



USER GUIDE

Cisco Small Business Pro

SPS208G/SPS224G4/SPS2024 Ethernet Switches



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

Chapter 1: Getting Started	8
Starting the Application	8
Understanding the Interface	10
Using the Device Command Buttons	11
Using Screen and Table Options	13
Adding Device Information	13
Modifying Device Information	14
Deleting Device Information	14
Resetting the Device	15
Logging Out of the Device	16
Chapter 2: Setup	17
Summary	18
Network Settings	20
DHCP Relay	22
L2 DHCP Relay Operation Mode	22
L2 DHCP Relay Quick Start	23
L2 DHCP Relay Operation	24
DHCP Relay in Practice - Examples	26
Time	27
Chapter 3: Port Management	35
Port Settings	35
Port Configuration	39
Link Aggregation	42
Link Aggregation Detail	44
LACP	47
Chapter 4: VLAN Management	50
Create VLAN	51
VLAN Port Settings	53

Ports to VLAN	55
Configuring Q-in-Q	58
Q-in-Q Overview	58
Q-in-Q Implementation	59
VLAN to Port	61
GVRP	64
Multicast TV Membership	66
Multicast TV VLAN	67
Multicast TV VLAN - IGMP Mapping	69
CPE VLAN Mapping	70

Chapter 5: Statistics 72

RMON Statistics	73
Resetting RMON Statistics Counters	75
RMON History	76
View History Table	78
RMON Alarms	80
RMON Events	82
Port Utilization	85
802.1x Statistics	87
GVRP Statistics	89
Resetting GVRP Statistics Counters	91
CPU Utilization	92
Interface Statistics	94
Resetting Interface Statistics Counters	97

Chapter 6: ACL 98

IP Based ACL	98
MAC Based ACL	103

Chapter 7: Network Security	107
RADIUS	108
TACACS+	111
ACL Binding	114
802.1x Settings	116
Port Authentication	121
Port Security	124
Management Access List	128
Storm Control	129
Chapter 8: Security Suite	133
DHCP Snooping	133
DHCP VLANs	136
DHCP Trusted Interfaces	138
DHCP Database	140
ARP Inspection	142
ARP Trusted Interfaces	144
ARP Inspection List	146
ARP VLANs	148
IP Source Guard	150
IP Source Guard Database	154
Chapter 9: QoS	157
QoS Modes	158
Service Types	160
Configuring QoS	161
CoS Settings	162
Queue Settings	165
DSCP Settings	166
Bandwidth	167

Basic Mode	170
Advanced Mode	171
Out of Profile DSCP Assignments	176
Policy Name	177
Class Map	178
Aggregate Policer	180
Interface To Policy	182

Chapter 10: Spanning Tree 184

STP Status	185
Global STP	187
STP Port Settings	190
RSTP Port Settings	195
MSTP Properties	199
MSTP Instance Settings	201
VLAN Instance Configuration	202
MSTP Interface Settings	204

Chapter 11: Multicast 208

IGMP Snooping	208
Bridge Multicast	212
Bridge Multicast Forward All	215

Chapter 12: SNMP 217

Global Parameters	218
Views	220
Group Profile	222
Group Membership	225
Communities	228
Notification Filter	232
Notification Recipient	235

Chapter 13: Admin	238
User Authentication	239
Static Address	242
Dynamic Address	244
Logging	246
Port Mirroring	249
Cable Test	252
Saving or Upgrading a Configuration	254
Enabling DCHP Option 67	259
Firmware Upgrade	260
Reboot	262
Factory Default	263
Server Logs	264
Memory Logs	267
Flash Logs	268
Chapter 14: Logout	270
Logout	270
Appendix A: Where to Go From Here	272
Product Resources	272
Related Documentation	272
Appendix B: Additional Information	273
Regulatory Compliance and Safety Information	273
Warranty	273
End User License Agreement (EULA)	273
Appendix C: Support Contacts	274

Getting Started

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

- Starting the Application
- Understanding the Interface
- Using the Device Command Buttons
- Using Screen and Table Options
- Resetting the Device
- Logging Out of the Device

Starting the Application

This section contains information for starting the Linksys User Interface.



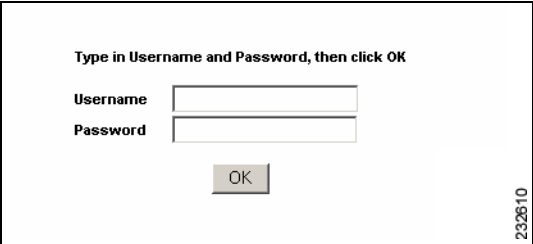
NOTE By default, the IP address of the device is assigned dynamically, although it can be changed to a static IP address by an administrator.

To open the User Interface:

STEP 1 Open a web browser.

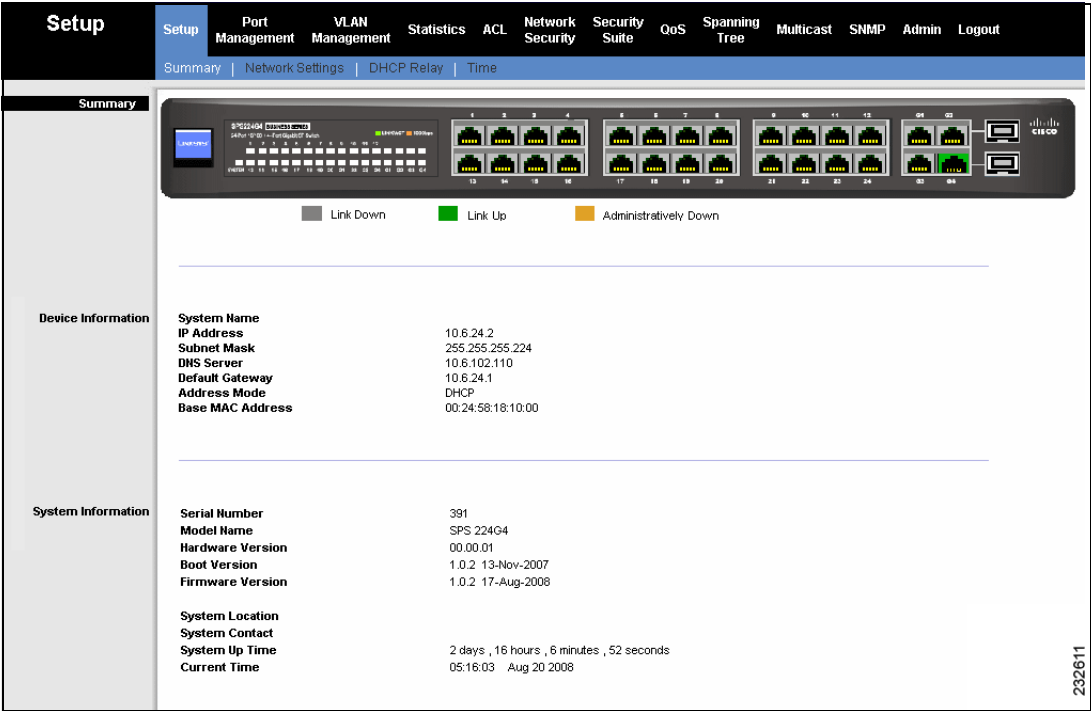
STEP 2 Type the device's IP address in the address bar and press **Enter**. The *Authentication Page* opens.

Figure 1 Authentication Page



- STEP 3** Enter a user name and password. The default user name is **admin**. The device is not configured with a default password, and can be configured without entering a password. Passwords are both case sensitive and alpha-numeric.
- STEP 4** Click **OK**. The *Summary Page* opens, and contains a graphical illustration of the SPS device's front panel.

Figure 2 Summary Page - SPS 208G



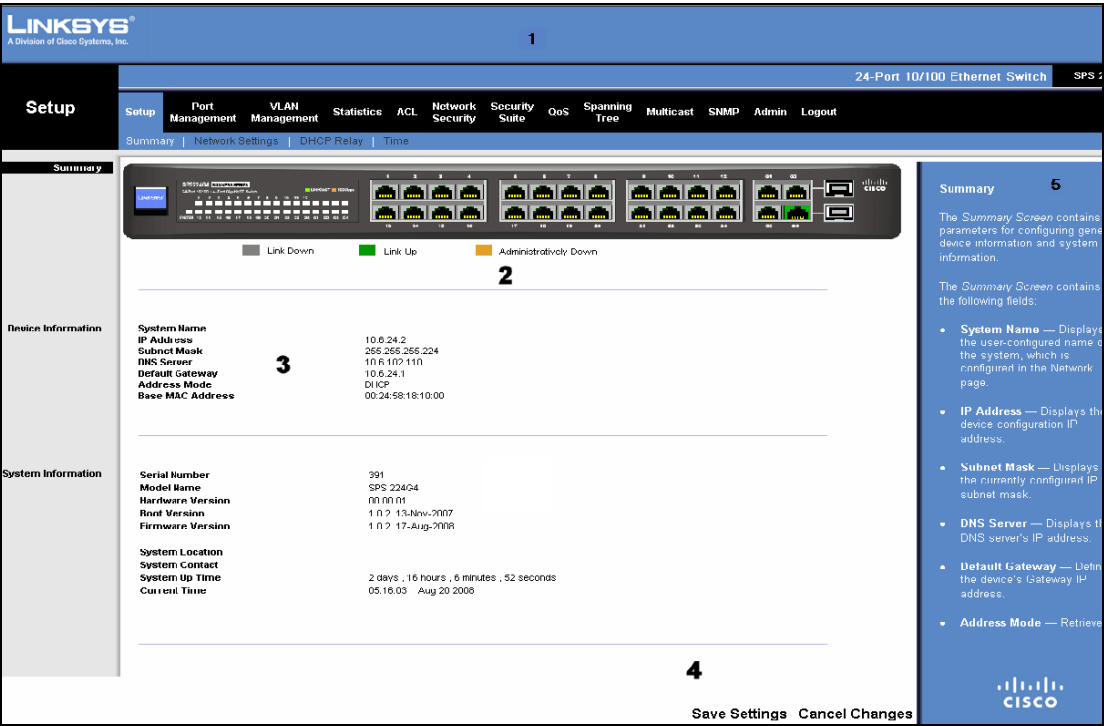
Understanding the Interface

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

Table 1 Interface Components

Component	Description
1. Menu Bar	The Menu Bar provides easy navigation through the configurable device features. Clicking the top menu bar provides access to subfeatures.
2. Device View	The Device View provides information about device ports, current configuration and status, table information, feature components and a color key of the link status.
3. Table Area	The Table Area enables viewing and configuration of the device features.
4. Configuration Commands	Clicking Save Settings saves the active settings on the current Table Area. Clicking Cancel Changes deletes any changes since the last time the configuration was changed.
5. Help Area	The Help Area displays help about the displayed feature.




Figure 3 Linksys User Interface Components


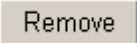

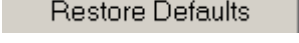
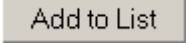
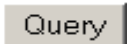



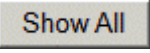


Using the Device Command Buttons

Device Command buttons provide an easy method of configuring device information. The following table describes the Web Management application's most common buttons:

Table 2 Device Command Buttons

Button Name	Button	Description
Save Settings		Saves changes to the device's running configuration.
Detail		Opens selected entry's configuration page.
Add		Opens an Add page.

Button Name	Button	Description
Update		Updates configuration changes.
Remove		Removes a selected entry from a table.
Delete		Deletes a selected entry from a table.
Reset the settings of Selected Port to Default		Resets the settings of a selected configuration to the default settings.
Add to List		Add a new configured entry to the table on the same page.
Query		Searches a database for addresses based on specified information.
Clear Counters		Clears statistic counters
Refresh Now		Refresh the displayed statistics.
Cancel		Cancels the configuration changes.
Show All		Opens a list showing all the items through which you can scroll.

Using Screen and Table Options

The Web Management application contains screens and tables for configuring devices.

Adding Device Information

User defined configuration information can be added to most Web Management application pages.

-
- STEP 1** Open the Web Management application page.
 - STEP 2** Edit the supplied fields.
 - STEP 3** Click **Add** or **Add To List**, according to the feature page.

Field Definitions

Fields which are user-defined can contain between 1 -159 characters, unless otherwise noted on the Web Management application page. All letters or characters can be used, except the following:

- \
- /
- :
- *
- ?
- <
- >

Modifying Device Information

Configuration information may be changed on most Web Management application pages, by selecting an existing entry and editing its configuration page.

-
- STEP 1** Open the Web Management application page.
 - STEP 2** Select a table entry.
 - STEP 3** Modify the relevant fields on the page and click **Update**.

-or-

Click the entry's **Details** button in the table. A Configuration page opens, for example, the *Port Settings Screen*. Define the fields and click **Save** or **Save & Close**.

The fields are modified, and the information is saved to the device.

Deleting Device Information

Configuration information may be deleted from the device on most Web Management application pages, by selecting an existing entry in the page's table and clicking the **Delete** button.

-
- STEP 1** Open the Web Management application page.
 - STEP 2** Select a table entry.
 - STEP 3** Click **Delete**. The entry configuration is deleted, and the device is updated.
-

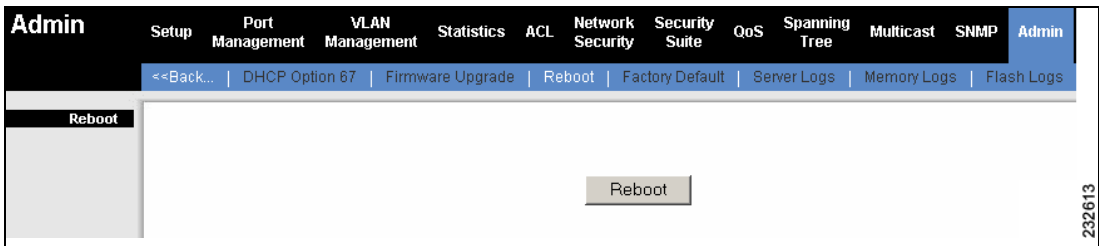
Resetting the Device

In the *Reboot Screen*, the user resets the device. To retain the device's current configuration, copy the Running Configuration file to the Startup Configuration file in the *Save Configuration Screen* before resetting the device.

To reset the device:

- STEP 1** Click **Admin > Reboot**. The *Reboot Screen* opens.

Figure 4 Reboot Screen



The *Reboot Screen* contains the following button:

Reboot — Resets the device.

- STEP 2** Click **Reboot** to restart and reset the device.

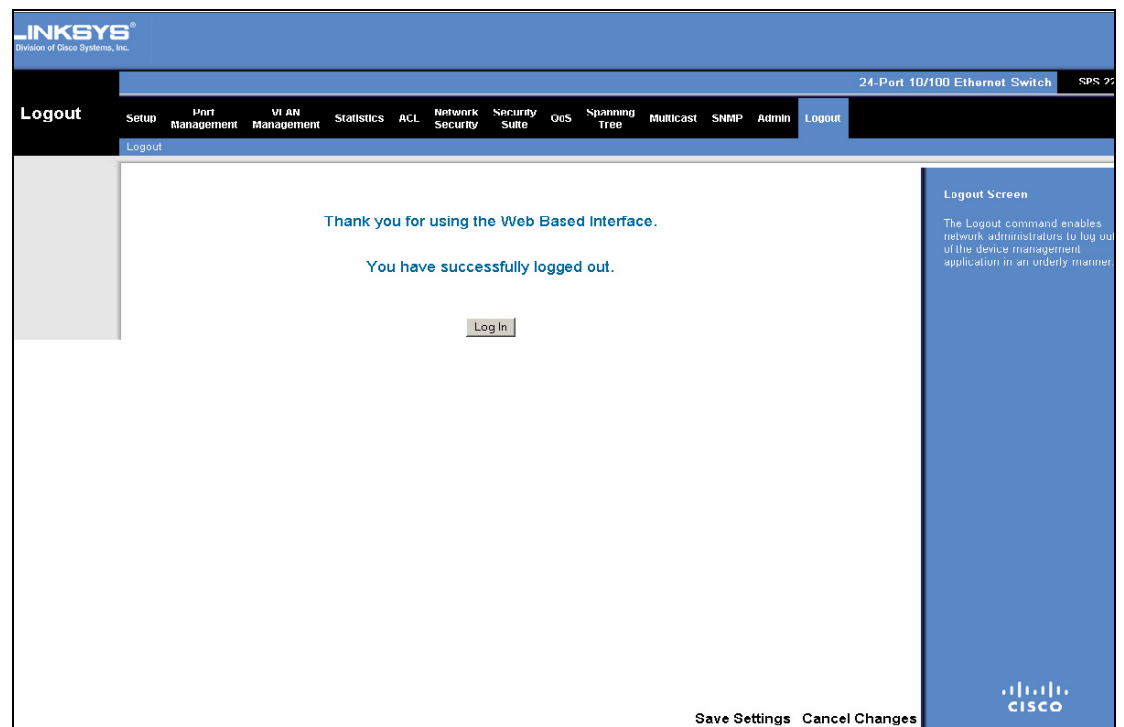
Logging Out of the Device

The Logout command enables network administrators to log out of the device management application in an orderly manner.

To log out of the device management application:

- STEP 1** Click **Logout**. The *Logout Screen* opens.

Figure 5 Logout Screen



The *Logout Screen* notifies whether logout was successful.

Setup

The Setup configuration options are as follows:

- Summary
- Zoom
- Network Settings
- DHCP Relay
- Time
- Stack Management

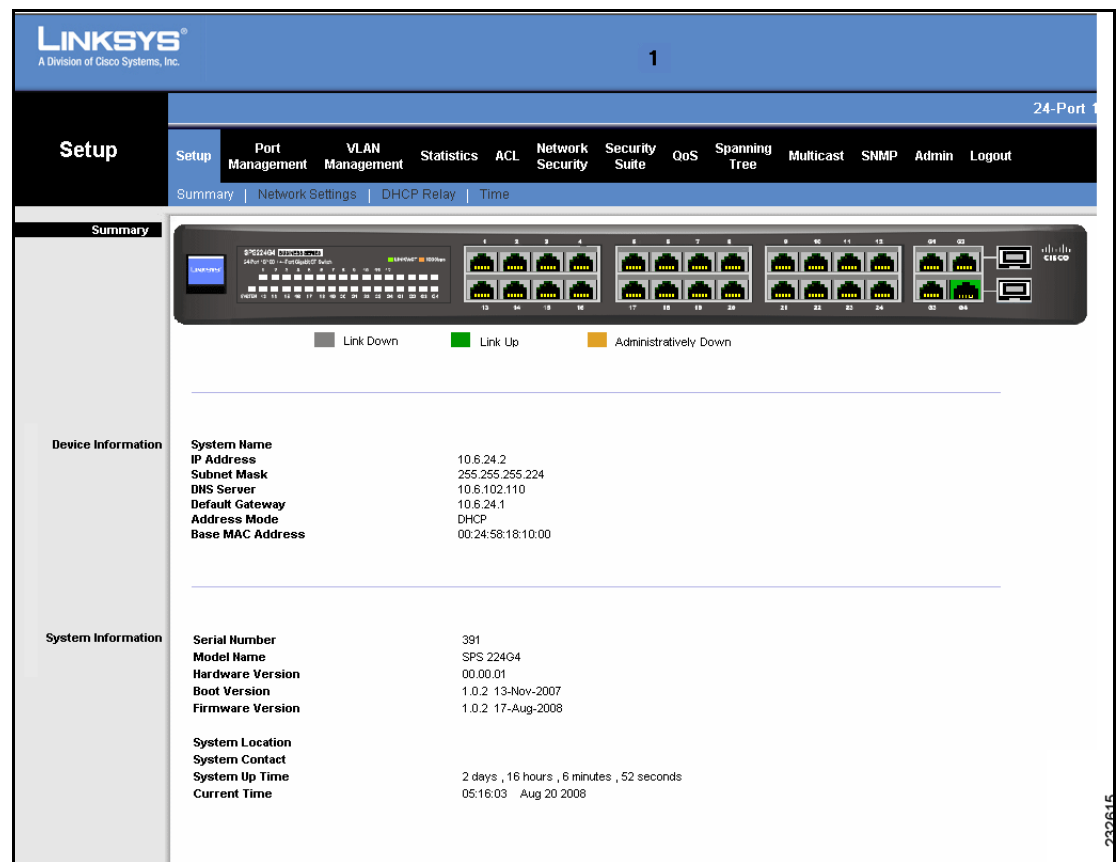
Summary

The *Summary Screen* contains parameters for configuring general device information.

To view device information:

STEP 1 Click **Setup** > **Summary**. The *Summary Screen* opens.

