#	DNS Server	Active Server	Remove
1	10.5.12.33	●	□

The *DNS Server Page* contains the following fields:

- **Enable DNS** — Enables translating the DNS names into IP addresses. The possible field values are:

  – *Checked* — Translates the domains into IP addresses.

  – *Unchecked* — Disables translating domains into IP addresses.
- **Default Domain Name** — Specifies the user-defined DNS server name.
- **Type** — Displays the IP address type. The possible

field values are:

– *Dynamic* — The IP address is dynamically created.

– *Static* — The IP address is a static IP address.

- **Remove** — Removes DNS servers. The possible field values are:

  – *Checked* — Removes the selected DNS server

  – *Unchecked* — Maintains the current DNS server list.

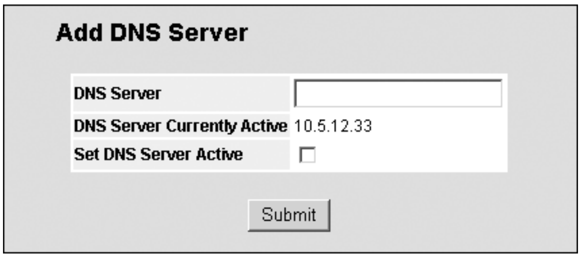
- **DNS Server** — Displays the DNS server IP address. DNS servers are added in the Add DNS Server Page.
- **Active Server** — Specifies the DNS server that is currently active. The possible field values are:

  – **Selected** — Activates the selected DNS server after the device is reset.

  – **Unselected** — Deactivates the selected DNS server after the device is reset. This is the default value.

2. Click the *Enable DNS* checkbox.
3. Define the *Default Domain Name*.
4. Click Create. The *Add DNS Server Page* opens:

Figure 62: Add DNS Server Page



Add DNS Server

DNS Server	
DNS Server Currently Active	10.5.12.33
Set DNS Server Active	□

5. Enter the *DNS Server* name and click *Set DNS Server Active*.
6. Click Submit. The new server is added, and device information is updated.

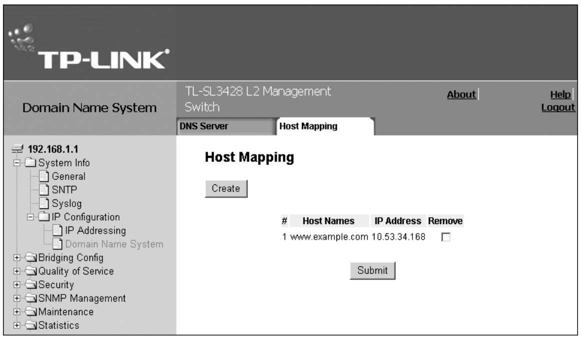
6.2.2 Configuring Host Mapping

The DNS Host Mapping Page provides information for defining DNS Host Mapping.

To define DNS host mapping:

1. Click **System > System Info > IP Configuration > Domain Name System > Host Mapping**. The *Host Mapping Page* opens:

Figure 63: Host Mapping Page



Host Mapping

#	Host Names	IP Address	Remove
1	www.example.com	10.53.34.168	□

The *Host Mapping Page* contains the following fields:

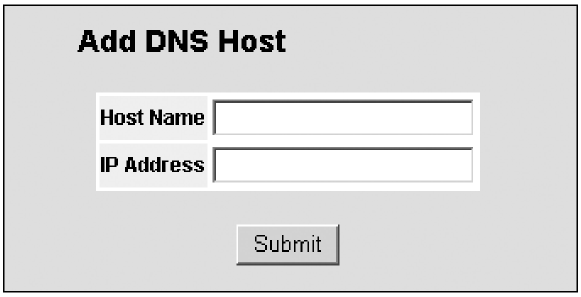
- **Host Names** — Displays a user-defined default domain name. When defined, the default domain name is applied to all unqualified host names. The Host Name field can contain up to 158 characters.
- **IP Address** — Displays the DNS host IP address.
- **Remove** — Removes default domain names. The possible field values are:

  – *Checked* — Removes the selected DNS host.

  – *Unchecked* — Maintains the current DNS host mapping list.

2. Click Create. The *Add DNS Host Page* opens:

Figure 64: Add DNS Host Page



Add DNS Host

Host Name	
IP Address	

3. Enter the *Host Name and IP Address.*

4. Click Submit. The new DNS host is added to the hosts list in the *Host Mapping Page.*

Section 7. Configuring Interfaces

This section contains the following topics:

- Configuring Ports
- Configuring LAGs
- Configuring VLANs

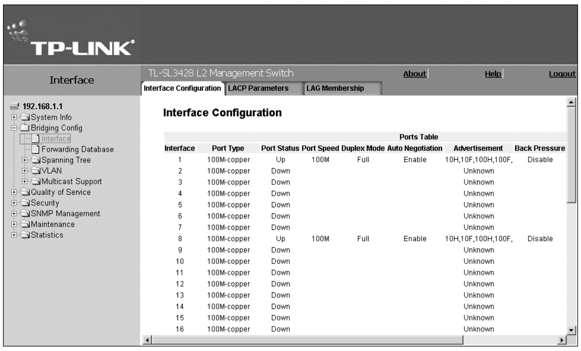
7.1 Configuring Ports

The *Interface Configuration Page* contains fields for defining port parameters.

To define port parameters:

1. Click **System > Bridging Config > Interface > Interface Configuration**. The *Interface Configuration Page* opens:

Figure 65: Interface Configuration Page



Interface Configuration

Ports Table

Interface	Port Type	Port Status	Port Speed	Duplex Mode	Auto Negotiation	Advertisement	Back Pressure
1	100M-copper	Up	100M	Full	Enable	10H,10F,100H,100F,	Disable
2	100M-copper	Down				Unknown	
3	100M-copper	Down				Unknown	
4	100M-copper	Down				Unknown	
5	100M-copper	Down				Unknown	
6	100M-copper	Down				Unknown	
7	100M-copper	Down				Unknown	
8	100M-copper	Up	100M	Full	Enable	10H,10F,100H,100F,	Disable
9	100M-copper	Down				Unknown	
10	100M-copper	Down				Unknown	
11	100M-copper	Down				Unknown	
12	100M-copper	Down				Unknown	
13	100M-copper	Down				Unknown	
14	100M-copper	Down				Unknown	
15	100M-copper	Down				Unknown	
16	100M-copper	Down				Unknown	

The *Interface Configuration Page* is divided into the following sections:

- Interface Configuration Ports Table
- Interface Configuration LAG Ports Table

The Interface Configuration Ports Table contains the following fields:

- **Interface** — Displays the port number.
- **Port Status** — Indicates whether the port is currently operational or non-operational. The possible field values are:
  – *Up* — Indicates the port is currently operating.
  – *Down* — Indicates the port is currently not operating.
- **Port Speed** — Displays the configured rate for the port. The port type determines what speed setting options are available. Port speeds can only be configured when auto negotiation is disabled. The possible field values are:
  – *10* — Indicates the port is currently operating at 10 Mbps.
  – *100* — Indicates the port is currently operating at 100 Mbps.
  – *1000* — Indicates the port is currently operating at 1000 Mbps.
- **Duplex Mode** — Displays the port duplex mode. This field is configurable only when auto negotiation is disabled, and the port speed is set to 10M or 100M. This field cannot be configured on LAGs. The possible field values are:
  – *Full* — The interface supports transmission between the device and its link partner in both directions simultaneously.
  – *Half* — The interface supports transmission between the device and the client in only one direction at a time.
- **Auto Negotiation** — Displays the auto negotiation status 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.
- Advertisement — Defines the auto negotiation setting the port advertises. The possible field values are:
  – *Max Capability* — Indicates that all port speeds and duplex mode settings are accepted.
  – *10 Half* — Indicates that the port advertises for a 10 Mbps speed port and half duplex mode setting.
  – *10 Full* — Indicates that the port advertises for a 10 Mbps speed port and full duplex mode setting.
  – *100 Half* — Indicates that the port advertises for a 100 Mbps speed port and half duplex mode setting.
  – *100 Full* — Indicates that the port advertises for a 100 Mbps speed port and full duplex mode setting.
  – *1000 Full* — Indicates that the port advertises for a 1000 Mbps speed port and full duplex mode setting.

– *1000 Half* — Indicates that the port advertises for a 1000 Mbps speed port and half duplex mode setting.

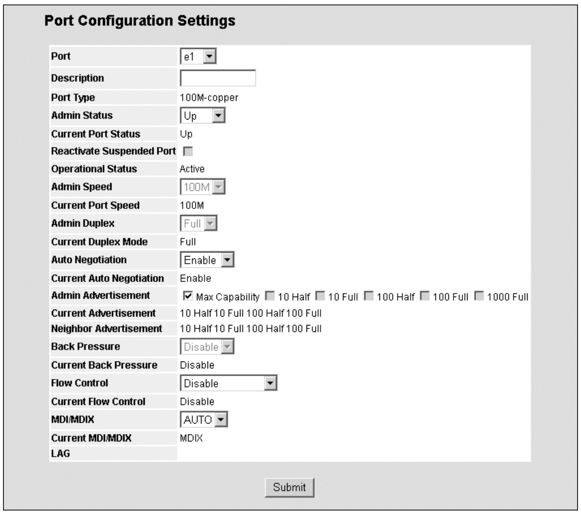
- **Back Pressure** — Displays the back pressure mode on the port. Back pressure mode is used with half duplex mode to disable ports from receiving messages.
- **Flow Control** — Displays the flow control status on the port. Operates when the port is in full duplex mode.
- **MDI/MDIX** — Displays the MDI/MDIX status on the port. 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 matched up properly. When two hubs or switches are connected to each other, or two end stations are connected to each other, a crossover cable is used to 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.
- **LAG** — Indicates whether the port is part of a Link Aggregation Group (LAG).

The Interface Configuration LAG table contains the following fields:

- **LAG** — Indicates whether the port is part of a Link Aggregation Group (LAG).
- **LAG Type** — Indicates the type of LAG defined by the first port assigned to the LAG. For example, 100-Copper, or 100-Fiber.
- **LAG Status** — Indicates whether the LAG is up or down.
- **LAG Speed** — Displays the configured aggregated rate for the LAG. The possible field values are:
  – *10* — Indicates the port is currently operating at 10 Mbps.
  – *100* — Indicates the port is currently operating at 100 Mbps.
  – *1000* — Indicates the port is currently operating at 1000 Mbps.
- **Auto Negotiation** — Displays the auto negotiation status of the LAG. 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.
- **Back Pressure** — Displays the back pressure mode on the LAG. Back pressure mode is used with half duplex mode to disable ports in the LAG from receiving messages.
- **Flow Control** — Displays the flow control status of the LAG.

2. Click ✎ next to the item to modify. The *Port or LAG Interface Configuration Settings Page* opens:

Figure 66: Interface Configuration Settings Page



Port Configuration Settings

Port	e1 ▾
Description	
Port Type	100M-copper
Admin Status	Up ▾
Current Port Status	Up
Reactivate Suspended Port	□
Operational Status	Active
Admin Speed	100M ▾
Current Port Speed	100M
Admin Duplex	Full ▾
Current Duplex Mode	Full
Auto Negotiation	Enable ▾
Current Auto Negotiation	Enable
Admin Advertisement	☑ Max Capability □ 10 Half □ 10 Full □ 100 Half □ 100 Full □ 1000 Full
Current Advertisement	10 Half 10 Full 100 Half 100 Full
Neighbor Advertisement	10 Half 10 Full 100 Half 100 Full
Back Pressure	Disable ▾
Current Back Pressure	Disable
Flow Control	Disable ▾
Current Flow Control	Disable
MDI/MDIX	AUTO ▾
Current MDI/MDIX	MDIX
LAG	

In addition to the fields in the *Interface Configuration Page*, the *Port or LAG Interface Configuration Settings Page* contains the following additional field:

- Reactivate Suspended Port - Reactivates a suspended port. The possible field values are:
  – *Checked* — Reactivates or unlocks the suspended port.
  – *Unchecked* — Maintains the port's locked/ suspended state.

3. Modify the *Admin Speed, Admin Duplex*, and *Admin Advertisement* fields.
4. Click Submit. The parameters are saved, and the device is updated.

7.2 Configuring LAGs

Link Aggregation optimizes port usage by linking a group of ports together to form a single LAG. Aggregating ports multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

The TP-Link device supports both static LAGs and Link Aggregation Control Protocol (LACP) LAGs. LACP LAGs negotiate aggregating 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.

When configuring LAGs, ensure the following:

- All ports within a LAG must be the same media type.
- A VLAN is not configured on the port.
- The port is not assigned to a different LAG.
- Auto-negotiation mode is not configured on the port.
- The port is in full-duplex mode.
- All ports in the LAG have the same ingress filtering and tagged modes.
- All ports in the LAG have the same back pressure and flow control modes.
- All ports in the LAG have the same priority.
- All ports in the LAG have the same transceiver type.
- The device supports up to eight LAGs, and eight ports in each LAG.
- Ports can be configured as LACP ports only if the ports are not part of a previously configured LAG.
- Ports added to a LAG lose their individual port configuration. When ports are removed from the LAG, the original port configuration is applied to the ports.

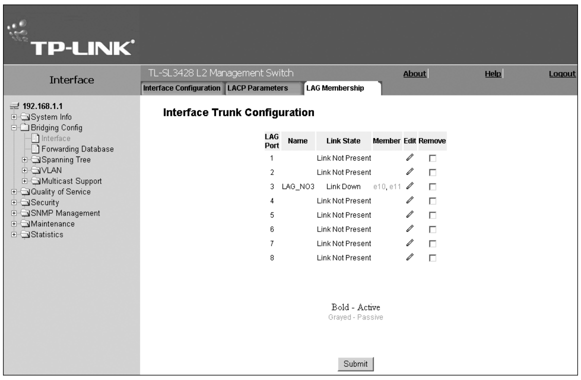
This section contains the following topics:

- Defining LAG Members
- Configuring LACP

7.2.1 Defining LAG Members

To define LAG members:

1. Click **System > Bridging Config > Interface > LAG Membership**. The *LAG Membership Page* opens:



Interface Trunk Configuration

LAG Port	Name	Link State	Member	Edit	Remove
1		Link Not Present		✎	☐
2		Link Not Present		✎	☐
3	LAG_NO3	Link Down	e10, e11	✎	☐
4		Link Not Present		✎	☐
5		Link Not Present		✎	☐
6		Link Not Present		✎	☐
7		Link Not Present		✎	☐
8		Link Not Present		✎	☐

Bold - Active
Grayed - Passive

Figure 67: LAG Membership Page

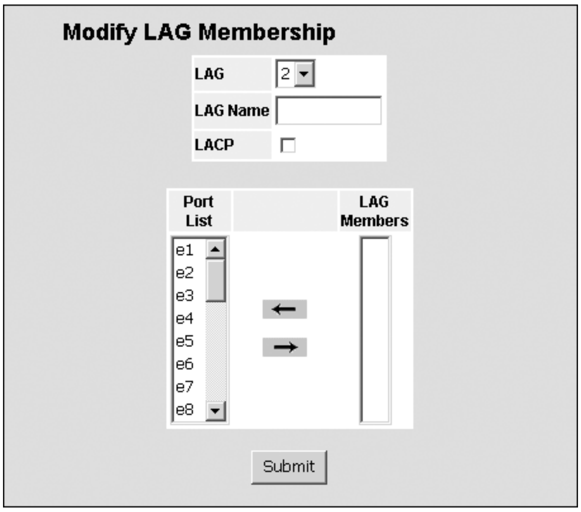
The *LAG Membership Page* contains the following fields:

- **LAG Port** — Displays the LAG number.
- **Name** — Displays the user-defined port name.
- **Link State** — Displays the link operational status.
- **Members**— Displays the ports configured to the LAG. Membership groups are indicated as bold when active and as grayed when passive.
- **Remove** — Removes the LAG. The possible field values:
  – *Checked* — Removes the selected LAG.
  – *Unchecked*— Maintains the LAGs.

To modify LAG Membership:

1. Click ✎ . The *LAG Membership Settings Page* opens.

Figure 68: LAG Membership Settings Page



Modify LAG Membership

LAG	2 ▾
LAG Name	
LACP	□

Port List		LAG Members
e1 e2 e3 e4 e5 e6 e7 e8	← →	

Submit

The *LAG Membership Settings Page* contains the following fields:

- **LAG** — Contains a user-defined drop-down LAG list.
- **Lag Name** — Displays the user-defined LAG name.
- **LACP** — Indicates if LACP is defined on the LAG. The possible field values are:
  – *Enable* — Enables LACP on the LAG.
  – *Disable* — Disables LACP on the LAG. This is the default value.
- **Port List** — Displays a list of ports. Ports in the Port List can be added to the LAG.
- **LAG Members** — Displays the list of the ports included in the LAG.

2. Define the *LAG* fields for the LAG port.
3. Click ports in the *Port List* and add the ports to the *LAG Members* list, using →.
4. Click Submit. The interface LAG membership properties are modified, and the device is updated.

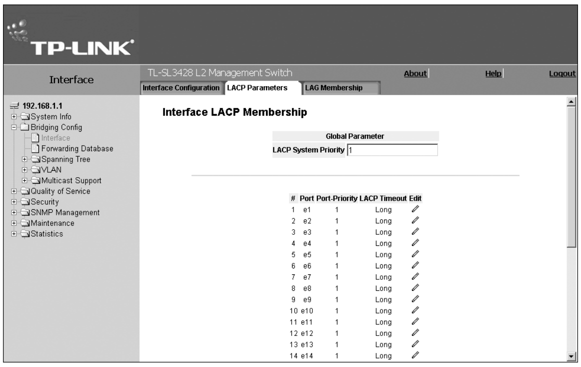
7.2.2 Configuring LACP

LAG ports can contain different media types if the ports are operating at the same speed. Aggregated links can be set up manually or automatically established by enabling LACP on the relevant links. Aggregate ports can be linked into link-aggregation port-groups. Each group is comprised of ports with the same speed. The LACP Parameters Page contains fields for configuring LACP LAGs.

To view and configure LACP:

1. Click **System > Bridging Config > Interface > LACP Parameters**. The *LACP Parameters Page* opens:

Figure 69: LACP Parameters Page



Interface LACP Membership

Global Parameter	
LACP System Priority	1

#	Port	Port-Priority	LACP Timeout	Edit
1	e1	1	Long	✎
2	e2	1	Long	✎
3	e3	1	Long	✎
4	e4	1	Long	✎
5	e5	1	Long	✎
6	e6	1	Long	✎
7	e7	1	Long	✎
8	e8	1	Long	✎
9	e9	1	Long	✎
10	e10	1	Long	✎
11	e11	1	Long	✎
12	e12	1	Long	✎
13	e13	1	Long	✎
14	e14	1	Long	✎

The *LACP Parameters Page* contains the following fields:

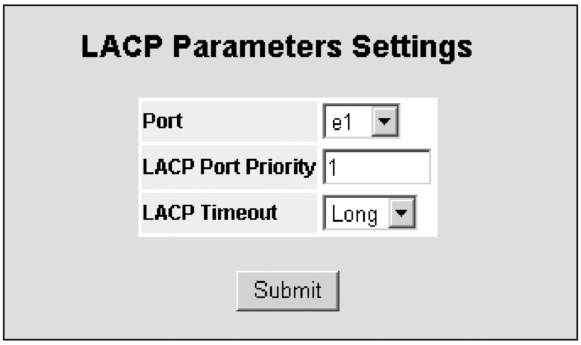
- **LACP System Priority** — Specifies system priority value. The field range is 1-65535. The field default is 1.
- **Port** — Displays the port number to which timeout and priority values are assigned.
- **Port Priority** — Displays the LACP priority value for the port. The field range is 1-65535.
- **LACP Timeout** — Displays the administrative LACP timeout.

2. Define the *LACP System Priority* and click Submit. The system priority for LACP is saved and the device is updated.

To modify LACP parameters:

1. Click **System > Bridging Config > Interface > LACP Parameters**. The *LACP Parameters Page* opens.
2. Click ✎ . The *LACP Parameters Settings Page* opens:

Figure 70: LACP Parameters Settings Page


LACP Parameters Settings

Port	e1
LACP Port Priority	1
LACP Timeout	Long

3. Define the *Port Priority* and *LACP Timeout* settings.
4. Click Submit. The LACP settings are saved and the device is updated.

7.3 Configuring VLANs

VLANs are logical subgroups with a Local Area Network (LAN) which combine user stations and network devices into a single unit, regardless of the physical LAN segment to which they are attached. VLANs allow network traffic to flow more efficiently within subgroups. VLANs use software to reduce the amount of time it takes for network changes, additions, and moves to be implemented.

VLANs have no minimum number of ports, and can be created per unit, per device, or through any other logical connection combination, since they 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 working at a protocol level is required to allow 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 4-byte tag to packet headers. The VLAN tag indicates to which VLAN the packets belong. VLAN tags are attached to the VLAN by either the end station or the network device. VLAN tags also contain VLAN network priority information.

Combining VLANs and GARP (Generic Attribute Registration Protocol) allows network managers to define network nodes into Broadcast domains.

This section contains the following topics:

- Adding VLAN
- Defining VLAN Properties
- Defining VLAN Membership
- Defining VLAN Interface Settings
- Configuring GARP
- Defining GVRP

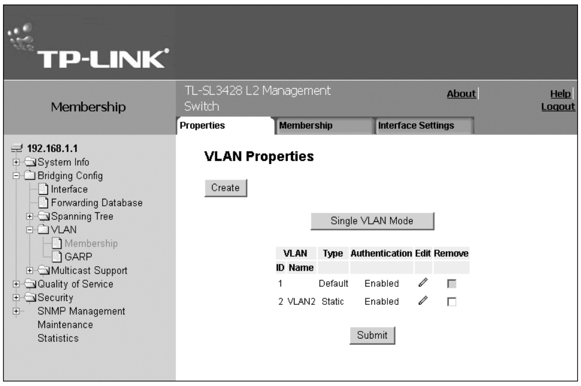
7.3.1 Defining VLAN Properties

The *VLAN Member Properties Page* provides information and global parameters for configuring and working with VLANs.

To add a new VLAN:

1. Click **System > Bridging Config > VLAN > Membership**. The *VLAN Member Properties Page* opens:

Figure 71: VLAN Member Properties Page



VLAN Properties

VLAN ID	VLAN Name	Type	Authentication	Edit	Remove
1		Default	Enabled	✎	□
2	VLAN2	Static	Enabled	✎	□

The *VLAN Member Properties Page* contains the following fields:

- **Select VLAN ID** — Displays the properties of the selected VLAN in the VLANs table below.
- **Show All** — Displays the properties of all defined VLANS in the VLANs table below.
- **VLAN ID** — Displays the VLAN ID.
- **Name** — Displays the user-defined VLAN name.
- **Type**— Displays the VLAN type. The possible field values are:

  – *Dynamic* — Indicates the VLAN was dynamically created through GARP.

  – *Static* — Indicates the VLAN is user-defined.

  – *Default* — Indicates the VLAN is the default VLAN.
- **Unauthenticaed VLAN** — Indicates whether unauthorized users can access a Guest VLAN. The possible field values are:

  – *Enabled* — Enables unauthorized users to use the Guest VLAN.

  – *Disabled* — Disables unauthorized users from using the Guest VLAN.
- **Remove** — Removes VLANs. The possible field values are:

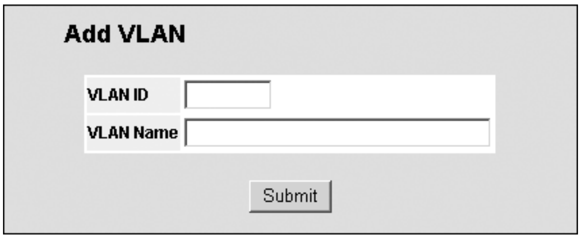
  – *Checked* — Removes the selected VLAN.

  – *Unchecked* — Maintains the current VLANs.

To add a new VLAN:

1. Click Create. The *Add VLAN Page* opens:

Figure 72: Add VLAN Page



Add VLAN

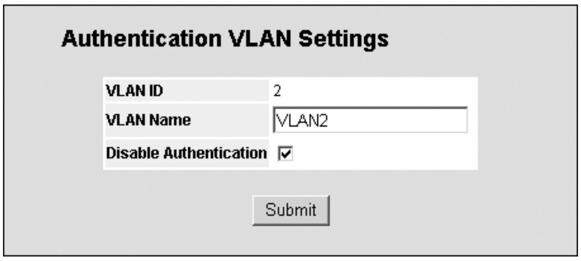
VLAN ID	
VLAN Name	

2. Define the VLAN ID and VLAN Name.
3. Click Submit. The new VLAN is saved and the device is updated.

To define VLAN properties:

1. Click ✎ . The *Edit VLAN Page* opens.

Figure 73: Edit VLAN Page



Authentication VLAN Settings

VLAN ID	2
VLAN Name	VLAN2
Disable Authentication	☑

2. Modify the *VLAN Name* and *Disable Authentication* fields.
3. Click Submit. The VLAN properties are saved.
4. In the *VLAN Member Properties Page*, Click Submit The VLAN information is saved and the device is updated.

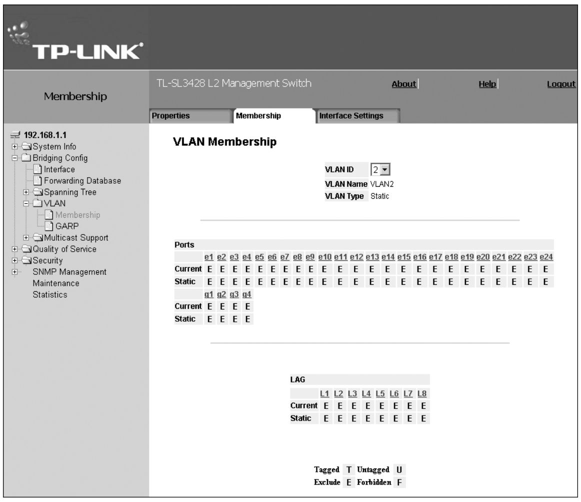
7.3.2 Defining VLAN Membership

The VLAN Member Membership Page contains a table that maps VLAN parameters to ports. Ports are assigned VLAN membership by toggling through the *Port Control* settings.