Figure 6 Summary Screen



The *Summary Screen* contains the following fields:

- **System Name** — Displays the user-configured name of the system, which is configured in the Network page.
- **IP Address** — Displays the device configuration IP address.
- **Subnet Mask** — Displays the currently configured IP subnet mask.
- **DNS Server** — Displays the DNS server's IP address.

- **Default Gateway** — Defines the device's Gateway IP address.
- **Address Mode** — Retrieves the IP addresses using DHCP or Static. The possible field values are:
 - *DHCP* — Retrieves the IP addresses using DHCP.
 - *Static* — The IP addresses are statically defined.
- **Base MAC Address** — Displays the device's base MAC address. If the system is in stack mode, the Base MAC Address of the master unit is displayed.
- **Switch Mode After Reset** — Indicates the mode of the device after reset. If "stack" is selected, the system will be in stacking mode after reset, and other units can be connected to this device in a stack. If "standalone" is selected, the system will be in standalone mode after reset, and cannot join a stack. In standalone mode all GE ports are available to the user, while in stacking mode, two GE ports are reserved for stacking and the two remaining GE ports can be used for other purposes.
- **Serial Number** — Displays the device's unique factory-defined serial number.
- **Model Name** — Displays the device model name.
- **Hardware Version** — Displays the hardware version number.
- **Boot Version** — Indicates the system boot version currently running on the device.
- **Firmware Version** — Displays the firmware version currently installed on the device.
- **System Location** — Displays the location where the system is currently running.
- **System Contact** — Displays the name of the contact person.
- **System Up Time** — Displays the amount of time that has elapsed since the last device reset. The system time is displayed in the following format: Days, Hours, Minutes and Seconds. For example: 41 days, 2 hours, 22 minutes and 15 seconds.
- **Current Time** — Displays the current time and date.

Network Settings

The *Network Settings Screen* contains parameters for configuring general device information, including the system name, location, and contact, the system MAC Address, System Object ID, System IP and MAC addresses.

To define the general system information:

STEP 1 Click **Setup > Network Settings**. The *Network Settings Screen* opens.

Figure 7 Network Settings Screen

LINKSYS®
A Division of Cisco Systems, Inc.

24-Port 1

Setup

Setup | Port Management | VLAN Management | Statistics | ACL | Network Security | Security Suite | QoS | Spanning Tree | Multicast | SNMP | Admin | Logout

Summary | Network Settings | DHCP Relay | Time

Network Settings Identification

System Name

System Location

System Contact

System Object ID 13.6.1.4.1.3955.6.9.224.1

Base MAC Address 00:24:58:18:10:00

Jumbo Frame ☐ Enable ☒ Disable

IP Configuration

Management VLAN 1

IP Address Mode DHCP

Renew DHCP Address

IP Address 10.6.24.2

Subnet Mask 255.255.255.224

Default Gateway 10.6.24.1

DNS Server 10.6.102.110

232616

The *Network Settings Screen* contains the following fields:

- **System Name** — Specifies the user-defined system name. The field range is 0-160 characters.
- **System Location** — Specifies the user-defined system location, for example, 3rd floor. The field range is 0-160 characters.
- **System Contact** — Specifies the user-defined system contact person. The field range is 0-160 characters.
- **System Object ID** — Displays the vendor's authoritative system object identification.
- **Base MAC Address** — Displays the master unit's base MAC address.

- **Base MAC Address** — Displays the device's base MAC address.
- **Jumbo Frame** — Enables Jumbo Frames on the device (packet size of up to 10 Kb is supported). Jumbo Frames enable the transportation of identical data in fewer frames. This ensures less overhead, lower processing time, and fewer interruptions. Jumbo Frames are supported on SPS 224G4 and SPS 2024 GE ports only. The possible field values are:
 - *Enable* — Switch recognizes and forwards Jumbo Frames.
 - *Disable* — Switch does not recognize Jumbo Frames.
- **Management VLAN** — Defines the management VLAN. If changed, the current web session ends and the user needs to log in again to continue working.
- **IP Address Mode** — Retrieves the IP addresses using DHCP or Static. The possible field values are:
 - *DHCP* — Retrieves the IP addresses using DHCP. If this option is selected, the IP Address, Subnet Mask, Default Gateway and DNS Server fields are defined dynamically.
 - *Static options* — The IP addresses are statically defined. If this option is selected, the IP Address, Subnet Mask, Default Gateway and DNS Server fields are defined manually once the user changes the IP address value, the new IP is automatically updated in the browser URL so the connection to the device is not lost.

STEP 2 If **DHCP IP Address Mode** is selected, click **Renew DHCP Address** to manually renew the DHCP address triggering the configuration update.



WARNING If **DHCP load configuration** is enabled (Admin --> Save Configuration), when pressing the **Renew DHCP Address** button, if there is a new configuration available on the server it will be downloaded and the system automatically reboots to apply it. If the device was configured with additional attributes over the configuration file, these settings are deleted. To prevent this, uncheck the load configuration option. In a normal DHCP renewal procedure (**not** manual), the device configuration is not overwritten.

- **IP Address** — Indicates the system IP address.
- **Subnet Mask** — Indicates the system IP address mask.
- **Default Gateway** — Indicates the system Default Gateway.

- **DNS Server** — Indicates the DNS server IP address.

STEP 3 Click **Save Settings**. The Network Settings are saved and the device is updated.

DHCP Relay

A DHCP Relay agent detects DHCP broadcasts from DHCP clients and relays those broadcasts to DHCP servers possibly on different subnets. The Relay agent information option (Option 82) in the DHCP protocol enables a DHCP relay agent to send additional client information upon requesting an IP address.

Option 82 specifies the relaying switch's MAC address, the port identifier, and the VLAN which forwarded the packet.

DHCP Snooping and L2 DHCP Relay implement the L2 DHCP Relay functionality in the switch. Each feature can insert option 82 into traversing packets.

- DHCP Snooping with option 82 insertion provides transparent L2 Relay agent functionality (as defined in TR-101 appendix B) if the DHCP server is on the same VLAN as the clients.
- The L2 DHCP Relay agent provides relay service for remote servers that are not on the same VLAN as clients.

L2 DHCP Relay Operation Mode

Transparent L2 DHCP Relay

The DHCP server must be located on the same VLAN as its clients. DHCP broadcasts are replaced and Option 82 is added to the replacement packets broadcast to the server.

This is implemented by the DHCP Snooping with Option 82 Insertion configuration. Ensure that DHCP Snooping on all relevant VLANs is enabled and that in the DHCP Snooping configuration, the DHCP server outgoing ports are set to "trusted".

This is an implementation of transparent L2 Relay agent (as described in TR-101 appendix B).

Full L2 DHCP Relay

Full L2 DHCP Relay is used when the client ingress VLAN is different than the VLAN on which the DHCP servers are connected. If DHCP servers are located on the ingress VLAN, transparent L2 DHCP Relay is used.

The Option 82 information is added to the packets that are relayed to DHCP server.

This mode also forces Option 82 insertion of DHCP Snooping, if activated.

L2 DHCP Relay Quick Start

L2 DHCP Relay

To set up Option 82 Insertion if the DHCP Server is located on a different VLAN than the clients:

-
- STEP 1** In the *DHCP Relay Screen*, select **Enable DHCP Relay**.
 - STEP 2** Add the clients (ingress) VLAN to the list of enabled VLAN. Ensure that the ingress VLAN does not have an assigned IP address.
 - STEP 3** Add the DHCP Server IP address to the list of DHCP Servers.
-



NOTE Using the Command Line Interface, ensure that the switch successfully pings the DHCP server.

Clients and DHCP Server on the Same VLAN

To set up Option 82 Insertion if the DHCP Server is located in the same VLAN as the clients:

-
- STEP 1** In the *DHCP Snooping Screen*, select **Enable DHCP Snooping**.
 - STEP 2** In the *DHCP Snooping Enabled VLAN Screen (SPS 224G4)*, add the clients VLAN to the list of enabled VLANs.
 - STEP 3** In the *DHCP Trusted Interface Screen*, set the DHCP server port as a trusted port.

STEP 4 In the *DHCP Relay Screen*, select **Enable DHCP Option 82 Insertion**.

L2 DHCP Relay Operation

DHCP Snooping with Option 82 Insertion

Requests

DHCP broadcasts are trapped on the CPU, and replacement broadcasts are forwarded with Option 82.



NOTE If Option 82 is present in the request received on an untrusted port, the following options are available:

- Pass-through enabled — The packet is forwarded, unchanged, to a trusted port.
- Pass-through disabled — The packet is discarded.

Replies

Replies from the DHCP servers are handled according to the DHCP Snooping rules, such as checking if the port is trusted before forwarding the packet.

L2 DHCP Relay

Requests

The switch traps DHCP broadcast messages (DHCP DISCOVER and DHCP REQUEST) from the DHCP clients:

- Packets arriving with Option-82 are discarded.
- If the giaddr field is 0.0.0.0 it is modified to the DHCP server's IP address.
- The packet is duplicated and relayed per each DHCP Server.



NOTE If L2 DHCP relay is enabled; and the DHCP server is on the DHCP request ingress VLAN, the outgoing relayed packet is sent as a broadcast.

Replies

The switch verifies if Option-82 is both included in the message and was inserted by the switch. In that case, the switch removes Option 82, determines the packet's VLAN and the egress port according to the information included in the removed Option 82, and forwards the packet.

To enable and configure DHCP Relay:

STEP 1 Click **Setup > DHCP Relay**. The *DHCP Relay Screen* opens.

Figure 8 DHCP Relay Screen

The *DHCP Relay Screen* contains the following fields:

- **Enable DHCP Relay** — Enable or disable DHCP Relay on the device. The possible values are:
 - *Checked* — Indicates that DHCP Relay is enabled on the device.
 - *Unchecked* — Indicates that DHCP Relay is disabled on the device.
- **Enable DHCP Option 82 Insertion** — Enable or disable DHCP Option 82 Insertion on the device. The possible values are:
 - *Checked* — Indicates that DHCP Option 82 Insertion is enabled on the device. This option enabled automatically (and grayed) when “Enabled DHP Relay” option is checked. When using Transparent L2 DHCP relay, the user must enable DHCP Snooping manually.

- *Unchecked* — Indicates that DHCP Option 82 Insertion is disabled on the device.

The following fields are available only if DHCP Relay is enabled:

- **Enable DHCP Relay on VLAN ID** — Defines specific VLAN on which to enable DHCP Relay and Option 82. Clicking **Add** displays the VLAN ID in the **Enabled VLANs** field.
- **Enabled VLANs** — Displays DHCP Relay-enabled VLANs. The VLAN must not have an IP address assignment. Selecting a VLAN and clicking **Remove** disables DHCP Relay on the VLAN.
- **Add DHCP Server** — Defines the IP address of the destination DHCP Server. Clicking **Add** displays the DHCP Server address in the **DHCP Server** field.
- **DHCP Servers** — Displays DHCP Relay-enabled DHCP servers. Selecting a DHCP Server and clicking **Remove** disables DHCP Relay to that destination.

STEP 2 Enable and/or disable DHCP Relay on the relevant VLANs and DHCP Servers.

STEP 3 Click **Save Settings** to save the DHCP Relay configuration. The device is updated.

DHCP Relay in Practice - Examples

Transparent L2 Relay

DHCP broadcasts are trapped on the switch and replacement broadcasts are forward with Option 82, in the Ingress VLAN only.

This functionality is set up in the DHCP Snooping configuration. It is necessary to define the following:

- Participating VLANs.
- Trusted ports.

L2 DHCP Relay with Option 82

Each incoming DHCP request in the ingress VLANs is trapped on the switch, and is replaced by a single Unicast DHCP request with Option 82 sent to each user-specified DHCP server IP address. The outgoing frame goes on a different VLAN than the one it arrived on. If the server is on a different IP subnet, packets are sent to the default gateway.

The only exception occurs if a DHCP server is on the same VLAN as the ingress VLAN. In that case, the packet with no Option 82 is broadcast.

Transparent L2 Relay and L2 DHCP Relay Together

Both features work independently and concurrently.

In Transparent L2 Relay, the agent adds Option 82 to DHCP requests passing through on the client ingress VLAN.

For any ingress VLAN where Full L2 DHCP Relay is enabled, an additional Transparent L2 Relay packet is relayed to any remote DHCP server configured by the user.

L2 DHCP Snooping Alone (with no Option 82)

DHCP broadcasts are bridged in the ingress VLAN without using CPU resources. DHCP Snooping database and related functionality are supported without Option 82 Insertion, but users can control incoming Option 82 per user configuration.

Time

The *Time Screen* 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 Time start and end times in specific countries:

- **Albania** — Last weekend of March until the last weekend of October.
- **Australia** — From the end of October until the end of March.
- **Australia - Tasmania** — From beginning of October until the end of March.
- **Armenia** — Last weekend of March until the last weekend of October.
- **Austria** — Last weekend of March until the last weekend of October.
- **Bahamas** — From April to October, in conjunction with U.S. summer hours.
- **Belarus** — Last weekend of March until the last weekend of October.
- **Belgium** — Last weekend of March until the last weekend of October.

- **Brazil** — From the 3rd Sunday in October until the 3rd Saturday in March. During the period of Daylight Saving Time, Brazilian clocks go forward one hour in most of the Brazilian southeast.
- **Chile** — The first Sunday in March or after 9th March. In addition, Easter Island DST starts 9th March and ends the 12th October.
- **China** — China does not operate Daylight Saving Time.
- **Canada** — From the first Sunday in April until the last Sunday of October. Daylight Saving Time is usually regulated by provincial and territorial governments. Exceptions may exist in certain municipalities.
- **Cuba** — From the last Sunday of March to the last Sunday of October.
- **Cyprus** — Last weekend of March until the last weekend of October.
- **Denmark** — Last weekend of March until the last weekend of October.
- **Egypt** — Last Friday in April until the last Thursday in September.
- **Estonia** — Last weekend of March until the last weekend of October.
- **Finland** — Last weekend of March until the last weekend of October.
- **France** — Last weekend of March until the last weekend of October.
- **Germany** — Last weekend of March until the last weekend of October.
- **Greece** — Last weekend of March until the last weekend of October.
- **Hungary** — Last weekend of March until the last weekend of October.
- **India** — India does not operate Daylight Saving Time.
- **Iran** — From 1st Farvardin until the 1st Mehr.
- **Iraq** — From 1st April until 1st October.
- **Ireland** — Last weekend of March until the last weekend of October.
- **Israel** — Varies year-to-year.
- **Italy** — Last weekend of March until the last weekend of October.
- **Japan** — Japan does not operate Daylight Saving Time.
- **Jordan** — Last weekend of March until the last weekend of October.
- **Latvia** — Last weekend of March until the last weekend of October.
- **Lebanon** — Last weekend of March until the last weekend of October.

- **Lithuania** — Last weekend of March until the last weekend of October.
- **Moldova** — Last weekend of March until the last weekend of October.
- **Montenegro** — Last weekend of March until the last weekend of October.
- **Netherlands** — Last weekend of March until the last weekend of October.
- **New Zealand** — From the first Sunday in October until the first Sunday on or after 15th March.
- **Norway** — Last weekend of March until the last weekend of October.
- **Paraguay** — From 6th April until 7th September.
- **Poland** — Last weekend of March until the last weekend of October.
- **Portugal** — Last weekend of March until the last weekend of October.
- **Romania** — Last weekend of March until the last weekend of October.
- **Russia** — Last weekend of March until the last weekend of October.
- **Serbia** — Last weekend of March until the last weekend of October.
- **Slovak Republic** — Last weekend of March until the last weekend of October.
- **South Africa** — South Africa does not operate Daylight Saving Time.
- **Spain** — Last weekend of March until the last weekend of October.
- **Sweden** — Last weekend of March until the last weekend of October.
- **Switzerland** — Last weekend of March until the last weekend of October.
- **Syria** — From 31st March until 30th October.
- **Taiwan** — Taiwan does not operate Daylight Saving Time.
- **Turkey** — Last weekend of March until the last weekend of October.
- **United Kingdom** — Last weekend of March until the last weekend of October.
- **United States of America** — From the second Sunday in March at 02:00 to the first Sunday in November at 02:00.

To open the *Time Screen*.

STEP 1 Click **Setup > Time**. The *Time Screen* opens.

Figure 9 Time Screen

The screenshot shows the Linksys Time Screen configuration interface. The top navigation bar includes 'Setup' and various other settings like Port Management, VLAN Management, etc. The left sidebar has a 'Time' section with sub-items: Set Time, Local Time, Daylight Savings, and SNTP Servers. The main content area is divided into four sections: 1. 'Set Time' with radio buttons for 'Use System Time' (selected) and 'Use SNTP Time'. 2. 'Local Time' with input fields for Hours (05), Minutes (30), Seconds (32), Month (08), Day (20), and Year (08), and a 'Time Zone' dropdown menu set to '(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London'. 3. 'Daylight Savings' with a checkbox for 'Daylight Savings' (unchecked), radio buttons for 'USA', 'European', and 'Custom' (selected), and fields for 'Time Set Offset' (30 Min), 'From' (DDMM/YY), 'To' (DDMM/YY), and 'Recurring' (checkbox checked) with 'From' and 'To' date and time fields. 4. 'SNTP Servers' with fields for 'Primary Server', 'Secondary Server', and 'SNTP Polling Interval' (1024 sec).

The *Time Screen* is divided into four configuration areas:

- Set Time
- Local Time
- Daylight Savings
- SNTP Servers

Set Time

The Set Time area contains the following fields:

- **Use System Time** — The device system time is taken from the management station time settings.
- **Use SNTP Time** — The device system time is configured from an SNTP server.

Local Time

The Local Time area contains the following fields:

- **Hours** — Sets the hours.
- **Minutes** — Sets the minutes.
- **Seconds** — Sets the seconds.
- **Month** — Sets the month.
- **Day** — Sets the day.
- **Year** — Sets the year.
- **Time Zone** — Specifies the difference between Greenwich Mean Time (GMT) and local time. For example, the Time Zone Offset for Paris is GMT +1, while the local time in New York is GMT -5.

Figure 10 Time – Daylight Savings

LINKSYS®
A Division of Cisco Systems, Inc.

24-Port T

Setup

SetupPort ManagementVLAN ManagementStatisticsACLNetwork SecuritySecurity SuiteQoSSpanning TreeMulticastSNMPAdminLogout

SummaryNetwork SettingsDHCP RelayTime

Time

Set Time

Local Time

Daylight Savings

SNTP Servers

☒ Use System Time

☐ Use SNTP Time

05Hours

30Minutes

32Seconds

08Month

20Day

08Year

(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

☒ Daylight Savings

☐ USA☐ European☒ Custom

Time Set Offset

60(Min)

From

(DD/MM/YY)

(HH:MM)

To

(DD/MM/YY)

(HH:MM)

☐ Recurring

From

DaySunWeekFirstMonthJanTime00:00(HH:MM)

To

DaySunWeekFirstMonthJanTime00:00(HH:MM)

Primary Server

Secondary Server

SNTP Polling Interval

1024(60-86400 sec)

Daylight Savings

There are two types of daylight savings settings, either by a specific date in a particular year or a recurring setting irrespective of the year. For a specific setting in a particular year complete the **Daylight Savings** area, and for a recurring setting, complete the **Recurring** area.

The Daylight Savings area contains the following fields:

- **Daylight Savings** — Enables the Daylight Savings Time (DST) on the device based on the devices location. The possible field values are:
 - *USA* — The device switches to DST at 2 a.m. local time on the second Sunday of March, and reverts to standard time at 2 a.m. on the first Sunday of November.
 - *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.

SPS208G/SPS224G4/SPS2024 Service Provider Switches User Guide

32

- *Custom* — The DST definitions are user-defined based on the device locality. If Custom is selected, the From and To fields must be defined.
- **Time Set Offset** — For non USA and European countries, specifies the amount of time for DST that can be set in minutes. The default time is 60 minutes.
- **From** — Specifies the time that DST begins in countries other than USA or Europe, in the format DayMonthYear in one field and time in another. For example, DST begins on the 25th October 2007 5:00 am, the two fields will be 25/Oct/07 and 05:00. The possible field values are:
 - DD/MM/YY — The date, month, and year in which DST begins.
 - HH:MM — The hour and minute at which DST begins.
 - *Day* — The date at which DST begins. The possible field range is 1-31.
 - *Month* — The month of the year in which DST begins. The possible field range is Jan-Dec.
 - *Year* — The year in which the configured DST begins.
 - *Time* — The time at which DST begins. The field format is Hour:Minute, for example, 05:30.
- **To** — Specifies the time that DST ends in countries other than USA or Europe in the format DayMonthYear in one field and time in another. For example, DST ends on the 23rd March 2008 12:00 am, the two fields will be 23/Mar/08 and 12:00. The possible field values are:
 - DD/MM/YY — The date, month, and year in which DST ends.
 - HH:MM — The hour and minute at which DST ends.
 - *Day* — The date at which DST ends. The possible field range is 1-31.
 - *Month* — The month of the year in which DST ends. The possible field range is Jan-Dec.
 - *Year* — The year in which the configured DST ends.
 - *Time* — The time at which DST starts. The field format is Hour:Minute, for example, 05:30.

- **Recurring** — Specifies the time that DST starts in countries other than USA or European where the DST is constant year to year. The possible field values are:
- **From** — Specifies the time that DST begins each year. For example, DST begins locally every second Sunday in April at 5:00 am. The possible field values are:
 - *Day* — The day of the week from which DST begins every year. The possible field range is Sunday-Saturday.
 - *Week* — The week within the month from which DST begins every year. The possible field range is 1-5.
 - *Month* — The month of the year in which DST begins every year. The possible field range is Jan.-Dec.
 - *Time* — The time at which DST begins every year. The field format is Hour:Minute, for example, 02:10.
- **To** — Specifies the recurring time that DST ends each year. For example, DST ends locally every fourth Friday in October at 5:00 am. The possible field values are:
 - *Day* — The day of the week at which DST ends every year. The possible field range is Sunday-Saturday.
 - *Week* — The week within the month at which DST ends every year. The possible field range is 1-5.
 - *Month* — The month of the year in which DST ends every year. The possible field range is Jan.-Dec.
 - *Time* — The time at which DST ends. The field format is Hour:Minute, for example, 05:30.

SNTP Servers

The SNTP Servers area contains information for enabling SNTP servers with the following fields:

- **Primary Server** — Indicates the IP address of the primary SNTP server.
- **Secondary Server** — Indicates the IP address of the secondary SNTP server.
- **SNTP Polling Interval** — Defines the interval (in seconds) at which the SNTP server is polled. The possible field values are *60-86400* seconds.

Port Management

The Port Management configuration options are as follows:

- Port Settings
- Link Aggregation
- LACP
- PoE Power Setting

Port Settings

The *Port Settings Screen* contains fields for defining port parameters.



NOTE If the Administrative Status of a port is set to **down**, then the **shutdown** command appears in the configuration file. If the Administrative status is set to **up**, then the **no shutdown** command appears.

Device	Port	Defaults	
		Administrative Status	Configuration
SPS2xx	FE ports (UNI ports)	down	shutdown
	GE ports (NNI ports)	up	no shutdown
SPS2024	Ports 12 & 24 (NNI ports)	up	no shutdown
	All other ports	down	shutdown

To modify port settings:

STEP 1 Click **Port Management > Port Settings**. The *Port Settings Screen* opens.

Figure 11 Port Settings Screen

LINKSYS®
A Division of Cisco Systems, Inc.

24-Port 1

Port Management Setup **Port Management** VLAN Management Statistics ACL Network Security Suite QoS Spanning Tree Multicast SNMP Admin Logout

Port Settings | Link Aggregation | LACP

Port Configuration

Enable Protected Ports ☒

<<Previous 1 2 3 Next>>

Port	Description	Administrative Status	Link Status	Speed	Duplex	MDI/MDIX	Flow Control	Type	LAG	PVE	Detail
e1		Up	Down	100M		Auto	Disable	100M-copper			Detail
e2		Up	Down	100M		Auto	Disable	100M-copper			Detail
e3		Up	Down	100M		Auto	Disable	100M-copper			Detail
e4		Up	Down	100M		Auto	Disable	100M-copper			Detail
e5		Up	Down	100M		Auto	Disable	100M-copper			Detail
e6		Up	Down	100M		Auto	Disable	100M-copper			Detail
e7		Up	Down	100M		Auto	Disable	100M-copper			Detail
e8		Up	Down	100M		Auto	Disable	100M-copper			Detail
e9		Up	Down	100M		Auto	Disable	100M-copper			Detail
e10		Up	Down	100M		Auto	Disable	100M-copper			Detail
e11		Up	Down	100M		Auto	Disable	100M-copper			Detail
e12		Up	Down	100M		Auto	Disable	100M-copper			Detail

232620

For 24-port devices, the *Port Settings Screen* displays the ports on multiple screens. To browse to a specific port entry, click the **Previous**, **1**, **2**, **3**, and **Next** links above the table.

The *Port Settings Screen* contains the following fields:

- **Enable Protected Ports** — The Protected Ports feature provides layer-2 isolation between ports that share the same broadcast domain (VLAN). The feature defines two types of ports:
 - **Protected ports:** Only sends traffic to uplink ports
 - **Uplink ports:** Can send traffic to any port

When selected, all FE ports are defined as protected ports for each VLAN, so that they are isolated from other ports within the same VLAN. The GE ports remain as unprotected ports that function as normal VLAN member ports.

- **Unit No.** — Indicates the stacking member being managed.
- **Port** — Displays the port number.
- **Description** — Displays the device port user-defined description.
- **Administrative Status** — Defines the port status. The possible field values are:
 - *Up* — Indicates the port is operating.
 - *Down* — Indicates the port is not operating.
- **Link Status** — Defines 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.
- **Speed** — Displays the current 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:
 - *10M* — Indicates the port is currently operating at 10 Mbps.
 - *100M* — Indicates the port is currently operating at 100 Mbps.
 - *1000M* — Indicates the port is currently operating at 1000 Mbps.
- **Duplex** — Displays the port duplex mode, can be either Full or Half. Full indicates that the interface supports transmission between the device and its link partner in both directions simultaneously. Half indicates that the interface supports transmission between the device and the client in only one direction at a time. The Duplex Mode field is configurable only when auto negotiation is disabled, and the port speed is set to 10M or 100M. The Duplex Mode field cannot be configured on LAGs.
- **MDI/MDIX** — Displays the Media Dependent Interface (MDI)/Media Dependent Interface with Crossover (MDIX) status on the port. Hubs and switches are deliberately wired the opposite of 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.

- *MDIX* — Use for end stations.
 - *MDI* — Use for hubs and switches.
- **Flow Control** — Displays the flow control status on the port. Operates when the port is in full duplex mode. The possible values are:
 - *Enable* — Flow control on the port is enabled.
 - *Disable* — Flow control on the port is disabled.
 - *Auto-Negotiate* — Auto-negotiation of flow control on the port is enabled.
- **Type** — Displays the port type.
- **LAG** — Indicates in which LAG the port is a member.
- **PVE** — Indicates that this port is protected by an uplink, so that the forwarding decisions are overwritten by those of the port that protects it. PVE is supported in Layer 2 mode.

Port Configuration

The **Detail** button displays the *Port Configuration Screen* with the following fields:

- STEP 1** Click **Detail**. The *Port Configuration Screen – Copper Port* opens.

Figure 12 Port Configuration Screen – Copper Port

The screenshot shows the 'Port Configuration' window for port 'e1'. The settings are as follows:

Field	Value
Port	e1
Description	
Port Type	100M-copper
Admin Status	Up
Current Port Status	Down
Reactivate Suspended Port	<input type="checkbox"/>
Operational Status	Active
Admin Speed	100M
Current Port Speed	
Admin Duplex	Full
Current Duplex Mode	
Auto Negotiation	Enable
Current Auto Negotiation	
Admin Advertisement	<input checked="" type="checkbox"/> Max. Capability <input type="checkbox"/> 10 Half <input type="checkbox"/> 10 Full <input type="checkbox"/> 100 Half <input type="checkbox"/> 100 Full
Current Advertisement	Unknown
Neighbor Advertisement	Unknown
Back Pressure	Disable
Current Back Pressure	
Flow Control	Disable
Current Flow Control	Disable
MDI/MDIX	Auto
Current MDI/MDIX	
PVE	None
LAG	

Buttons at the bottom: Save, Save & Close, Close.

The *Port Configuration Screen – Copper Port* contains the following fields:

- **Port** — Displays the port number.
- **Description** — Defines the device port (user-defined description).
- **Port Type** — Displays the port type. The possible field values are:
 - *100M-copper* — Indicates the port has a 100 MB copper port connection.
 - *1000M-copper* — Indicates the port has a 1000 MB copper port connection.

- **Admin Status** — Enables or disables traffic forwarding through the port.
 - *Up* — Indicates traffic forwarding is enabled through this port.
 - *Down* — Indicates traffic forwarding is disabled through this port.
- **Current Port Status** — Displays the port connection status.
- **Reactivate Suspended Port** — Reactivates a link if the port has been disabled through the locked port security option.
- **Operational Status** — Displays whether the port is currently operational or non-operational.
- **Admin Speed** — The configured rate for the port. The port type determines what speed setting options are available. The auto negotiation should be disabled before setting the speed manually.
- **Current Port Speed** — Displays the current port speed.
- **Admin Duplex** — The port duplex mode. Full indicates that the interface supports transmission between the device and the client in both directions simultaneously. Half indicates that the interface supports transmission between the device and the client in only one direction at a time.
- **Current Duplex Mode** — Displays the port current duplex mode.
- **Auto Negotiation** — Enables Auto Negotiation on the port. Auto Negotiation is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode and flow control abilities to its partner.
- **Current Auto Negotiation** — Displays the Auto Negotiation status on the port.
- **Admin Advertisement** — Specifies the capabilities to be advertised by the port. The possible field values are:
 - *Max Capability* — Indicates that all port speeds and Duplex mode settings can be accepted.
 - *10 Half* — Indicates that the port is advertising a 10 mbps speed and half Duplex mode setting.
 - *10 Full* — Indicates that the port is advertising a 10 mbps speed and full Duplex mode setting.
 - *100 Half* — Indicates that the port is advertising a 100 mbps speed and half Duplex mode setting.

- *100 Full*— Indicates that the port is advertising a 100 mbps speed and full Duplex mode setting.
 - *1000 Full*— Indicates that the port is advertising a 1000 mbps speed and full Duplex mode setting.
- **Current Advertisement** — The port advertises its capabilities to its neighbor port to start the negotiation process. The possible field values are those specified in the Admin Advertisement field.
- **Neighbor Advertisement** — The neighbor port (the port to which the selected interface is connected) advertises its capabilities to the port to start the negotiation process. The possible values are those specified in the Admin Advertisement field.
- **Back Pressure** — Enables Back Pressure mode on the port. Back Pressure mode is used with Half Duplex mode to disable ports from receiving messages. The Back Pressure mode is configured for ports currently in the Half Duplex mode.
- **Current Back Pressure** — Displays the Back Pressure mode on the port.
- **Flow Control** — Enables or disables flow control or enables the auto negotiation of flow control on the port.
- **Current Flow Control** — Displays the current Flow Control setting.
- **MDI/MDIX** — Defines the Media Dependent Interface (MDI)/Media Dependent Interface with Crossover (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* — Use for end stations.
 - *MDIX* — Use for hubs and switches.

- **Current MDI/MDIX** — Displays the current MDI/MDIX setting.
- **PVE** — Indicates that this port is protected by an uplink, so that the forwarding decisions are overwritten by those of the port that protects it. PVE is supported in Layer 2 mode.
- **LAG** — Indicates the LAG number of which this port is a member, if relevant.

STEP 2 Define the relevant fields.

STEP 3 Click **Save & Close** to save the modifications and close the *Port Configuration Screen* (clicking **Save** keeps the *Port Configuration Screen* open).

Link Aggregation

Link Aggregated Groups (LAGs) optimize port usage by linking a group of ports together to form a single aggregated group. Link aggregated groups multiply the bandwidth between the devices, increase port flexibility, and provide link redundancy.

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

To modify LAG settings:

STEP 1 Click **Port Management > Link Aggregation**. The *Link Aggregation Screen* opens.

Figure 13 Link Aggregation Screen

LAG	Description	Admin Status	Type	Link Status	Speed	Flow Control	LAG Mode	Detail
1		Up	Static		Unknown	Disable	off	Detail
2		Up	Static		Unknown	Disable	off	Detail
3		Up	Static		Unknown	Disable	off	Detail
4		Up	Static		Unknown	Disable	off	Detail
5		Up	Static		Unknown	Disable	off	Detail
6		Up	Static		Unknown	Disable	off	Detail

The *Link Aggregation Screen* contains the following fields:

- **LAG** — Displays the LAG ID number.
- **Description** — Defines the user-defined LAG name.
- **Admin Status** — Enables or disables traffic forwarding through the selected LAG. The possible field values are:
 - *Up* — Indicates traffic forwarding is enabled through this LAG.
 - *Down* — Indicates traffic forwarding is disabled through this LAG.
- **Type** — Displays the LAG type. Only ports matching this type can join this LAG.
- **Link Status** — Indicates if the LAG is currently linked. The possible field values are:
 - *Up* — Indicates the LAG is currently linked, and is forwarding or receiving traffic.
 - *Down* — Indicates the LAG is not currently linked, and is not forwarding or receiving traffic.
- **Speed** — Displays the configured aggregated rate for the LAG. The possible field values are:
 - *10M* — Indicates the LAG is currently operating at 10 Mbps.
 - *100M* — Indicates the LAG is currently operating at 100 Mbps.
 - *1000M* — Indicates the LAG is currently operating at 1000 Mbps.
- **Flow Control** — Displays the flow control status of the LAG.
 - *Enable* — Indicates that the Flow Control is enabled.
 - *Disable* — Indicates that the Flow Control is disabled.
 - *Auto Negotiation* — Enables Auto Negotiation for the Flow Control. Auto Negotiation is a protocol between two link partners that enables a port to advertise its flow control state to its partner.
- **LAG Mode** — Displays the type of link aggregation. The possible field values are:
 - *LACP* — Link aggregation is set up using LACP.
 - *Static* — LACP is disabled. Instead, link aggregation is set up.

Link Aggregation Detail

The **Detail** button displays the *Link Aggregation Screen* with the following fields:

STEP 1 Click **Detail**. The *Link Aggregation Details Screen* opens.

Figure 14 Link Aggregation Details Screen

Link Aggregation

LAG Configuration

LAG 1

Description

LACP Mode Static

LAG Type

Admin Status Up

Current Status

Reactivate Suspended

Operational Status Active

Admin Auto Negotiation Enable

Current Auto Negotiation

Admin Speed

Current Speed

Admin Flow Control Disable

Current Flow Control

Admin Advertisement ☒ Max Capability ☐ 10 Full ☐ 100 Full ☐ 1000 Full

Ethernet	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Static	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Gigabit	1	2	3	4																				
Static	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																				

Save Save & Close Close

232623

The *Link Aggregation Details Screen* contains the following fields:

LAG Configuration

- **LAG** — Defines the LAG ID number.
- **Description** — Defines the user-defined LAG name.
- **LACP Mode** — Enables or disables Link Aggregation Control Protocol (LACP). The possible field values are:
 - *LACP* — LACP is enabled on the LAG.
 - *Static* — LACP is disabled on the LAG.

- **LAG Type** — Displays the LAG type. The possible field values are:
 - *100 MB copper*
 - *1000 MB copper*
- **Admin Status** — Enables or disables traffic forwarding through the selected LAG. The possible field values are:
 - *Up* — Traffic forwarding is enabled through this LAG.
 - *Down* — Traffic forwarding is disabled through this LAG.
- **Current Status** — Indicates if the LAG is currently up or down.
- **Oper Duplex** — Indicates the LAG's duplex type when auto-negotiation is disabled. The possible values are:
 - *Half* — LAG operates in half-duplex.
 - *Full* — LAG operates in full-duplex.
- **Reactivate Suspended** — Reactivates a LAG if the LAG has been disabled. A LAG is **suspended** if a Lock Port action has been applied on a LAG member.
- **Operational Status** — Defines whether the port is currently operational or non-operational.
- **Admin Auto Negotiation** — Enables or disables Auto Negotiation on the LAG. Auto-negotiation is a protocol between two link partners that enables a LAG to advertise its transmission rate, duplex mode and flow control (the flow control default is disabled) abilities to its partner.
- **Current Auto Negotiation** — The current Auto Negotiation setting.
- **Admin Speed** — The configured speed at which the LAG is operating. The auto negotiation should be disabled before setting the speed manually.
- **Current Speed** — The current speed at which the LAG is operating.
- **Admin Flow Control** — Enables or disables flow control or enables the auto negotiation of flow control on the LAG.
- **Current Flow Control** — The user-designated Flow Control setting.

- **Admin Advertisement** — Specifies the capabilities to be advertised by the LAG. The possible field values are:
 - *Max Capability* — Indicates that all port speeds and Duplex mode settings can be accepted.
 - *10 Half* — Indicates that the port is advertising a 10 mbps speed and half Duplex mode setting.
 - *10 Full* — Indicates that the port is advertising a 10 mbps speed and full Duplex mode setting.
 - *100 Half* — Indicates that the port is advertising a 100 mbps speed and half Duplex mode setting.
 - *100 Full* — Indicates that the port is advertising a 100 mbps speed and full Duplex mode setting.
 - *1000 Full* — Indicates that the port is advertising a 1000 mbps speed and full Duplex mode setting.
- **Current Advertisement** — The port advertises its capabilities to its neighbor port to start the negotiation process. The possible field values are those specified in the Admin Advertisement field.
- **Neighbor Advertisement** — The neighbor port (the port to which the selected interface is connected) advertises its capabilities to the port to start the negotiation process. The possible values are those specified in the Admin Advertisement field.
- **Unit No.** — Indicates the stacking member being managed.
- **Eth/Gigabit Static** — Select the ports to join to the LAG.

STEP 2 Define the relevant fields.

STEP 3 Click **Save & Close** to save the modifications and close the *LAG Aggregation Screen* (clicking **Save** keeps the *LAG Aggregation Screen* open).

LACP

Aggregate ports can be linked into link-aggregation port groups. Each group is comprised of ports with the same speed, set to full-duplex operations.

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

To define LACP settings:

STEP 1 Click **Port Management > LACP**. The *LACP Screen* opens.

Figure 15 LACP Screen

LINKSYS®
A Division of Cisco Systems, Inc.

24-Port 1

Port Management

SetupPort ManagementVLAN ManagementStatisticsACLNetwork SecuritySecurity SuiteQoSSpanning TreeMulticastSNMPAdminLogout

Port Settings | Link Aggregation | LACP

LACP

System Priority

Port Priority

LACP Port Table

LACP System Priority (1-65535)

6

Port

e1

LACP Port Priority

8

LACP Timeout

Long

Admin Key

0

Update

<<Previous123Next>>

Port	Port Priority	LACP Timeout	Admin Key
e1	8	Long	0
e2	1	Long	0
e3	1	Long	0
e4	1	Long	0
e5	1	Long	0
e6	1	Long	0
e7	1	Long	0
e8	1	Long	0
e9	1	Long	0
e10	1	Long	0
e11	1	Long	0
e12	1	Long	0

232624

The *LACP Screen* is divided into the following areas for configuring LACP LAGs:

- System Priority
- Port Priority
- LACP Port Table

The *System Priority* area contains the following field:

- **LACP System Priority (1-65535)** — Indicates the global LACP priority value. The possible range is 1- 65535. The default value is 1.

The *Port Priority* area contains the following fields:

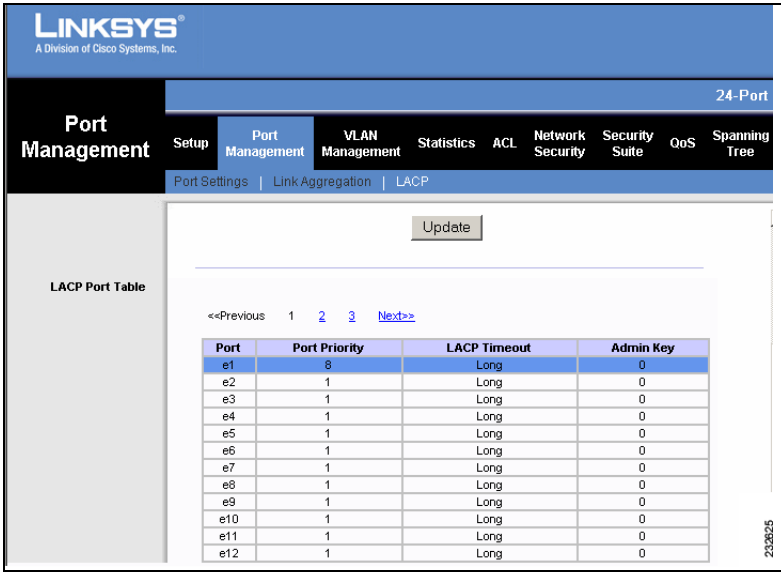
- **Unit No.** — Indicates the stacking member being managed.
- **Port** — Defines the port number to which timeout and priority values are assigned.
- **LACP Port Priority** — Defines the LACP priority value for the port. The field range is 1-65535.
- **LACP Timeout** — Administrative LACP timeout. The possible field values are:
 - *Short* — Defines a short timeout value.
 - *Long* — Defines a long timeout value. This is the default value.
- **Admin Key** — A value assigned to a LAG.