To define VLAN membership:

1. Click **System > Bridging Config > VLAN >Membership > Membership**. The *VLAN Member Membership Page* opens:

Figure 74: VLAN Member Membership Page



VLAN Membership

VLAN ID: 2
VLAN Name: VLAN2
VLAN Type: Static

Ports

	e1	e2	e3	e4	e5	e6	e7	e8	e9	e10	e11	e12	e13	e14	e15	e16	e17	e18	e19	e20	e21	e22	e23	e24
Current	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E
Static	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E

	g1	g2	g3	g4
Current	E	E	E	E
Static	E	E	E	E

LAG

	L1	L2	L3	L4	L5	L6	L7	L8
Current	E	E	E	E	E	E	E	E
Static	E	E	E	E	E	E	E	E

Tagged	T	Untagged	U
Exclude	E	Forbidden	F

The *VLAN Member Membership Page* contains the following fields:

- **VLAN ID** — Displays the user-defined VLAN ID.
- **VLAN Name** — Displays the name of the VLAN
- **VLAN Type** — Indicates the VLAN type. The possible field values are:
  – *Dynamic* — Indicates the VLAN was dynamically created through GARP.
  – *Static* — Indicates the VLAN is user-defined.
  – *Default* — Indicates the VLAN is the default VLAN.
- **Port** — Indicates the port membership.
- **LAG** — Indicates the LAG membership.
- **U** — Indicates the interface is an untagged VLAN member. Packets forwarded by the interface are untagged.
- **T** — Indicates the interface is a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.
- **I** — Includes the port in the VLAN.
- **E** — Excludes the interface from the VLAN. However, the interface can be added to the VLAN through GARP.
- **R** — Denies the interface VLAN membership, even if GARP indicates the port is to be added.

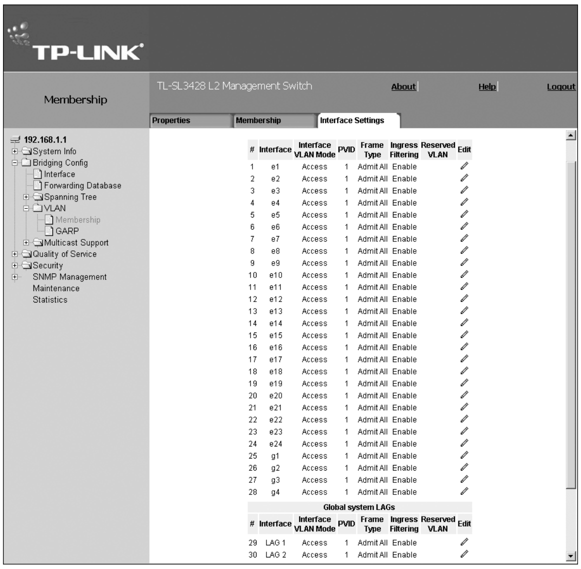
7.3.3 Defining VLAN Interface Settings

The *VLAN Interface Settings Page* contains fields for managing ports that are part of a VLAN. The Port Default VLAN ID (PVID) is configured on the VLAN Interface Settings Page. All untagged packets arriving at the device are tagged with the port PVID.

To define VLAN interfaces:

1. Click **System > Bridging Config > VLAN > Membership > Interface Settings**. The *VLAN Interface Settings Page* opens.

Figure 75: VLAN Interface Settings Page



#	Interface	Interface VLAN Mode	PVID	Frame Type	Ingress Filtering	Reserved VLAN	Edit
1	e1	Access	1	Admit All	Enable		✎
2	e2	Access	1	Admit All	Enable		✎
3	e3	Access	1	Admit All	Enable		✎
4	e4	Access	1	Admit All	Enable		✎
5	e5	Access	1	Admit All	Enable		✎
6	e6	Access	1	Admit All	Enable		✎
7	e7	Access	1	Admit All	Enable		✎
8	e8	Access	1	Admit All	Enable		✎
9	e9	Access	1	Admit All	Enable		✎
10	e10	Access	1	Admit All	Enable		✎
11	e11	Access	1	Admit All	Enable		✎
12	e12	Access	1	Admit All	Enable		✎
13	e13	Access	1	Admit All	Enable		✎
14	e14	Access	1	Admit All	Enable		✎
15	e15	Access	1	Admit All	Enable		✎
16	e16	Access	1	Admit All	Enable		✎
17	e17	Access	1	Admit All	Enable		✎
18	e18	Access	1	Admit All	Enable		✎
19	e19	Access	1	Admit All	Enable		✎
20	e20	Access	1	Admit All	Enable		✎
21	e21	Access	1	Admit All	Enable		✎
22	e22	Access	1	Admit All	Enable		✎
23	e23	Access	1	Admit All	Enable		✎
24	e24	Access	1	Admit All	Enable		✎
25	g1	Access	1	Admit All	Enable		✎
26	g2	Access	1	Admit All	Enable		✎
27	g3	Access	1	Admit All	Enable		✎
28	g4	Access	1	Admit All	Enable		✎

Global system LAGs

#	Interface	Interface VLAN Mode	PVID	Frame Type	Ingress Filtering	Reserved VLAN	Edit
29	LAG 1	Access	1	Admit All	Enable		✎
30	LAG 2	Access	1	Admit All	Enable		✎

The *VLAN Interface Settings Page* contains the following fields:

- **Interface** — Displays the port number included in the VLAN.
- **Interface VLAN Mode** — Displays the port mode. The possible values are:
  – *General* — Indicates the port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full IEEE802.1q mode).
  – *Access* — Indicates a 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 or

disabled on an access port.

– *Trunk* — Indicates the port belongs to VLANs in which all ports are tagged, except for one port that can be untagged.

– *PVE - Promiscuous* — Indicates the port is part of a PV Promiscuous VLAN.

– *PVE - Isolated* — Indicates the port is part of a PV Isolated VLAN.

– *PVE - Community* — Indicates the port is part of a PV Community VLAN.

- **Dynamic** — Assigns a port to a VLAN based on the host source MAC address connected to the port.
- **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** — Specifies the packet type accepted on the port. The possible field 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** — Indicates whether ingress filtering is enabled on the port. The possible field values are:

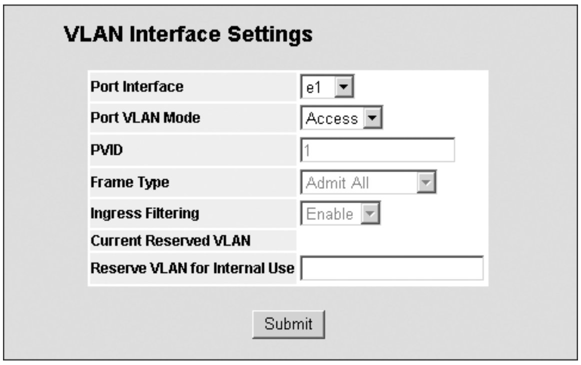
  – *Enable* — Enables ingress filtering on the device. Ingress filtering discards packets that are defined to VLANs of which the specific port is not a member.

  – *Disable* — Disables ingress filtering on the device.
- **Reserve VLAN** — Indicates that the VLAN selected by the user is reserved, if not in use by the system.

To modify VLAN interface or LAG settings:

1. Click ✎ . The *VLAN / LAG Interface Settings Page* opens.

Figure 76: VLAN / LAG Interface Settings Page



VLAN Interface Settings

Port Interface	e1
Port VLAN Mode	Access
PVID	1
Frame Type	Admit All
Ingress Filtering	Enable
Current Reserved VLAN	
Reserve VLAN for Internal Use	

2. Modify the *Port VLAN Mode, Dynamic, Frame Type, Ingress FIltering, and Reserve VLAN* fields.
3. Click Submit. The VLAN or LAG interface is configured and device information is updated.

7.3.4 Configuring GARP

This section contains information for configuring Generic Attribute Registration Protocol (GARP). This section includes the following topics:

- Defining GARP
- Defining GVRP

7.3.4.1 Defining GARP

Generic Attribute Registration Protocol (GARP) protocol 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.

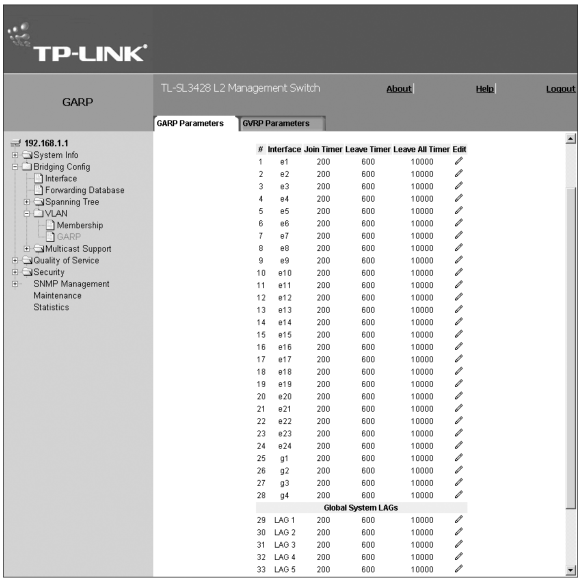
When configuring GARP, ensure the following:

- 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, the GARP application does not operate successfully.

To define GARP:

1. Click **System > Bridging Config > VLAN > GARP**. The *GARP Parameters Page* opens:

Figure 77: GARP Parameters Page



#	Interface	Join Timer	Leave Timer	Leave All Timer	Edit
1	e1	200	600	10000	✎
2	e2	200	600	10000	✎
3	e3	200	600	10000	✎
4	e4	200	600	10000	✎
5	e5	200	600	10000	✎
6	e6	200	600	10000	✎
7	e7	200	600	10000	✎
8	e8	200	600	10000	✎
9	e9	200	600	10000	✎
10	e10	200	600	10000	✎
11	e11	200	600	10000	✎
12	e12	200	600	10000	✎
13	e13	200	600	10000	✎
14	e14	200	600	10000	✎
15	e15	200	600	10000	✎
16	e16	200	600	10000	✎
17	e17	200	600	10000	✎
18	e18	200	600	10000	✎
19	e19	200	600	10000	✎
20	e20	200	600	10000	✎
21	e21	200	600	10000	✎
22	e22	200	600	10000	✎
23	e23	200	600	10000	✎
24	e24	200	600	10000	✎
25	g1	200	600	10000	✎
26	g2	200	600	10000	✎
27	g3	200	600	10000	✎
28	g4	200	600	10000	✎
Global System LAGs					
29	LAG 1	200	600	10000	✎
30	LAG 2	200	600	10000	✎
31	LAG 3	200	600	10000	✎
32	LAG 4	200	600	10000	✎
33	LAG 5	200	600	10000	✎

The *GARP Parameters Page* contains the following fields:

- **Copy from Entry Number** — Indicates the row number from which GARP parameters are copied.
- **To Entry Number** — Indicates the row number to which GARP parameters are copied.
- **Interface** — Displays the port or LAG on which GARP is enabled.
- **Join Timer**— Indicates the amount of time, in centiseconds, that PDUs are transmitted. The default value is 20 centiseconds.
- **Leave Timer**— Indicates the amount of time lapse, in centiseconds, 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 default value is 60 centiseconds.
- **Leave All Timer** — Indicates the amount of time lapse, in centiseconds, that all device waits before leaving the GARP state. The leave all time must be greater than the leave time. The default value is 1000 centiseconds.

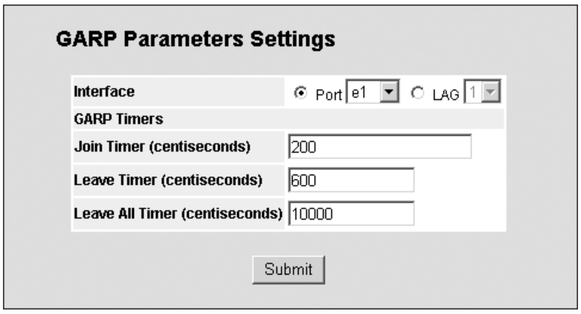
2. In the *Copy From Entry Number* field, enter the interface #; in the *To Row Number(s)* field, enter the row number of the required interface.

3. Click Submit. The GARP parameters are modified, and the device is updated.

To modify GARP settings:

1. Click ✎ next to the item to modify. The *GARP Parameters Settings Page* opens:

Figure 78: GARP Parameters Settings Page


GARP Parameters Settings

Interface	● Port e1 ○ LAG 1
GARP Timers	
Join Timer (centiseconds)	200
Leave Timer (centiseconds)	600
Leave All Timer (centiseconds)	10000

2. Modify the *Timer* parameters.

3. Click Submit. The GARP parameters are modified, and the device is updated.

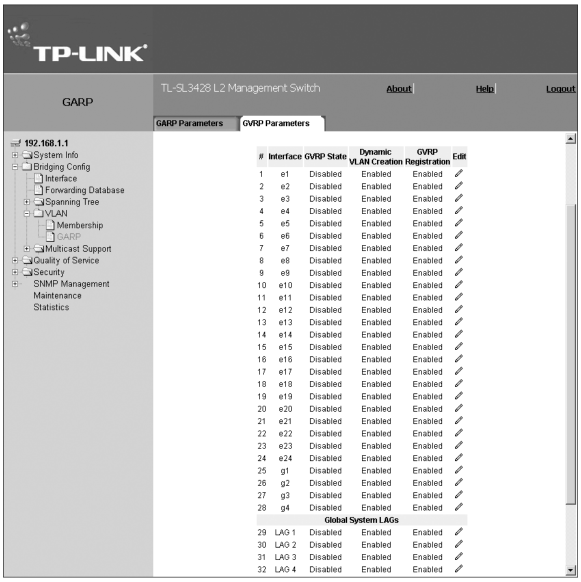
7.3.5 Defining GVRP

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 define GVRP on the device:

1. Click **System > Bridging Config > VLAN > GARP > GVRP**. The *GVRP Parameters Page* opens:

Figure 79: GVRP Parameters Page



#	Interface	GVRP State	Dynamic VLAN Creation	GVRP Registration	Edit
1	e1	Disabled	Enabled	Enabled	✎
2	e2	Disabled	Enabled	Enabled	✎
3	e3	Disabled	Enabled	Enabled	✎
4	e4	Disabled	Enabled	Enabled	✎
5	e5	Disabled	Enabled	Enabled	✎
6	e6	Disabled	Enabled	Enabled	✎
7	e7	Disabled	Enabled	Enabled	✎
8	e8	Disabled	Enabled	Enabled	✎
9	e9	Disabled	Enabled	Enabled	✎
10	e10	Disabled	Enabled	Enabled	✎
11	e11	Disabled	Enabled	Enabled	✎
12	e12	Disabled	Enabled	Enabled	✎
13	e13	Disabled	Enabled	Enabled	✎
14	e14	Disabled	Enabled	Enabled	✎
15	e15	Disabled	Enabled	Enabled	✎
16	e16	Disabled	Enabled	Enabled	✎
17	e17	Disabled	Enabled	Enabled	✎
18	e18	Disabled	Enabled	Enabled	✎
19	e19	Disabled	Enabled	Enabled	✎
20	e20	Disabled	Enabled	Enabled	✎
21	e21	Disabled	Enabled	Enabled	✎
22	e22	Disabled	Enabled	Enabled	✎
23	e23	Disabled	Enabled	Enabled	✎
24	e24	Disabled	Enabled	Enabled	✎
25	g1	Disabled	Enabled	Enabled	✎
26	g2	Disabled	Enabled	Enabled	✎
27	g3	Disabled	Enabled	Enabled	✎
28	g4	Disabled	Enabled	Enabled	✎
Global System LAGs					
29	LAG 1	Disabled	Enabled	Enabled	✎
30	LAG 2	Disabled	Enabled	Enabled	✎
31	LAG 3	Disabled	Enabled	Enabled	✎
32	LAG 4	Disabled	Enabled	Enabled	✎

The *GVRP Parameters Page* is divided into port and LAG parameters. The field definitions are the same.

The *GVRP Parameters Page* contains the following fields:

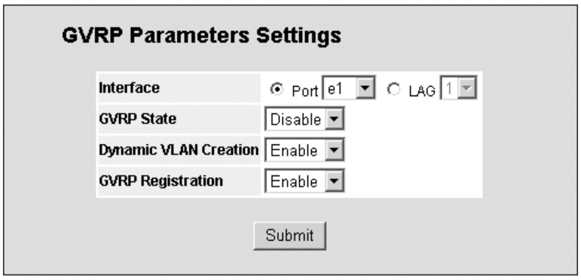
- **GVRP Global** — Indicates if GVRP is enabled on the device. The possible field values are:
  – *Enable* — Enables GVRP on the selected device.
  – *Disable* — Disables GVRP on the selected device.
- **Interface** — Displays the port on which GVRP is enabled. The possible field values are:
  – *Port* — Indicates the port number on which GVRP is enabled.
  – *LAG* — Indicates the LAG number on which GVRP is enabled.
- **GVRP State** — Indicates if GVRP is enabled on the port. The possible field values are:
  – **Enable** — Enables GVRP on the selected port.
  – *Disable* — Disables GVRP on the selected port.
- **Dynamic VLAN Creation** — Indicates if Dynamic VLAN creation is enabled on the interface. The possible field values are:
  – *Enable* — Enables Dynamic VLAN creation on the interface.
  – *Disable* — Disables Dynamic VLAN creation on the interface.
- **GVRP Registration** — Indicates if VLAN registration through GVRP is enabled on the device. The possible field values are:
  – *Enable* — Enables GVRP registration on the device.
  – *Disable* — Disables GVRP registration on the device.

2. Select the *GVRP Global* status and click Submit. The global GVRP parameters are saved.

To modify global GVRP or LAG parameters:

1. Click ✎ next to GVRP or LAG global interface settings item. The *GVRP Parameters Settings Page* opens:

Figure 80: GVRP Parameters Settings Page



GVRP Parameters Settings

Interface	● Port e1 ○ LAG 1
GVRP State	Disable
Dynamic VLAN Creation	Enable
GVRP Registration	Enable

2. Enable or disable *GVRP State, Dynamic VLAN Creation* and *GVRP Registration*.

3. Click Submit. The global GVRP or LAG parameters are modified, and the device is updated.

Section 8. Defining the Forwarding Database

Packets addressed to destinations stored in either the Static or Dynamic databases are immediately forwarded to the port. The Dynamic MAC Address Table can be sorted by interface, VLAN, or MAC Address, whereas MAC addresses are dynamically learned as packets from sources that arrive at the device. Static addresses are configured manually.

An address becomes associated with a port by learning the port from the frame's source address, but if a frame that is addressed to a destination MAC address is not associated with a port, that frame is flooded to all relevant VLAN ports. To prevent the bridging table from overflowing, a dynamic MAC address, from which no traffic arrives for a set period, is erased.

This section contains information for defining both static and dynamic forwarding addresses, and includes the following topics:

- Configuring Static Addresses
- Configuring Dynamic Forwarding Addresses

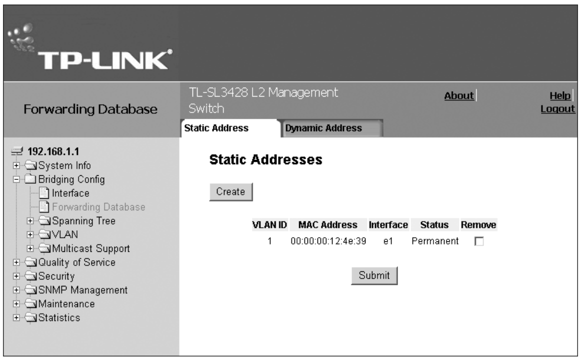
8.1 Configuring Static Addresses

The *Forwarding Database Static Addresses Page* contains parameters for defining the age interval on the device. To prevent static MAC addresses from being deleted when the device is reset, ensure that the port attached to the MAC address is locked. To prevent static MAC addresses from being deleted when the device is reset, ensure that the port attached to the MAC address is locked.

To define Static addressing for the forwarding database:

1. Click **System > Bridging Config > Forwarding Database > Static Addresses**. The *Forwarding Database Static Addresses Page* opens:

Figure 81: Forwarding Database Static Addresses Page



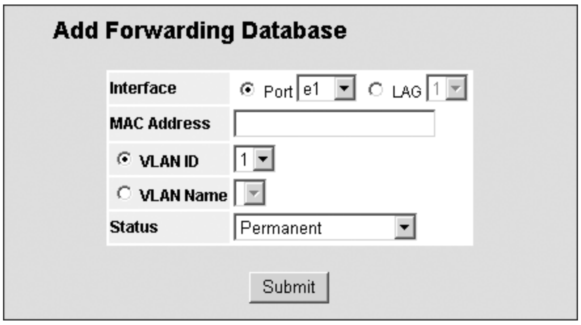
VLAN ID	MAC Address	Interface	Status	Remove
1	00:00:00:12:4e:39	e1	Permanent	□

The *Forwarding Database Static Addresses Page* contains the following fields:

- **VLAN ID** — Displays the VLAN ID number to which the entry refers.
- **MAC Address** — Displays the MAC address to which the entry refers.
- **Interface** — Displays the interface to which the entry refers:
  – *Port* — The specific port number to which the forwarding database parameters refer.
  – *LAG* — The specific LAG number to which the forwarding database parameters refer.
- **Status** — Displays how the entry was created. The possible field values are:
  – *Secure* — The MAC Address is defined for locked ports.
  – *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** — Removes the entry. The possible field values are:
  – *Checked* — Removes the selected entry.
  – *Unchecked* — Maintains the current static forwarding database.

2. Click Create. The *Add Forwarding Database Page* opens:

Figure 82: Add Forwarding Database Page



Add Forwarding Database

Interface	● Port e1 ○ LAG 1
MAC Address	
● VLAN ID	1
○ VLAN Name	
Status	Permanent

3. Define the *Interface, MAC Address, VLAN ID or VLAN Name*, and *Status* fields.

4. Click Submit. The forwarding database information is modified, and the device is updated.

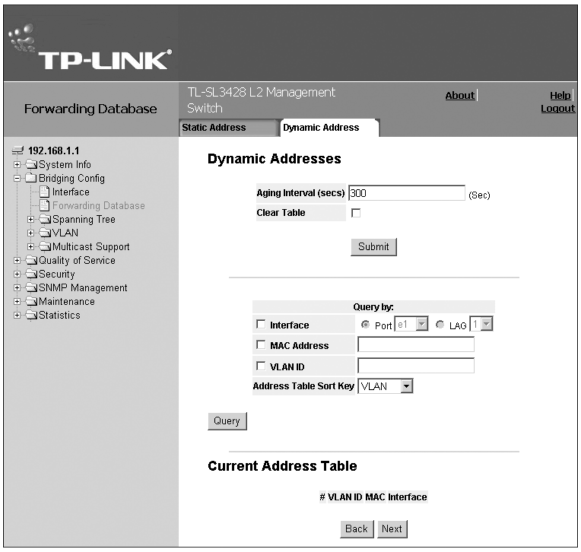
8.2 Configuring Dynamic Forwarding Addresses

The *Dynamic Addresses Page* contains parameters for querying information in the Dynamic MAC Address Table, including the interface type, MAC addresses, VLAN, and table storing. The Dynamic MAC Address Table contains information about the aging time before a dynamic MAC address is erased, and includes parameters for querying and viewing the Dynamic MAC Address table. The Dynamic MAC Address table contains address parameters by which packets are directly forwarded to the ports. The Dynamic Address Table can be sorted by interface, VLAN, and MAC Address.

To define the dynamic forwarding addresses:

1. Click **System > Bridging Config > Forwarding Database > Dynamic Addresses**. The *Dynamic Addresses Page* opens:

Figure 83: Dynamic Addresses Page



Dynamic Addresses

Aging Interval (secs) 300 (Sec)

Clear Table □

Query by:

□ Interface	● Port e1 ○ LAG 1
□ MAC Address	
□ VLAN ID	
Address Table Sort Key	VLAN

Current Address Table

#	VLAN ID	MAC	Interface

The *Dynamic Addresses Page* contains the following fields:

- **Address Aging (Sec.)** — Specifies the amount of time in seconds that the MAC address remains in the Dynamic MAC Address table before being timed out, if no traffic from the source is detected. The default value is 300 seconds.
- **Clear Table** — Clears the *Current Address Table*.

The *Query by*: section contains the following fields:

- **Interface** — Specifies the interface (Port or LAG) for which the table is queried.
- **MAC Address** — Specifies the MAC address for which the table is queried.
- **VLAN ID** — Specifies the VLAN ID for which the table is queried.
- **Address Table Sort Key** —Specifies the means by which the Dynamic MAC Address Table is sorted. The address table can be sorted by address, VLAN, or interface.

The *Current Address Table* section displays the parameters of the dynamic addresses defined: VLAN ID, MAC (Address) and Interface.

2. To browse the addresses, click Back Next.

To query the Dynamic MAC Address Table:

1. Click **System > Bridging Config > Forwarding Database > Dynamic Addresses**. The *Dynamic Addresses Page* opens.
2. Select the Interface, the *MAC Address*, and the *VLAN ID*.
3. Select an *Address Table Sort Key*.
4. Click Query. The Dynamic MAC Address Table is queried, and the results are displayed in the *Current Address Table*.

Section 9. Configuring the Spanning Tree Protocol

The Spanning *Tree Protocol* (STP) provides tree topography for any arrangement of bridges. STP also provides a single path between end stations on a network, eliminating loops. Loops occur when alternate routes exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reducing network efficiency.

The TP-Link device supports the following STP versions:

- **Classic STP** — Provides a single path between end stations, avoiding and eliminating loops.
  For more information on configuring Classic STP, see *Configuring the Classic STP*.
- **Rapid STP** — Detects and uses network topologies that provide faster convergence of the spanning tree, without creating forwarding loops.
  For more information on configuring Rapid STP, see *Configuring the Rapid STP*.
- **Multiple STP** — Provides various load balancing scenarios. For example, if port A is blocked in one STP instance, the same port can be placed in the *Forwarding State* in another STP instance.
  For more information on configuring Multiple STP, see *Configuring the Multiple STP*.