STEP 2 Define the relevant fields.

STEP 3 Click **Update** to save the modifications. The changes appear in the LACP Port Table and the device is updated.

For 24-port devices, the *LACP Screen* displays the ports on multiple screens. To browse to a specific port entry, click the **Previous**, **1**, **2**, **3**, and **Next** links above the table.

Figure 16 LACP Port Table



VLAN Management

The VLAN Management configuration options are as follows:

- Create VLAN
- VLAN Port Settings
- Ports to VLAN
- Configuring Q-in-Q
- VLAN to Port
- GVRP
- Multicast TV Membership
- Multicast TV Membership
- Multicast TV VLAN - IGMP Mapping
- CPE VLAN Mapping

Create VLAN

The *Create VLAN Screen* provides information and global parameters for configuring and working with VLANs.

To create a new VLAN:

- STEP 1** Click **VLAN Management > Create VLAN**. The *Create VLAN Screen* opens.

Figure 17 Create VLAN Screen

LINKSYS®
A Division of Cisco Systems, Inc.

VLAN Management 24-Port

Setup Port Management **VLAN Management** Statistics ACL Network Security Security Suite QoS Spanning Tree Multicast SNMP Admin Logout

Create VLAN | Port Setting | Port to VLAN | VLAN to Port | GVRP | Multicast TV VLAN | More...>>

Create VLAN

Single VLAN

VLAN ID:

VLAN Name:

VLAN Range

VLAN Range: -

VLAN Table

VLAN ID	VLAN NAME	Status
1		Default
2		Static
1000		Static
1001		Static
1002		Static
1003		Static
1004		Static

Total existing VLANs: 255

The *Create VLAN Screen* is divided into the following areas:

- Single VLAN
- VLAN Range
- VLAN Table

The Single VLAN area contains the following fields:

- **VLAN ID** — Indicates the ID number of the VLAN being configured. The possible range is 2-4093 (for SPS-208 and SPS-224G4) or 2-4094 (for SPS-2024)2-40934094. Up to 255 VLANs can be created. This field is used to add VLANs one at a time. To add the defined VLAN ID number, press **Add**.
- **VLAN Name** — Defines the VLAN name.

The VLAN Range area contains the following field:

- **VLAN Range** — Indicates a range of VLANs (up to 20 at a single time) being configured. To add the defined range of VLAN ID numbers, press **Add Range**.

In addition to fields described previously, the VLAN Table area contains the following fields:

- **Status** — Indicates the VLAN type. The possible field values are:
 - *Static* — Indicates the VLAN is user-defined.
 - *Default* — Indicates the VLAN is the default VLAN.
- **Total Existing VLANs** — Indicates the total number of defined VLANs on the device.

STEP 2 Define the **VLAN ID** and **VLAN Name** and click **Add**, or define the **VLAN Range** and click **Add Range**. The VLAN details appear in the **VLAN Table** and the device is updated.

To delete a VLAN from the device:

STEP 3 In the VLAN Table, select the VLAN.

STEP 4 Click **Delete**. The selected VLAN is deleted from the device.

VLAN Port Settings

The *VLAN Port Settings Screen* provides parameters for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the *VLAN Port Settings Screen*. All untagged packets arriving at the device are tagged by the ports PVID.

To modify the VLAN ports settings:

- STEP 1** Click **VLAN Management > Port Settings**. The *VLAN Port Settings Screen* opens.

Figure 18 VLAN Port Settings Screen

Port	Mode	Acceptable Frame Type	PVID	Ingress Filtering	LAG	Multicast TV Vlan
e1	Access	All	2	<input checked="" type="checkbox"/>		
e2	Access	All	1	<input checked="" type="checkbox"/>		
e3	Access	All	1	<input checked="" type="checkbox"/>		
e4	Access	All	1	<input checked="" type="checkbox"/>		
e5	Access	All	1	<input checked="" type="checkbox"/>		
e6	Access	All	1	<input checked="" type="checkbox"/>		
e7	Access	All	1	<input checked="" type="checkbox"/>		
e8	Access	All	1	<input checked="" type="checkbox"/>		
e9	Access	All	1	<input checked="" type="checkbox"/>		
e10	Access	All	1	<input checked="" type="checkbox"/>		
e11	Access	All	1	<input checked="" type="checkbox"/>		
e12	Access	All	1	<input checked="" type="checkbox"/>		

For 8-port devices, the *VLAN Port Settings Screen* displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, and **Next** links above the table.

For 24-port devices, the *VLAN Port Settings Screen* displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, **3**, and **Next** links above the table.

The *VLAN Port Settings Screen* contains the following fields:

- **Unit No.** — Indicates the stacking member being managed.

- **Port** — Indicates the port number.
- **Mode** — Indicates 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 VLANs are tagged, except for one VLAN that is untagged. Ingress filtering cannot be enabled or disabled on a trunk port.
 - *Customer* — Indicates that the port is used in Q-in-Q configuration. Packets egressing through this port are encapsulated into the outer VLAN and classified according to the port's VLAN ID. Packets ingressing from this port are transferred after the outer VLAN is extracted.
- **Acceptable Frame Type** — Packet type accepted on the port. The possible values are:
 - *Tagged* — Indicates that only tagged packets are accepted on the port.
 - *All* — Indicates that both tagged and untagged packets are accepted on the port.
- **PVID** — Assigns a VLAN ID to untagged packets. The possible values are 1 to 4093, and 4095. VLAN 4095 is defined as per standard and industry practice as the discard VLAN. Packets classified to the Discard VLAN are dropped.
- **Ingress Filtering** — Enables or disables Ingress filtering on the port. Ingress filtering discards packets that do not match port ingress rules. Ingress Filtering can be disabled only on ports in Multiple User or Multiple Session modes.
- **LAG** — Indicates to which LAG this port belongs. If the port is a LAG member, the LAG settings override the port settings.
- **Multicast TV VLAN** — Indicates if the port is joined to a Multicast TV VLAN, enabling multicast TV transmissions to egress to subscribers through this port. The Port **Mode** must be defined as *Access*. Packets passing through the port are untagged.

- STEP 2
- Define the relevant fields.
- STEP 3
- Click **Save Settings** to save the VLAN port modifications. The device is updated.

Ports to VLAN

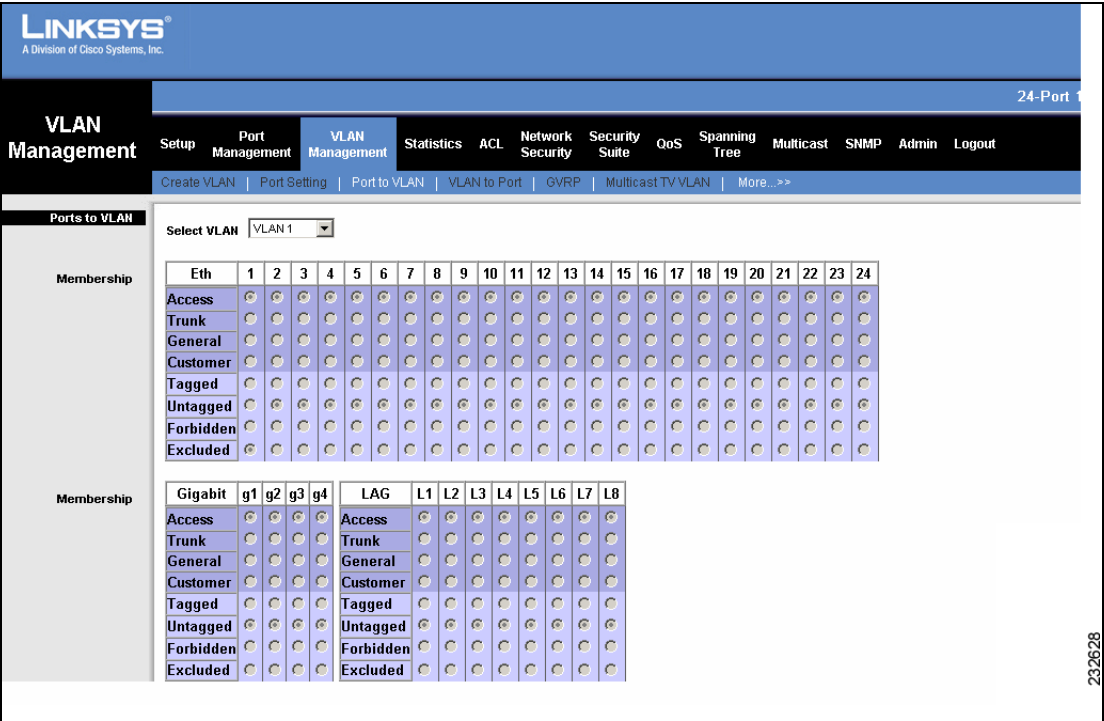
The *Ports To VLAN Screen* contains fields for configuring ports to a VLAN. The port default VLAN ID (PVID) is configured on the *Create VLAN Screen*. All untagged packets arriving at the device are tagged by the ports PVID.

The *Ports To VLAN Screen* contains Membership Tables for Ethernet ports, Gigabit ports, and LAGs. Ports and LAGs are assigned VLAN membership by selecting and configuring the presented configuration options. Ports can have the following configuration options:

To assign VLAN membership to ports:

- STEP 1
- Click **VLAN Management > Ports to VLAN**. The *Ports To VLAN Screen* opens.

Figure 19 Ports To VLAN Screen



The *Ports To VLAN Screen* contains the following fields:

- **Select VLAN** — Indicates the VLAN for which the port membership is configured.
- **Unit No.** — Indicates the stacking member being managed.

Each port's mode is indicated in the table, and is configurable in the *VLAN Port Settings Screen*. Possible port modes are:

- **Access** — Indicates a port belongs to a single untagged VLAN.
- **Trunk** — Indicates the port belongs to VLANs in which all VLANs are tagged, except for one VLAN that is untagged.
- **General** — Indicates the port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full IEEE802.1q mode).
- **Customer** — The port belongs to a VLAN in which all ports are untagged.

Configuration options are as follows:

- **Tagged** — Defines the interface as a tagged member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.
- **Untagged** — Packets forwarded by the interface are untagged.
- **Forbidden** — Port cannot be included in the VLAN.
- **Excluded** — Excludes the interface from the VLAN.

STEP 2 Click **Show All** to display a list showing all the items through which you can scroll.

Figure 20 Show All Ports Table

Show All			
Port	Mode	PVID	VLANs
e1	Access	2	2U
e2	Access	1	1U
e3	Access	1	1U
e4	Access	1	1U
e5	Access	1	1U
e6	Access	1	1U
e7	Access	1	1U
e8	Access	1	1U
e9	Access	1	1U
e10	Access	1	1U
e11	Access	1	1U
e12	Access	1	1U
e13	Access	1	1U
e14	Access	1	1U
e15	Access	1	1U
e16	Access	1	1U
e17	Access	1	1U
e18	Access	1	1U
e19	Access	1	1U
e20	Access	1	1U
e21	Access	1	1U
e22	Access	1	1U
e23	Access	1	1U
e24	Access	1	1U
g1	Access	1	1U
g2	Access	1	1U
g3	Access	1	1U
g4	Access	1	1U
LAG 1	Access	1	1U
LAG 2	Access	1	1U
LAG 3	Access	1	1U
LAG 4	Access	1	1U

The *Show All Ports Table* contains the following columns:

- **Port** — Lists the Ethernet ports, Gigabit ports, and LAGs.
- **Mode** — Indicates the possible port mode: Access, Trunk, General, or Customer.
- **PVID** — Indicates the port default VLAN ID.
- **VLANs** — Indicates the VLAN for which the port membership is configured.

STEP 3 Select the relevant configuration options for the interfaces that are included in the VLAN.

STEP 4 Click **Save Settings** to save the VLAN membership configuration. The device is updated.

Configuring Q-in-Q

Q-in-Q (also called Stackable VLANs) enables service providers to aggregate all of a specific customer's traffic into a single VLAN, therefore dedicating the VLAN exclusively to that customer, even if the customer's network consists of multiple VLANs.

Q-in-Q Overview

Q-in-Q tagging allows network managers to add a service tag to previously tagged packets. The added tag provides a VLAN ID to each customer, ensuring transparent and secure network traffic. In a Q-in-Q supported VLAN, traffic coming in through ingress ports are forwarded unmodified through egress ports throughout the network, where the added tag is removed. For example, transmitted VLAN-tagged frames arrive at their destinations with their VLAN tags preserved.

The designated port then provides additional services to the packets with the double-tags, allowing administrators to expand service to VLAN users. Additionally, the VLAN's customers cannot send traffic to, or see, traffic belonging to other customers.

Q-in-Q (also called Stackable VLANs) enables service providers to concentrate all of a specific customer's VLANs into a single VLAN, therefore dedicating the VLAN exclusively to that customer, even if the customer's network consists of multiple VLANs. This lets large ISPs create L2 Virtual Private Networks and transparent LANs for their customers, which will connect two or more customer nodes over the network without complex configurations on the client's side.

Q-in-Q has several advantages, such as:

- Added security via robust isolation of customer traffic. The VLAN's customers cannot send traffic to, nor see traffic belonging to other customers.
- Backward compatibility which preserves existing customer VLAN structures. Customers may send VLAN-tagged frames and those frames will retain the same VLAN tags when they arrive at their destination.
- Simplified operation, because the service provider does not have to manage the configurations of customer equipment devices.
- Increased VLAN scalability, providing up to 4000 private VLANs per subscriber, up to 4000 subscribers.

Q-in-Q Implementation

The following describes the Q-in-Q implementation when the system transmits customer data from customer port to another customer port across a service provider network.

1. Incoming traffic on an ingress port is assigned to a service-provider-assigned VLAN regardless of the frame content. If the received frame is VLAN-Tagged, the VLAN-tag is considered part of the frame's data.
2. Outgoing traffic to the service provider's network through a tagged port. The original packet is encapsulated, and a VLAN Tag with the VID of the service-provider assigned VLAN is added to the frame as it goes out. If the frame was originally tagged, the new VLAN tag adds a second (outer) level of tagging. The service VLAN tagging format complies with IEEE802.1Q, and 0x8100 is used as a tag-indicator value.
3. Incoming traffic from the service provider's network is considered tagged and assigned to the service-provider-assigned VLAN. This prevents the packets from travelling through ports assigned to other customers.
4. Customer-mode ports (through which frames are sent to customers) are untagged members of the service-provider-assigned VLAN. Therefore, no VLAN tag is added to the frame. If the frame is tagged, the original tag remains part of the data. The customer can send frames tagged with a temporary VLAN ID, and the original tag is preserved during transmission through the service provider's network.

VLANs in Customer mode are untagged. A port in a Customer VLAN handles traffic in any of the following ways:

Received Frame Type	Destination Port Type	Resulting Frame Type
Tagged	Tagged (Trunk or General)	Customer port forwards Double-tagged frames, containing the tag it received from the sender and the destination port tag.
Tagged	Untagged (Customer, General, or Access)	Customer port forwards single-tagged frame, containing the tag it received from the sender.
Untagged	Tagged (Trunk or General)	Customer port forwards single-tagged frame, containing the destination port tag.
Untagged	Untagged (Customer, General, or Access)	Customer port forwards untagged frame.



NOTE

- A port in Customer mode can support many users, but all the users must belong to the same VLAN.
- A user may be assigned to multiple ports, but all the ports must have the same VLAN ID.
- Uplink ports may be defined in either General VLAN mode or LAG VLAN mode.

To configure customer VLANs:

- STEP 1** Click **VLAN Management > Create VLAN**.
- STEP 2** In the *Create VLAN Screen*, create and configure a new VLAN ID (see *Create VLAN*).
- STEP 3** Click **VLAN Management > Port Settings**.
- STEP 4** In the *VLAN Port Settings Screen*, define the ingress ports that operate in Customer mode (see *VLAN Port Settings*).
- STEP 5** Click **VLAN Management > Ports to VLAN**.
- STEP 6** In the *Ports to VLAN Screen*, define all the VLAN Member egress ports that attach VLAN tags to packets passing through them (see *Ports to VLAN*).

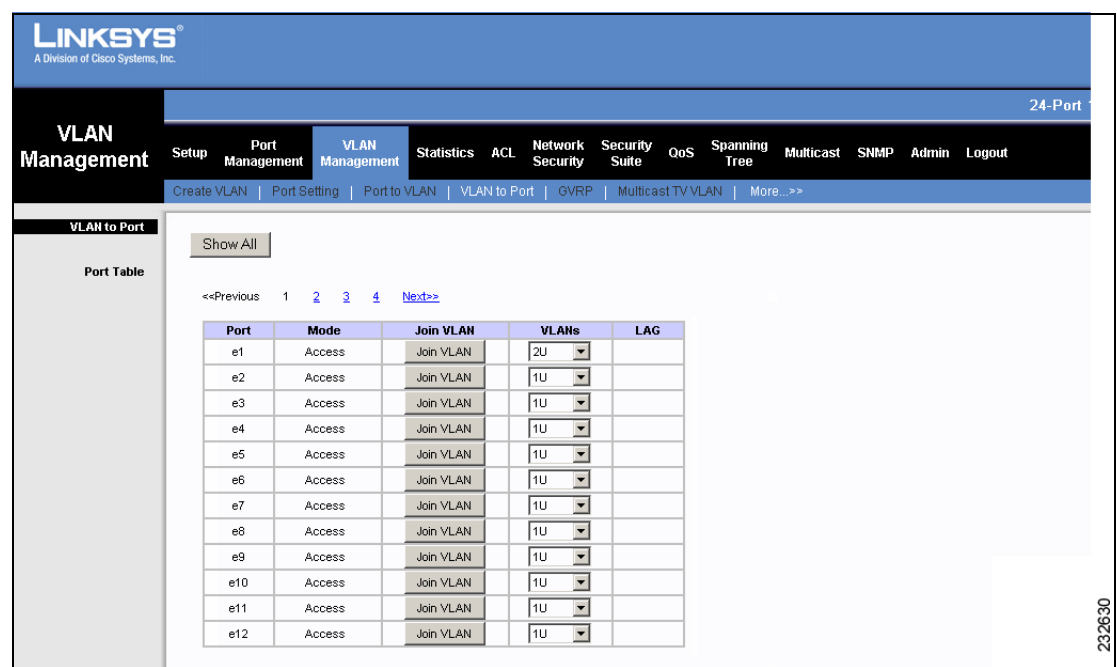
VLAN to Port

The *VLAN To Port Screen* contains fields for configuring VLANs to ports.

To add VLAN membership to a port:

STEP 1 Click **VLAN Management > VLAN to Port**. The *VLAN To Port Screen* opens.

Figure 21 VLAN To Port Screen



For 24-port devices, the *VLAN to Port Screen* displays the ports on multiple screens. To browse to a specific port entry, click the **Previous**, **1**, **2**, **3**, and **Next** links above the table.

The *VLAN To Port Screen* contains the following fields:

- **Unit No.** — Indicates the stacking member being managed.
- **Port** — Displays the port number.
- **Mode** — Indicates 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.

- *Trunk* — Indicates the port belongs to VLANs in which all VLANs are tagged, except for one VLAN that is untagged.
- *Customer* — The port belongs to a VLAN in which all ports are untagged.
- **Join VLAN** — Defines the VLANs to which the interface is joined. Pressing the Join VLAN button displays the *Join VLAN to Port Screen*. Select the VLAN to which to add the port, select the VLANs to be tagged or untagged and click **Add**. To remove the VLAN allocation to the port, select the VLAN already assigned to the port and click **Remove**.
- **VLANs** — Specifies the VLAN in which the port is a member.
- **LAG** — if the port is a member of a LAG, the LAG number is displayed. A member of a LAG cannot be configured to a VLAN, but that same LAG can be configured to a VLAN.

STEP 2 Click **Show All** to display a list showing all the items through which you can scroll.