This section contains the following topics:

- Configuring the Classic STP
- Configuring the Rapid STP
- Configuring the Multiple STP

9.1 Configuring the Classic STP

This section describes the following topics:

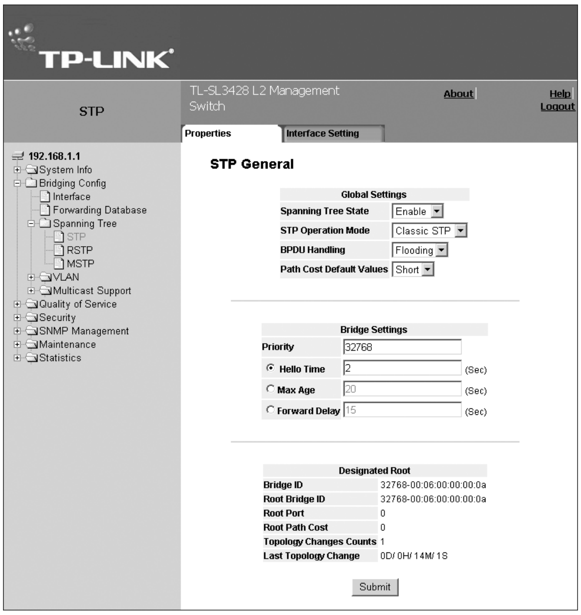
- Defining STP Properties
- Defining STP Interface Settings

9.1.1 Defining STP Properties

The *STP Properties Page* contains parameters for enabling STP on the device.

To define STP properties:

1. Click **System > Bridging Info > Spanning Tree > STP > Properties**. The *STP Properties Page* opens:



STP General

Global Settings	
Spanning Tree State	Enable
STP Operation Mode	Classic STP
BPDU Handling	Flooding
Path Cost Default Values	Short

Bridge Settings		
Priority	32768	
● Hello Time	2	(Sec)
○ Max Age	20	(Sec)
○ Forward Delay	15	(Sec)

Designated Root	
Bridge ID	32768-00:06:00:00:00:0a
Root Bridge ID	32768-00:06:00:00:00:0a
Root Port	0
Root Path Cost	0
Topology Changes Counts	1
Last Topology Change	0D/ 0H/ 14M/ 1S

Figure 84: STP Properties Page

The *STP Properties Page* contains the following fields:

- **Spanning Tree State** — Indicates whether STP is enabled on the device. The possible field values are:
  – *Enable* — Enables STP on the device.
  – *Disable* — Disables STP on the device.
- **STP Operation Mode** — Specifies the STP mode that 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.
– *Multiple STP* — Enables Multiple STP on the device.

- **BPDU Handling** — Determines how BPDU packets are managed when STP is disabled on the port or 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. This is the default value.
  – *Flooding* — Floods BPDU packets when spanning tree is disabled on an interface.
- **Path Cost Default Values** — Specifies the method used to assign default path cost to STP ports.
  The possible field values are:
  – *Short* — Specifies 1 through 65,535 range for port path cost. This is the default value.
  – *Long* — Specifies 1 through 200,000,000 range for port path cost. The default path cost assigned to an interface varies according to the selected method (Hello Time, Max Age, or Forward Delay).

The *Bridge Settings* section contains the following fields:

- **Priority (0-65535)** — Specifies the bridge priority value. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the device with the lowest priority value becomes the Root Bridge. The default value is 32768. The port priority value is provided in increments of 4096.
- **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 is the amount of time in seconds a bridge waits before sending configuration messages. The default Maximum Age Time is 20 seconds.
- **Forward Delay (4-30)** — Specifies the device Forward Delay Time. The Forward Delay Time is the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. The default is 15 seconds.

The *Designated Port* section contains the following fields:

- **Bridge ID** — Identifies the Bridge priority and MAC address.
- **Root Bridge ID** — Identifies the Root Bridge priority and MAC address.
- **Root Port** — Indicates the port number that offers the lowest cost path from this bridge to the Root Bridge. This field is significant when the bridge is not the Root Bridge. The default is zero.
- **Root Path Cost** — The cost of the path from this bridge to the Root Bridge.
- **Topology Changes Counts** — Specifies the total amount of STP state changes that have occurred.
- **Last Topology Change** — Indicates the amount of time that has elapsed since the bridge was initialized or reset, and the last topographic change that occurred. The time is displayed in a day-hour-minute-second format, such as 2 days 5 hours 10 minutes and 4 seconds.

2. Complete the *Spanning Tree State* and *Bridge Settings* fields.
3. Click Submit. The new STP definition is added and device information is updated.

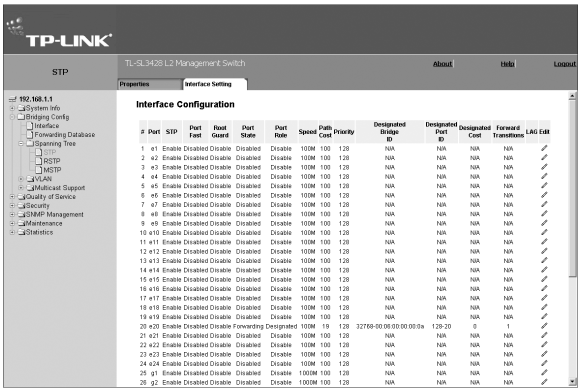
9.1.2 Defining STP Interface Settings

Network administrators can assign STP settings to specific interfaces using the *STP Interface Settings Page*. The Global LAGs section displays the STP information for Link Aggregated Groups.

To assign STP settings to an interface:

1. Click **System > Bridging Info > Spanning Tree > STP > Interface Settings**. The *STP Interface Settings Page* opens:

Figure 85: STP Interface Settings Page



Interface Configuration

#	Port	STP	Port Fast	Root Guard	Port State	Port Role	Speed	Path Cost	Priority	Designated Bridge ID	Designated Port ID	Designated Cost	Forward Transitions	LAG	Edit
1	e1	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
2	e2	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
3	e3	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
4	e4	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
5	e5	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
6	e6	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
7	e7	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
8	e8	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
9	e9	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
10	e10	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
11	e11	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
12	e12	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
13	e13	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
14	e14	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
15	e15	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
16	e16	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
17	e17	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
18	e18	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
19	e19	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
20	e20	Enable	Disabled	Disable	Forwarding	Designated	100M	19	128	32768-00:06:00:00:00:0a	128-20	0	1		✎
21	e21	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
22	e22	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
23	e23	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
24	e24	Enable	Disabled	Disable	Disabled	Disable	100M	100	128	N/A	N/A	N/A	N/A		✎
25	g1	Enable	Disabled	Disable	Disabled	Disable	1000M	100	128	N/A	N/A	N/A	N/A		✎
26	g2	Enable	Disabled	Disable	Disabled	Disable	1000M	100	128	N/A	N/A	N/A	N/A		✎

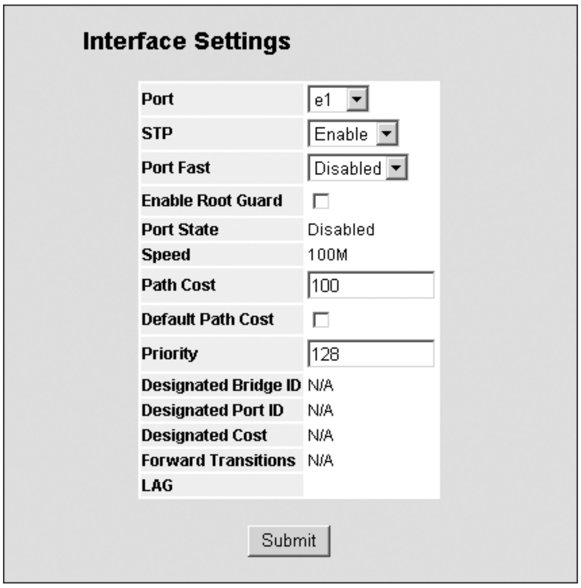
The *STP Interface Settings Page* contains the following fields:

- **Interface** — The interface for which the information is displayed.
- **STP Status** — Indicates if STP is enabled on the port. The possible field values are:
  – *Enabled* — Enables the STP on the port.
  – *Disabled* — Disables the STP on the port.
- **Fast Link** — Indicates if Fast Link is enabled on 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 optimizes the STP protocol convergence. STP convergence can take 30-60 seconds in large networks.
- **Root Guard** — Prevents devices outside the network core from being assigned the spanning tree root.
- **Port State** — Displays the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:
  – *Disabled* — Indicates that STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.
  – *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses. Blocking is displayed when Classic STP is enabled.
- **Speed** — Indicates the speed at which the port is operating.
- **Path Cost** — Indicates 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 is re-routed.
- **Priority** — Indicates the 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 determined in increments of 16.
- **Designated Bridge ID** — Indicates the bridge priority and the MAC Address of the designated bridge.
- **Designated Port ID** — Indicates the selected port priority and interface.
- **Designated Cost** — Indicates the 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** — Indicates the number of times the port has changed from Forwarding state to Blocking state.
- **LAG** — Indicates the LAG to which the port belongs.

To modify the STP settings:

1. Click ✎ . The *STP Interface Settings Page* opens.

Figure 86: STP Interface Settings Page



Interface Settings

Port	e1 ▾
STP	Enable ▾
Port Fast	Disabled ▾
Enable Root Guard	□
Port State	Disabled
Speed	100M
Path Cost	100
Default Path Cost	□
Priority	128
Designated Bridge ID	N/A
Designated Port ID	N/A
Designated Cost	N/A
Forward Transitions	N/A
LAG	

2. Click the *STP* enable checkbox.
3. Define the fields.
4. Click Submit. The settings for the selected interface are modified, and device information is updated.

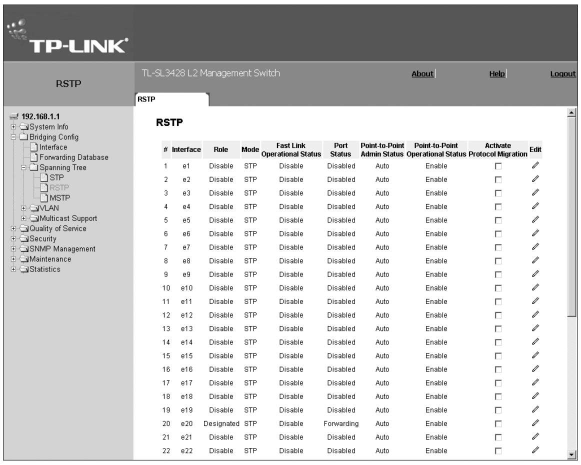
9.2 Configuring the Rapid STP

While Classic STP prevents Layer 2 forwarding loops in a general network topology, convergence can take between 30-60 seconds. This time may delay detecting possible loops and propagating status topology changes. *Rapid Spanning Tree Protocol* (RSTP) detects and uses network topologies that allow a faster STP convergence without creating forwarding loops. The Global System LAG information displays the same field information as the ports, but represent the LAG RSTP information.

To view and define RSTP:

1. Click **System > Bridging Info > Spanning Tree > RSTP**. The *RSTP Page* opens:

Figure 87: RSTP Page



RSTP

#	Interface	Role	Mode	Fast Link Operational Status	Port Status	Point-to-Point Admin Status	Point-to-Point Operational Status	Activate Protocol Migration	Edit
1	e1	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
2	e2	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
3	e3	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
4	e4	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
5	e5	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
6	e6	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
7	e7	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
8	e8	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
9	e9	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
10	e10	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
11	e11	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
12	e12	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
13	e13	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
14	e14	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
15	e15	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
16	e16	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
17	e17	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
18	e18	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
19	e19	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
20	e20	Designated	STP	Disable	Forwarding	Auto	Enable	□	✎
21	e21	Disable	STP	Disable	Disabled	Auto	Enable	□	✎
22	e22	Disable	STP	Disable	Disabled	Auto	Enable	□	✎

The *RSTP Page* contains the following fields:

- **Interface** — Displays the port or LAG on which Rapid STP is enabled.
- **Role** — Displays the port role assigned by the STP algorithm to provide to STP paths.

  The possible field values are:

  – *Root* — Provides the lowest cost path to forward packets to the root switch.

  – *Designated* — Indicates the port or LAG through which the designated switch is attached to the LAN.

  – *Alternate* — Provides an alternate path to the root switch 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 by a point-to-point link, or when a LAN has two or more connections connected to a shared segment.

  – *Disabled* — Indicates that the port is not participating in the Spanning Tree.
- **Mode** — Displays the current STP mode. The STP mode is selected in the *STP Properties Page*.

  The possible field values are:

  – *STP* — Indicates that Classic STP is enabled on the device.

  – *Rapid STP* — Indicates that Rapid STP is enabled on the device.

  – *Multiple STP* — Indicates that Multiple STP is enabled on the device.
- **Fast Link Operational Status** — Indicates whether 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** — Indicates whether a point-to-point link is established, or if the device is permitted to establish a point-to-point link. The possible field values are:

  – *Enable* — The device is permitted to establish a point-to-point link, or is configured 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 Protocol* (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. This is the actual switch port link type. It may differ from the administrative state.

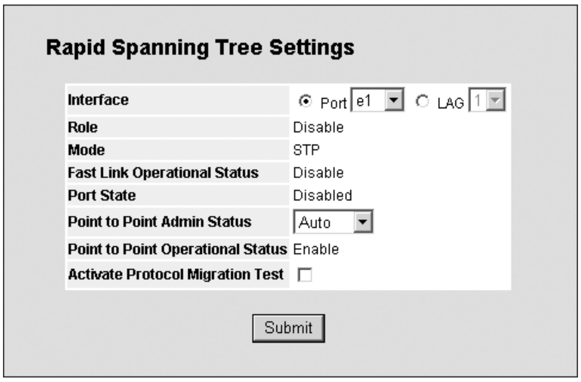
  – *Disable* — Disables point-to-point link.

  – *Auto* — Enables a point-to-point link automatically.

- **Point-to-Point Operational Status** — Displays the point-to-point operating state.
- **LAG** — Displays the LAG to which the interface is attached.

2. Click ✎ . The *RSTP Settings Page* opens:

Figure 88: RSTP Settings Page



Rapid Spanning Tree Settings

Interface	● Port e1 ▾ ○ LAG 1 ▾
Role	Disable
Mode	STP
Fast Link Operational Status	Disable
Port State	Disabled
Point to Point Admin Status	Auto ▾
Point to Point Operational Status	Enable
Activate Protocol Migration Test	□

The *RSTP Settings Page* contains the following fields in addition to the settings listed in the *RSTP Page*:

- **Activate Protocol Migration** — Indicates whether sending *Link Control Protocol* (LCP) packets to configure and test the data link is enabled. The possible field values are:
  – *Checked* — Enables the Protocol Migration.
  – *Unchecked* — Disables the Protocol Migration.

3. In the *RSTP Settings Page*, modify the following fields as required: *Point-to-Point Admin Status, Point-to-Point Operational Status*.

4. Check the "Activate Protocol Migration Test" check box to activate *Protocol Migration*.
5. Click Submit.
6. Click Submit in the *RSTP Page*. The RSTP parameters are saved, and the device is updated.

9.3 Configuring the Multiple STP

Multiple Spanning Tree Protocol (MSTP) provides differing load balancing scenarios. For example, while port A is blocked in one STP instance, the same port can be placed in the Forwarding state in another STP instance.

This section contains the following topics:

- Defining MSTP Properties
- Configuring MSTP Instances
- Configuring MSTP VLAN Instances
- Configuring MSTP Interface Settings

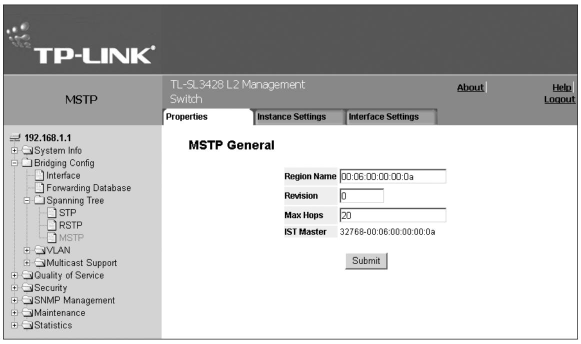
9.3.1 Defining MSTP Properties

The *MSTP Properties Page* contains information for defining global MSTP settings, including region names, MSTP revisions, and maximum hops.

To define MSTP:

1. Click **System > Bridging Config > Spanning Tree > MSTP > Properties**. The *MSTP Properties Page* opens:

Figure 89: MSTP Properties Page



MSTP General

Region Name	00:06:00:00:00:0a
Revision	0
Max Hops	20
IST Master	32768-00:06:00:00:00:0a

The *MSTP Properties Page* contains the following fields:

- **Region Name** — Indicates the name of the user-defined STP region.
- **Revision** — Indicates that an unsigned 16-bit number that identifies the revision of the current MSTP configuration. The revision number is required as part of the MSTP configuration.
  The possible range is 0-65535.
- **Max Hops** — Specifies the total number of hops that occur in a specific region before the BPDU is discarded. Once the BPDU is discarded, the port information is aged out. The possible field range is 1-40. The default value is 20 hops.
- **IST Master** — Identifies the Spanning Tree Master instance. The IST Master is the specified instance root.

2. Define the *Region Name, Revision* and *Max Hops* fields.
3. Click Submit. The device information is updated.

9.3.2 Configuring MSTP Instances

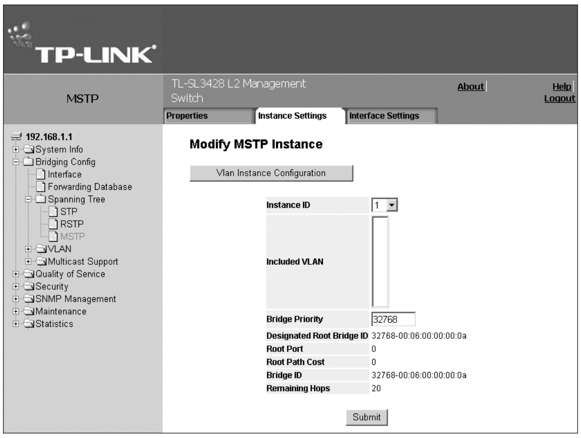
MSTP maps VLANs into STP instances. Packets assigned to various VLANs are transmitted along different paths within Multiple Spanning Tree Regions (MST Regions). Regions are one or more Multiple Spanning Tree bridges by which frames can be transmitted. In configuring MSTP, the MST region to which the device belongs is defined. A configuration consists of the name, revision, and region to which the device belongs.

Network administrators can define the MSTP instance settings using the *MSTP Instance Settings Page*.

To define instance settings for MSTP:

1. Click **System > Bridging Config > Spanning Tree > MSTP > Instance Settings.** The *MSTP Instance Settings Page* opens:

Figure 90: MSTP Instance Settings Page



Modify MSTP Instance

Instance ID	1
Included VLAN	
Bridge Priority	32768
Designated Root Bridge ID	32768-00:06:00:00:00:0a
Root Port	0
Root Path Cost	0
Bridge ID	32768-00:06:00:00:00:0a
Remaining Hops	20

The *MSTP Instance Settings Page* page contains the following fields:

- **Instance ID** — Specifies the VLAN group to which the interface is assigned.
- **Included VLAN** — Maps the selected VLANs to the selected instance. Each VLAN belongs to one instance.
- **Bridge Priority** — Specifies the selected spanning tree instance device priority. The field range is 0-61440
- **Designated Root Bridge ID** — Indicates the ID of the bridge with the lowest path cost to the instance ID.
- **Root Port** — Indicates the selected instance's root port.
- **Root Path Cost** — Indicates the selected instance's path cost.
- **Bridge ID** — Indicates the bridge ID of the selected instance.
- **Remaining Hops** — Indicates the number of hops remaining to the next destination.

2. Define the fields.

3. Click Submit. The MSTP settings are saved and the device is updated.

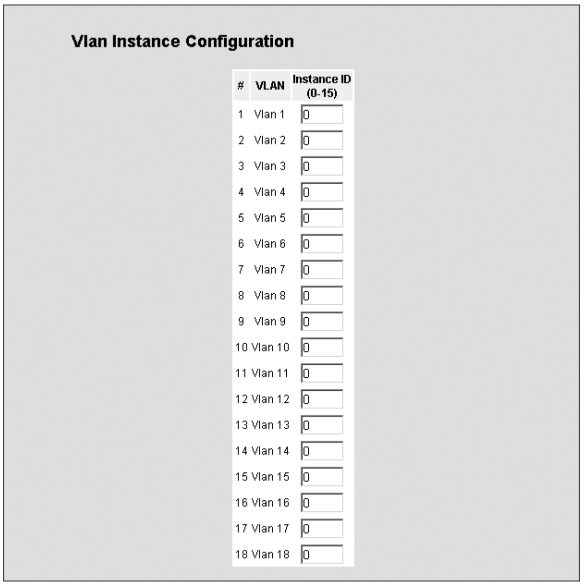
9.3.3 Configuring MSTP VLAN Instances

Network Administrator can assign MSTP for VLAN instances.

To define MSTP for VLAN instances:

1. Click **System > Bridging Info > Spanning Tree > MSTP > Instance Settings > VLAN Instance Configuration.** The *MSTP VLAN Instance Configuration Page* opens:

Figure 91: MSTP VLAN Instance Configuration Page



Vlan Instance Configuration

#	VLAN	Instance ID (0-15)
1	Vlan 1	0
2	Vlan 2	0
3	Vlan 3	0
4	Vlan 4	0
5	Vlan 5	0
6	Vlan 6	0
7	Vlan 7	0
8	Vlan 8	0
9	Vlan 9	0
10	Vlan 10	0
11	Vlan 11	0
12	Vlan 12	0
13	Vlan 13	0
14	Vlan 14	0
15	Vlan 15	0
16	Vlan 16	0
17	Vlan 17	0
18	Vlan 18	0

The *MSTP VLAN Instance Configuration Page* page contains the following fields:

- **VLAN ID** — Maps the selected VLANs to the selected instance. Each VLAN belongs to one instance.
- **Instance ID** — Specifies the VLAN group to which the interface is assigned.
- **VLAN** — Maps the selected VLANs to the selected instance. Each VLAN belongs to one instance.
- **Instance ID** — Lists the configured instances for the selected VLAN.

To add a new VLAN instance:

1. Select the *VLAN ID* and enter the *Instance ID*.
2. Click Submit. The device information is updated.

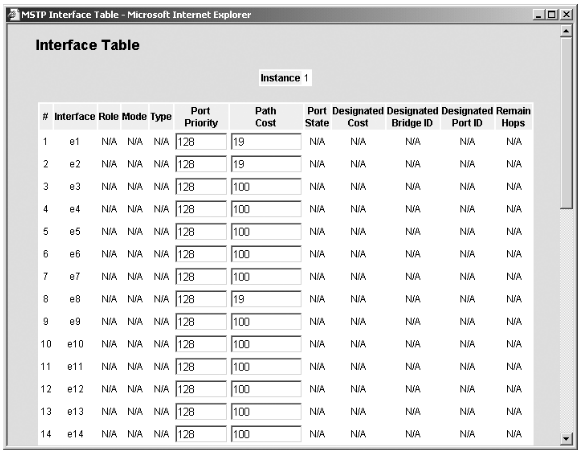
9.3.4 Configuring MSTP Interface Settings

Network Administrators can assign MSTP interface settings using the *MSTP Interface Settings Page*.

To define interface for MSTP:

1. Click **System > Bridging Config > Spanning Tree > MSTP > Interface Settings > Interface Table.** The *MSTP Interface Settings Page* opens:

Figure 92: MSTP Interface Table Page



Interface Table

Instance 1

#	Interface	Role	Mode	Type	Port Priority	Path Cost	Port State	Designated Cost	Designated Bridge ID	Designated Port ID	Remain Hops
1	e1	N/A	N/A	N/A	128	19	N/A	N/A	N/A	N/A	N/A
2	e2	N/A	N/A	N/A	128	19	N/A	N/A	N/A	N/A	N/A
3	e3	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
4	e4	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
5	e5	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
6	e6	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
7	e7	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
8	e8	N/A	N/A	N/A	128	19	N/A	N/A	N/A	N/A	N/A
9	e9	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
10	e10	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
11	e11	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
12	e12	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
13	e13	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A
14	e14	N/A	N/A	N/A	128	100	N/A	N/A	N/A	N/A	N/A

The *MSTP Interface Settings Page* contains the following fields:

- **Instance** — Lists the MSTP instances configured on the device. The possible range is 0-15.
- **Interface** — Displays the interface for which the MSTP settings are displayed. The possible field values are:
  - *Port* — Specifies the port for which the MSTP settings are displayed.
  - *LAG* — Specifies the LAG for which the MSTP settings are displayed.
- **Role** — Indicates the port role assigned by the STP algorithm to provide to STP paths.

The possible field values are:

– *Root* — Provides the lowest cost path to forward packets to the root device.

– *Designated* — Indicates the port or LAG through 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 by a point-to-point link or when a LAN has two or more connections connected to a shared segment.

– *Disabled* — Indicates the port is not participating in the Spanning Tree.

- **Mode** — Indicates the STP mode by which STP is enabled on the device. The possible field values are:

  – *Classic STP* — Classic STP is enabled on the device. This is the default value.

  – *Rapid STP* — Rapid STP is enabled on the device.

  – *Multiple STP* — Multiple STP is enabled on the device.
- **Type** — Indicates whether the port is a Boundary or Master port. The possible field values are:

  – *Boundary Port* — Indicates that the port is a Boundary port. A Boundary port attaches MST bridges to LANs in an outlying region. If the port is a Boundary port, this field also indicates whether the device on the other side of the link is working in RSTP or STP mode

  – *Master Port* — Indicates the port is a master port. A Master port provides connectivity from a MSTP region to the outlying CIST root.
- **Interface Priority** — Defines the Interface priority for the specified instance. The default value is 128.
- **Path Cost** — Indicates the port contribution to the Spanning Tree instance. The range should always be 1-200,000,000.
- **Port State** — Indicates whether the port is enabled for the specific instance. The possible field values are:

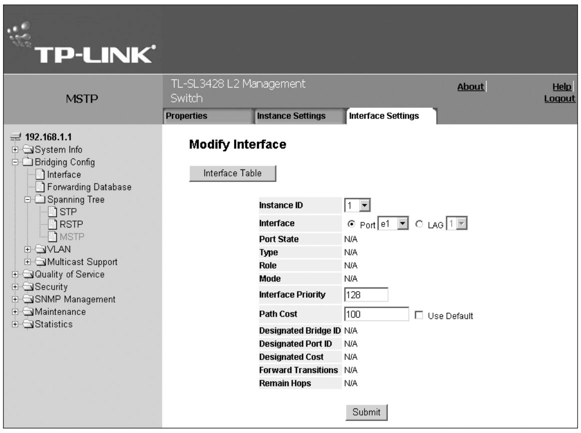
  – *Enabled* — Enables the port for the specific instance.

  – *Disabled* — Disables the port for the specific instance.
- **Designated Cost** — Indicates that the default path cost is assigned according to the method selected on the Spanning Tree Global Settings page.
- **Designated Bridge ID** — Displays the ID of the bridge that connects the link or shared LAN to the root.
- **Designated Port ID** — Displays the ID of the port on the designated bridge that connects the link or the shared LAN to the root.
- **Remain Hops** — Indicates the hops remaining to the next destination.

2. Select the Instance.
3. Modify the *Port Priority* and *Path Cost*.
4. Click Submit. The device information is updated.

To add new interface settings for MSTP:

Figure 93: MSTP Interface Settings Page



Modify Interface

Instance ID	1
Interface	● Port e1 ○ LAG 1
Port State	N/A
Type	N/A
Role	N/A
Mode	N/A
Interface Priority	128
Path Cost	100 □ Use Default
Designated Bridge ID	N/A
Designated Port ID	N/A
Designated Cost	N/A
Forward Transitions	N/A
Remain Hops	N/A

1. Define the instance properties fields.
2. Click Submit. The interface settings are added to the list in the MSTP Interface Settings Page. The device information is updated.

Section 10. Configuring Multicast Forwarding

Multicast forwarding enables transmitting packets from either a specific multicast group to a source, or from a nonspecific source to a multicast group.

This section contains the following topics:

- Enabling IGMP Snooping
- Defining Multicast Bridging Groups
- Defining Multicast Forward All Parameters

10.1 Configuring Multicast Forwarding

When IGMP Snooping is enabled globally, all IGMP packets are forwarded to the CPU. The CPU analyzes the incoming packets and determines:

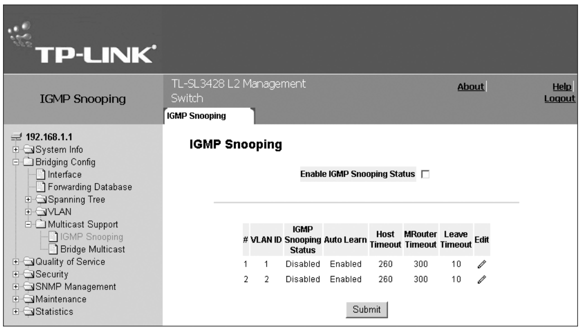
- Which ports want to join which Multicast groups.
- Which ports have Multicast routers generating IGMP queries.
- Which routing protocols are forwarding packets and Multicast traffic.

Ports requesting to join a specific Multicast group issue an IGMP report, specifying that Multicast group is accepting members. This results in the creation of the Multicast filtering database.

To enable IGMP Snooping:

1. Click **System > Bridging Config > Multicast Support > IGMP Snooping.** The *IGMP Snooping Page* opens:

Figure 94: IGMP Snooping Page



IGMP Snooping

Enable IGMP Snooping Status □

#	VLAN ID	IGMP Snooping Status	Auto Learn	Host Timeout	MRouter Timeout	Leave Timeout	Edit
1	1	Disabled	Enabled	260	300	10	✎
2	2	Disabled	Enabled	260	300	10	✎

The *IGMP Snooping Page* contains the following fields:

- **Enable IGMP Snooping Status** — Indicates if IGMP Snooping is enabled on the device. IGMP Snooping can be enabled only if Bridge Multicast Filtering is enabled. The possible field values are:
  – *Checked* — Enables IGMP Snooping on the device.
  – *Unchecked* — Disables IGMP Snooping on the device.
- **VLAN ID** — Specifies the VLAN ID.
- **IGMP Snooping Status** — Indicates if IGMP Snooping is enabled on the VLAN.
  The possible field values are:
  – *Enable* — Enables IGMP Snooping on the VLAN.
  – *Disable* — Disables IGMP Snooping on the VLAN.
- **Auto Learn** — Indicates if Auto Learn is enabled on the device. If Auto Learn is enabled, the devices automatically learns where other Multicast groups are located. Enables or disables Auto Learn on the Ethernet device.The possible field values are:
  – *Enable* — Enables auto learn
  – *Disable* — Disables auto learn
- **Host Timeout** — Indicates the amount of time host waits to receive a message before timing out. The default time is 260 seconds.
- **MRouter Timeout** — Indicates the amount of the time the Multicast router waits to receive a message before it times out.

The default value is 300 seconds.

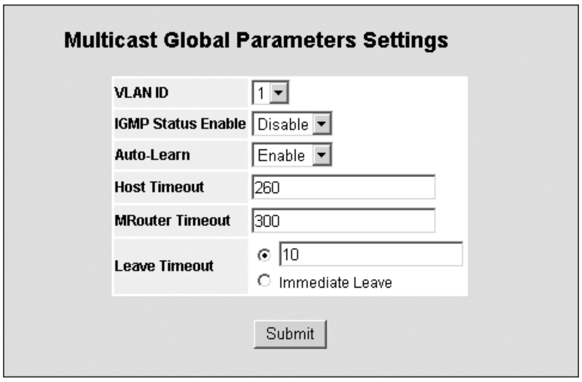
- **Leave Timeout** — Indicates the amount of time the host waits, after requesting to leave the IGMP group and not receiving a Join message from another station, before timing out. If a Leave Timeout occurs, the switch notifies the Multicast device to stop sending traffic The Leave Timeout value is either user-defined, or an immediate leave value. The default timeout is 10 seconds.

2. Click the *Enable IGMP Snooping Status* checkbox.
3. Click Submit. IGMP Snooping is enabled on the device.

To modify IGMP Snooping:

1. Click ✎ . The *Multicast Global Parameters Settings Page* opens:

Figure 95: Multicast Global Parameters Settings Page



Multicast Global Parameters Settings

VLAN ID	1
IGMP Status Enable	Disable
Auto-Learn	Enable
Host Timeout	260
MRouter Timeout	300
Leave Timeout	● 10 ○ Immediate Leave

2. Modify the *VLAN ID, IGMP Status Enable, Enable Auto Learn, Host Timeout, MRouter Timeout,* and *Leave Timeout* fields.
3. Click Submit. The IGMP global parameters are modified, and the device is updated.

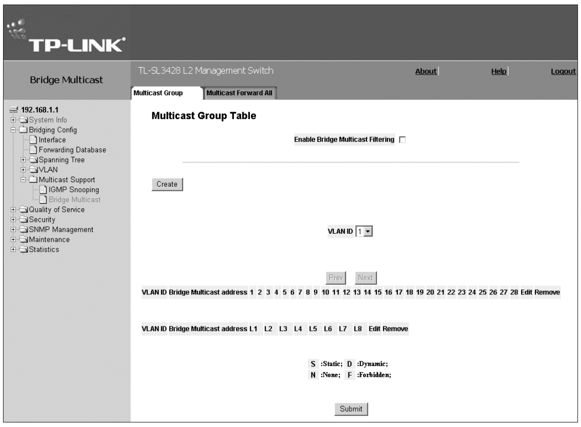
10.2 Defining Multicast Bridging Groups

The *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 *Multicast Group Page* permits new Multicast service groups to be created. The Multicast Group Page also assigns ports to a specific Multicast service address group.

To define multicast groups:

1. Click **System > Bridging Config > Multicast Support > Bridge Multicast > Multicast Group.** The *Multicast Group Page* opens:

Figure 96: Multicast Group Page



Multicast Group Table

Enable Bridge Multicast Filtering □

VLAN ID 1

VLAN ID	Bridge Multicast address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	Edit	Remove

VLAN ID	Bridge Multicast address	L1	L2	L3	L4	L5	L6	L7	L8	Edit	Remove

S :Static; D :Dynamic;
N :None; F :Forbidden;

The *Multicast Group Page* contains the following information:

- **Enable Bridge Multicast Filtering** — Indicates if Bridge Multicast filtering is enabled on the device.
  The possible field values are:
  – *Checked* — Enables Multicast filtering on the device.
  – *Unchecked* — Disables Multicast filtering on the device. If Multicast filtering is disabled, Multicast frames are flooded to all ports in the relevant VLAN. Disabled is the default value.
- **VLAN ID** — Identifies a VLAN and contains information about the Multicast group address.

- **Bridge Multicast Address** — Identifies the Multicast group MAC address/IP address.
- **Port** — Displays the port that can be added to a Multicast service.
- **LAG** — Displays the LAG that can be added to a Multicast service.

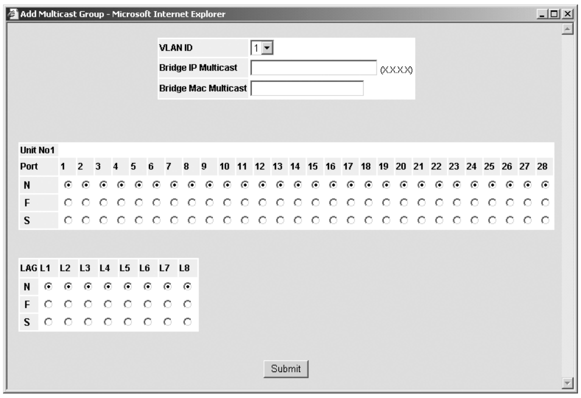
The following table contains the IGMP port and LAG members management settings:

Table 5: IGMP Port/LAG Members Table Control Settings

Port Control	Definition
D	Dynamically joins ports/LAG to the Multicast group 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 ports are not included the Multicast group, even if IGMP snooping designated the port to join a Multicast group.
Blank	The port is not attached to a Multicast group.

2. Click Create. The Add Multicast Group Page opens:

Figure 97: Add Multicast Group Page



VLAN ID: 1
Bridge IP Multicast: (X.X.X.X)
Bridge Mac Multicast:

Unit No1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
N	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
F	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
S	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

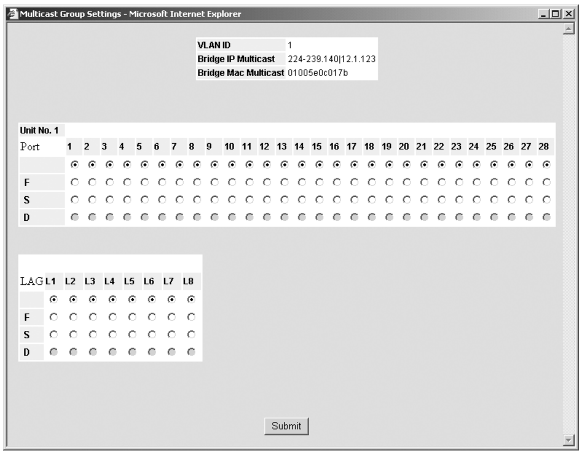
LAG	L1	L2	L3	L4	L5	L6	L7	L8
N	●	●	●	●	●	●	●	●
F	○	○	○	○	○	○	○	○
S	○	○	○	○	○	○	○	○

3. Define the *VLAN ID, Bridge Multicast IP Address*, and *Bridge Multicast MAC Address* fields.
4. Click Submit.
5. In the *Multicast Group Page*, select ports to join the Multicast group.
6. Define the Multicast port settings.
7. Click Submit. The Multicast group is defined, and the device is updated.

To modify the Multicast group settings:

1. Click **System > Bridging Config > Multicast Support > Bridge Multicast > Multicast Group.** The *Multicast Group Page* opens.
2. Click ✎ . The *Multicast Group Settings Page* opens:

Figure 98: Multicast Group Settings Page



VLAN ID: 1
Bridge IP Multicast: 224-239.140|12.1.123
Bridge Mac Multicast: 01005e0c017b

Unit No. 1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
F	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
S	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
D	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

LAG	L1	L2	L3	L4	L5	L6	L7	L8
	●	●	●	●	●	●	●	●
F	○	○	○	○	○	○	○	○
S	○	○	○	○	○	○	○	○
D	○	○	○	○	○	○	○	○

3. Select Ports/LAGs for the selected VLAN and define the port settings.
4. Click Submit. The Multicast group settings are modified and device information is updated.

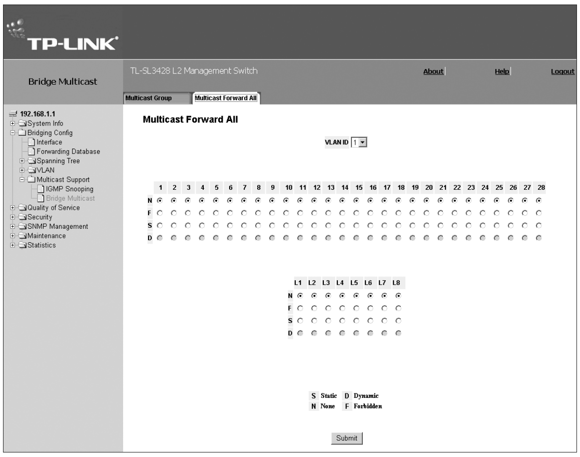
10.3 Defining Multicast Forward All Parameters

The *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. Unless LAGs are defined, only a Multicast Forward All table displays.

To define Multicast Forward All settings:

1. Click **System > Bridging Config > Multicast Support > Bridge Multicast > Multicast Forward All**. The *Multicast Forward All Page* opens:

Figure 99: Multicast Forward All Page



Multicast Forward All

VLAN ID 1

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
N	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
F	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
S	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
D	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

	L1	L2	L3	L4	L5	L6	L7	L8
N	●	●	●	●	●	●	●	●
F	○	○	○	○	○	○	○	○
S	○	○	○	○	○	○	○	○
D	○	○	○	○	○	○	○	○

S	Static	D	Dynamic
N	None	F	Forbidden

The *Multicast Forward All Page* contains the following fields:

- **VLAN ID** — Lists the VLAN for which Multicast parameters are displayed.
- **Port/LAG** — Ports that can be added to a Multicast service.

The following table summarizes the Multicast settings which can be assigned to ports, using the *Multicast Forward All Page*.

Table 6: Bridge Multicast Forward All Router/Port Control Settings Table

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.
N	The port is not attached to a Multicast router or switch.

2. Select a VLAN in the *VLAN ID* dropdown list.
3. Define the VLAN port settings.
4. Click Submit. The *Multicast Forward All* settings for the selected VLAN are defined and the device is updated.

Section 11. Configuring SNMP Management

Simple Network Management Protocol (SNMP) provides a method for managing network devices. The device supports the following SNMP versions:

- SNMP version 1
- SNMP version 2c
- SNMP version 3

11.1 SNMP v1 and v2c

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 SNMP agent 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.

11.2 SNMP v3

SNMP v3 applies access control and a new traps mechanism. In addition, User Security Model (USM) parameters are defined for SNMPv3, including:

- **Authentication** — Provides data integrity and data origin authentication.
- **Privacy** — Protects against the disclosure of message content. Cipher Block-Chaining (CBC) is used for encryption. Either authentication is enabled on a SNMP message, or both authentication and privacy are enabled on a SNMP message. However, privacy cannot be enabled without authentication.
- **Timeliness** — Protects against message delay or message redundancy. The SNMP agent compares incoming message to the message time information.
- **Key Management** — Defines key generation, key updates, and key use.

The device supports SNMP notification filters based on Object IDs (OIDs). OIDs are used by the system to manage device features.

SNMP v3 supports the following features:

- Security
- Feature Access Control
- Traps

The device generates the following traps:

- Copy trap

This section contains the following topics:

- Defining SNMP Security
- Configuring SNMP Notification Settings

11.3 Defining SNMP Security

This section describes configuring of SNMP security parameters, and contains the following topics:

- Defining SNMP Global Parameters
- Defining SNMP Views
- Defining SNMP Group Profiles

- Defining SNMP Group Members
- Defining SNMP Communities

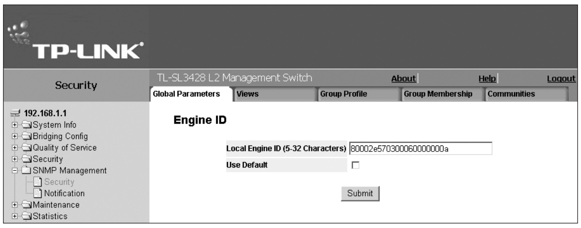
11.3.1 Defining SNMP Global Parameters

The SNMP Security Global Parameters Page permits the enabling of both SNMP and Authentication notifications.

To define SNMP security global parameters:

1. Click **System > SNMP Management > Security > Global Parameters**. The *SNMP Security Global Parameters Page* opens:

Figure 100: SNMP Security Global Parameters Page



Engine ID

Local Engine ID (5-32 Characters) 80002e570300060000000a

Use Default □

The *SNMP Security Global Parameters Page* contains the following fields:

- **Local Engine ID (0-32 Characters)** — Displays the local device Engine ID. The field value is a hexadecimal string. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or a colon. The Engine ID must be defined before SNMPv3 is enabled. Select a default Engine ID that is comprised of an Enterprise number and the default MAC address.
- **Use Default** — Uses the device-generated Engine ID. The default Engine ID is based on the device MAC address and is defined per standard as:

  – *First 4 octets* — first bit = 1, the rest is IANA Enterprise number.

  – *Fifth octet* — Set to 3 to indicate the MAC address that follows.

  – *Last 6 octets* — MAC address of the device.

2. Define the *Local Engine ID* and *Use Default* fields.

3. Click Submit. The SNMP global security parameters are set, and the device is updated.

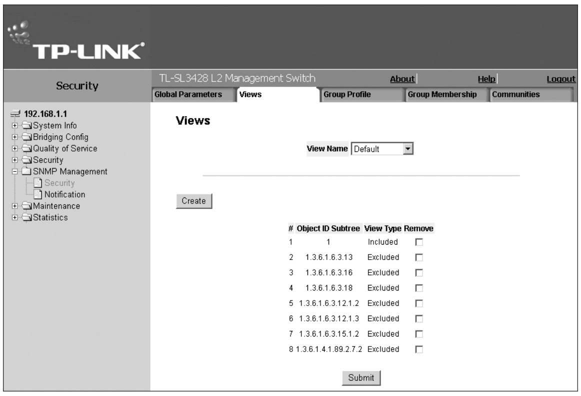
11.3.2 Defining SNMP Views

SNMP Insert space views provide or block access to device features or portions of features. For example, a view can be defined which provides that SNMP group A has Read Only (R/O) access to Multicast groups, while SNMP group B has Read-Write (R/W) access to Multicast groups. Feature access is granted via the MIB name or MIB Object ID.

To define SNMP views:

1. Click **System > SNMP Management > Security > Views**. The *SNMP Security Views Page* opens:

Figure 101: SNMP Security Views Page



Views

View Name Default

#	Object ID Subtree	View Type	Remove
1	1	Included	□
2	1.3.6.1.6.3.13	Excluded	□
3	1.3.6.1.6.3.16	Excluded	□
4	1.3.6.1.6.3.18	Excluded	□
5	1.3.6.1.6.3.12.1.2	Excluded	□
6	1.3.6.1.6.3.12.1.3	Excluded	□
7	1.3.6.1.6.3.15.1.2	Excluded	□
8	1.3.6.1.4.1.89.2.7.2	Excluded	□

The *SNMP Security Views Page* contains the following fields:

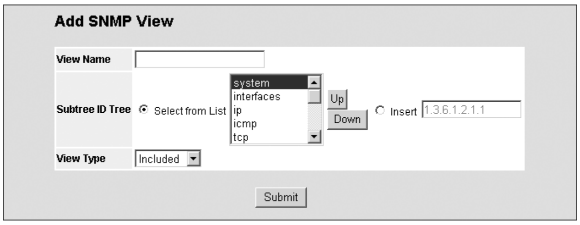
- **View Name** — Displays the user-defined views. The view name can contain a maximum of 30 alphanumeric characters.
- **Object ID Subtree** — Displays the device feature OID included in or excluded from the selected SNMP view.
- **View Type** — Indicates whether the defined OID branch will be included in or excluded from the selected

SNMP view.

- **Remove** — Deletes the currently selected view. The possible field values are:
  – *Checked* — Removes the selected view.
  – *Unchecked* — Maintains the list of views.

2. Click Create. The *Add SNMP View Page* opens:

Figure 102: Add SNMP View Page



Add SNMP View

View Name:

Subtree ID Tree: ● Select from List (system, interfaces, ip, icmp, tcp) Up Down ○ Insert 1.3.6.1.2.1.1

View Type: Included

Submit

3. Define the *View Name* field.
4. Define the view using Up and Down .
5. Define the *View Type* field.
6. Click Submit. The view is defined, and the device is updated.

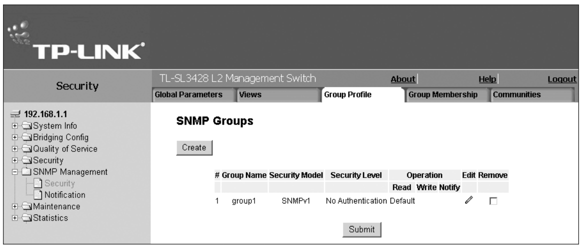
11.3.3 Defining SNMP Group Profiles

The *SNMP Security Group Profile Page* provides information for creating SNMP groups, and assigning SNMP access control privileges to SNMP groups. Groups allow network managers to assign access rights to specific device features, or feature aspects.

To define an SNMP group:

1. Click **System > SNMP Management > Security > Group Profile**. The *SNMP Security Group Profile Page* opens:

Figure 103: SNMP Security Group Profile Page



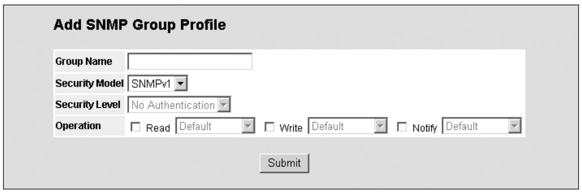
SNMP Groups

#	Group Name	Security Model	Security Level	Operation			Edit	Remove
				Read	Write	Notify		
1	group1	SNMPv1	No Authentication	Default			✎	□

The *SNMP Security Group Profile Page* contains the following fields:

- **Group Name** — Displays the user-defined group to which access control rules are applied. The field range is up to 30 characters.
- **Security Model** — Defines the SNMP version attached to the group. The possible field values are:
  – *SNMPv1* — SNMPv1 is defined for the group.
  – *SNMPv2c* — SNMPv2c is defined for the group.
  – *SNMPv3* — SNMPv3 is defined for the group.
- **Security Level** — Defines the security level attached to the group. Security levels apply to SNMPv3 only.
  The possible field values are:
  – *No Authentication* — Indicates that neither the Authentication nor the Privacy security levels are assigned to the group.
  – *Authentication* — Authenticates SNMP messages, and ensures that the SNMP message's origin is authenticated.
  – *Privacy* — Encrypts SNMP messages.
- **Operation** — Defines the group access rights. The possible field values are:
  – *Read* — Management access is restricted to read-only, and changes cannot be made to the assigned SNMP view.
  – *Write* — Management access is read-write and changes can be made to the assigned SNMP view.
  – *Notify* — Sends traps for the assigned SNMP view.
- **Remove** — Removes SNMP groups. The possible field values are:
  – *Checked* — Removes the selected SNMP group.
  – *Unchecked* — Maintains the SNMP groups.

2. Click Create. The *Add SNMP Group Profile Page* opens:



Add SNMP Group Profile

Group Name:

Security Model: SNMPv1

Security Level: No Authentication

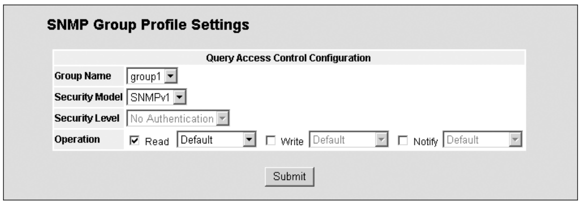
Operation: □ Read Default □ Write Default □ Notify Default

Figure 104: Add SNMP Group Profile Page

3. Define the *Group Name, Security Model, Security Level*, and *Operation* fields.
4. Click Submit. The SNMP group profile is added, and the device is updated.

To modify the SNMP Group settings:

1. Click **System > SNMP Management > Security > Group Profile**. The *SNMP Security Group Profile Page* opens.
2. Click ✎. The *SNMP Group Profile Settings Page* opens:



SNMP Group Profile Settings

Query Access Control Configuration

Group Name: group1

Security Model: SNMPv1

Security Level: No Authentication

Operation: ☑ Read Default □ Write Default □ Notify Default

Figure 105: SNMP Group Profile Settings Page

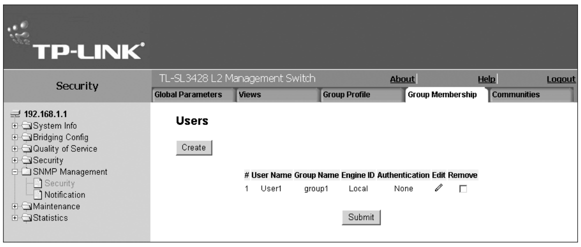
3. Modify the *Group Name, Security Model, Security Level*, and *Operation* fields.
4. Click Submit. The SNMP group profile is modified, and the device is updated.

11.3.4 Defining SNMP Group Members

The *SNMP Security Group Membership Page* enables assigning system users to SNMP groups, as well as defining the user authentication method.

To define SNMP group membership:

1. Click **System > SNMP Management > Security > Group Membership**. The *SNMP Security Group Membership Page* opens:



Users

#	User Name	Group Name	Engine ID	Authentication	Edit	Remove
1	User1	group1	Local	None	✎	□

Figure 106: SNMP Security Group Membership Page

The SNMP Security Group Membership Page contains the following fields:

- **User Name** — Contains a list of user-defined user names. The field range is up to 30 alphanumeric characters.
- **Group Name** — Contains a list of user-defined SNMP groups. SNMP groups are defined in the SNMP Group Profile Page.
- **Engine ID** — Displays either the local or remote SNMP entity to which the user is connected. Changing or removing the local SNMP Engine ID deletes the SNMPv3 user database.
  – *Local* — Indicates that the user is connected to a local SNMP entity.
  – *Remote* — Indicates that the user is connected to a remote SNMP entity. If the Engine ID is defined, remote devices receive inform messages.
- **Authentication** — Displays the method used to authenticate users. The possible field values are:
  – *MD5 Key* — Users are authenticated using the HMAC-MD5 algorithm.
  – *SHA Key* — Users are authenticated using the HMAC-SHA-96 authentication level.
  – *MD5 Password* — The HMAC-MD5-96 password is used for authentication. The user should enter a password.