Figure 22 Show All Ports Table

Show All			
Port	Mode	PVID	VLANs
e1	Access	2	2U
e2	Access	1	1U
e3	Access	1	1U
e4	Access	1	1U
e5	Access	1	1U
e6	Access	1	1U
e7	Access	1	1U
e8	Access	1	1U
e9	Access	1	1U
e10	Access	1	1U
e11	Access	1	1U
e12	Access	1	1U
e13	Access	1	1U
e14	Access	1	1U
e15	Access	1	1U
e16	Access	1	1U
e17	Access	1	1U
e18	Access	1	1U
e19	Access	1	1U
e20	Access	1	1U
e21	Access	1	1U
e22	Access	1	1U
e23	Access	1	1U
e24	Access	1	1U
g1	Access	1	1U
g2	Access	1	1U
g3	Access	1	1U
g4	Access	1	1U
LAG 1	Access	1	1U
LAG 2	Access	1	1U
LAG 3	Access	1	1U
LAG 4	Access	1	1U
LAG 5	Access	1	1U
LAG 6	Access	1	1U
LAG 7	Access	1	1U
LAG 8	Access	1	1U

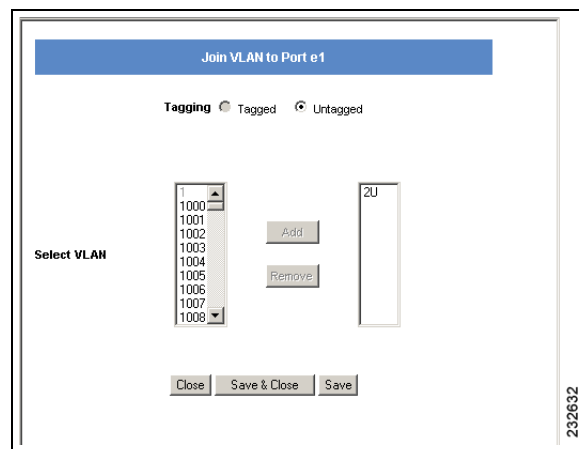
232631

The *Show All Ports Table* contains the following columns:

- **Port** — Lists the Ethernet ports, Gigabit ports, and LAGs.
- **Mode** — Indicates the possible port mode: Access, Trunk, General, or Customer.
- **PVID** — Indicates the port default VLAN ID.
- **VLANs** — Indicates the VLAN for which the port membership is configured.

STEP 3 In the *VLAN To Port* table, click **Join VLAN** in the relevant port entry. The *Join VLAN To Port Screen* opens.

Figure 23 Join VLAN To Port Screen



STEP 4 Define the selected VLAN as *Tagged* or *Untagged*.

STEP 5 From the left list, select the relevant VLAN and click **Add**. The selected VLAN then appears in the right list. Up to 20 VLANs at a single time may be joined to the port.

STEP 6 Click **Save & Close** to save the modifications and close the *Join VLAN To Port Screen* (clicking **Save** keeps the *Join VLAN To Port Screen* open).

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.

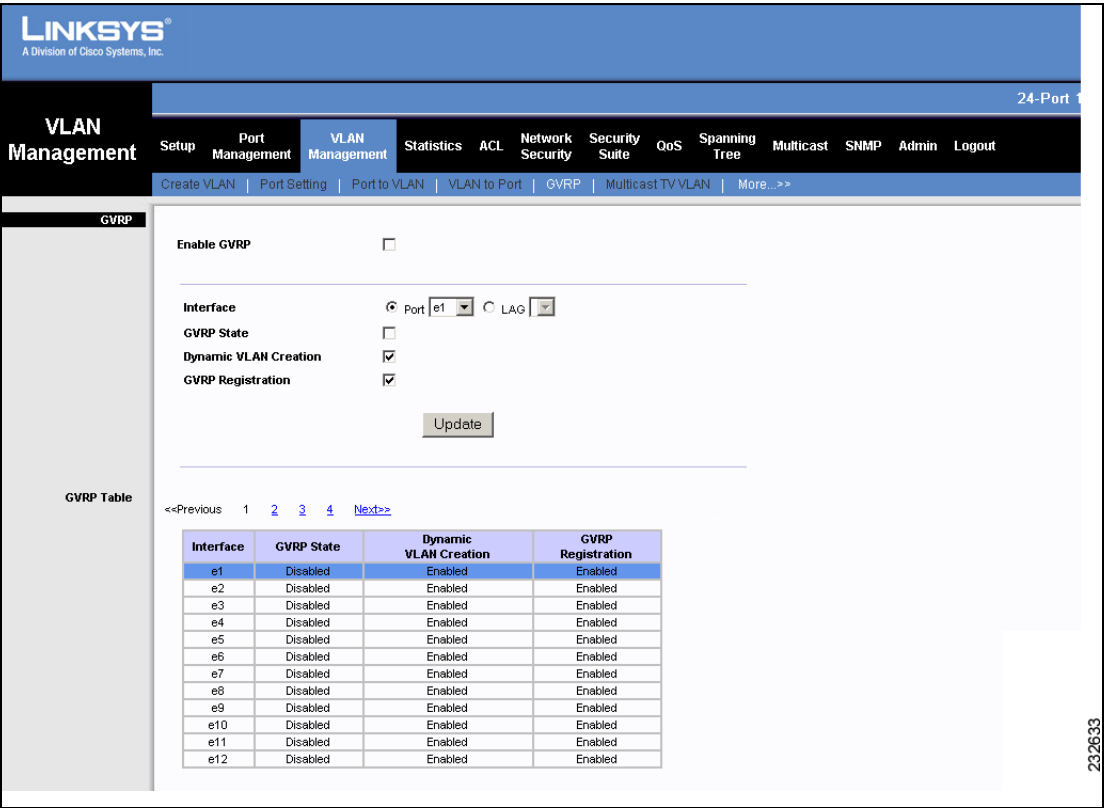
In the *GVRP Screen*, users can do the following tasks, and the results are displayed in the GVRP Table:

- Configuring GVRP
- Enabling/Disabling GVRP on a port /LAG

To define GVRP on the device:

STEP 1 Click **VLAN Management > GVRP**. The *GVRP Screen* opens.

Figure 24 GVRP Screen



The *GVRP Screen* is divided into the following areas:

- GVRP Parameters
- GVRP Table

The GVRP Parameters area contains the following fields:

- **Enable GVRP** — Enable or disable GVRP on the device. The possible field values are:
 - *Checked* — Enables GVRP on the device.
 - *Unchecked* — Disables GVRP on the device.
- **Interface** — Displays the port or LAG number on which GVRP is enabled.
- **GVRP State** — Enable or disable GVRP on the selected interface. The possible field values are:
 - *Checked* — Enables GVRP on the selected interface.
 - *Unchecked* — Disables GVRP on the selected interface.
- **Dynamic VLAN Creation** — Enable or disable Dynamic VLAN creation on the interface. The possible field values are:
 - *Checked* — Enables Dynamic VLAN creation on the selected interface.
 - *Unchecked* — Disables Dynamic VLAN creation on the selected interface.
- **GVRP Registration** — Enable or disable VLAN registration through GVRP on the device. The possible field values are:
 - *Checked* — Enables GVRP registration on the device.
 - *Unchecked* — Disables GVRP registration on the device.

STEP 2 Select **Enable GVRP**.

STEP 3 Select the interface.

STEP 4 Define the GVRP parameters.

STEP 5 Click **Update**. The interface's GVRP parameters are displayed in the GVRP Table, and the device is updated.

For 8-port devices, the *GVRP Screen* displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, and **Next** links above the table.

For 24-port devices, the *GVRP Screen* displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, **3**, and **Next** links above the table.

STEP 6 Click **Save Settings** to save the GVRP configuration. The device is updated.

Multicast TV Membership

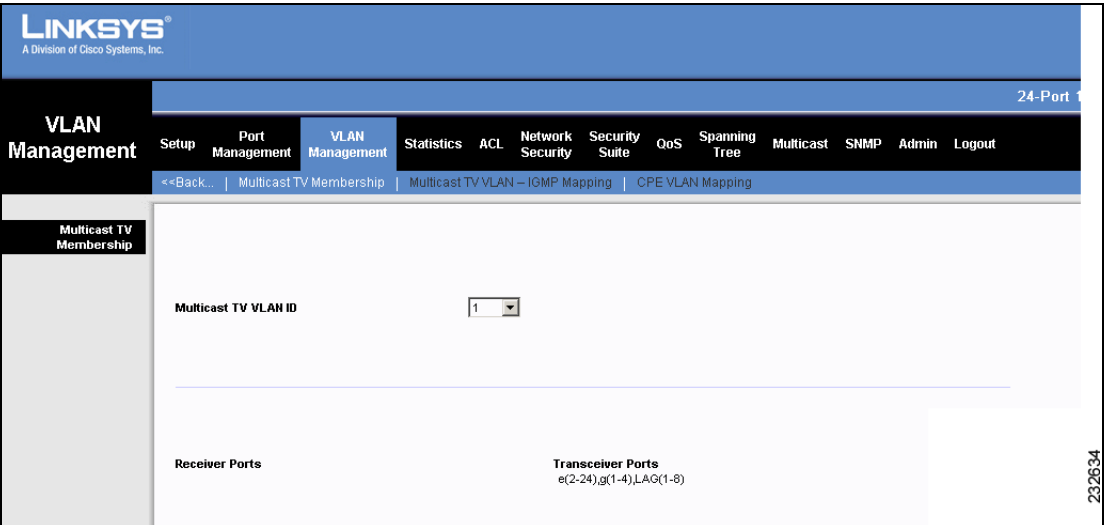
The *Multicast TV Membership Screen* displays the Multicast TV VLAN's source and receiving ports and LAGs.

- Multicast Receiver ports can display Multicast transmissions (Multicast TV VLAN or Triple Play), and can be in any VLAN. Receiver ports cannot initiate Multicast TV transmissions.
- Multicast Transceiver (source) ports may send Multicast traffic, and must be VLAN members.

To display the Multicast TV VLAN member ports and LAGs:

STEP 1 Click **VLAN Management > Multicast TV Membership**. The *Multicast TV Membership Screen* opens.

Figure 25 Multicast TV Membership Screen



The *Multicast TV Membership Screen* contains the following fields:

- **Multicast TV VLAN ID** — Defines the Multicast TV VLAN whose port membership is displayed.
- **Receiver Ports** — Indicates the interfaces which can only receive traffic from the VLAN.
- **Transceiver Ports** — Indicates the interfaces which can both transmit traffic to and receive traffic from the VLAN.

STEP 2 Select the active Multicast TV VLAN. The interfaces which are members of the VLAN are displayed.

Multicast TV VLAN

Multicast TV allows subscribers to join the same Multicast stream, even if the subscribers are not members of the same VLAN, eliminating television traffic duplication. The *Multicast TV VLAN Screen* assigns ports in Customer mode (see “*Port Settings*”) to a Multicast TV VLAN. This is required to supply Multicast transmissions to Level 2-isolated subscribers, without replicating the Multicast transmissions for each subscriber VLAN.

Any VLAN can be a Multicast TV VLAN. A port assigned to a Multicast TV VLAN:

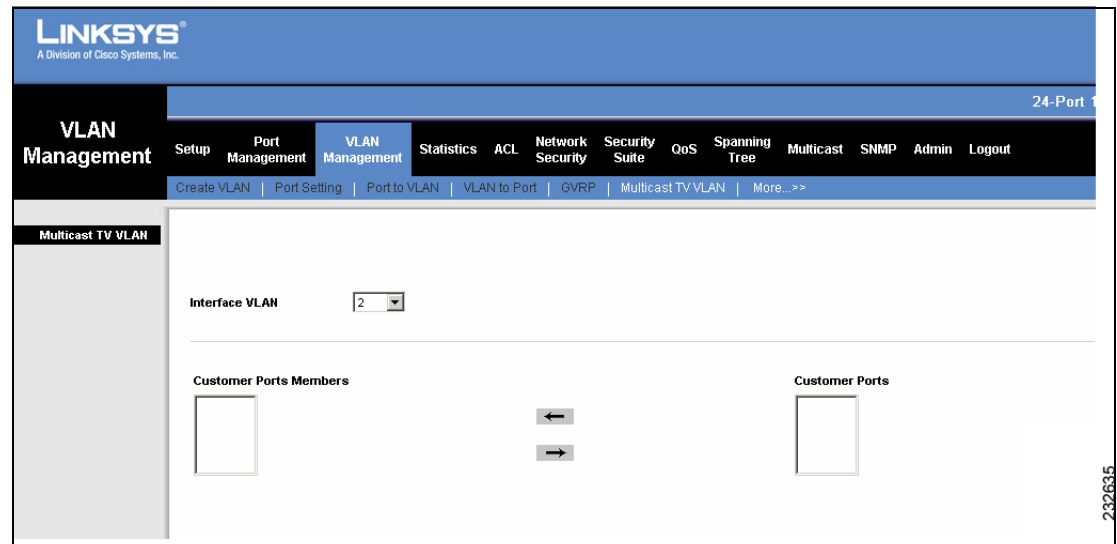
- Joins the Multicast TV VLAN.
- Packets passing through egress ports in the Multicast TV VLAN are untagged.
- The port’s Frame Type parameter is set to **Admit All**, allowing untagged packets (see “*Port Settings*”).

The Multicast TV VLAN configuration is defined per port. Multicast TV VLAN has been implemented to resemble *Multicast VLAN Registration* (MVR), which is the industry standard.

To define the Multicast TV VLAN member ports:

- STEP 1** Click **VLAN Management > Multicast TV VLAN**. The *Multicast TV VLAN Screen* opens.

Figure 26 Multicast TV VLAN Screen



The *Multicast TV VLAN Screen* contains the following fields:

- **Interface VLAN** — Defines the VLAN to which the ports are assigned.
- **Customer Ports Members** — Defines the ports already assigned to the Multicast TV VLAN.
- **Customer Ports** — Lists the ports available for assigning to the Multicast TV VLAN.

- STEP 2** Select ports from the **Customer Ports** list and click the left arrow button to move the ports to the **Customer Ports Member** list.
- STEP 3** Click **Save Settings**. Multicast TV VLAN settings are modified, and the device is updated.

Multicast TV VLAN - IGMP Mapping

IGMP messages are used to indicate which ports are requesting to join or leave the Multicast group. The *Multicast TV VLAN - IGMP Mapping Screen* allows network managers to activate IGMP snooping on Multicast TV VLANs.

To map a TV VLAN to a Multicast group:

- STEP 1** Click **VLAN Management > More > Multicast TV VLAN - IGMP Mapping**. The *Multicast TV VLAN - IGMP Mapping Screen* opens.

Figure 27 Multicast TV VLAN - IGMP Mapping Screen

The screenshot shows the Linksys web interface for VLAN Management. The top navigation bar includes links for Setup, Port Management, VLAN Management (selected), Statistics, ACL, Network Security, Security Suite, QoS, Spanning Tree, Multicast, SNMP, Admin, and Logout. Below this, a breadcrumb trail shows the path: <<Back... | Multicast TV Membership | Multicast TV VLAN - IGMP Mapping | CPE VLAN Mapping. The main content area is titled 'Multicast TV Membership' and contains a form with a 'Multicast TV VLAN ID' field set to '2'. Below this field are two sections: 'Receiver Ports' and 'Transceiver Ports' (with a sub-label 'e1'). The interface is branded with the Linksys logo and 'A Division of Cisco Systems, Inc.' in the top left corner.

The *Multicast TV VLAN - IGMP Mapping Screen* contains the following fields:

- **TV VLAN ID** — Defines the VLAN to map to the Multicast group.
- **Multicast Group** — Defines the Multicast group IP address to map to the VLAN specified in the TV VLAN ID field.

- STEP 2** Define the mapping between a VLAN and a Multicast group IP address.
- STEP 3** Click **Add to List**. The new VLAN-Multicast group mapping is displayed in the table at the bottom of the screen.
- STEP 4** Click **Save Settings**. TV VLAN-Multicast group mapping is defined, and the device is updated.

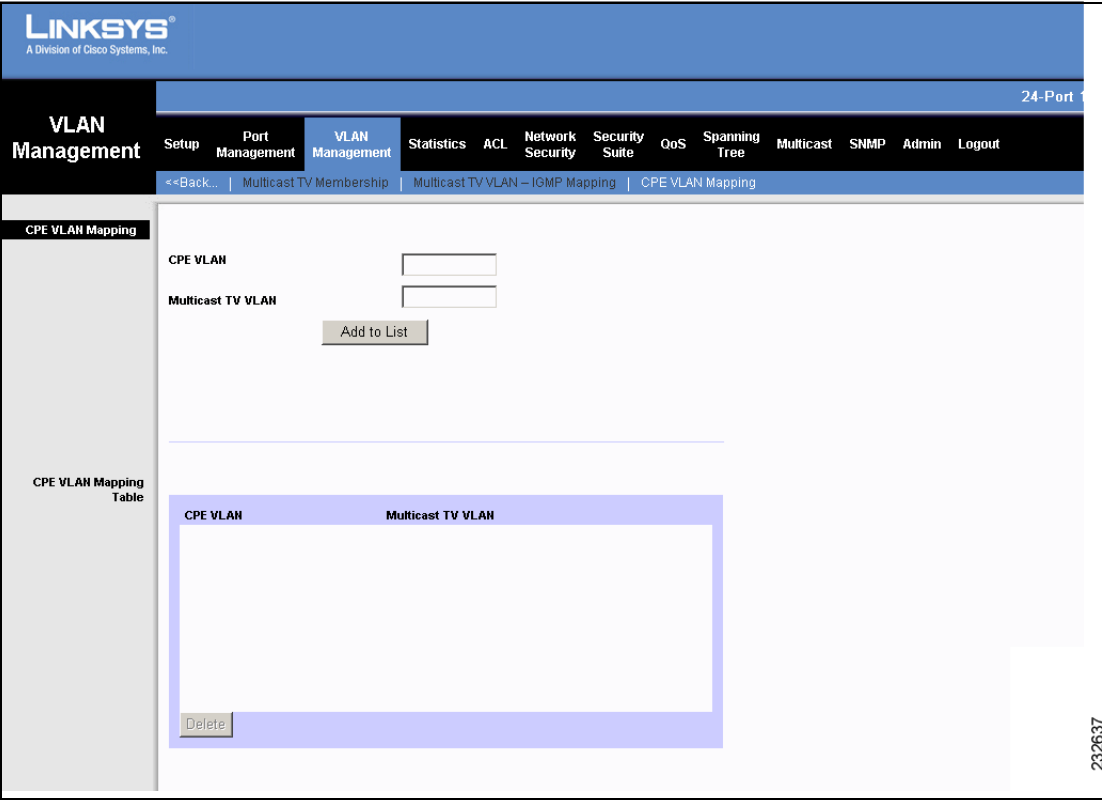
CPE VLAN Mapping

A CPE VLAN is an inner VLAN assigned to service provider customers. In a Q-in-Q configuration, the *CPE VLAN Mapping Screen* enables network managers to map CPE VLANs to Multicast TV VLANs.

To map CPE VLANs:

- STEP 1
- Click **VLAN Management > More > CPE VLAN Mapping**. The *CPE VLAN Mapping Screen* opens.

Figure 28 CPE VLAN Mapping Screen



The *CPE VLAN Mapping Screen* is divided into the following areas:

- Mapping Parameters
- CPE VLAN Mapping Table

The Mapping Parameters area contains the following fields:

- **CPE VLAN** — Indicates the CPE VLAN which is mapped to the Multicast TV VLAN.
- **Multicast TV VLAN** — Indicates the Multicast TV VLAN which is mapped to the CPE VLAN.

STEP 2 Define the mapping.

STEP 3 Click **Add to List**. The mapped VLANs are displayed in the CPE VLAN Mapping table.

The CPE VLAN Mapping Table displays the mapped VLANs.

STEP 4 Click **Save Settings**. The device is updated.

Statistics

This section describes device statistics for RMON, interfaces, GVRP, EAP, and Etherlike statistics. The Statistics configuration options are as follows:

- RMON Statistics
- RMON History
- RMON Alarms
- RMON Events
- Port Utilization
- 802.1x Statistics
- GVRP Statistics
- CPU Utilization
- Interface Statistics

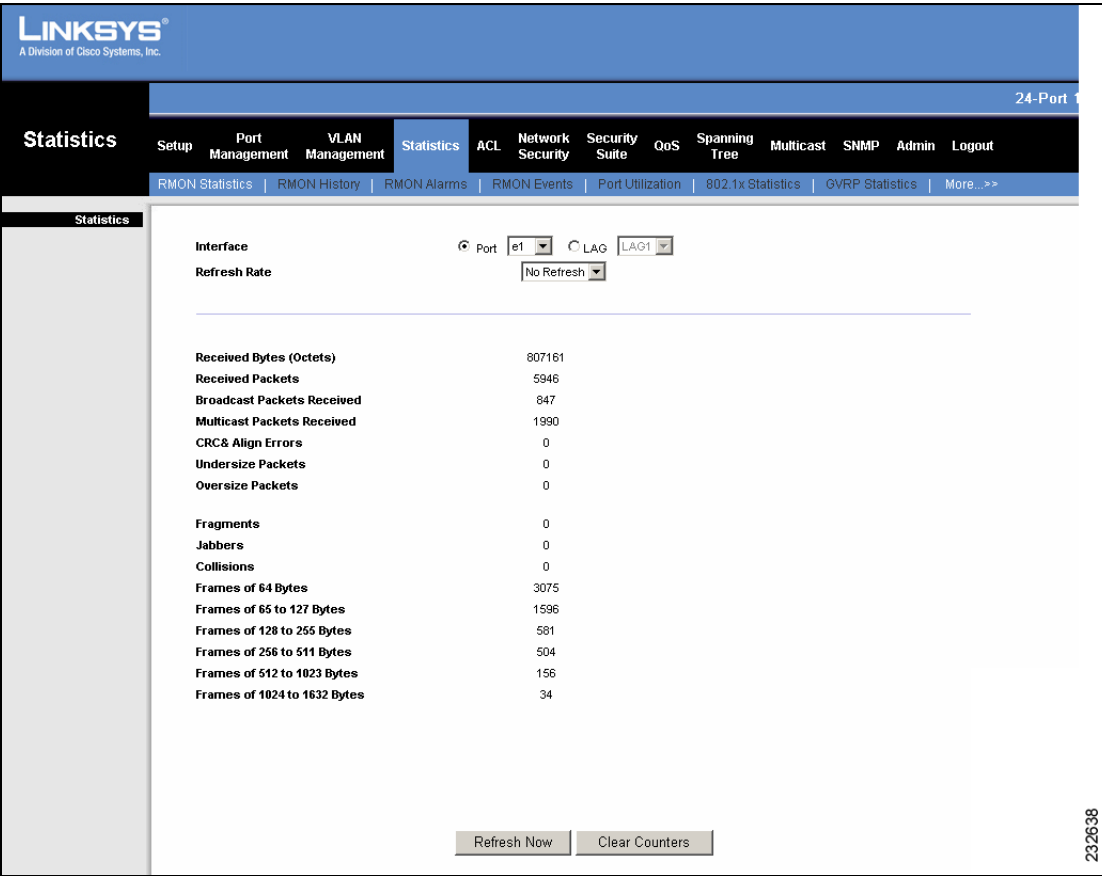
RMON Statistics

The *RMON Statistics Screen* contains fields for viewing traffic statistics and errors that occurred on the interface.

To view RMON statistics:

- STEP 1
- Click **Statistics > RMON Statistics**. The *RMON Statistics Screen* opens.

Figure 29 RMON Statistics Screen



The *RMON Statistics Screen* contains the following fields:

- **Interface** — Indicates the device for which statistics are displayed. The possible field values are:
 - *Unit No.* — Indicates the stacking member being managed.
 - *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:
 - *No Refresh* — Indicates that the RMON statistics are not refreshed.
 - *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.
- **Drop Events** — Displays the number of dropped packets since the device startup or since the counters were cleared.
- **Received Bytes (Octets)** — Displays the number of octets received on the interface since the device startup or since the counters were cleared. 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 startup or since the counters were cleared.
- **Broadcast Packets Received** — Displays the number of good Broadcast packets received on the interface since the device startup or since the counters were cleared. This number does not include Multicast packets.
- **Multicast Packets Received** — Displays the number of good Multicast packets received on the interface since the device startup or since the counters were cleared.
- **CRC & Align Errors** — Displays the number of CRC and Align errors that have occurred on the interface since the device startup or since the counters were cleared.
- **Undersize Packets** — Displays the number of undersized packets (less than 64 octets) received on the interface since the device startup or since the counters were cleared.
- **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the device startup or since the counters were cleared.

- **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 startup or since the counters were cleared.
- **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 startup or since the counters were cleared.
- **Frames of xx Bytes** — Number of *xx*-byte frames received on the interface since the device startup or since the counters were cleared.

STEP 2 Select an interface in the **Interface** field. The RMON statistics are displayed.

Resetting RMON Statistics Counters

STEP 1 Click **Statistics > RMON Statistics**. The *RMON Statistics Screen* opens.

STEP 2 Click **Clear Counters**. The RMON statistics counters are reset.

To reset the statistics counters, click the **Clear Counters** button.

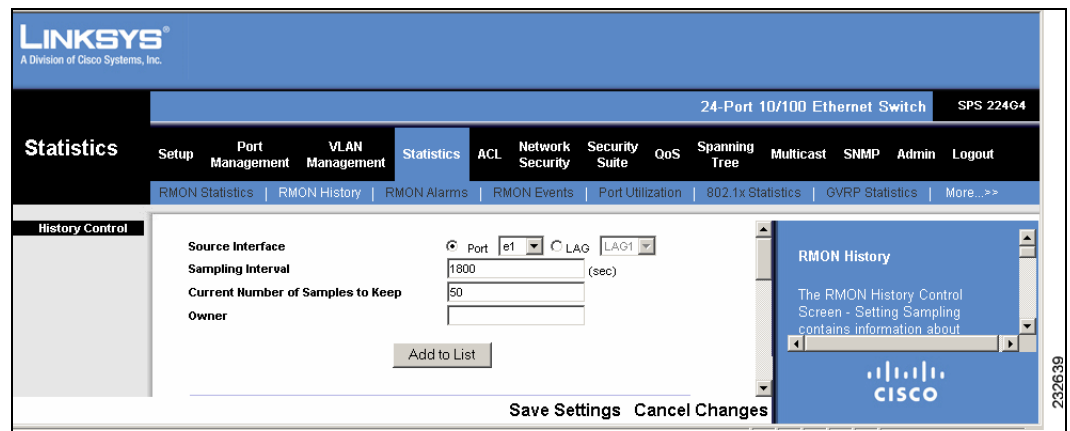
RMON History

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

To view RMON history information:

STEP 1 Click **Statistics > RMON History**. The *RMON History Control Screen* opens.

Figure 30 RMON History Control Screen - Setting Sampling



The *RMON History Control Screen* is divided into the following areas:

- RMON History
- Log Table

The RMON History area contains the following fields:

- **Source Interface** — Indicates the interface from which the history samples were taken. The possible field values are:
 - *Unit No.* — Indicates the stacking member being managed.
 - *Port* — Specifies the port from which the RMON information was taken.
 - *LAG* — Specifies the LAG 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).

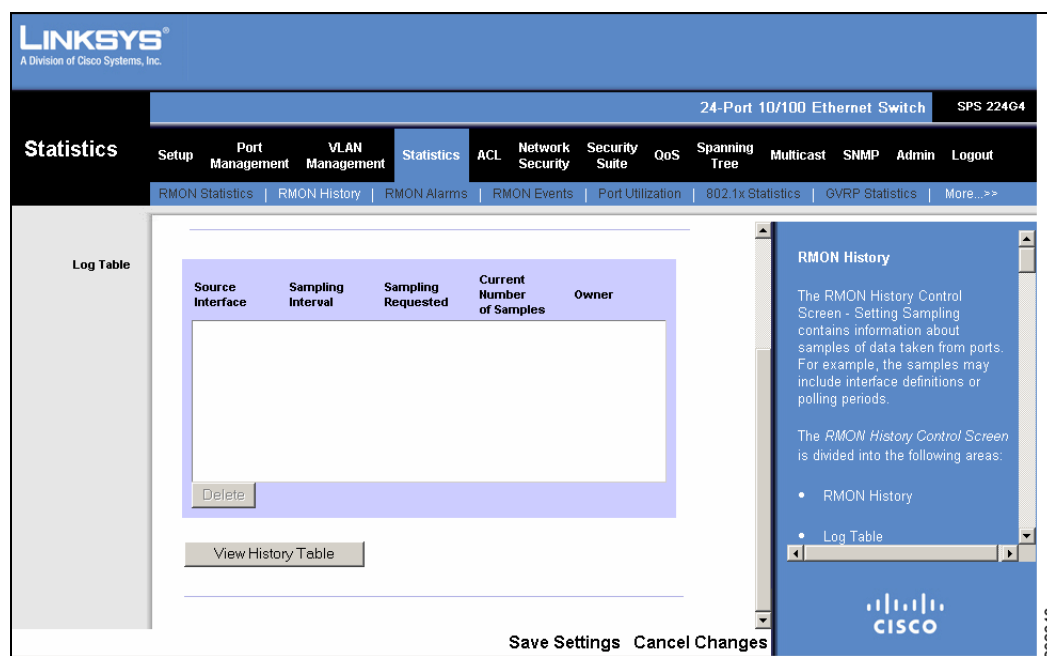
- **Current Number of Samples to Keep** — Indicates the number of samples to save.
- **Owner** — Displays the RMON station or user that requested the RMON information. The field range is 0-20 characters.

STEP 2 Define the sampling fields.

STEP 3 Click **Add To List**. The statistics from the requested sample appears in the Log Table.

The **Add to List** button adds the RMON History Table entry.

Figure 31 RMON History Control Screen - Log Table



The *RMON History Control Screen - Log Table* contains the following additional fields:

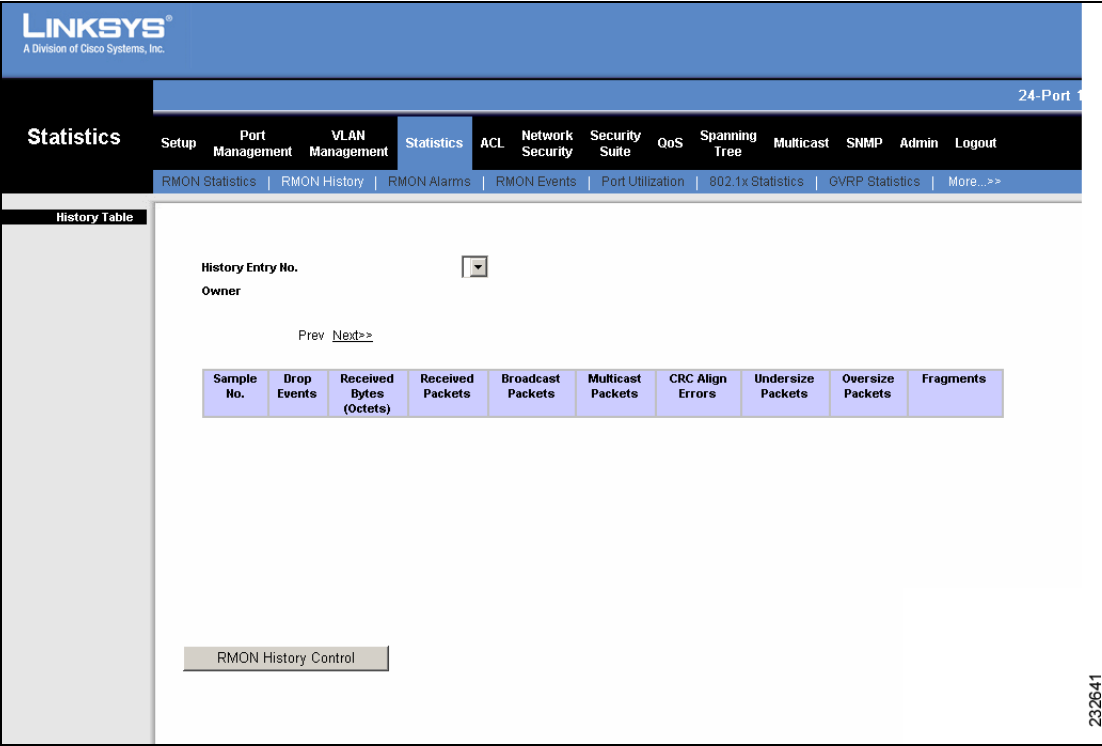
- **Sampling Requested** — Displays the number of samples to be saved. The field range is 1-65535. The default value is 50.
- **Current Number of Samples** — Displays the current number of samples taken.

STEP 4 In the *RMON History Control Screen*, click **View History Table**.

View History Table

The *View History Table* contains the specified history entry’s statistical samplings. Each table entry represents all counter values compiled during a single sample.

Figure 32 View History Table



The *View History Table* contains the following fields:

- **History Entry No.** — Displays the entry number for the History Control Log Table.
- **Owner** — Displays the RMON station or user that requested the RMON information.
- **Sample No.** — Indicates the sample number from which the statistics were taken.
- **Drop Events** — Displays the number of dropped packets since the device startup or since the counters were cleared.
- **Received Bytes (Octets)** — Displays the number of octets received on the interface since the device startup or since the counters were cleared. 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 startup or since the counters were cleared.
- **Broadcast Packets** — Displays the number of good Broadcast packets received on the interface since the device startup or since the counters were cleared. This number does not include Multicast packets.
- **Multicast Packets** — Displays the number of good Multicast packets received on the interface since the device startup or since the counters were cleared.
- **CRC Align Errors** — Displays the number of CRC and Align errors that have occurred on the interface since the device startup or since the counters were cleared.
- **Undersize Packets** — Displays the number of undersized packets (less than 64 octets) received on the interface since the device startup or since the counters were cleared.
- **Oversize Packets** — Displays the number of oversized packets (over 1518 octets) received on the interface since the device startup or since the counters were cleared.
- **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 startup or since the counters were cleared.
- **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 startup or since the counters were cleared.
- **Utilization** — Displays the percentage of the interface utilized.



NOTE Click **Next** or **Prev** to view additional History Table columns.

RMON Alarms

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

To set RMON alarms:

- STEP 1** Click **Statistics > RMON Alarms**. The *RMON Alarms Screen* opens.

Figure 33 RMON Alarms Screen

The screenshot shows the Linksys web interface for a 24-Port 10/100/1000 Ethernet Switch. The 'Statistics' tab is selected, and the 'RMON Alarms' sub-tab is active. The 'Add Alarm' section is visible, showing the following fields:

- Alarm Entry:** 1
- Interface:** Port g1 (selected), LAG Lag1 (available)
- Counter Name:** Total Bytes (Octets)- Receive
- Sample Type:** Absolute
- Rising Threshold:** (checkbox)
- Rising Event:** (dropdown)
- Falling Threshold:** (checkbox)
- Falling Event:** (dropdown)
- Startup Alarm:** Rising Alarm
- Interval:** 0
- Owner:** (text field)

An 'Add to List' button is located at the bottom right of the form.

The *RMON Alarms Screen* is divided into the following areas:

- Add Alarm
- Alarm Table

The *Add Alarm* area contains the following fields:

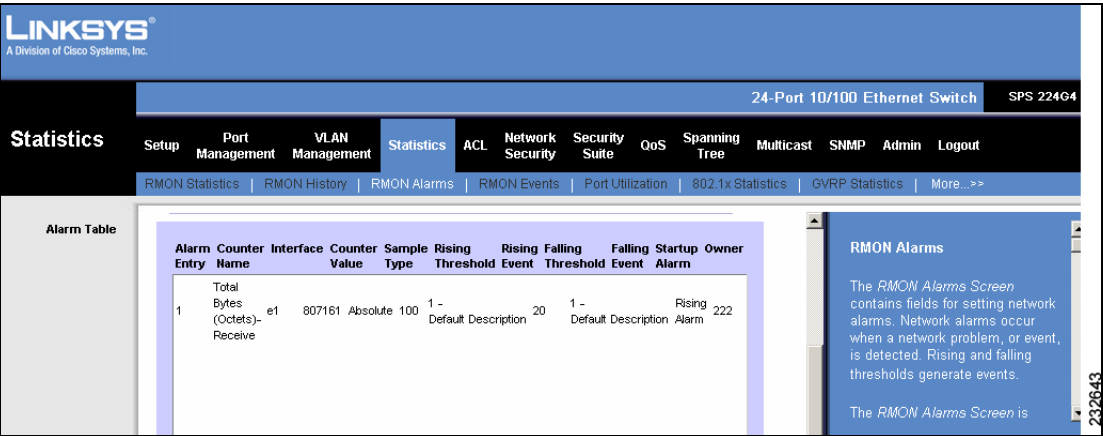
- **Alarm Entry** — Indicates a specific alarm.
- **Interface** — Indicates the interface for which RMON statistics are displayed. The possible field values are:
 - *Unit No.* — Indicates the stacking member being managed.

- *Port* — Displays the RMON statistics for the selected port.
- *LAG* — Displays the RMON statistics for the selected LAG.
- **Counter Name** — Displays the MIB variable (statistic counter type).
- **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.
- **Rising Event** — Selects an event that is defined in the Events table, which triggers the rising threshold alarm. The Events Table is displayed in the *RMON Events Screen*.
- **Falling Threshold** — Displays the falling counter value that triggers the falling threshold alarm.
- **Falling Event** — Selects an event that is defined in the Events table, which triggers the falling threshold alarm. The Events Table is displayed in the *RMON Events Screen*.
- **Startup Alarm** — Displays the trigger that activates the alarm generation. The possible field values are:
 - *Rising Alarm* — The alarm is triggered when a counter value crosses from a low-value threshold to a higher-value threshold.
 - *Falling Alarm* — The alarm is triggered when a counter value crosses from a high-value threshold to a lower-value threshold.
 - *Rising and Falling* — Both rising and falling alarms are triggers.
- **Interval** — Defines the alarm interval time in seconds.
- **Owner** — Displays the device or user that defined the alarm.

STEP 2 Define the relevant fields.

STEP 3 Click **Add To List**. The new alarm is defined, and a new alarm entry appears in the Alarm Table.

Figure 34 RMON Alarms Table



The Alarm Table area contains the following additional field:

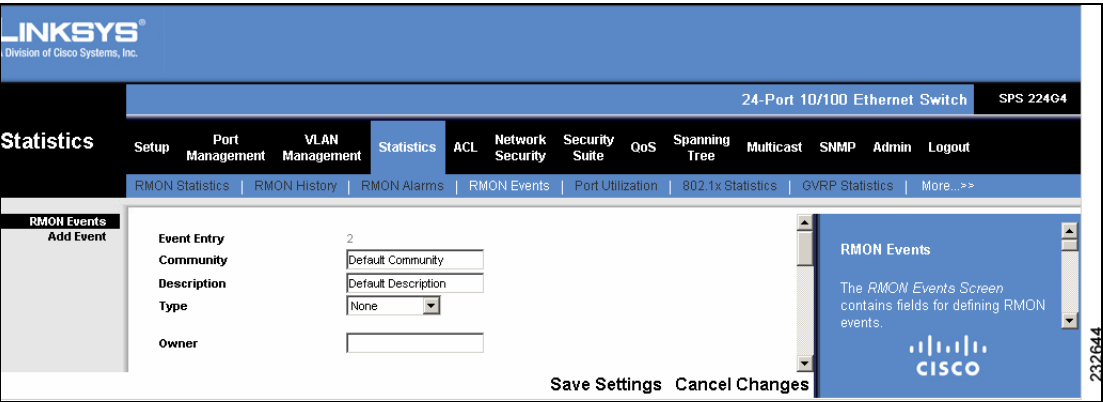
- **Counter Value** — Displays the current counter value for the particular alarm.

RMON Events

The *RMON Events Screen* contains fields for defining RMON events.
To define RMON events:

STEP 1 Click **Statistics > RMON Events**. The *RMON Events Screen* opens.

Figure 35 RMON Events Screen - Add Event Area



The *RMON Events Screen* is divided into the following areas:

- Add Event
- Event Table

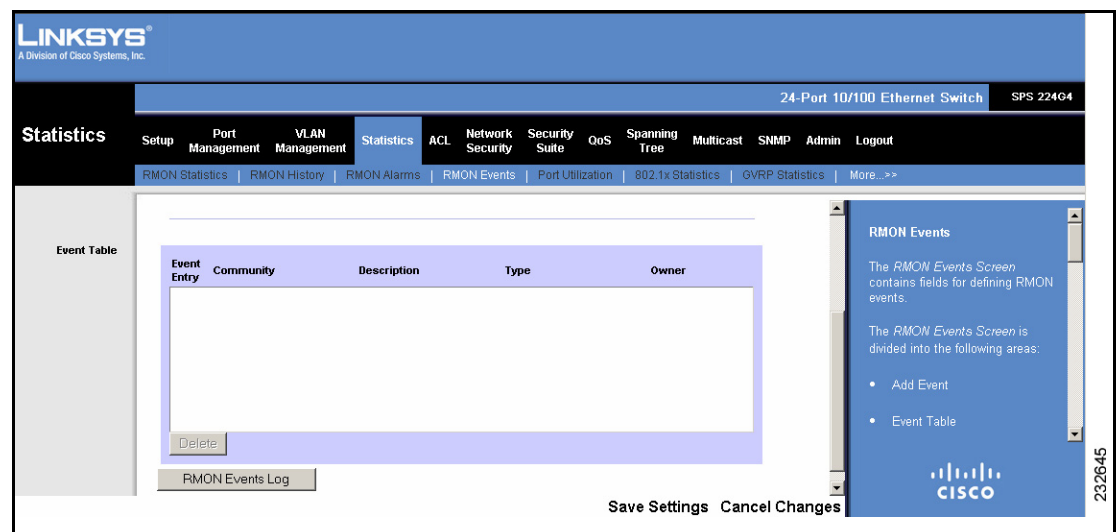
The Add Event area contains the following fields:

- **Event Entry** — Displays the event number.
- **Community** — Defines the community to which the event belongs.
- **Description** — Defines the user-defined event description.
- **Type** — Describes the event type. Possible values are:
 - *None* — Indicates that no event occurred.
 - *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.
- **Owner** — Defines the device or user that defined the event.