– *SHA Password* — Users are authenticated using the HMAC-SHA-96 authentication level. The user should enter a password.

– *No Authentication* — No user authentication is used.

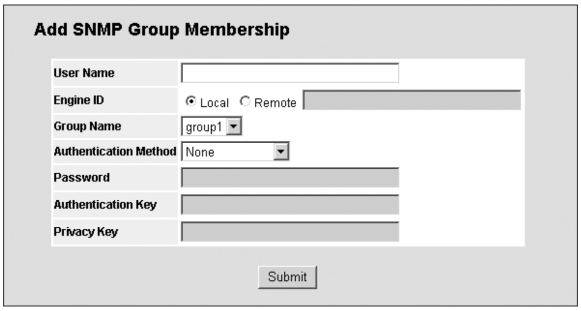
- **Remove** — Removes users from a specified group. The possible field values are:

  – *Checked* — Removes the selected user.

  – *Unchecked* — Maintains the list of users.

2. Click Create. The Add SNMP Group Membership Page opens:

Figure 107: Add SNMP Group Membership Page



Add SNMP Group Membership

User Name	
Engine ID	● Local ○ Remote
Group Name	group1
Authentication Method	None
Password	
Authentication Key	
Privacy Key	

Submit

In addition to the fields in the *SNMP Security Group Membership Page*, The *Add SNMP Group Membership Page* contains the following fields:

- **Authentication Method** — Defines the SNMP authentication method.
- **Authentication Key** — Defines the HMAC-MD5-96 or HMAC-SHA-96 authentication level. The authentication and privacy keys are entered to define the authentication key. If only authentication is required, 16 bytes are defined. If both privacy and authentication are required, 32 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or a colon.
- **Privacy Key** — Defines the privacy key (LSB). If only authentication is required, 20 bytes are defined. If both privacy and authentication are required, 36 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon.
- **Password** — Defines the password for the group member

3. Define the *User Name, Group Name, Engine ID, Authentication Method, Password, Authentication Key*, and *Privacy Key* fields.

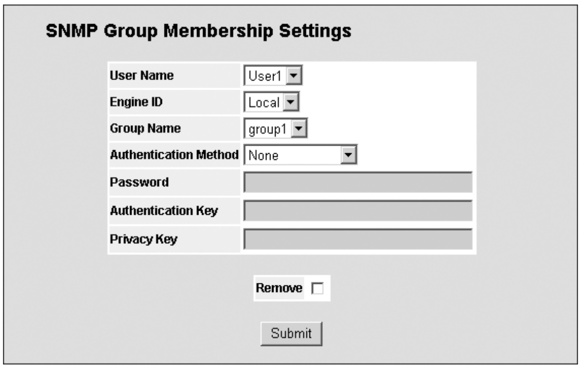
4. Click Submit. The SNMP group membership is modified, and the device is updated.

To modify SNMP Group Membership settings:

1. Click **System > SNMP Management > Security > Group Membership**. The *SNMP Security Group Membership Page* opens.

2. Click ✎ . The *SNMP Group Membership Settings Page* opens:

Figure 108: SNMP Group Membership Settings Page



SNMP Group Membership Settings

User Name	User1
Engine ID	Local
Group Name	group1
Authentication Method	None
Password	
Authentication Key	
Privacy Key	

Remove □

Submit

3. Modify the *Group Name, Engine ID, Authentication Method, Password, Authentication Key*, and P*rivacy Key* fields.

4. Click Submit. The SNMP group membership is modified, and the device is updated.

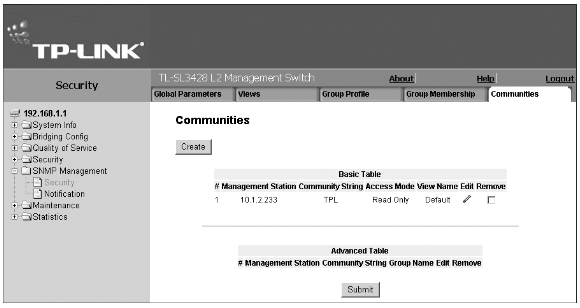
11.3.5 Defining SNMP Communities

Access rights are managed by defining communities in the *SNMP Communities Page*. When the community names are changed, access rights are also changed. SNMP communities are defined only for SNMP v1 and SNMP v2c.

To define SNMP communities:

1. Click **System > SNMP Management > Security > Communities**. The *SNMP Security Communities Page* opens:

Figure 109: SNMP Security Communities Page



Communities

Basic Table

#	Management Station	Community String	Access Mode	View Name	Edit	Remove
1	10.1.2.233	TPL	Read Only	Default	✎	□

Advanced Table

#	Management Station	Community String	Group Name	Edit	Remove

The *SNMP Security Communities Page* is divided into the following tables:

- Basic Table
- Advanced Table

11.3.5.1 SNMP Communities Basic Table

The *SNMP Communities Basic Table* contains the following fields:

- **Management Station** — Displays the management station IP address for which the basic SNMP community is defined.
- **Community String** — Defines the password used to authenticate the management station to the device.
- **Access Mode** — Defines the access rights of the community. The possible field values are:
  – *Read Only* — Management access is restricted to read-only, and changes cannot be made to the community.
  – *Read Write* — Management access is read-write and changes can be made to the device configuration, but not to the community.
  – *SNMP Admin* — User has access to all device configuration options, as well as permissions to modify the community.
- **View Name** — Contains a list of user-defined SNMP views
- **Remove** — Removes a community. The possible field values are:
  – *Checked* — Removes the selected SNMP community.
  – *Unchecked* — Maintains the SNMP communities.

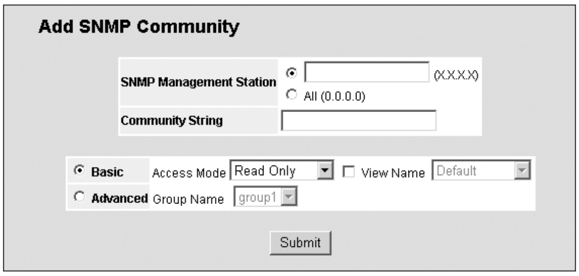
11.3.5.2 SNMP Communities Advanced Table

The *SNMP Communities Advanced Table* contains the following fields:

- **Management Station** — Displays the management station IP address for which the advanced SNMP community is defined.
- **Community String** — Defines the password used to authenticate the management station to the device.
- **Group Name** — Defines advanced SNMP community group names.
- **Remove** — Removes a community. The possible field values are:
  – *Checked* — Removes the selected SNMP communities.
  – *Unchecked* — Maintains the SNMP communities.

2. Click Create. The *Add SNMP Community Page* opens:

Figure 110: Add SNMP Community Page



Add SNMP Community

SNMP Management Station ● [ ] (X.X.X.X) ○ All (0.0.0.0)

Community String [ ]

● Basic Access Mode Read Only ▾ □ View Name Default ▾

○ Advanced Group Name group1 ▾

3. Define the *SNMP Management Station, Community String*, and *Basic or Advanced* fields.

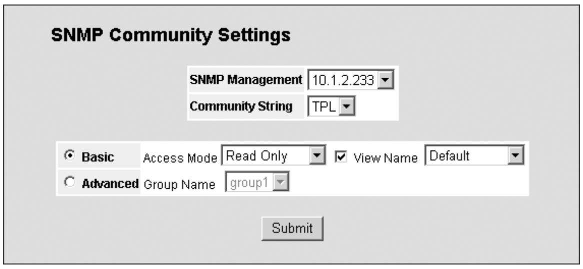
4. Click Submit. The SNMP community is added, and

the device is updated.

To modify SNMP Group Membership settings:

1. Click **System > SNMP Management > Security > Communities**. The *SNMP Community Settings Page* opens:

Figure 111: SNMP Community Settings Page



SNMP Community Settings

SNMP Management: 10.1.2.233

Community String: TPL

● Basic — Access Mode: Read Only — ☑ View Name: Default

○ Advanced — Group Name: group1

2. Modify the *SNMP Management Station, Community String*, and *Basic or Advanced* fields.
3. Click Submit. The SNMP community is modified, and the device is updated.

11.4 Configuring SNMP Notification Settings

This section describes configuring of SNMP Notifications, and contains the following topics:

- Defining SNMP Notification Properties
- Defining Notification Filters
- Defining Notification Receivers

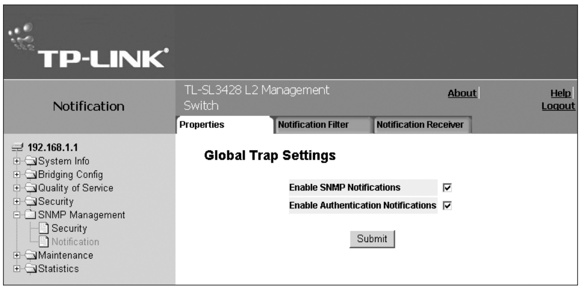
11.4.1 Defining SNMP Notification Properties

The *SNMP Notification Properties Page* contains parameters for defining SNMP notification parameters.

To define SNMP notification global parameters:

1. Click **System > SNMP Management > Notification > Properties**. The *SNMP Notification Properties Page* opens:

Figure 112: SNMP Notification Properties Page



Global Trap Settings

Enable SNMP Notifications ☑

Enable Authentication Notifications ☑

The *SNMP Notification Properties Page* contains the following fields:

- **Enable SNMP Notifications** — Specifies whether the device can send SNMP notifications. The possible field values are:
  – *Enable* — Enables SNMP notifications.
  – *Disable* — Disables SNMP notifications.
- **Enable Authentication Notifications** — Specifies whether SNMP authentication failure notification is enabled on the device. The possible field values are:
  – *Enable* — Enables the device to send authentication failure notifications.
  – *Disable* — Disables the device from sending authentication failure notifications.

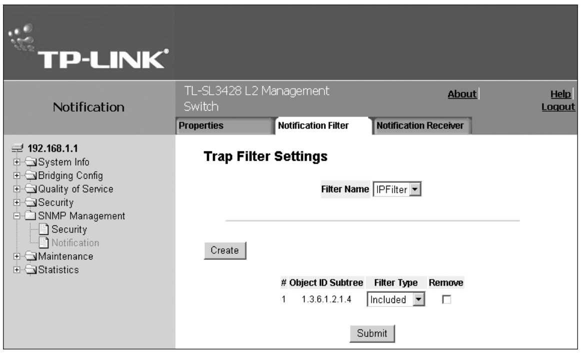
2. Define the *Enable SNMP Notification* and *Enable Authentication Notifications* fields.
3. Click Submit. The SNMP notification properties are defined, and the device is updated.

11.4.2 Defining Notification Filters

The *SNMP Notification Filter Page* permits filtering traps based on OIDs. Each OID is linked to a device feature or a portion of a feature. The SNMP Notification Filter Page also allows network managers to filter notifications.

To define notification filters:

1. Click **System > SNMP Management > Notification > Notification Filter**. The *SNMP Notification Filter Page* opens:



Trap Filter Settings

Filter Name: IPFilter

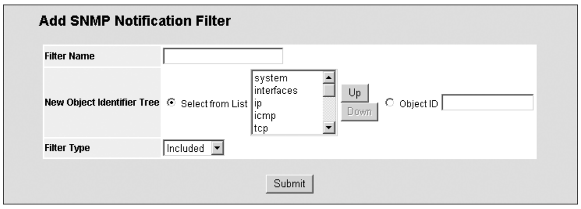
#	Object ID Subtree	Filter Type	Remove
1	1.3.6.1.2.1.4	Included	□

Figure 113: SNMP Notification Filter Page

The *SNMP Notification Filter Page* contains the following fields:

- **Filter Name** — Contains a list of user-defined notification filters.
- **Object ID Subtree** — Displays the OID for which notifications are sent or blocked. If a filter is attached to an OID, traps or informs are generated and sent to the trap recipients. OIDs are selected from either the *Select from* field or the *Object ID* field.
- **Filter Type** — Indicates whether to send traps or informs relating to the selected OID.
  – *Excluded* — Does not send traps or informs.
  – *Included* — Sends traps or informs.
- **Remove** — Deletes filters.
  – *Checked* — Deletes the selected filter.
  – *Unchecked* — Maintains the list of filters.

2. Click Create. The *Add SNMP Notification Filter Page* opens:



Add SNMP Notification Filter

Filter Name:

New Object Identifier Tree: ● Select from List (system, interfaces, ip, icmp, tcp) ○ Object ID

Filter Type: Included

Figure 114: Add SNMP Notification Filter Page

3. Define the Filter Name, New Object Identifier Tree, and Filter Type fields.

4. Click Submit. The SNMP notification filter is defined, and the device is updated.

11.4.3 Defining Notification Receivers

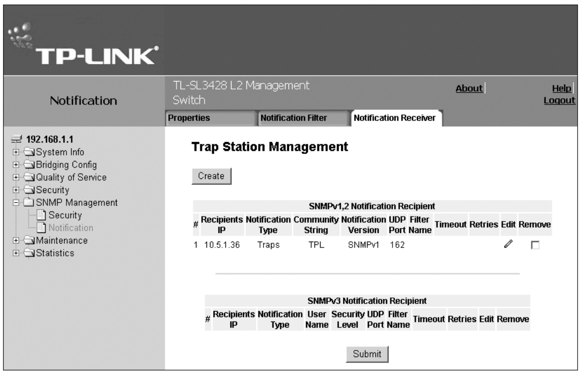
The *SNMP Notification Receiver Page* contains information for defining filters that determine whether traps are sent to specific users, and the trap type sent. SNMP notification filters provide the following services:

- Identifying Management Trap Targets
- Trap Filtering
- Selecting Trap Generation Parameters
- Providing Access Control Checks

To define SNMP notification filters:

1. Click **System > SNMP Management > Notification > Notification Receiver**. The *SNMP Notification Receiver Page* opens:

Figure 115: SNMP Notification Receiver Page



Trap Station Management

SNMPv1,2 Notification Recipient

#	Recipients IP	Notification Type	Community String	Notification Version	UDP Port	Filter Name	Timeout	Retries	Edit	Remove
1	10.5.1.36	Traps	TPL	SNMPv1	162				✎	□

SNMPv3 Notification Recipient

#	Recipients IP	Notification Type	User Name	Security Level	UDP Port	Filter Name	Timeout	Retries	Edit	Remove

The *SNMP Notification Receiver Page* c is divided into the following tables:

- SNMPv1,2c Notification Recipient
- SNMPv3 Notification Recipient

11.4.3.1 SNMPv1,2c Notification Recipient

The *SNMP v1, v2c Recipient* table contains the following fields:

- **Recipients IP** — Displays the IP address to which the traps are sent.
- **Notification Type** — Displays the type of notification sent. The possible field values are:
  – *Trap* — Indicates traps are sent.
  – *Inform* — Indicates informs are sent.
- **Community String** — Displays the community string of the trap manager.
- **Notification Version** — Displays the trap type. The possible field values are:
  – *SNMP V1* — Indicates that SNMP Version 1 traps are sent.
  – *SNMP V2c* — Indicates that SNMP Version 2 traps are sent.
- **UDP Port** — Displays the UDP port used to send notifications. The field range is 1-65535. The default is 162.
- **Filter Name** — Indicates if the SNMP filter for which the SNMP Notification filter is defined.
- ***Timeout*** — Indicates the amount of time (in seconds) the device waits before resending informs. The field range is 1-300. The default is 15 seconds.
- **Retries** — Indicates the number of times the device resends an inform request. The field range is 1-255. The default is 3.
- **Remove** — Deletes the currently selected recipient. The possible field values are:
  – *Checked* — Removes the selected recipient from the list of recipients.
  – *Unchecked* — Maintains the list of recipients.

11.4.3.2 SNMPv3 Notification Recipient

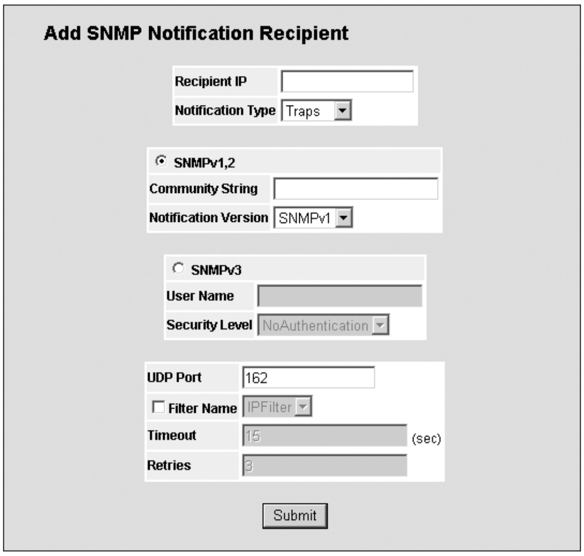
The *SNMPv3 Notification Recipient* table contains the following fields:

- **Recipient IP** — Displays the IP address to which the traps are sent.
- **Notification Type** — Displays the type of notification sent. The possible field values are:
  – *Trap* — Indicates that traps are sent.
  – *Inform* — Indicates that informs are sent.
- **User Name** — Displays the user to which SNMP notifications are sent.
- **Security Level** — Displays the means by which the packet is authenticated. The possible field values are:
  – *No Authentication* — Indicates that the packet is neither authenticated nor encrypted.
  – *Authentication* — Indicates that the packet is authenticated.
- **UDP Port** — Displays the UDP port used to send notifications. The field range is 1-65535. The default is 162.
- ***Filter Name*** — Includes or excludes SNMP filters.
- **Timeout** — Indicates the amount of time (in seconds) the device waits before resending informs. The field range is 1-300. The default is 15 seconds.
- **Retries** — Indicates the number of times the device resends an inform request. The field range is 1-255. The default is 3.
- **Remove** — Deletes the currently selected recipient. The possible field values are:
  – *Checked* — Removes the selected recipient from the list of recipients.

– *Unchecked* — Maintains the list of recipients.

2. Click Create. The *Add SNMP Notification Receiver Page* opens:

Figure 116: Add SNMP Notification Receiver Page



Add SNMP Notification Recipient

Recipient IP

Notification Type: Traps

● SNMPv1,2

Community String

Notification Version: SNMPv1

○ SNMPv3

User Name

Security Level: NoAuthentication

UDP Port: 162

□ Filter Name: IPFilter

Timeout: 15 (sec)

Retries: 3

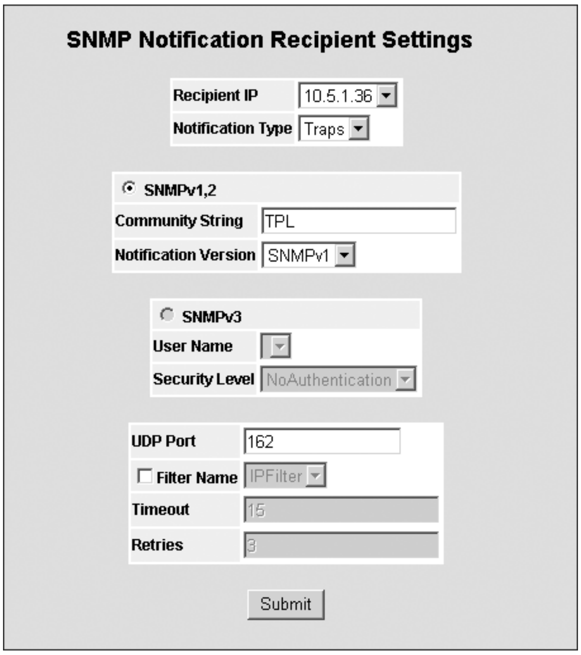
Submit

3. Define the *Recipient IP, Notification Type, SNMPV1,v2c or SNMPv3, UPD Port, Filter Name, Timeout*, and *Retries* fields.
4. Click Submit. The SNMP Notification recipients are defined, and the device is updated.

To modify SNMP notification recipients:

1. Click **System > SNMP Management > Notification > Notification Receiver**. The *SNMP Notification Receiver Page* opens:
2. Click ✎ . The *SNMP Notification Receiver Settings Page* opens:

Figure 117: SNMP Notification Receiver Settings Page



SNMP Notification Recipient Settings

Recipient IP: 10.5.1.36

Notification Type: Traps

● SNMPv1,2

Community String: TPL

Notification Version: SNMPv1

○ SNMPv3

User Name

Security Level: NoAuthentication

UDP Port: 162

□ Filter Name: IPFilter

Timeout: 15

Retries: 3

Submit

3. Modify the *Notification Type, SNMPV1,v2c or SNMPv3, UPD Port, Filter Name, TImeout*, and *Retries* fields.
4. Click Submit. The SNMP notification recipients are defined, and the device is updated.

Section 12. Configuring Quality of Service

This section contains the following topics:

- Quality of Service Overview
- Enabling Quality of Service
- Mapping Queues

12.1 Quality of Service Overview

Network traffic is usually unpredictable, and the only basic assurance that can be offered is best effort traffic delivery. To overcome this challenge, Quality of Service (QoS) is applied throughout the network. This ensures that network traffic is prioritized according to specified criteria, and that specific traffic receives preferential treatment. QoS in the network optimizes network performance and entails two basic facilities:

- Classifying incoming traffic into handling classes, based on an attribute, including:
  – The ingress interface
  – Packet content
  – A combination of these attributes
- Providing various mechanisms for determining the allocation of network resources to different handling classes, including:
  – The assignment of network traffic to a particular hardware queue
  – The assignment of internal resources
  – Traffic shaping

In this document, the terms Class of Service (CoS) and QoS are used in the following context:

- CoS provides varying Layer 2 traffic services. CoS refers to classification of traffic to traffic-classes, which are handled as an aggregate whole, with no per-flow settings. CoS is usually related to the 802.1p service that classifies flows according to their Layer 2 priority, as set in the VLAN header.
- QoS refers to Layer 2 traffic and above. QoS handles per-flow settings, even within a single traffic class.
- The QoS facility involves the following elements:
- **Traffic Classification** — Classifies each incoming packet as belonging to a given traffic class, based on the packet contents and/or the context.
- **Assignment to Hardware Queues** — Assigns incoming packets to forwarding queues. Packets are sent to a particular queue for handling as a function of the traffic class to which they belong, as defined by the classification mechanism.
- **Traffic Class-Handling Attributes** — Applies QoS/CoS mechanisms to different classes, including:
  – Bandwidth Management
  – Shaping/ Rate Limiting
  – Policing

12.1.1 Mapping to Queues

Queues are used in both Basic and Advanced QoS modes. Default settings are applied to maps in Service QoS mode. A Trust Behavior can be selected, or the output service fields can be selected, including:

- **VLAN Priority Tags (VPT)** — VPTs are mapped to an output queues based on the VPT. While queue mapping is user-defined, the VPT default mapping to the output queue is as follows. In the VPT default mapping, Queue 1 has the lowest priority.

The following table contains the VPT to Queue default settings:

Table 7: VPT Default Mapping Table

VPT Value	Queue Number
0	2
1	1
2	1
3	2
4	3
5	3
6	4
7	4

Mapping of the VPT to the output queue is performed on a system-wide basis, and can be enabled or disabled per port.

- **Default CoS**— Packets arriving untagged are assigned to a default VPT, which can be set by the user on a per port basis. Once the VPT is assigned, the packet is treated as if it had arrived with this tag. The VPT mapping to the output queue is based on the same user-defined 802.1p tag-based definitions.
- **DSCP** — Users can configure the system to use the IP DSCP of the incoming packet to the output priority queues. The mapping of the IP DSCP to priority queue is set on a per system basis. If this mode is active, a non-IP packet is always classified to the best effort queue.

The default mapping is shown in the following table:

Table 8: DSCP Default Mapping Table

DSCP Value	Queue Number
0-15	q1 (lowest priority)
16-31	q2
32-47	q3
48-64	q4

All network traffic which is not assigned a DSCP value is forwarded with Best Effort service.

After packets are assigned to a specific queue, using the chosen classification method various services can be applied. Scheduling for output queues can be configured, including:

- Strict priority
- Weighted Round Robin (WRR)

Scheduling schemes are specified per system. WRR weights to the queues can be assigned in any order. For each interface or queue, the following output shaping can also be configured:

- Committed Burst Size (CBS)
- Committed Information Rate (CIR)
- Actions for over-the-limit traffic

12.1.2 QoS Modes

The device supports the following QoS modes:

- Basic QoS Mode
- Advanced QoS Mode

Note:

When moving to and from basic and advanced QoS modes, some settings may be lost.

12.1.2.1 Basic QoS Mode

Basic Mode supports activating one of the following Trust settings:

- VLAN Point Tag
- DiffServ Code Point
- None

In addition, a single IP-based ACL can be attached directly to the interface (see section on network security for more information). Only packets that have a **Forward** action are assigned to the output queue, based on the specified classification. By properly configuring the output queues, the following basic mode services can be set:

- **Minimum Delay** — The queue is assigned to a strict priority policy, and traffic is assigned to the highest priority queue.
- **Best Effort** — Traffic is assigned to the lowest priority queue
- **Bandwidth Assignments** — Bandwidths are assigned by configuring the WRR scheduling scheme and choosing the right weights.

12.1.2.2 Advanced QoS Mode

Advanced QoS mode provides rules for specifying flow classification and assigning rule actions that relate to bandwidth management.

After assigning packets to a specific queue, services such as configuring output queues for the scheduling scheme, or configuring output shaping for burst size, CIR, or CBS per interface or per queue, can be applied. In Advanced Mode packets may egress with a different VPT tag than expected.

12.2 Enabling Quality of Service

This section contains the following topics:

- Enabling Quality of Service
- Mapping Queues

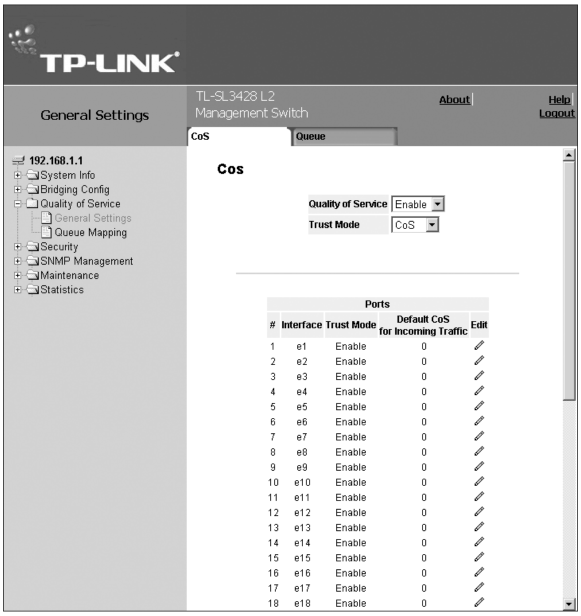
12.2.1 Enabling Quality of Service

The *CoS 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 egress queue settings.