STEP 2 Define the relevant fields.

STEP 3 Click **Add To List**. The new event is defined, and a new event entry appears in the Event Table.

Figure 36 RMON Event Table

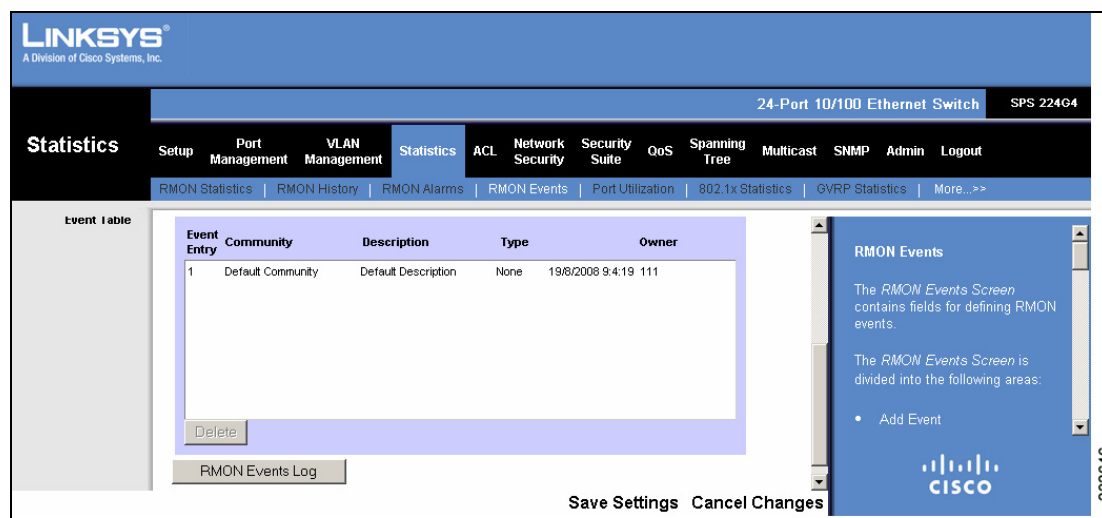


STEP 4 In the *RMON Event Table*, click **RMON Events Log**.

The **RMON Events Log** button displays the *RMON Events Logs Screen*.

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

Figure 37 RMON Events Log Screen



The *RMON Events Log Screen* 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.

To return to the *RMON Events Screen*, click the **RMON Events Control** button.

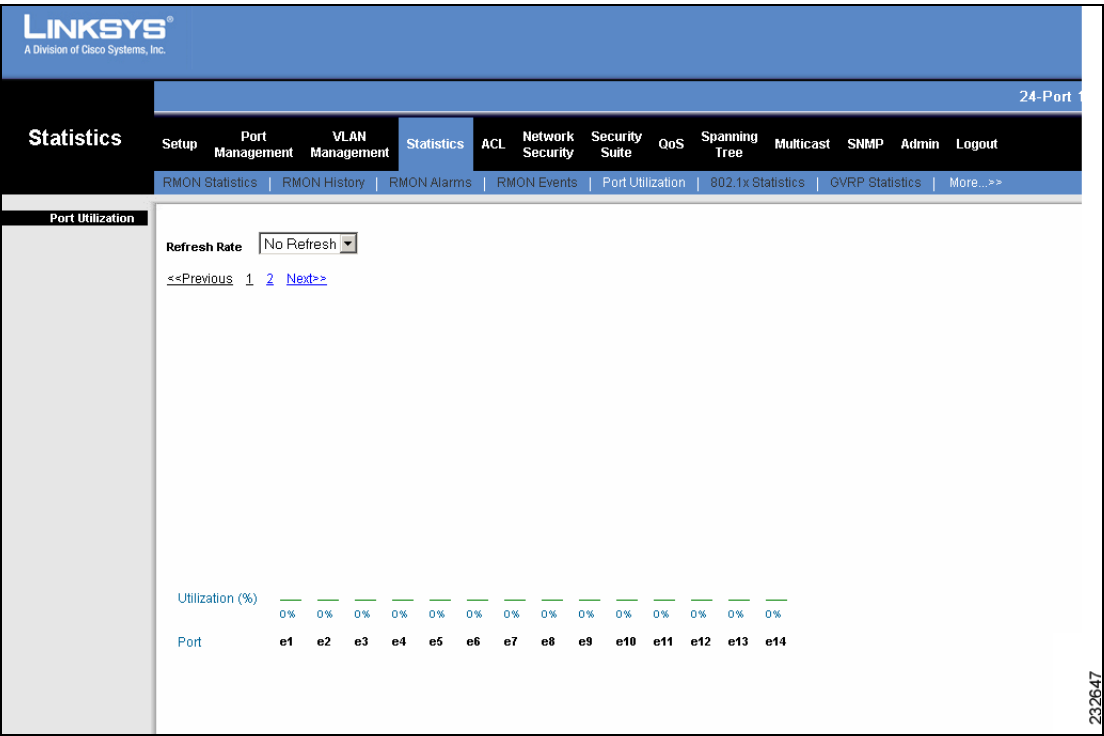
Port Utilization

The *Port Utilization Screen* displays the amount of resources each interface is currently consuming. Ports in green are functioning normally, while ports in red are currently transmitting an excessive amount of network traffic.

To view port utilization:

- STEP 1** Click **Statistics > Port Utilization**. The *Port Utilization Screen* opens.

Figure 38 Port Utilization Screen



For 24-port devices, the *Port Utilization Screen* displays the ports on multiple screens. To browse to a specific port entry, click the **Previous**, **1**, **2**, **3**, **4**, and **Next** links above the table. To view all device ports in the same window, click **View All Ports**.

The *Port Utilization Screen* contains the following fields:

- **Unit No.** — Indicates the stacking member being managed.
- **View All Ports** — Displays all ports per unit.

- **Global Overload Setting** — User-defined value that indicates the port is overloaded.
- **Refresh Rate** — Defines the amount of time that passes before the port utilization statistics are refreshed. The possible field values are:
 - *No Refresh* — Indicates that the port utilization statistics are not refreshed.
 - *15 Sec* — Indicates that the port utilization statistics are refreshed every 15 seconds.
 - *30 Sec* — Indicates that the port utilization statistics are refreshed every 30 seconds.
 - *60 Sec* — Indicates that the port utilization statistics are refreshed every 60 seconds.
- **Utilization %** — Displays the percentage of the interface's resources that are utilized.
- **Port** — Displays the interface number for which utilization is displayed.

The graphs show the port utilization percentages for the following factors:

- **Inbound Utilization** — Percentage of port resources used for input traffic.
- **Outbound Utilization** — Percentage of port resources used for output traffic.
- **Global Overload Line** — The port is overloaded.

802.1x Statistics

The *802.1x Statistics Screen* contains information about Extensible Authentication Protocol (EAP) packets received on a specific port.

To view the EAP statistics:

- STEP 1** Click **Statistics > 802.1x Statistics**. The *802.1x Statistics Screen* opens.

Figure 39 802.1x Statistics Screen

802.1x Statistics

The 802.1x Statistics Screen contains information about Extensible Authentication Protocol (EAP) packets received on a specific port.

The 802.1x Statistics Screen contains the following fields:

- Port** — Indicates the port which is polled for EAP statistics.
- Refresh Rate** — Defines the amount of time that passes before the EAP statistics are refreshed. The possible field values are:
 - No Refresh** — Indicates that the EAP statistics are not refreshed.
 - 15 Sec** — Indicates that the EAP statistics are refreshed every 15 seconds.
 - 30 Sec** — Indicates that the EAP statistics are refreshed every 30 seconds.

Name	Description	Number of Frames
Received EAPOL Start	The number of EAPOL Start frames that have been received by this Authenticator	0
Received EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator	0
Received EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized	0
Received EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator	0
Received EAP Request	The number of EAP Request frames that have been received by this Authenticator	0
Received EAP Response	The number of valid EAP Response frames (other than Request frames) that have been received by this Authenticator	0
Received EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid	0
Received Last EAPOL Ver	The protocol version number carried in the most recently received EAPOL frame	0
Received Last EAPOL Src	The source MAC address carried in the most recently received EAPOL frame	00:00:00:00:00:00
Transmit EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator	1
Transmit EAPOL As	The number of EAP Request frames that have been transmitted by this Authenticator	0
Transmit EAPOL Rqst	The number of EAP Request frames (other than Request frames) that have been transmitted by this Authenticator	0

Save Settings Cancel Changes

The *802.1x Statistics Screen* contains the following fields:

- **Unit Number** — Indicates the stacking member for which the EAP statistics are displayed.
- **Port** — Indicates the port which is polled for EAP statistics.
- **Refresh Rate** — Defines the amount of time that passes before the EAP statistics are refreshed. The possible field values are:
 - *No Refresh* — Indicates that the EAP statistics are not refreshed.
 - *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.
- **Received EAPOL Start** — Indicates the number of EAPOL Start frames received on the port.
- **Received EAPOL Logoff** — Indicates the number of EAPOL Logoff frames that have been received on the port.
- **Receive EAPOL Invalid** — Indicates the number of unrecognized EAPOL frames that have been received by on this port.
- **Received EAPOL Total** — Indicates the number of valid EAPOL frames received on the port.
- **Received EAP Resp/Id** — Indicates the number of EAP Resp/Id frames that have been received on the port.
- **Received EAP Resp/Oth** — Indicates the number of valid EAP Response frames (other than Resp/Id frames) that have been received on the port.
- **Received EAP LenError** — Indicates the number of EAPOL frames with an invalid Packet Body Length received on this port.
- **Received Last EAPOL Ver** — Indicates the protocol version number attached to the most recently received EAPOL frame.
- **Received Last EAPOL Src** — Indicates the source MAC address attached to the most recently received EAPOL frame.
- **Transmit EAPOL Total** — Indicates the number of EAPOL frames transmitted via the port.
- **Transmit EAPOL/Id** — Indicates the number of EAP Req/Id frames transmitted via the port.
- **Transmit EAPOL/Oth** — Indicates the number of EAP Request frames (other than Rq/Id frames) transmitted via the port.

STEP 2 Define the **Port** and **Refresh Rate**.

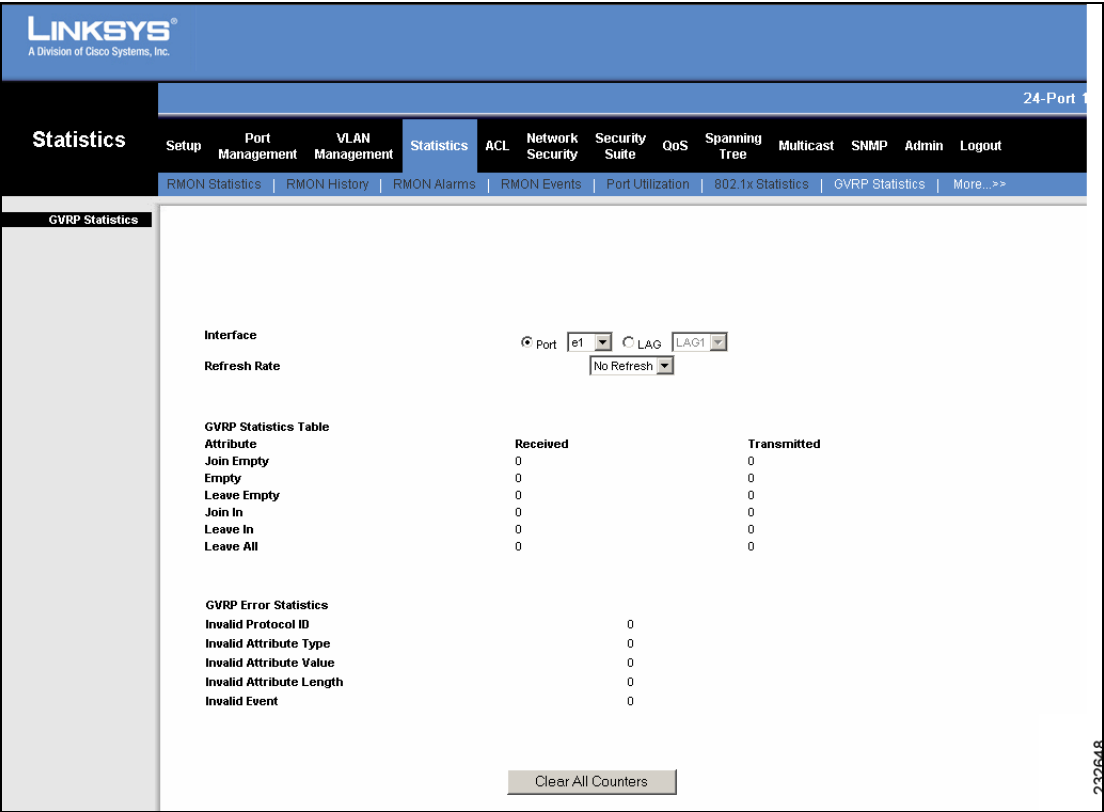
GVRP Statistics

The *GVRP Statistics Screen* contains statistics for GVRP communication on the device. The statistics counters are only displayed for interfaces on which GVRP is enabled.

To view the GVRP statistics:

- STEP 1
- Click **Statistics > GVRP Statistics**. The *GVRP Statistics Screen* opens.

Figure 40 GVRP Statistics Screen



The *GVRP Statistics Screen* is divided into two areas, GVRP Statistics Table and GVRP Error Statistics.

The following fields are relevant for both tables:

- **Interface** — Indicates the interface for which GVRP statistics are displayed. The possible field values are:
 - *Unit No.* — Indicates the stacking member for which GVRP statistics are displayed.
 - *Port* — Displays the GVRP statistics for the selected port.
 - *LAG* — Displays the GVRP statistics for the selected LAG.
- **Refresh Rate** — Indicates the amount of time that passes before the GVRP statistics are refreshed. The possible field values are:
 - *No Refresh* — Indicates that the GVRP statistics are not refreshed.
 - *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.

The GVRP Statistics Table contains the following statistics for received and transmitted traffic on the interface:

- **Join Empty** — Displays the GVRP Join Empty statistics.
- **Empty** — Displays the GVRP Empty statistics.
- **Leave Empty** — Displays the GVRP Leave Empty statistics.
- **Join In** — Displays the GVRP Join In statistics.
- **Leave In** — Displays the GVRP Leave In statistics.
- **Leave All** — Displays the GVRP Leave All statistics.

The GVRP Error Statistics Area contains the following fields:

- **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 Events statistics.

STEP 2 Define the **Interface** and **Refresh Rate**.

Resetting GVRP Statistics Counters

STEP 1 Click **Statistics > More > GVRP Statistics**. The *GVRP Statistics Screen* opens.

STEP 2 Click **Clear Counters**. The GVRP statistics counters are cleared.

STEP 3 Click **Save Settings**. The device starts recording GVRP Statistics from zero.

To clear the statistics counters, click the **Clear Counters** button and **Save Settings**.

CPU Utilization

The *CPU Utilization Screen* contains information about the system's CPU resource utilization.

To view CPU resource utilization:

STEP 1 Click **Statistics > More > CPU Utilization**. The *CPU Utilization Screen* opens.

Figure 41 CPU Utilization Screen



The *CPU Utilization Screen* contains the following fields:

- **Refresh Rate** — Amount of time that passes before the statistics are refreshed. The possible field values are:
 - *No Refresh* — Indicates that the CPU utilization statistics are not refreshed.
 - *15 Sec* — Indicates that the CPU utilization statistics are refreshed every 15 seconds.

- *30 Sec* — Indicates that the CPU utilization statistics are refreshed every 30 seconds.
- *60 Sec* — Indicates that the CPU utilization statistics are refreshed every 60 seconds.
- **Percentage** — Graph's y-axis indicates the percentage of the CPU's resources consumed by the device.
- **Time** — Displays a graph x-axis that contains a sliding window of 20 seconds where the CPU load is measured and usage samples are taken.

STEP 2 Define the **Refresh Rate**.

Interface Statistics

The *Interface Statistics Screen* is divided into two areas:

- Interface
- Ethernet-like Statistics

To view Interface statistics:

STEP 1 Click **Statistics > More > Interface Statistics**. The *Interface Statistics Screen* opens.

Figure 42 Interface Statistics Screen - Interface Area

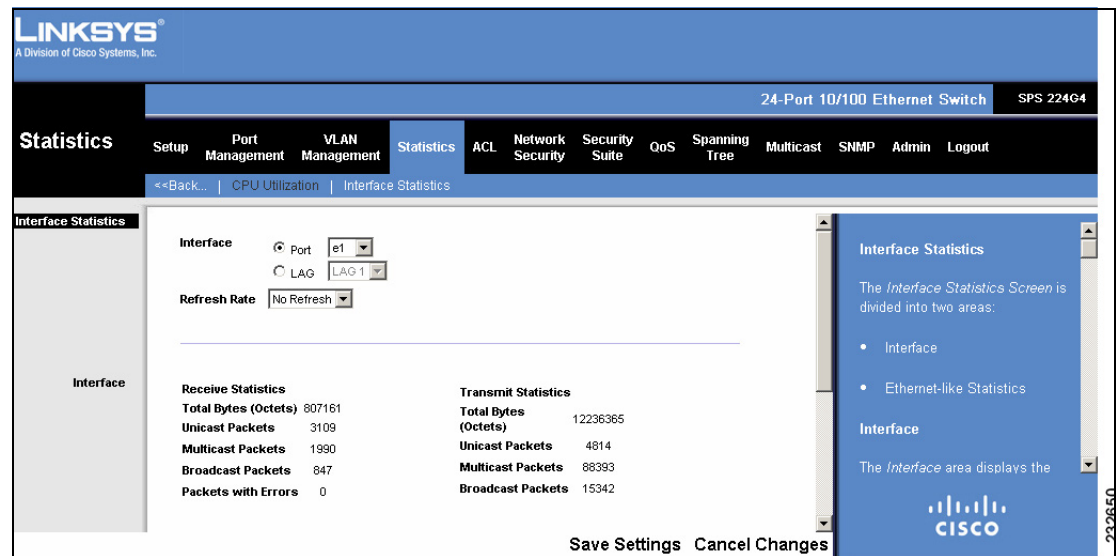
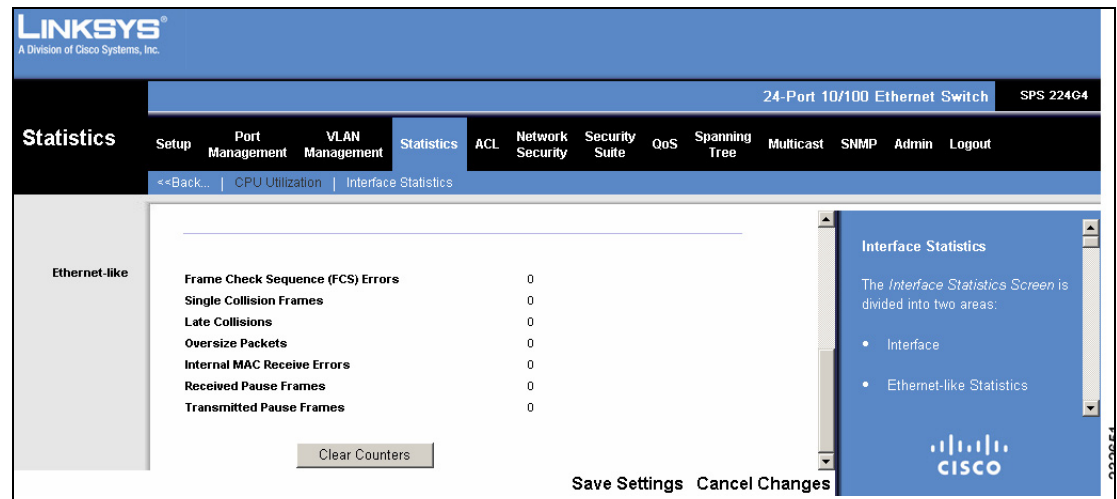


Figure 43 Interface Statistics Screen - Ethernet-Like Statistics Area



Interface

The *Interface* area displays the statistics for received and transmitted packets, and contains the following fields:

- **Interface** — Indicates the interface for which Interface statistics are displayed. The possible field values are:
 - *Unit No.* — Indicates the stacking member being managed.
 - *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:
 - *No Refresh* — Indicates that the Interface statistics are not refreshed.
 - *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.

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.