To enable QoS and define basic settings:

1. Click **System > Quality of Service > General Settings > CoS Settings**. The *CoS Settings Page* opens:

Figure 118: CoS Settings Page



Cos

Quality of Service: Enable
Trust Mode: CoS

Ports				
#	Interface	Trust Mode	Default CoS for Incoming Traffic	Edit
1	e1	Enable	0	✎
2	e2	Enable	0	✎
3	e3	Enable	0	✎
4	e4	Enable	0	✎
5	e5	Enable	0	✎
6	e6	Enable	0	✎
7	e7	Enable	0	✎
8	e8	Enable	0	✎
9	e9	Enable	0	✎
10	e10	Enable	0	✎
11	e11	Enable	0	✎
12	e12	Enable	0	✎
13	e13	Enable	0	✎
14	e14	Enable	0	✎
15	e15	Enable	0	✎
16	e16	Enable	0	✎
17	e17	Enable	0	✎
18	e18	Enable	0	✎

The *CoS Settings Page* contains the following fields:

- **Quality of Service**— Indicates if QoS is enabled on the interface. The possible values are:
  – *Enable* — Enables QoS on the interface.
  – *Disable* — Disables QoS on the interface.
- **Trust Mode** — Selects the trust mode. If a packet' s CoS tag and DSCP tags are mapped to different queues, the Trust mode determines the queue to which the packet is assigned. The possible field values are:
  – *None* — Sets the Trust mode to none. All packets are sent to the lowest queue.
  – *CoS* — Sets the Trust mode to CoS. Packets are queued based on their CoS tag value.
  – *DSCP* — Sets the Trust mode to CoS. Packets are queued based on their DSCP tag value.

In the QoS parameters list:

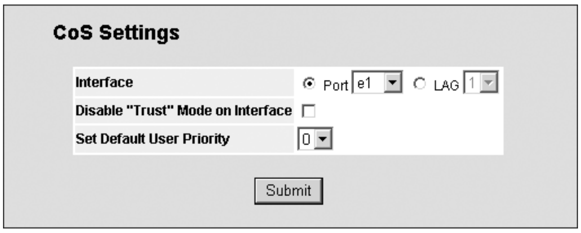
- **# Number** — Indicates the number of the interface for which the global QoS parameters are defined.
- **Interface** — Displays the name of the interface for which the global QoS parameters are defined.
- **Trust Mode** — Indicates if the trust mode is enabled for the interface.
- **Default CoS for Incoming Traffic** — Displays the current settings for the default CoS value for incoming packets for which a VLAN tag is not defined. The possible field values are 0-7. The default CoS is 0.

2. Select Enable in the *Quality of Service* field.
3. Select the *Trust Mode*.
4. Click Submit. QoS is configured and enabled on the device.

To modify interface settings:

1. Click ✎ . The QoS Interface Settings Page opens.

Figure 119: QoS Interface Settings Page



CoS Settings

Interface: ● Port e1 ○ LAG 1
Disable "Trust" Mode on Interface: □
Set Default User Priority: 0

2. Define the fields.
3. Click Submit. The interface settings are updated.

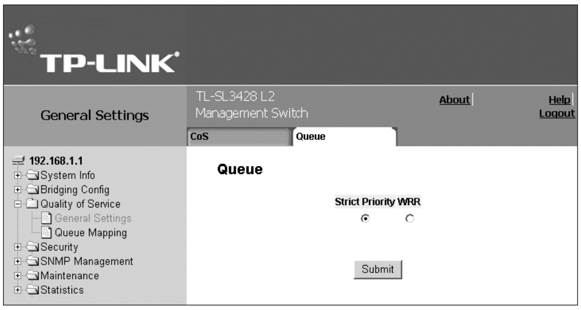
12.2.2 Defining Queues

The *QoS Queue Settings Page* contains fields for defining the QoS queue forwarding types. The queue settings are set system-wide.

To define queue settings for Quality of Service:

1. Click **System > Quality of Service > General Settings > Queue Settings**. The *QoS Queue Settings Page* opens:

Figure 120: QoS Queue Settings Page



Queue

Strict Priority ● WRR ○

The *QoS Queue Settings Page* contains the following fields:

- **Queue** — Indicates the queue number.
- **Scheduling**
  - – *Strict Priority* — Indicates that traffic scheduling for the selected queue is based strictly on the queue priority.
  - – *WRR* — Indicates that traffic scheduling for the selected queue is based strictly on the WRR.
  - – *WWR Weight* — If WRR is selected, indicates the predetemined weights 8, 2, 4, and 1 for queues 4,3,2 and 1.
  - – *% of WWR Bandwidth* — If WWR weight is selected, indicates the percentage

2. Define the fields.
3. Click Submit. The QoS queue settings are saved and the device is updated.

12.3 Mapping Queues

This section contains the following topics:

- Mapping CoS Values to Queues
- Mapping QoS Values to Queues

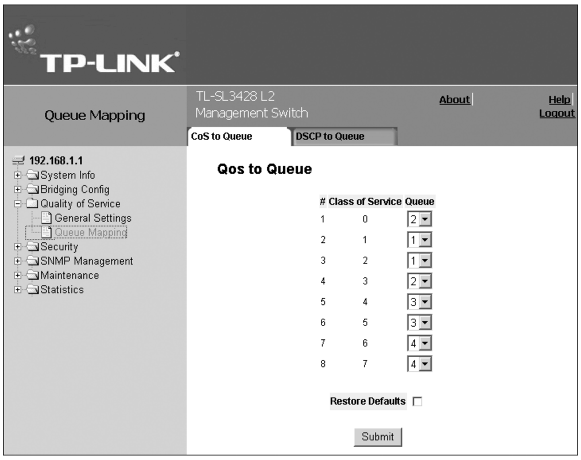
12.3.1 Mapping CoS Values to Queues

The *CoS to Queue Page* contains fields for classifying CoS settings to traffic queues.

To set CoS to Queue:

1. Click **System > Quality of Service > Queue Mapping > CoS to Queue**. The *CoS to Queue Page* opens:

Figure 121: CoS to Queue Page



Qos to Queue

#	Class of Service	Queue
1	0	2
2	1	1
3	2	1
4	3	2
5	4	3
6	5	3
7	6	4
8	7	4

Restore Defaults □

- **Class of Service** — Specifies the CoS priority tag values, where zero is the lowest and 8 is the highest.
- **Queue** — Defines the traffic forwarding queue to which the CoS priority is mapped. Four traffic priority queues are supported, where zero is the lowest and 8 is the highest.
- **Restore Defaults** — Allows you to restore default settings.

2. Modify the *Queue values or select Restore Defaults*.
3. Click Submit. The CoS to Queue mapping settings are saved and the device is updated.

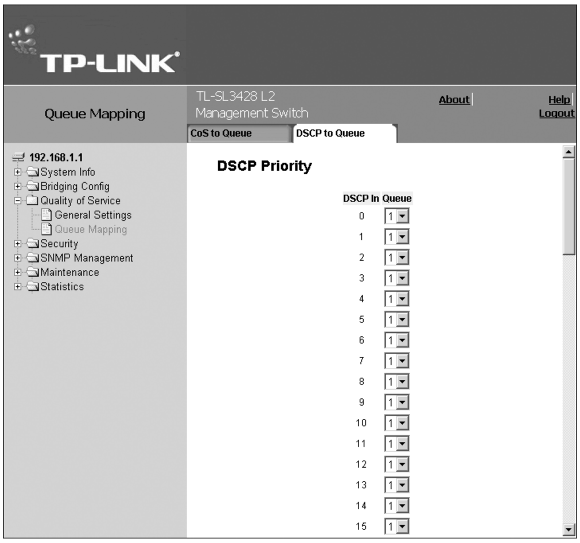
12.3.2 Mapping QoS Values to Queues

The *DSCP to Queue Page* contains fields for classifying DSCP settings to traffic queues. For example, a packet with a DSCP tag value of 3 can be assigned to queue 2.

To set DSCP to queues:

1. Click **System > Quality of Service > Queue Mapping > DSCP to Queue**. The *DSCP to Queue Page* opens:

Figure 122: DSCP to Queue Page



DSCP Priority

DSCP In	Queue
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1
9	1
10	1
11	1
12	1
13	1
14	1
15	1

The *CoS Settings Page* page contains the following fields:

- **DSCP In** — Displays the incoming packet's DSCP value.
- **Queue** — Defines the traffic forwarding queue to which the DSCP priority is mapped. Four traffic priority queues are supported.

2. Modify the Queue values.
3. Click Submit. The *DSCP to Queue* mapping is updated.

Section 13. Managing System Files

File maintenance on the device includes configuration file management and device access. The configuration file structure consists of the following configuration files:

- **Startup configuration file** — Contains the commands required to reconfigure the device to the same settings as when the device is powered down or rebooted. The Startup file is created by copying the configuration commands from the Running Configuration file or the Backup Configuration file.
- **Running configuration file** — Contains all configuration file commands, as well as all commands entered during the current session. After the device is powered down or rebooted, all commands stored in the Running Configuration file are lost. During the startup process, all commands in the Startup file are copied to the Running Configuration File and applied to the device. During the session, all new commands entered are added to the commands existing in the Running Configuration file. Commands are not overwritten. To update the Startup file, before powering down the device, the Running Configuration file must be copied to the Startup Configuration file. The next time the device is restarted, the commands are copied back into the Running Configuration file from the Startup Configuration file.
- **Image files** — Software upgrades are used when a new version file is downloaded. The file is checked for the right format, and that it is complete. After a successful download, the new version is marked, and is used after the device is reset.

This section contains the following topics:

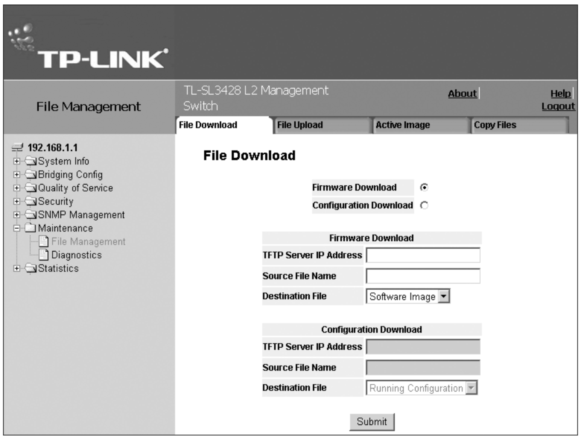
- Downloading System Files
- Uploading System Files
- Activating Image Files
- Copying System Files

13.1 Downloading System Files

To download system files:

1. **Click System > Maintenance > File Management > File Download**. The *File Download Page* opens:

Figure 123: File Download Page



File Download

Firmware Download ●
Configuration Download ○

Firmware Download	
TFTP Server IP Address	
Source File Name	
Destination File	Software Image

Configuration Download	
TFTP Server IP Address	
Source File Name	
Destination File	Running Configuration

The *File Download Page* is divided into the following sections:

- Download Type
- Firmware Download
- Configuration Download

13.1.1 Download Type

The *Upload Type* section contains the following fields:

- **Firmware Download** — Indicates that the download is for firmware. If *Firmware Download* is selected, the *Configuration Download* fields are grayed out.
- **Configuration Download** — Indicates that the download is for configuration files. If *Configuration Download* is selected, the *Firmware Download* fields are grayed out.

13.1.2 Firmware Download

The *Firmware Download* section contains the following fields:

- **TFTP Server IP Address** — Specifies the address of the TFTP server from which files are downloaded.
- **Source File Name** — Specifies the file to be downloaded.
- **Destination File** — Specifies the destination file to which system file is downloaded. The possible field values are:

  – *Software Image* — Downloads the Image file.

  – *Boot Code* — Downloads the Boot file.
- **Download to Master Only** — Downloads the system file only to the Master.
- **Download to All Units** — Downloads the system file to all units.

13.1.3 Configuration Download

The *Configuration Download* section contains the following fields:

- **TFTP Server IP Address** — Specifies the address of the TFTP server from which the configuration files are downloaded.
- **Source File Name** — Specifies the configuration files to be downloaded.
- **Destination File** — Specifies the destination file to which 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 the old Startup Configuration file.

2. Open the *File Download Page*.
3. Select the download type.
4. Define the TFTP server address.
5. Define the *Source File Name* and *Destination File* fields.
6. Click Submit. The requested files are downloaded to the specified destination.

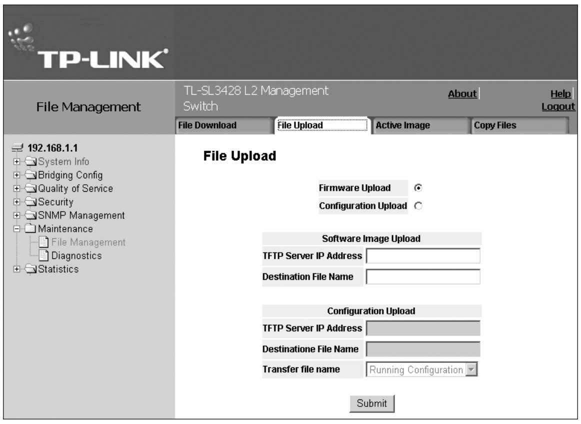
13.2 Uploading System Files

The *Copy Files Page* contains fields for uploading the software from the device to the TFTP server.

To upload system files:

1. Click **System > Maintenance > File Management > File Upload**. The *File Upload Page* opens:

Figure 124: File Upload Page



File Upload

Firmware Upload ●

Configuration Upload ○

Software Image Upload

TFTP Server IP Address

Destination File Name

Configuration Upload

TFTP Server IP Address

Destinatione File Name

Transfer file name: Running Configuration

The *File Upload Page* is divided into the following sections:

- Upload Type
- Software Image Upload
- Configuration Upload

13.2.1 Upload Type

The *Upload Type* section contains the following fields:

- **Firmware Upload** — Specifies that the software image file is uploaded. If *Firmware Upload* is selected, the Configuration Upload fields are grayed out.
- **Configuration Upload** — Specifies that the Configuration file is uploaded. If *Configuration Upload* is selected, the Software Image Upload fields are grayed out.

13.2.2 Software Image Upload

The *Software Image Upload* section contains the following fields:

- **TFTP Server IP Address** — Specifies the address of the TFTP server to which the Software Image is uploaded.
- **Destination File Name** — Specifies the name of the software image file to which the Software Image is uploaded.

13.2.3 Configuration Upload

The *Configuration Upload* section contains the following fields:

- **TFTP Server IP Address** — Specifies the address of the TFTP server to which the Configuration file is uploaded.
- **Destination File Name** — Specifies the name of the file to which the Startup Configuration file is uploaded.
- **Transfer File Name** — Specifies the name of the Configuration file that is uploaded.
  The possible field values are:
  – *Running Configuration* — Uploads the Running Configuration file.
  – *Startup Configuration* — Uploads the Startup Configuration file.

2. Open the *Copy Files Page*. See “Copying System Files” in section 13.4.
3. Define the file type to upload.
4. Define the fields.
5. Click Submit. The software is uploaded to the device.

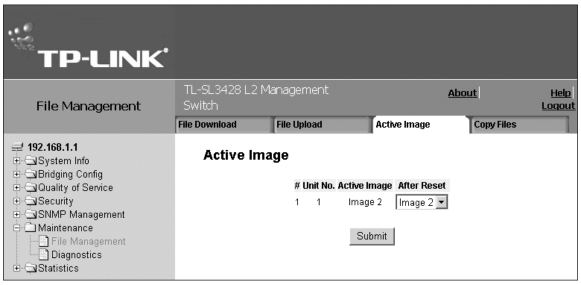
13.3 Activating Image Files

The *Active Image Page* allows network managers to select and reset the Image files.

To download system files:

1. Click **System > Maintenance > File Management > Active Image**. The *Active Image Page* opens:

Figure 125: Active Image Page



Active Image

#	Unit No.	Active Image	After Reset
1	1	Image 2	Image 2

The *Active Image Page* contains the following fields:

- **Unit No.** — The unit number for which the Image file is selected.
- **Active Image** — The Image file which is currently active on the unit.
- **After Reset** — The Image file which is active on the unit after the device is reset.
  The possible field values are:
  – *Image 1* — Activates Image file 1 after the device is reset.
  – *Image 2* — Activates Image file 2 after the device is reset.

2. Define the *After Reset* field.
3. Click Submit. The selected image file is activated after the device is reset.

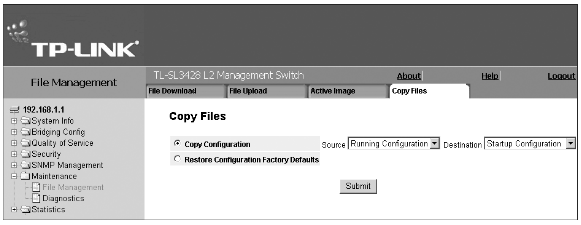
13.4 Copying System Files

Files can be copied and deleted using the *Copy Files Page*.

To copy system files:

1. Click **System > Maintenance > File Management > Copy Files**. The *Copy Files Page* opens:

Figure 126: Copy Files Page



Copy Files

● Copy Configuration Source: Running Configuration Destination: Startup Configuration

○ Restore Configuration Factory Defaults

The *Copy Files Page* contains the following fields:

- **Copy Configuration** — Copies the Running Configuration file to the Startup Configuration file.
- **Source** — Indicates the Running Configuration file is selected.
- **Destination** — Indicates the Startup Configuration file is selected.
- Restore Configuration Factory Defaults — Resets the Configuration file to the factory defaults. The factory defaults are reset after the device is reset. When unselected, the device maintains the current Configuration file.

2. Select *Copy Configuration*.
3. Click Submit. The file is copied.

To restore the default configuration:

1. Click **System > File Management > Copy Files**. The *Copy Files Page* opens.
2. Select *Restore Configuration Factory Defaults*.
3. Click Submit. The factory defaults are restored, and the device is updated.

Section 14. Performing Device Diagnostics

This section contains the following topics:

- Configuring Port Mirroring
- Viewing Integrated Cable Tests
- Viewing Optical Transceivers

14.1 Configuring Port Mirroring

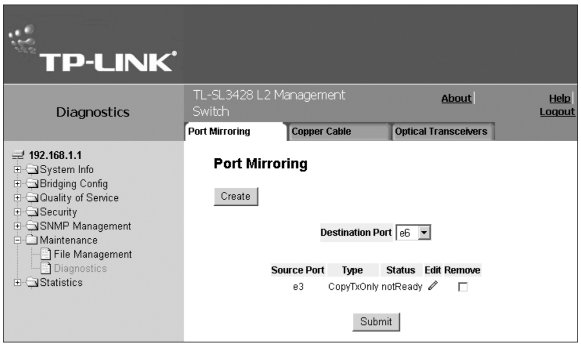
Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port. Port mirroring can be used as a diagnostic tool as well as a debugging feature. Port mirroring also enables switch performance monitoring.

Network administrators can configure port mirroring by selecting a specific port from which to copy all packets, and other ports to which the packets copied.

To perform port mirroring diagnostics:

1. Click **System > Maintenance > Diagnostics > Port Mirroring**. The *Port Mirroring Page* opens:

Figure 127: Port Mirroring Page



Port Mirroring

Destination Port: e6

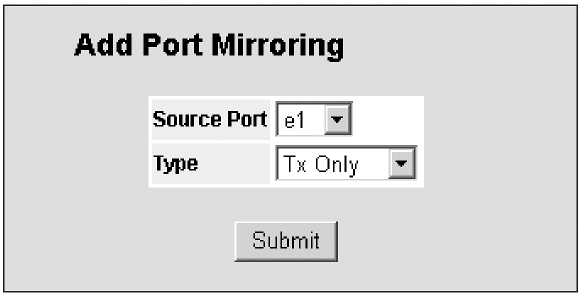
Source Port	Type	Status	Edit	Remove
e3	CopyTxOnly	notReady	✎	□

The Port Mirroring Page contains the following fields:

- **Destination Port** — Defines the port number to which port traffic is copied.
- **Transmit Packets** — Defines the how the packets are mirrored. The possible field values are:
  – *Untagged* — Mirrors packets as untagged VLAN packets. This is the default value.
  – *Tagged* — Mirrors packets as tagged VLAN packets.
- **Source Port** — Indicates the port from which the packets are mirrored.
- **Type** — Indicates the port mode configuration for port mirroring. The possible field values are:
  – *RX* — Defines the port mirroring on receiving ports.
  – *TX* — Defines the port mirroring on transmitting ports.
  – *Both* — Defines the port mirroring on both receiving and transmitting ports. This is the default value.
- **Remove** — Removes the port mirroring session. The possible field values are:
  – *Checked* — Removes the selected port mirroring sessions.
  – *Unchecked* — Maintains the port mirroring session.

2. Click Create. The Add Port Mirroring Page opens:

Figure 128: Add Port Mirroring Page



Add Port Mirroring

Source Port: e1

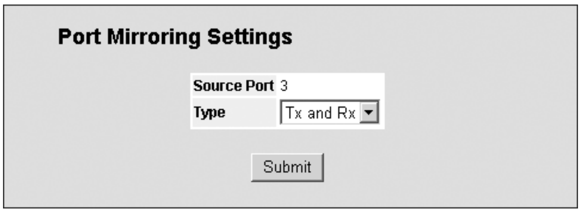
Type: Tx Only

3. Select a port in the Source Port field.
4. Select a port type in the Type field.
5. Click Submit. The port mirroring session is defined, and the device is updated.

To modify port mirroring settings:

1. Click ✎ . The *Port Mirroring Settings Page* opens.

Figure 129: Port Mirroring Settings Page



Port Mirroring Settings

Source Port	3
Type	Tx and Rx

2. Modify the *Type* field.
3. Click Submit. Port mirroring settings are modified, and the device is updated.

To remove port mirroring:

1. Click **Maintenance > Diagnostics > Port Mirroring**. The *Port Mirroring Page* opens.
2. Click the Remove checkbox for selected item, and click Submit.

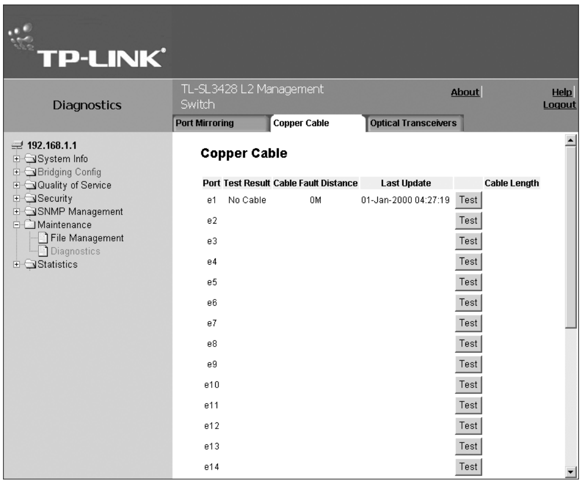
14.2 Viewing Integrated Cable Tests

The *Copper Cable 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 view cable test results:

- Click **System > Maintenance > Diagnostics > Copper Cable**. The *Copper Cable Page* opens:

Figure 130: Copper Cable Page



Copper Cable

Port	Test Result	Cable Fault Distance	Last Update		Cable Length
e1	No Cable	0M	01-Jan-2000 04:27:19	Test	
e2				Test	
e3				Test	
e4				Test	
e5				Test	
e6				Test	
e7				Test	
e8				Test	
e9				Test	
e10				Test	
e11				Test	
e12				Test	
e13				Test	
e14				Test	

The *Copper Cable Page* contains the following fields:

- **Port** — Specifies the port to which the cable is connected.
- **Test Result** — Displays the cable test results. Possible values are:
  – *No Cable* — Indicates that a cable is not connected to the port.
  – *Open Cable* — Indicates that a cable is connected on only one side.
  – *Short Cable* — Indicates that a short has occurred in the cable.
  – *OK* — Indicates that the cable passed the test.
- **Cable Fault Distance** — Indicates the distance from the port where the cable error occurred.
- **Last Update** — Indicates the last time the port was tested.
- **Cable Length** — Indicates the approximate cable length. This test can only be performed when the port is up and operating at 1 Gbps.

To perform a test:

1. Click ✎ . The test parameters are displayed in the *Copper Cable Test Page*:

14.3 Viewing Optical Transceivers

The *Optical Transceivers Page* allows network managers to perform tests on fiber-optic cables.

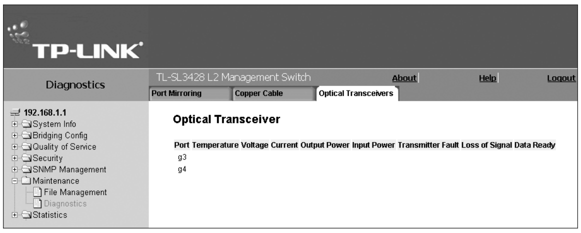
Note:

Optical transceiver diagnostics can be performed only when the link is present.

To test cables:

- Click **System > Maintenance > Diagnostics > Optical Transceivers**. The *Optical Transceivers Page* opens:

Figure 131: Optical Transceivers Page



Optical Transceiver

Port	Temperature	Voltage	Current	Output Power	Input Power	Transmitter Fault	Loss of Signal	Data Ready
g3								
g4								

The *Optical Transceivers Page* contains the following fields:

- **Port** — Displays the port IP address on which the cable is tested.
- **Temperature** — Displays the temperature (°C) at which the cable is operating.
- **Voltage** — Displays the voltage at which the cable is operating.
- **Current** — Displays the current at which the cable is operating.
- **Output Power** — Indicates the rate at which the output power is transmitted.
- **Input Power** — Indicates the rate at which the input power is transmitted.
- **Transmitter Fault** — Indicates if a fault occurred during transmission.
- **Loss of Signal** — Indicates if a signal loss occurred in the cable.
- **Data Ready** — Indicates the transceiver has achieved power up and data is ready.

Section 15. Viewing Statistics

This section describes how to view and manage device statistics for interfaces, GVRP, EAP, and Etherlike and how to view and define as RMON statistics, history and alarms.

This section contains the following topics:

- Viewing Interface Statistics
- Managing RMON Statistics

15.1 Viewing Interface Statistics

This section contains the following topics:

- Viewing Device Interface Statistics
- Viewing Etherlike Statistics
- Viewing GVRP Statistics
- Viewing EAP Statistics

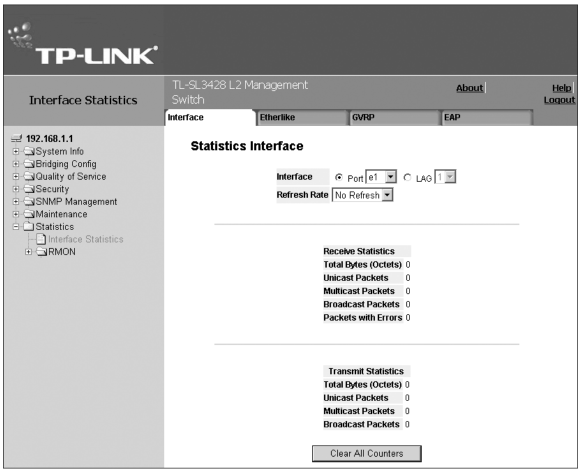
15.1.1 Viewing Device Interface Statistics

The *Interface Statistics Page* contains statistics for both received and transmitted packets.

To view interface statistics:

1. Click **System > Statistics > Interface Statistics**. The *Interface Statistics Page* opens:

Figure 132: Interface Statistics Page



Statistics Interface

Interface ● Port e1 ○ 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

The *Interface Statistics Page* contains the following fields:

- **Interface** — Indicates the device for which statistics are displayed. The possible field values are:
  – *Port* — Defines the specific port for which interface statistics are displayed.
  – *LAG* — Defines the specific LAG for which interface statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the interface statistics are refreshed.
  The possible field values are:
  – *15 Sec* —Indicates that the Interface statistics are refreshed every 15 seconds.
  – *30 Sec* —Indicates that the Interface statistics are refreshed every 30 seconds.
  – *60 Sec* —Indicates that the Interface statistics are refreshed every 60 seconds.
  – *No Refresh* —Indicates that the Interface statistics are not refreshed.

Receive Statistics

- **Total Bytes (Octets)** — Displays the number of octets received on the selected interface.
- **Unicast Packets** — Displays the number of Unicast packets received on the selected interface.
- **Multicast Packets** — Displays the number of Multicast packets received on the selected interface.
- **Broadcast Packets** — Displays the number of Broadcast packets received on the selected interface.

- **Packets with Errors** — Displays the number of error packets received from the selected interface.

Transmit Statistics

- **Total Bytes (Octets)** — Displays the number of octets transmitted from the selected interface.
- **Unicast Packets** — Displays the number of Unicast packets transmitted from the selected interface.
- **Multicast Packets** — Displays the number of Multicast packets transmitted from the selected interface.
- **Broadcast Packets** — Displays the number of Broadcast packets transmitted from the selected interface.

2. Select an interface in the *Interface* field. The interface statistics are displayed.

To reset interface statistics counters:

1. Open the *Interface Statistics Page*.
2. Click Clear All Counters. The interface statistics counters are cleared.

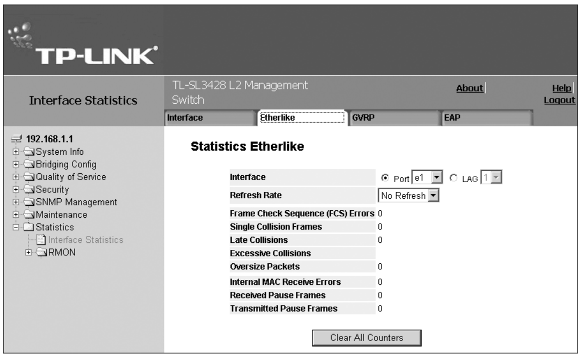
15.1.2 Viewing Etherlike Statistics

The *Etherlike Statistics Page* contains interface statistics.

To view Etherlike interface statistics:

1. Click **System > Statistics > Interface Statistics > Etherlike**. The *Etherlike Statistics Page* opens:

Figure 133: Etherlike Statistics Page



Statistics Etherlike

Interface	● Port e1 ○ LAG 1
Refresh Rate	No Refresh
Frame Check Sequence (FCS) Errors	0
Single Collision Frames	0
Late Collisions	0
Excessive Collisions	
Oversize Packets	0
Internal MAC Receive Errors	0
Received Pause Frames	0
Transmitted Pause Frames	0

The *Etherlike Statistics Page* contains the following fields:

- **Interface** — Indicates the device for which statistics are displayed. The possible field values are:
  - – *Port* — Defines the specific port for which Etherlike statistics are displayed.
  - – *LAG* — Defines the specific LAG for which Etherlike statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the interface statistics are refreshed. The possible field values are:
  - – *15 Sec* — Indicates that the Etherlike statistics are refreshed every 15 seconds.
  - – *30 Sec* — Indicates that the Etherlike statistics are refreshed every 30 seconds.
  - – *60 Sec* — Indicates that the Etherlike statistics are refreshed every 60 seconds.
  - – *No Refresh* — Indicates that the Etherlike statistics are not refreshed.
- **Frame Check Sequence (FCS) Errors** — Displays the number of FCS errors received on the selected interface.
- **Single Collision Frames** — Displays the number of single collision frames received on the selected interface.
- **Late Collisions** — Displays the number of late collision frames received on the selected interface.
- **Excessive Collisions** — Displays the number of excessive collisions received on the selected interface.
- **Internal MAC Transmit Errors** — Displays the number of internal MAC transmit errors on the selected interface.
- **Oversize Packets** — Displays the number of oversized packet errors on the selected interface.
- **Internal MAC Receive Errors** — Number of internal MAC received errors on the selected interface.
- **Received Pause Frames** — Displays the number of received paused frames on the selected interface.
- **Transmitted Paused Frames** — Displays the number of paused frames transmitted from the selected interface.

2. Select an interface (Port or LAG) in the *Interface* field. The Etherlike statistics are displayed.

To update the refresh time:

- To change the refresh rate for statistics, select another rate from the Refresh Rate dropdown list.

To reset Etherlike interface statistics counters:

1. Open the *Etherlike Statistics Page*.
2. Click Clear All Counters. The Etherlike interface statistics counters are cleared.

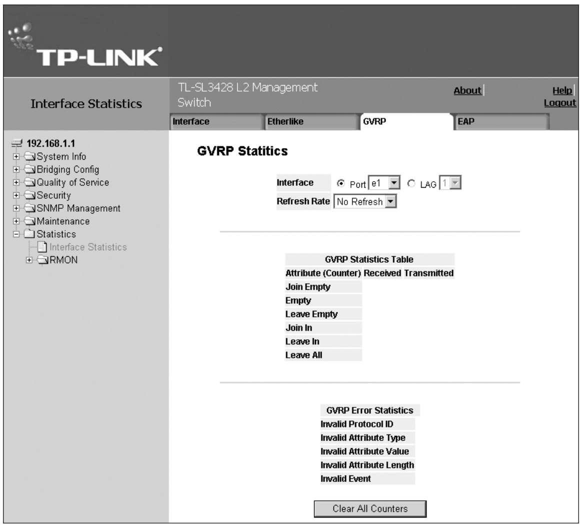
15.1.3 Viewing GVRP Statistics

The GVRP Statistics Page contains device statistics for GVRP.

To view GVRP interface statistics:

1. Click **System > Statistics > Interface Statistics > GVRP**. The *GVRP Statistics Page* opens:

Figure 134: GVRP Statistics Page



GVRP Statitics

Interface ● Port e1 ○ 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
Invalid Attribute Length
Invalid Event

The *GVRP Statistics Page* contains the following fields:

- **Interface** — Specifies the interface type for which the statistics are displayed.
  – *Port* — Indicates port statistics are displayed.
  – *LAG* — Indicates LAG statistics are displayed.
- **Refresh Rate** — Indicates the amount of time that passes before the GVRP statistics are refreshed. The possible field values are:
  – *15 Sec* — Indicates that the GVRP statistics are refreshed every 15 seconds.
  – *30 Sec* — Indicates that the GVRP statistics are refreshed every 30 seconds.
  – *60 Sec* — Indicates that the GVRP statistics are refreshed every 60 seconds.
  – *No Refresh* — Indicates that the GVRP statistics are not refreshed.
- **Join Empty** — Displays the device GVRP Join Empty statistics.
- **Empty** — Displays the device GVRP Empty statistics.
- **Leave Empty** — Displays the device GVRP Leave Empty statistics.
- **Join In** — Displays the device GVRP Join In statistics.
- **Leave In** — Displays the device GVRP Leave in statistics.
- **Leave All** — Displays the device GVRP Leave all statistics.
- **Invalid Protocol ID** — Displays the device GVRP Invalid Protocol ID statistics.
- **Invalid Attribute Type** — Displays the device GVRP Invalid Attribute ID statistics.
- **Invalid Attribute Value** — Displays the device GVRP Invalid Attribute Value statistics.
- **Invalid Attribute Length** — Displays the device GVRP Invalid Attribute Length statistics.
- **Invalid Event** — Displays the device GVRP Invalid Event statistics.

2. Select an interface (Port or LAG) in the *Interface* field. The GVRP statistics are displayed.

To update the refresh time:

- To change the refresh rate for statistics, select another rate from the *Refresh Rate* dropdown list.

To reset GVRP interface statistics counters:

1. Open the *GVRP Statistics Page*.
2. Click Clear All Counters. The GVRP interface statistics counters are cleared.

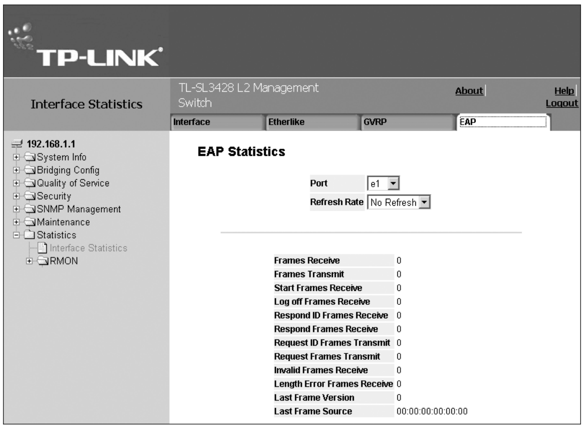
15.1.4 Viewing EAP Statistics

The *EAP Statistics Page* contains information about EAP packets received on a specific port.

To view the EAP Statistics:

1. Click **System > Statistics > Interface Statistics > EAP**. The *EAP Statistics Page* opens:

Figure 135: EAP Statistics Page



EAP Statistics

Port: e1
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

The *EAP Statistics Page* contains the following fields:

- **Port** — Indicates the port, which is polled for statistics.
- **Refresh Rate** — Indicates the amount of time that passes before the EAP statistics are refreshed. The possible field values are:
  - – *15 Sec* — Indicates that the EAP statistics are refreshed every 15 seconds.
  - – *30 Sec* — Indicates that the EAP statistics are refreshed every 30 seconds.
  - – *60 Sec* — Indicates that the EAP statistics are refreshed every 60 seconds.
  - – *No Refresh* — Indicates that the EAP statistics are not refreshed.
- **Frames Receive** — Indicates the number of valid EAPOL frames received on the port.
- **Frames Transmit** — Indicates the number of EAPOL frames transmitted via the port.
- **Start Frames Receive** — Indicates the number of EAPOL Start frames received on the port.
- **Log off Frames Receive** — Indicates the number of EAPOL Logoff frames that have been received on the port.
- **Respond ID Frames Receive** — Indicates the number of EAP Resp/Id frames that have been received on the port.
- **Respond Frames Receive** — Indicates the number of valid EAP Response frames received on the port.
- **Request ID Frames Transmit** — Indicates the number of EAP Req/Id frames transmitted via the port.
- **Request Frames Transmit** — Indicates the number of EAP Request frames transmitted via the port.
- **Invalid Frames Receive** — Indicates the number of unrecognized EAPOL frames that have been received by on this port.
- **Length Error Frames Receive** — Indicates the number of EAPOL frames with an invalid Packet Body Length received on this port.
- **Last Frame Version** — Indicates the protocol version number attached to the most recently received EAPOL frame.
- **Last Frame Source** — Indicates the source MAC address attached to the most recently received EAPOL frame.

2. Select a port from the *Port* dropdown list. The port statistics are displayed.

To update the refresh time:

- To change the refresh rate for statistics, select another rate from the *Refresh Rate* dropdown list.

15.2 Managing RMON Statistics

This section describes how to view and manage *Remote Monitoring On Network* (RMON) statistics, history and alarms.

This section contains the following topics:

- Viewing RMON Statistics

- Configuring RMON History
- Defining RMON Alarms

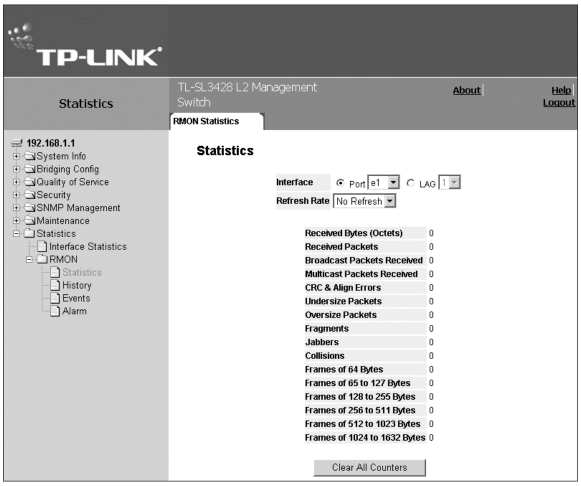
15.2.1 Viewing RMON Statistics

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

To view RMON statistics:

1. Click **System > Statistics > RMON > Statistics**. The *RMON Statistics Page* opens:

Figure 136: RMON Statistics Page



Statistics

Interface ● Port e1 ○ LAG 1

Refresh Rate No Refresh

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
Jabbers	0
Collisions	0
Frames of 64 Bytes	0
Frames of 65 to 127 Bytes	0
Frames of 128 to 255 Bytes	0
Frames of 256 to 511 Bytes	0
Frames of 512 to 1023 Bytes	0
Frames of 1024 to 1632 Bytes	0

The *RMON Statistics Page* contains the following fields:

- **Interface** — Indicates the device for which statistics are displayed. The possible field values are:
  - *– Port* — Defines the specific port for which RMON statistics are displayed.
  - *– LAG* — Defines the specific LAG for which RMON statistics are displayed.
- **Refresh Rate** — Defines the amount of time that passes before the interface statistics are refreshed.
  The possible field values are:
  - *– 15 Sec* — Indicates that the RMON statistics are refreshed every 15 seconds.
  - *– 30 Sec* — Indicates that the RMON statistics are refreshed every 30 seconds.
  - *– 60 Sec* — Indicates that the RMON statistics are refreshed every 60 seconds.
- **Received Bytes (Octets)** — Displays the 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** — Displays the number of packets received on the interface, including bad packets, Multicast and broadcast packets, since the device was last refreshed.
- **Broadcast Packets Received** — Displays the 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** — Displays the number of good Multicast packets received on the interface since the device was last refreshed.
- **CRC & Align Errors** — Displays the number of CRC and Align errors that have occurred on the interface since the device was last refreshed.
- **Undersize Packets** — Displays the number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.
- **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.
- **Fragments** — Displays the 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** — Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.
- **Collisions** — Displays the number of collisions received on the interface since the device was last refreshed.

- **Frames of xx Bytes** — Number of xx-byte frames received on the interface since the device was last refreshed.

2. Select an interface (*Port or LAG*) in the *Interface* field. The RMON statistics are displayed.

To update the refresh time:

- To change the refresh rate for statistics, select another rate from the *Refresh Rate* dropdown list.

To reset RMON statistics counters:

1. Open the *RMON Statistics Page*.
2. Click Clear All Counters. The RMON statistics counters are cleared.

15.2.2 Configuring RMON History

This section contains the following topics:

- Defining RMON History Control
- Viewing the RMON History Table

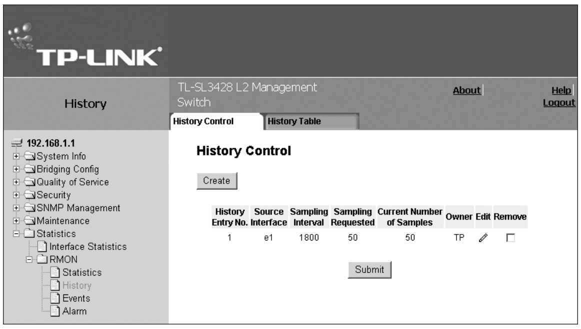
15.2.2.1 Defining RMON History Control

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 set RMON history control:

1. Click **System > Statistics > RMON > History**. The *RMON History Control Page* opens:

Figure 137: RMON History Control Page



History Control

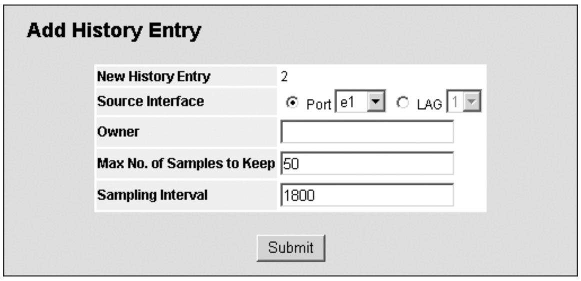
History Entry No.	Source Interface	Sampling Interval	Sampling Requested	Current Number of Samples	Owner	Edit	Remove
1	e1	1800	50	50	TP	✎	□

The *RMON History Control Page* contains the following fields:

- **History Entry No.** — Displays the entry number for the History Control Table page.
- **Source Interface** — Displays the interface from which the history samples were taken. The possible field values are:
  – *Port* — Specifies the port from which the RMON information was taken.
  – *LAG* — Specifies the port from which the RMON information was taken.
- **Sampling Interval** — Indicates in seconds the time that samplings are taken from the ports. The field range is 1-3600. The default is 1800 seconds (equal to 30 minutes).
- **Samples Requested** — Displays the number of samples to be saved. The field range is 1-65535. The default value is 50.
- **Current Number of Samples in List** — Displays the current number of samples taken.
- **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
- **Remove** — Removes History Control entries. The possible field values are:
  – *Checked* — Removes the selected History Control entry.
  – *Unchecked* — Maintains the current History Control entries.

2. Click Create. The *Add History Entry User Page* opens:

Figure 138: Add History Entry User Page



Add History Entry

New History Entry	2
Source Interface	● Port e1 ○ LAG 1
Owner	
Max No. of Samples to Keep	50
Sampling Interval	1800

3. Define the fields.

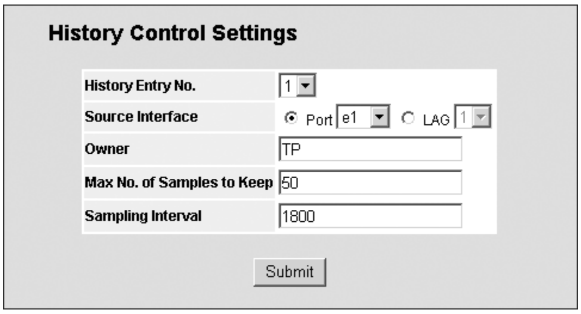
4. Click Submit. The entry is added to the *RMON History Control Page*, and the device is updated.

To modify a history entry user:

1. Open the *RMON History Control Page*.

2. Click . The *Edit Local History Entry User Page* opens:

Figure 139: Edit Local History Entry User Page



History Control Settings

History Entry No.	1
Source Interface	● Port e1 ○ LAG 1
Owner	TP
Max No. of Samples to Keep	50
Sampling Interval	1800

3. Define the fields.

4. Click Submit.The entry is updated in the *RMON History Control Page*, and the device is updated.

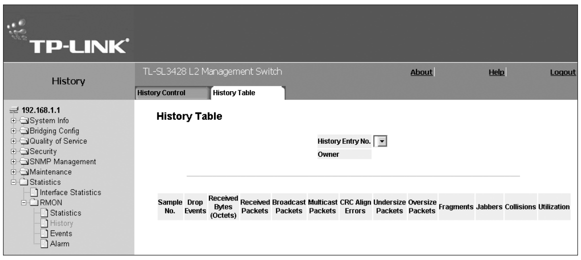
15.2.2.2 Viewing the RMON History Table

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

To view the RMON History Table:

1. Click **System > Statistics > RMON > History > History Table**. The *RMON History Table Page* opens:

Figure 140: RMON History Table Page



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	Fragments	Jabbers	Collisions	Utilization

The *RMON History Table Page* contains the following fields:

- **History Entry No.** — Displays the entry number for the History Control Table page.
- **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.
- **Sample No.** — Indicates the sample number from which the statistics were taken.
- **Drop Events** — Displays the number of dropped events that have occurred on the interface since the device was last refreshed.
- **Received Bytes (Octets)** — Displays the 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** — Displays the number of packets received on the interface since the device was last refreshed, including bad packets, Multicast and Broadcast packets.
- **Broadcast Packets** — Displays the number of good Broadcast packets received on the interface since the device was last refreshed. This number does not include Multicast packets.
- **Multicast Packets** — Displays the number of good Multicast packets received on the interface since the device was last refreshed.
- **CRC Align Errors** — Displays the number of CRC and Align errors that have occurred on the interface since the device was last refreshed.
- **Undersize Packets** — Displays the number of undersized packets (less than 64 octets) received on the interface since

the device was last refreshed.

- **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.
- **Fragments** — Displays the 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** — Displays the total number of received packets that were longer than 1518 octets. This number excludes frame bits, but includes FCS octets that had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number. The field range to detect jabbers is between 20 ms and 150 ms.
- **Collisions** — Displays the number of collisions received on the interface since the device was last refreshed.
- **Utilization** — Displays the percentage of the interface utilized.

2. Select an entry in the *History Entry No.* field.
3. Click Submit. The statistics are displayed.

15.2.3 Configuring RMON Events

This section includes the following topics:

- Defining RMON Events Control
- Viewing the RMON Events Logs

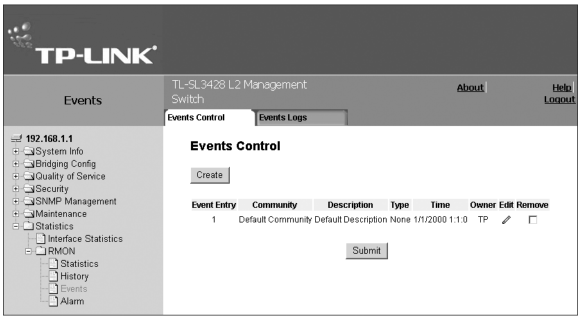
15.2.3.1 Defining RMON Events Control

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

To set RMON events:

1. Click **System > Statistics > RMON > Events**. The *RMON Events Control Page* opens:

Figure 141: RMON Events Control Page



Events Control

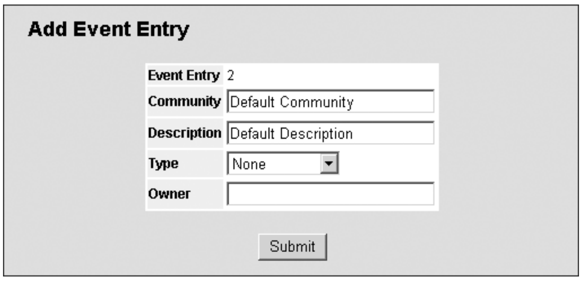
Event Entry	Community	Description	Type	Time	Owner	Edit	Remove
1	Default Community	Default Description	None	1/1/2000 1:1:0	TP	✎	□

The *RMON Events Control Page* contains the following fields:

- **Event Entry** — Displays the event.
- **Community** — Displays the community to which the event belongs.
- **Description** — Displays the user-defined event description.
- **Type** — Describes the event type. Possible values are:
  – *Log* — Indicates that the event is a log entry.
  – *Trap* — Indicates that the event is a trap.
  – *Log and Trap* — Indicates that the event is both a log entry and a trap.
  – *None* — Indicates that no event occurred.
- **Time** — Displays the time that the event occurred.
- **Owner** — Displays the device or user that defined the event.
- **Remove** — Removes a RMON event. The possible field values are:
  – *Checked* — Removes a selected RMON event.
  – *Unchecked* — Maintains RMON events.

2. Click Create. The *Add RMON Event User Page* opens:

Figure 142: Add RMON Event User Page



Add Event Entry

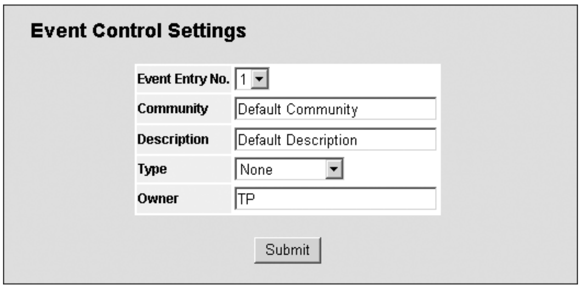
Event Entry	2
Community	Default Community
Description	Default Description
Type	None
Owner	

3. Define the fields.
4. Click Submit. The entry is added to the *RMON Events Control Page*, and the device is updated.

To modify an RMON Event user:

1. Click **System > Statistics > RMON > Events**. The *RMON Events Control Page* opens, displaying defined event entries.
2. Click ✎ next to an entry. The *Edit RMON Event User Page* opens:

Figure 143: Edit RMON Event User Page



Event Control Settings

Event Entry No.	1
Community	Default Community
Description	Default Description
Type	None
Owner	TP

3. Modify the local user properties fields.
4. Click Submit. The entry is updated in the *RMON Events Control Page*, and the device is updated.

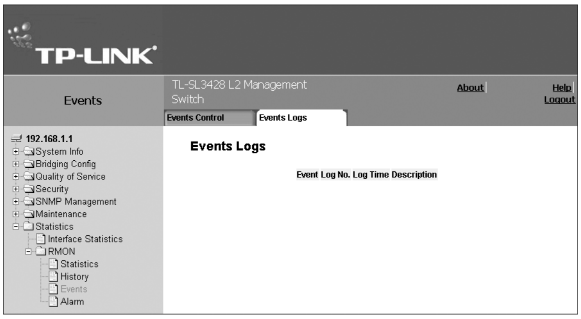
15.2.3.2 Viewing the RMON Events Logs

The *RMON Events Logs Page* contains a list of RMON events.

To view RMON event logs:

1. Click **System > Statistics > RMON > Events**. The *RMON Events Logs Page* opens:

Figure 144: RMON Events Logs Page



Events Logs

Event	Log No.	Log Time	Description

The *RMON Events Logs Page* contains the following fields:

- **Event** — Displays the RMON Events Log entry number.
- **Log No.** — Displays the log number.
- **Log Time** — Displays the time when the log entry was entered.
- **Description** — Displays the log entry description.

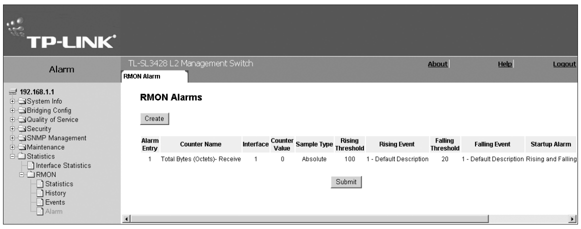
15.2.4 Defining RMON Alarms

The *RMON Alarm Page* contains fields for setting network alarms. Network alarms occur when a network problem, or event, is detected. Rising and falling thresholds trigger alarms.

To set RMON alarms:

1. Click **System > Statistics > RMON > Alarm**. The *RMON Alarm Page* opens:

Figure 145: RMON Alarm Page



RMON Alarms

Alarm Entry	Counter Name	Interface	Counter Value	Sample Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event	Startup Alarm
1	Total Bytes (Octets)- Receive	1	0	Absolute	100	1 - Default Description	20	1 - Default Description	Rising and Falling

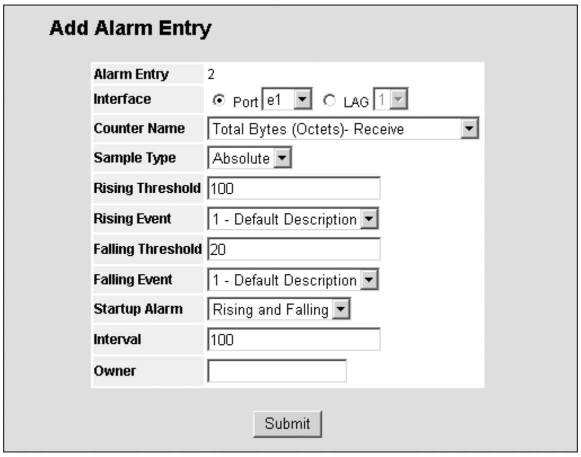
The *RMON Alarm Page* contains the following fields:

- **Alarm Entry** — Indicates a specific alarm.
- **Counter Name** — Displays the selected MIB variable.

- **Interface** — Displays interface for which RMON statistics are displayed. The possible field values are:
  - *Port* — Displays the RMON statistics for the selected port.
  - *LAG* — Displays the RMON statistics for the selected LAG.
- **Counter Value** — Displays the selected MIB variable value.
- **Sample Type** — Defines 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** — Displays 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 Event** — Displays the mechanism in which the alarms are reported. The possible field values are:
  - *LOG* — Indicates there is not a saving mechanism for either the device or in the management system. If the device is not reset, the entry remains in the Log Table.
  - *TRAP* — Indicates that an SNMP trap is generated, and sent via the Trap mechanism. The Trap can also be saved using the Trap mechanism.
  - *Both* — Indicates that both the Log and Trap mechanism are used to report alarms.
- **Falling Threshold** — Displays the falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on top of the graph bars. Each monitored variable is designated a color.
- **Falling Event** — Displays the mechanism in which the alarms are reported.
- **Startup Alarm** — Displays 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** — Defines the alarm interval time in seconds.
- **Owner** — Displays the device or user that defined the alarm.
- **Remove** — Removes the RMON Alarms Table entry.

2. Click Create. The *Add RMON Alarm User Page* opens:

Figure 146: Add RMON Alarm User Page



Add Alarm Entry

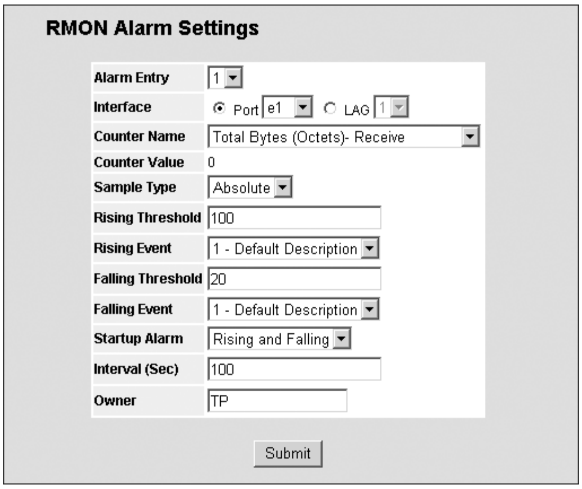
Alarm Entry	2
Interface	● Port e1 ○ LAG 1
Counter Name	Total Bytes (Octets)- Receive
Sample Type	Absolute
Rising Threshold	100
Rising Event	1 - Default Description
Falling Threshold	20
Falling Event	1 - Default Description
Startup Alarm	Rising and Falling
Interval	100
Owner	

3. Define the fields.
4. Click Submit. The RMON alarm user is added to the list in *RMON Alarm Page*, and the device is updated.

To modify an RMON alarm user:

1. Click ✎ . The *Edit RMON Alarm User Page* opens.

Figure 147: Edit RMON Alarm User Page



RMON Alarm Settings

Alarm Entry	1
Interface	● Port e1 ○ LAG 1
Counter Name	Total Bytes (Octets)- Receive
Counter Value	0
Sample Type	Absolute
Rising Threshold	100
Rising Event	1 - Default Description
Falling Threshold	20
Falling Event	1 - Default Description
Startup Alarm	Rising and Falling
Interval (Sec)	100
Owner	TP

2. Modify the fields.
3. Click Submit. The entry is updated in the *RMON Alarm Page*, and the device is updated.

Glossary

This glossary contains terms commonly used in Embedded Web System documentation.

Term	Definition
A	
Access Mode	Specifies the method by which user access is granted to the system.
Access Profile	Allows network managers to define profiles and rules for accessing the device. Access to management functions can be limited to user groups, which are defined by the following criteria: • Ingress interfaces. • Source IP address and/or Source IP subnets.
ACE	Filters in Access Control Lists (ACL) that determine which network traffic is forwarded. ACE are based on the following criteria: • Protocol. • Protocol ID. • Source Port. • Destination Port. • Wildcard Mask. • Source IP Address. • Destination IP Address.
ACL	*Access Control List*. Access Control Lists are used to grant, deny, or limit access to devices, features, or applications.
Aggregated VLAN	Groups several VLANs into a single aggregated VLAN. Aggregating VLANs enables routers to respond to ARP requests for nodes located on different sub-VLANs belonging to the same Super VLAN. Routers respond with their MAC address.
AH	*Authentication Header Protocol*. Provides source host authentication and data integrity.
ARP	*Address Resolution Protocol*. A TCP/IP protocol that converts IP addresses into physical addresses.
ASIC	*Application Specific Integrated Circuit*. A custom chip designed for a specific application.
Asset Tag	Specifies the user-defined device reference.
Authentication Profile	Set of rules that enable login to and authentication of users and applications.
Auto-negotiation	Allows 10/100 Mpbs or 10/100/1000 Mbps Ethernet ports to establish for the following features: • Duplex/ Half Duplex Mode. • Flow Control. • Speed.
B	
Back Pressure	A mechanism used with Half Duplex mode that enables a port not to receive a message.
Backbone	The main segment of a network. Backbone types include: • Building. • Campus. • Metropolitan. • National Data. • Telecommunications.

Term	Definition
Backplane	The main BUS that carries information in the device.
Bandwidth	Specifies the amount of data that can be transmitted in a fixed amount of time. For digital devices, bandwidth is defined in Bits per Second (bps) or Bytes per Second.
Bandwidth Assignment	Indicates the amount of bandwidth assigned to a specific application, user, and/or interface.
Baud	Indicates the number of signaling elements transmitted each second.
Best Effort	Indicates that traffic is assigned to the lowest priority queue, and packet delivery is not guaranteed.
BGP	*Border Gateway Protocol*. Enables information sharing, routing information between groups of routers.
Boot Version	Indicates the boot version.
BootP	*Bootstrap Protocol*. Enables a workstation to discover its IP address, an IP address of a BootP server on a network, or a configuration file loaded into the boot of a device.
BPDU	*Bridge Protocol Data Unit*. Provide bridging information in a message format. BPDUs are sent across switch information with in Spanning Tree configuration. BPDU packets contain information on ports, addresses, priorities, and forwarding costs.
Bridge	A device that connects two networks. Bridges are hardware-specific, however they are protocol-independent. Bridges operate at Layer 1 and Layer 2 levels.
Broadcast Domain	Device sets that receive broadcast frames originating from any device within a designated set. Routers bind broadcast domains, because routers do not forward broadcast frames.
Broadcast Storm	An excessive amount of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses are heaped onto the network, overloading network resources or causing the network to time out.
Broadcasting	A method of transmitting packets to all ports on a network.
Burst	A packet transmission at faster than normal rates. Bursts are limited in time and only occur under specific conditions.
Burst Size	Indicates the burst size transmitted at a faster than normal rate.
C	
CBS	*Committed Burst Size*. Indicates the maximum number of data bits transmitted within a specific time interval.
CDB	*Configuration Data Base.* A file containing a device's configuration information.
CIDR	*Classless Interdomain Routing*. Based on route aggregation. Routers group routes together, and reduce the amount of routing information carried by the core routers. Several IP networks appear to networks outside the group as a single, larger entity.
CIR	*Committed Information Rate*. Indicates the rate (Bps) that data is transmitted using frame relay services (FRS). The rate is averaged over a minimum time increment.
Class Map	An aspect of Quality of Service system that is comprised of an IP ACL and/or a MAC ACL. Class maps are configured to match packet criteria, and are matched to packets in a first-fit fashion.
Class of Service	*Class of Service (CoS)*. The 802.1p priority scheme. CoS provides a method for tagging packets with priority information. A CoS value between 0-7 is added to the Layer II header of packets, where zero is the lowest priority and seven is the highest.
Classless Inter-Domain Routing	Creates new addresses on the internet. The new addresses are distributed to ISPs for their customers' use. CIDR reduces the Internet routers' burden by combining routes. One IP address represents thousands of addresses serviced by a major backbone provider.

Term	Definition
CLI	*Command Line Interface*. A set of line commands used to configure the system.
Client	A computer system or process that requires services or processes for another computer, typically a server.
CLL	*Classification Control Lists*. Devices that grant, deny, or limit access to devices, features, or applications in QoS.
Collision	A overlapping transmission of two or more packets that collide. The data transmitted cannot be used, and the session is restarted.
Combo Port	A single logical port with two physical connections, including an RJ-45 connection and a SFP connection.
Community	Specifies a group of users which retains the same system access rights.
CPU	*Central Processing Unit*. The part of a computer that processes information.CPUs are composed of a control unit and an ALU.
D	
Damp	Indicates a state where an interface is not advertising links to the neighboring interface due to Flapping.
DHCP	*Dynamic Host Configuration Protocol*. DHCP dynamically assigns IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. DHCP also supports a mix of static and dynamic IP addresses.
DHCP Client	An Internet host using DHCP to obtain configuration parameters, such as a network address.
DHCP Server	An Internet host that returns configuration parameters to DHCP clients.
Domain	A group of computers and devices on a network that are grouped with common rules and procedures.
DSCP	*DiffServe Code Point.* DSCP provides a method of tagging IP packets with QoS priority information.
DSL	*Digital Subscriber Line*. Increases the digital capacity of telephone lines.
Duplex Mode	Permits simultaneous transmissions and reception of data. There are two different types of duplex mode: • *Full Duplex Mode* — Permits bisynchronous communication, for example, a telephone. Two parties can transmit information at the same time. • *Half Duplex Mode* — Permits asynchronous communication, for example, a walkie-talkie. Only one party can transmit information at a time.
DVMRP	*Distance Vector Multicast Routing Protocol*. DVMRP tunnels multicast messages within unicast packets. DVMRP supports rate limiting and distribution control based on destination address.
E	
Egress Port	Port from which network traffic is transmitted.
EIGRP	*Enhanced Interior Gateway Routing Protocol*. Provides fast convergence, support for variable-length subnet mask, and supports multiple network layer protocols.
End System	An end user device on a network.
EPG	*Exterior Gateway Protocol*. Permits exchanging routing information between two neighboring gateway hosts in an autonomous systems network.
ESP	*Encapsulating Security Payload.* Provides a variety of security services for IPv4 and IPv6.

Term	Definition
Ethernet	Uses a bus or star topology and supports data transfer rates of Mpbs. A newer version called Fast Ethernet supports 100 Mbps. Ethernet is standardized as per IEEE 802.3. Ethernet is the most commonly implemented LAN standard.
EWS	*Embedded Web Server.* Provides device management via a standard web browser. Embedded Web Servers are used in addition to or in place of a CLI or NMS.
F	
FE	*Fast Ethernet*. Fast Ethernet transmits at 100 Mbps rather than 10 Mbps.
FFT	*Fast Forward Table*. Provides information about forwarding routes. If a packet arrives at a device with a known route, the packet is forwarded via a route listed in the FFT. If there is not a known route, the CPU forwards the packet and updates the FFT.
FIFO	*First In First Out*. A queuing process where the first packet in the queue is the first to be transmitted.
Flapping	Flapping occurs when an interface's state is constantly changing. For example, an STP port constantly changes from listening to learning to forwarding. This may cause detrimental traffic loss.
Flow Control	Enables lower speed devices to communicate with higher speed devices. This is implemented by the higher speed device refraining from sending packets.
Fragment	Ethernet packets smaller than 576 bits.
Frame	Packets containing the header and trailer information required by the physical medium.
FTP	*File Transfer Protocol.* Transfers files between network nodes.
G	
GARP	*General Attributes Registration Protocol*. Registers client stations into a multicast domain.
GBIC	*GigaBit Interface Converter*. A hardware module used to attach network devices to fiber-based transmission systems. GBIC converts the serial electrical signals to serial optical signals and vice versa.
Gigabit Ethernet	Gigabit Ethernet transmits at 1000 Mbps, and is compatible with existing 10/100 Ethernet standards.
GRE	*Generic Routing Encapsulation*. Enables tunneling using encapsulation with various protocol packet types. GRE creates a virtual point-to-point link to remote IP internetwork routers.
GVRP	*GARP VLAN Registration Protocol*. Registers client stations into a VLAN.
H	
HMP	*Host Monitoring Protocol*. Collects network information from various networks hosts. HMP monitors hosts spread over the internet as well as hosts in a single network.
HOL	*Head of Line*. Packets are queued. Packets at the head of the queue are forwarded before packets at the end.
Hop	The path between two network devices, for example, two routers.
Host	A computer that acts as a source of information or services to other computers.
Hot Swapping	Allows specific modules to be removed and/or replaced while the host device is running without reconfiguring the device.
HTTP	*HyperText Transport Protocol*. Transmits HTML documents between servers and clients on the internet.

Term	Definition
I	
IAD	*Integrated Access Device.* Device that multiplexes varied communication technologies onto a single telephone line for transmission to the carrier.
IC	*Integrated Circuit*. Small electronic devices composed from semiconductor material.
ICMP	*Internet Control Message Protocol*. Allows the gateway or destination host to communicate with the source host. For example, to report a processing error.
IDRP	*Inter-Domain Routing Protocol*. Specifies how routers communicate with different domain routers.
IEEE	*Institute of Electrical and Electronics Engineers*. An engineering organization that develops communications and networking standards.
IEEE 802.1d	Used in the Spanning Tree Protocol, IEEE 802.1d supports MAC bridging to avoid network loops.
IEEE 802.1p	Prioritizes network traffic at the data-link/MAC sub-layer.
EEE 802.1q	Defines the operation of VLAN Bridges that permit the definition, operation, and administration of VLANs within Bridged LAN infrastructures.
IGMP	*Internet Group Management Protocol*. Allows hosts to notify their local switch or router that they want to receive transmissions assigned to a specific multicast group.
IGP	*Interior Gateway Protocol*. Allows for routing information exchange between gateways in an autonomous network.
Image File	System images are saved in two Flash sectors called images image 1 and image 2). The active image stores the active copy; while the other image stores a second copy.
Ingress Port	Ports on which network traffic is received.
IP	*Internet Protocol*. Specifies the format of packets and their addressing method.IP addresses packets and forwards the packets to the correct port.
IP Address	*Internet Protocol Address*. A unique address assigned to a network device with two or more interconnected LANs or WANs.
IPM	*IP Multicast*. Transmits multicast packets in a network. Multicast routing copies one packet to several ports.
TPv6	*IP Version 6*. Provides a newer version of the Internet Protocol, and follows IP version 4 (IPv4). IPv6 increases the IP address size from 32 bits to 128 bits. In addition, IPv6 support more levels of addressing hierarchy, more addressable nodes, and supports simpler auto-configuration of addresses.
IPX	*Internetwork Packet Exchange*. Transmits connectionless communications.
ISIS	*Intermediate System to Intermediate System*. Provides Link State PDUs (LSPs) authentication by including authentication information as part of the LSP.
J	
Jumbo Frames	Enable transporting identical data in fewer frames. Jumbo Frames reduce overhead, lower the processing time, and ensure fewer interruptions.
K	
Key Chain	Group of MD5 keys assigned to an interface. Key chains are assigned to interfaces in the RIP or OSPF interface parameters.
L	

Term	Definition
L2TP	*Layer 2 Tunnel Protocol*. Helps build virtual private networks in the dial access space, and provides *Layer 2 Forwarding* L2F) protocol and *Point-to-Point Tunneling Protocol* (PPTP).
LAG	*Link Aggregated Group*. Aggregates ports or VLANs into a single virtual port or VLAN.
LAN	*Local Area Network*. A network contained within a single room, building, campus or other limited geographical area.
Layer 2	*Data Link Layer or MAC Layer*. Contains the physical address of a client or server station. Layer 2 processing is faster than Layer 3 processing because there is less information to process.
Layer 3	*Network Layer*. Contains the logical address and protocol type (IP, IPX, etc.). Layer 3 traffic can also be prioritized and forwarded based on packet information, such as the source and destination address. Layer 3 processing takes longer than Layer 2 processing, as there is more information to process.
Layer 4	Establishes connections and ensures that all data arrives at the correct destination. Packets inspected at the Layer 4 level are analyzed and forwarding decisions are based on their applications.
LCP	*Link Control Protocol*. Manages authentication, compression, and encryption.
Load Balancing	Enables the even distribution of data and/or processing packets across available network resources. For example, load balancing may distribute the incoming packets evenly to all servers, or redirect the packets to the next available server.
M	
MAC Address	*Media Access Control Address*. The MAC Address is a hardware specific address that identifies each network node.
MAC Address Learning	Characterizes a learning bridge, in which the packet's source MAC address is recorded. Packets destined for that address are forwarded only to the bridge interface on which that address is located. Packets addressed to unknown addresses are forwarded to every bridge interface. MAC Address Learning minimizes traffic on the attached LANs.
MAC Layer	A sub-layer of the Data Link Control (DTL) layer.
MAN	*Metropolitan Area Network*. A communications network covering a metropolitan area or a suburb.
Mask	A filter that includes or excludes certain values, for example parts of an IP address.
MD5	*Message Digest 5*. 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 and authenticates the origin of the communication.
MDI	*Media Dependent Interface.* A cable used for end stations.
MDIX	*Media Dependent Interface with Crossover (MDIX)*. A cable used for hubs and switches.
MDU	*Multiply-Divide Unit.* A high-speed circuit that performs multiplication and division within the CPU.
MIB	*Management Information Base*. MIBs contain information describing specific aspects of network components.
MTU	*Maximum Transfer Unit*. Specifies the maximum frame size that can be transmitted over a network. Frames that exceed the MTU must be broken into smaller frames.
Multicast	Transmits copies of a single packet to multiple ports.
N	
Network Processor	CPU chips that are optimized for networking and communications functions.

Term	Definition
NMS	*Network Management System*. An interface that provides a method of managing a system.
Node	A network connection endpoint or a common junction for multiple network lines. Nodes include: • Processors. • Controllers. • Workstations.
O	
OID	Object Identifier. Used by SNMP to identify managed objects. In the SNMP Manager/ Agent network management paradigm, each managed object must have an OID to identify it.
OSPF	*Open Shortest Path First*. A TCP/IP Interior Gateway protocol that calculates the lowest-cost route, multipath routing, and load balancing.
P	
Packet	Blocks of information for transmission in packet switched systems.
PDU	*Protocol Data Unit*. A data unit specified in a layer protocol consisting of protocol control information and layer user data.
PING	*Packet Internet Groper*. Verifies if a specific IP address is available. A packet is sent to another IP address and waits for a reply.
Policing	Determines if traffic levels are within a specified profile. Policing manages the maximum traffic rate used to send or receive packets on an interface.
Port	Physical ports provide connecting components that allow microprocessors to communicate with peripheral equipment.
Port Mirroring	Monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port.
Port Speed	Indicates port speed. Port speeds include: • Ethernet 10 Mbps. • Fast Ethernet 100Mbps. • Gigabit Ethernet 1000 Mbps.
PPP	*Point-to-Point Protocol*. Enables connecting to the Internet over a serial link. PPP establishes sessions between a PC and an ISP using the Link Control Protocol (LCP).
Privilege	An authorizations set that performs security-relevant functions, for example, user access to a device.
Protocol	A set of rules that governs how devices exchange information across networks.
Protocol Stack	Layered set of protocols working together to provide networking functions.
Q	
QoS	*Quality of Service*. QoS provides policies that contain sets of filters (rules). QoS allows network managers to decide how and what network traffic is forwarded according to priorities, application types, and source and destination addresses.
Query	Extracts information from a database and presents the information for use.
R	
RADIUS	*Remote Authentication Dial-In User Service*. A method for authenticating system users, and tracking connection time.
RDP	*Remote Desktop Protocol*. Allows a clients to communicate with the Terminal Server over the network.

Term	Definition
Redundancy	Provides duplication of devices, services, or events. If a device, service, or event fails, redundancy provides a backup that can replace the lost functionality.
Relay Agent	An Internet host or router that passes DHCP messages between DHCP clients and DHCP servers.
RIP	*Routing Information Protocol*. Stipulates how routing table information is exchanged between routers.
RJ-11 Connector	Grips up to four wires. RJ-11 connector plugs the handset into the telephone, and the telephone into the wall.
RJ-45 Connector	Grips up to eight copper wires and resembles a standard RJ-11 telephone connector. RJ-45 connectors are commonly used with Ethernet devices.
RMON	*Remote Monitoring on Network*. Provides network information to be collected from a single workstation.
ROS	*Real Time Operating System*. An operating system designed for use in a real time computer system.
Router	A device that connects to separate networks. Routers forward packets between two or more networks. Routers operate at a Layer 3 level.
RSTP	*Rapid Spanning Tree Protocol*. Detects and uses network topologies that allow a faster convergence of the spanning tree, without creating forwarding loops.
Running Configuration File	Contains all Startup file commands, as well as all commands entered during the current session. After the device is powered down or rebooted, all commands stored in the Running Configuration file are lost.
RVSP	*Resource V....Reservation Protocol*. Enables Internet applications to obtain differing service resources for traffic flows.
S	
Segmentation	Divides LANs into separate LAN segments for bridging and routing. Segmentation eliminates LAN bandwidth limitations.
Server	A central computer that provides services to other computers on a network. Services may include file storage and access to applications.
SNMP	*Simple Network Management Protocol*. Manages LANs. SNMP-based software communicates with network devices with embedded SNMP agents. SNMP agents gather network activity and device status information and send the information back to a workstation.
SoC	*System on a Chip*. An ASIC that contains an entire system. For example, a telecom SoC application can contain a microprocessor, digital signal processor, RAM, and ROM.
Spanning Tree Protocol	Prevents loops in network traffic. The Spanning Tree Protocol (STP) provides tree topography for any arrangement of bridges. STP provides one path between end stations on a network, eliminating loops.
SSH	*Secure Shell*. Logs into a remote computer via a network, executes commands, and transfers files from one computer to another.
Stand-alone Mode	Permits a device to operate independently from other devices.
Startup Configuration	Retains the exact device configuration when the device is powered down or rebooted.
Subnet	Sub-network. Subnets are portions of a network that share a common address component. In TCP/IP networks, devices that share a prefix are part of the same subnet. For example, all devices with a prefix of 157.100.100.100 are part of the same subnet.

Term	Definition
Subnet Mask	Used to mask all or part of an IP address used in a subnet address. Switch Filters and forwards packets between LAN segments. Switches support any packet protocol type.
T	
TCP/IP	*Transmissions Control Protocol*. Enables two hosts to communicate and exchange data streams. TCP guarantees packet delivery, and guarantees packets are transmitted and received in the order the are sent.
Telnet	*Terminal Emulation Protocol*. Enables system users to log in and use resources on remote networks.
TFTP	*Trivial File Transfer Protocol*. Uses User Data Protocol (UDP) without security features to transfer files.
Trap	A message sent by the SNMP that indicates that system events have occurred.
Trunking	*Link Aggregation*. Optimizes port usage by linking a group of ports together to form a single trunk (aggregated groups).
U	
UDP	*User Data Protocol*. Communication protocol that transmits packets but does not guarantee their delivery.
Unicast	A form a routing that transmits one packet to one user.
V	
VLAN	*Virtual Local Area Networks.* Logical subgroups that constitute a Local Area Network (LAN). This is done in software rather than defining a hardware solution.
VSDL	*Very High Bit Rate DSL*. An asymmetric DSL version used at the fiber optic junction point final drop to nearby customers.
W	
WAN	*Wide Area Networks*. Networks that cover a large geographical area.
Wildcard Mask	Specifies which IP address bits are used, and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important. For example, if the destination IP address is 149.36.184.198 and the wildcard mask is 255.36.184.00, the first two bits of the IP address are used, while the last two bits are ignored.

71035590

TP-LINK TECHNOLOGIES CO., LTD.
E-mail: support@tp-link.com
Website: http://www.tp-link.com
Add: 3/F., Building R1-B, Hi-tech Industrial Park, Shennan Rd., Shenzhen, P.R.China