Ethernet-like Statistics

The *Ethernet-like Statistics* area contains the following fields:

- **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.
- **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 Pause Frames** — Displays the number of paused frames transmitted from the selected interface.

STEP 2 Define the **Interface** and **Refresh Rate**.

STEP 3 Click **Save Settings**. The device displays the Interface statistics for the specified interface.

Resetting Interface Statistics Counters

STEP 1 Click **Statistics > Interface Statistics**. The *Interface Statistics Screen* opens.

STEP 2 Click **Clear Counters**. The Interface statistics counters are cleared.

To clear the statistics counters, click the **Clear Counters** button.

ACL

The ACL configuration options are as follows:

- IP Based ACL
- MAC Based ACL

IP Based ACL

Access Control Lists (ACL) allow network managers to define classification actions and rules for specific ingress ports. The device supports up to 1,024 ACLs. Packets entering an ingress port, with an active ACL, are either admitted or denied entry and the ingress port is disabled. If they are denied entry, the user can disable the port. For example, a network administrator defines an ACL rule that states, port number 20 can receive TCP packets, however, if a UDP packet is received, the packet is dropped. ACLs are composed of access control entries (ACEs) that are made of the filters that determine traffic classifications. The total number of ACEs that can be defined in all ACLs together is 1024.



NOTE ACL configuration may take several minutes, depending on the device's usage of Ternary Content Addressable Memory (TCAM) resources.

To define IP based ACLs:

STEP 1 Click **ACL > IP Based ACL**. The *IP Based ACL Screen* opens.

Figure 44 IP Based ACL Screen

The screenshot shows the 'IP Based ACL' configuration page. At the top, there's a navigation bar with 'ACL' selected. Below it, the 'IP based ACL' tab is active. The main configuration area includes fields for 'ACL Name' (with a 'Delete ACL' button), 'New ACL Name', and a list of existing ACLs. The 'Action' is set to 'Permit'. The 'Protocol' is 'Any'. Under 'TCP Flags', 'Urg', 'Ack', 'Psh', 'Rst', 'Syn', and 'Fin' are all set to 'Set'. The 'ICMP Code' is 'Echo-reply(0)'. The 'Source Port' and 'Destination Port' are both 'Any'. The 'Source IP Address' and 'Destination IP Address' are both 'Any'. The 'Match DSCP' and 'Match IP Precedence' are both 'Any'. There is an 'Add to List' button. At the bottom, there's a table with columns: Action, Protocol, Flag Set, ICMP Code, ICMP Port, Source Port, Destination Port, Source IP Address, Source IP Mask, Destination IP Address, Destination IP Mask, Match DSCP, Match IP Precedence. A sidebar on the right contains information about ACLs and a note about TCAM resources.

The *IP Based ACL Screen* contains the following fields:

- **ACL Name** — User-defined ACLs.
- **New ACL Name** — Defines a new ACL name. Enter the name in the box.
- **Delete ACL** — Removes the IP based ACLs. The possible field values are:
 - *Checked* — Deletes the selected IP based ACL.
 - *Unchecked* — Maintains the IP based ACLs.

STEP 2 To display an IP Based ACL configuration, select an **ACL Name** or enter a new name to create a new ACL.

- **Action** — Indicates the ACL forwarding action. The possible field values are:
 - *Permit* — Forwards packets which meet the ACL criteria.

- *Deny* — Drops packets which meet the ACL criteria.
- *Shutdown* — Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed.
- **Protocol** — Enables creating an ACE based on a specific protocol. The possible field values are:
 - *ICMP* — *Internet Control Message Protocol* (ICMP). The ICMP allows the gateway or destination host to communicate with the source host. For example, to report a processing error.
 - *IGMP* — *Internet Group Management Protocol* (IGMP). Allows hosts to notify their local switch or router that they want to receive transmissions assigned to a specific Multicast group.
 - *IP* — *IP in IP (Encapsulation) Protocol* (IP). A method by which an IP datagram may be encapsulated (carried as payload) within an IP datagram, and can transmit data using a tunneling method.
 - *TCP* — *Transmission Control Protocol* (TCP). Enables two hosts to communicate and exchange data streams. TCP guarantees that packets are transmitted and received in the order they are sent.
 - *EGP* — *Exterior Gateway Protocol* (EGP). Permits exchanging routing information between two neighboring gateway hosts in an autonomous systems network.
 - *IGP* — *Interior Gateway Protocol* (IGP). Allows for routing information exchange between gateways in an autonomous network.
 - *UDP* — *User Datagram Protocol* (UDP). Communication protocol that transmits packets but does not guarantee their delivery.
 - *HMP* — *Host Mapping Protocol* (HMP). Collects network information from various networks hosts. HMP monitors hosts spread over the Internet as well as hosts in a single network.
 - *RDP* — *Remote Desktop Protocol* (RDP). Allows clients to communicate with the Terminal Server over the network.
 - *IDPR* — Matches the packet to the *Inter-Domain Policy Routing* (IDPR) Protocol. Routing protocol used to construct and maintain routes between source and destination administrative domains.
 - *IDRP* — Matches the packet to the *Inter-Domain Routing Protocol* (IDRP). Specifies how routers in different domains within an OSI environment communicate with each other.

- *RVSP* — Matches the packet to the *ReSerVation Protocol*(RSVP). Set of rules that allows channels or paths on the Internet to be reserved for Multicast transmission.
- *GRE* — Matches the packet to the *Generic Route Encapsulation* (GRE) protocol, which is used for creating VPNs between clients or between clients and servers.
- *ESP* — Matches the packet to the *Encapsulation Security Payload* (ESP), a security protocol used to provide confidentiality (encryption), data origin authentication, integrity, optional antireplay service, and limited traffic flow confidentiality by defeating traffic flow analysis.
- *AH* — *Authentication Header* (AH). Provides source host authentication and data integrity.
- *EIGRP* — *Enhanced Interior Gateway Routing Protocol*(EIGRP). Provides fast convergence, support for variable-length subnet mask, and supports multiple network layer protocols.
- *OSPF* — *Open Shortest Path First* (OSPF) protocol is a link-state, hierarchical interior gateway protocol (IGP) for network routing Layer Two (2) Tunneling Protocol, which is an extension to the PPP protocol that enables ISPs to operate Virtual Private Networks (VPNs).
- *IPIP* — *IP over IP* (IPIP). Encapsulates IP packets to create tunnels between two routers. This ensures that the IPIP tunnel appears as a single interface, rather than several separate interfaces. IPIP provides an alternative to IP loose source routing.
- *PIM* — Matches the packet to *Protocol Independent Multicast* (PIM). PIM is a set of multicast routing protocols.
- *L2TP* — Matches the packet to *Layer 2 Tunneling Protocol* (L2TP). is a tunneling protocol used to operate virtual private networks (VPNs).
- *ISIS* — *Intermediate System - Intermediate System* (ISIS). Distributes IP routing information throughout a single Autonomous System in IP networks
- *Protocol ID To Match* — Adds user-defined protocols by which packets are matched to the ACE. Each protocol has a specific protocol number which is unique. The possible field range is 0-255.
- *Any* — Matches the protocol to any protocol.
- **TCP Flags** — Sets the indicated TCP flag that can be triggered.

- **ICMP** — Specifies an ICMP message type for filtering ICMP packets.
 - *Select from List* — Select from known ICMP types.
 - *ICMP Type* — Define an ICMP Type which is not listed in the device.
 - *Any* — Use any ICMP type.
- **ICMP Code** — Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type. It can also be filtered by the ICMP message code.
- **IGMP** — IGMP packets can be filtered by IGMP message type.
 - *Select from List* — Select from known IGMP types.
 - *IGMP Type* — Define an IGMP Type which is not listed in the device.
 - *Any* — Use any IGMP type.
- **Source Port** — Defines the TCP/UDP source port.
 - *Any* — Use any TDP/UDP source port.
- **Destination Port** — Defines the TCP/UDP destination port.
 - *Any* — Use any TDP/UDP destination port.
- **Source IP Address** — Matches the source port IP address to which packets are addressed to the ACE.
 - *Wildcard Mask* — Defines the source IP address wildcard mask. Wildcard masks specify which bits are used and which bits are ignored. A wildcard of 0.0.0.0 indicates that all the bits are important. For example, if the source IP address 149.36.184.198 and the wildcard mask is 255.36.184.00, the first eight bits of the IP address are ignored, while bits above 36 in the second octet, bits above 184 in the third octet, and the last eight bits in the last octet are used.
 - *Any* — Any IP address can be the source IP address.
- **Destination IP Address** — Matches the destination port IP address to which packets are addressed to the ACE.
 - *Destination Mask* — Defines the destination IP address wildcard mask.
 - *Any* — Any IP address can be the destination IP address.

- **Match DSCP** — Matches the packet DSCP value to the ACL. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. The possible field range is 0-63.
- **Match IP Precedence** — Indicates matching ip-precedence with the packet ip-precedence value. IP Precedence enables marking frames that exceed CIR threshold. In a congested network, frames containing a higher are discarded before frames with a lower DP.

STEP 3 Define the relevant fields.

STEP 4 Click **Add To List**. The ACL is defined, and it is listed in the IP Based ACL Table at the bottom of the *IP Based ACL Screen*.

At the bottom of the *IP Based ACL Screen*, the table lists the defined ACLs. To browse to a specific ACL entry, click the **First**, **Previous**, **1**, **2**, **Next**, and **Last** links above the table.

To delete an ACL:

STEP 1 Click **ACL > IP Based ACL**. The *IP Based ACL Screen* opens.

STEP 2 In the IP Based ACL Table, select the ACL entry to delete.

STEP 3 Click **Delete**. The ACL entry is removed from the IP Based ACL Table and deleted from the device.

MAC Based ACL

The *MAC Based ACL Screen* allows MAC- based ACLs to be defined. ACEs can be added only if an ACL is not bound to an interface.



NOTE ACL configuration may take several minutes, depending on the device's usage of Ternary Content Addressable Memory (TCAM) resources.

To define MAC Based ACLs:

STEP 1 Click **ACL > MAC Based ACL**. The *MAC Based ACL Screen* opens.

Figure 45 MAC Based ACL Screen

The screenshot shows the Linksys web interface for configuring MAC-based ACLs. The top navigation bar includes 'Setup', 'Port Management', 'VLAN Management', 'Statistics', 'ACL', 'Network Security', 'Security Suite', 'QoS', 'Spanning Tree', 'Multicast', 'SNMP', 'Admin', and 'Logout'. The 'ACL' section is expanded, showing 'IP based ACL' and 'MAC based ACL'. The 'MAC based ACL' section is active, displaying a form with the following fields:

- ACL Name**: A text input field.
- New ACL Name**: A text input field.
- Delete ACL**: A checkbox.
- Action**: A dropdown menu with 'Permit' selected.
- Source MAC Address**: A text input field.
- Dest. MAC Address**: A text input field.
- VLAN ID**: A text input field.
- Ether Type**: A text input field.
- Inner VLAN**: A text input field.

Below the form is an 'Add to List' button. At the bottom, there is a table with the following columns: Action, Source Address, Source Mask, Destination Address, Destination Mask, VLAN ID, Ethertype, and Inner VLAN. A 'Delete' button is located at the bottom left of the table.

The *MAC Based ACL Screen* contains the following fields:

- **ACL Name** — User-defined ACLs.
- **New ACL Name** — Defines a new ACL name. Enter the name in the box.
- **Delete ACL** — Removes MAC based ACLs. The possible field values are:
 - *Checked* — Deletes the selected MAC based ACL.
 - *Unchecked* — Maintains the MAC based ACLs.

STEP 2 To display a MAC Based ACL configuration, select an **ACL Name** or enter a new name to create a new ACL.

In addition to the fields above, the following fields appear in the IP Based ACL Table:

- **Action** — Indicates the ACL forwarding action. Possible field values are:
 - *Permit* — Forwards packets which meet the ACL criteria.
 - *Deny* — Drops packets which meet the ACL criteria.
 - *Shutdown* — Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed.
- **Source MAC Address** — Matches the source MAC address to which packets are addressed to the ACE.
 - *Wild Card Mask* — Indicates the source MAC Address wild card mask. Wildcards are used to mask all or part of a source MAC Address. Wild card masks specify which octets are used and which octets are ignored. A wild card mask of ff:ff:ff:ff:ff:ff indicates that no octet is important. A wildcard of 00:00:00:00:00:00 indicates that all the octets are important. For example, if the source MAC address 09:00:07:A9:B2:EB and the wildcard mask is 00:ff:00:ff:00:ff, the 1st, 3rd, and 5th octets of the MAC address are checked, while the 2nd, 4th, and 6th octets are ignored.
 - *Any* — Any MAC address can be the source MAC address.
- **Destination MAC Address** — Matches the destination MAC address to which packets are addressed to the ACE.
 - *Wild Card Mask* — Indicates the destination MAC Address wild card mask. Wildcards are used to mask all or part of a destination MAC Address. Wild card masks specify which octets are used and which octets are ignored. A wild card mask of ff:ff:ff:ff:ff:ff indicates that no octet is important. A wildcard of 00:00:00:00:00:00 indicates that all the octets are important. For example, if the destination IP address 09:00:07:A9:B2:EB and the wildcard mask is 00:ff:00:ff:00:ff, the 1st, 3rd, and 5th octets of the MAC address are checked, while the 2nd, 4th, and 6th octets are ignored.
 - *Any* — Any MAC address can be the destination MAC address.
- **VLAN ID** — Matches the packet's VLAN ID to the ACE. The possible field values are 1 to 4095.
- **Ethertype** — Indicates the Ethertype packet by which the packets are filtered.

STEP 3 Define the relevant fields.

STEP 4 Click **Add To List**. The ACL is defined, and it is listed in the MAC Based ACL Table at the bottom of the *MAC Based ACL Screen*.

To delete an ACL:

STEP 1 Click **ACL > MAC Based ACL**. The *MAC Based ACL Screen* opens.

STEP 2 In the MAC Based ACL Table, select the ACL entry to delete.

STEP 3 Click **Delete**. The ACL entry is removed from the MAC Based ACL Table and deleted from the device.

Network Security

The Network Security configuration options are as follows:

- RADIUS
- TACACS+
- ACL Binding
- 802.1x Settings
- Port Authentication
- Port Security
- Management Access List
- Storm Control

RADIUS

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

To configure RADIUS servers:

STEP 1 Click **Network Security > RADIUS**. The *RADIUS Screen* opens.

Figure 46 RADIUS Screen

LINKSYS®
A Division of Cisco Systems, Inc.

24-Port

Network Security

SetupPort ManagementVLAN ManagementStatisticsACLNetwork SecuritySecurity SuiteQoSSpanning TreeMulticastSNMPAdminLogout

RADIUSTACACS+ACL Binding802.1x SettingsPort AuthenticationPort SecurityManagement Access ListMore...>>

RADIUS
Parameters

IP Address
Priority
Number of Retries
Timeout for Reply
Dead Time
Key String
Source IP Address
Authenticate
Authentication Port

0

3

3

(sec)

0

(Min)

(Alphanumeric)

0.0.0.0

Login

1812

Add to List

Table

IP Address	Priority	Number of Retries	Timeout for Reply	Dead Time	Source IP Address	Authenticate	Authentication Port

Delete

The *RADIUS Screen* contains the following fields:

- **RADIUS Accounting** — The authentication method used for RADIUS session accounting. Possible field values are:
 - *None* — No authentication is used to initiate accounting.
 - *Login* — Login authentication is used to initiate accounting.

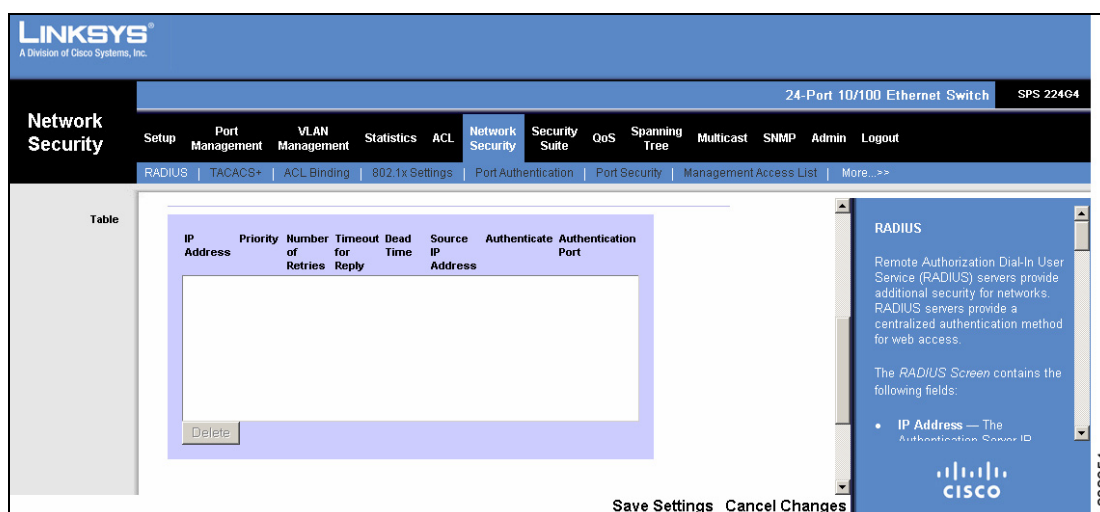
- *802.1x* — 802.1x authentication is used to initiate accounting.
 - *All* — Both 802.1x and login authentication are used to initiate accounting.
- **IP Address** — The Authentication Server IP address.
- **Priority** — The server priority. The possible values are 0-65535, where 0 is the highest value. The RADIUS Server priority is used to configure the server query order.
- **Number of Retries** — Defines the number of transmitted requests sent to 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 the time in seconds the device waits for an answer from the RADIUS server before retrying the query, or switching to the next server. The possible field values are 1 - 30. Three is the default value.
- **Dead Time** — Defines the amount of time (minutes) that a RADIUS server is bypassed for service requests. The range is 1-2000.
- **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 Source IP Address that is used in the packet it sends to the RADIUS server. This address is placed both in the source IP address field and in the NAS source IP field, a RADIUS attribute embedded in the packet's data.
- **Authenticate** — Specifies the RADIUS server authentication type. The default value is *Login*. The possible field values are:
 - *Login* — Indicates that the RADIUS server is used for authenticating user name and passwords.
 - *802.1X* — Indicates that the RADIUS server is used for 802.1X authentication.
 - *All* — Indicates that the RADIUS server is used for authenticating user name and passwords, and 802.1X port authentication.
- **Authentication Port** — Identifies the authentication port. The authentication port is used to verify the RADIUS server authentication. The authenticated port default is 1812.

- STEP 2** Define the relevant fields.
- STEP 3** Click **Add To List**. The RADIUS server is defined, and it is listed in the RADIUS Table at the bottom of the *RADIUS Screen*.
- STEP 4** Click **Save Settings**. The device is updated with the RADIUS server configuration.

To delete a RADIUS server:

- STEP 1** Click **Network Security > RADIUS**. The *RADIUS Screen* opens. Scroll down to display the RADIUS table.

Figure 47 RADIUS Table



- STEP 2** In the RADIUS Table, select the RADIUS server entry to delete.
- STEP 3** Click **Delete**. The RADIUS server configuration is removed from the RADIUS Table.
- STEP 4** Click **Save Settings**. The device is updated and the RADIUS server configuration is deleted from the device.

TACACS+

Terminal Access Controller Access Control System (TACACS+) provides centralized security user access validation.

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.

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+ server.

To define TACACS+ server authentication settings:

STEP 1 Click **Network Security > TACACS+**. The *TACACS+ Screen* opens.

Figure 48 TACACS+ Screen

The screenshot displays the TACACS+ configuration interface. The top navigation bar includes 'Network Security' and various other settings. The main content area is titled 'TACACS+ Parameters' and contains the following fields:

- Host IP Address: [Empty text box]
- Priority: [0]
- Source IP Address: [0.0.0.0]
- Key String: [Empty text box]
- Authentication Port: [49]
- Timeout for Reply: [5]
- Status: [Not Connected]
- Single Connection: [Unchecked checkbox]

At the bottom right, there is a 'Save Settings' button and a 'Cancel Changes' button. A sidebar on the right side of the screen contains the following text:

TACACS+
Terminal Access Controller Access Control System (TACACS+) provides centralized security user access validation.
TACACS+ provides a centralized user management system, while

The Cisco logo is visible at the bottom of the sidebar.

The *TACACS+ Screen* 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.
- **Key String** — Defines the default authentication and encryption key for TACACS+ communication between the device and the TACACS+ server.
- **Authentication Port** — 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 1-30 seconds. The default is 5 seconds.
- **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.
- **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.

STEP 2 Define the relevant fields.

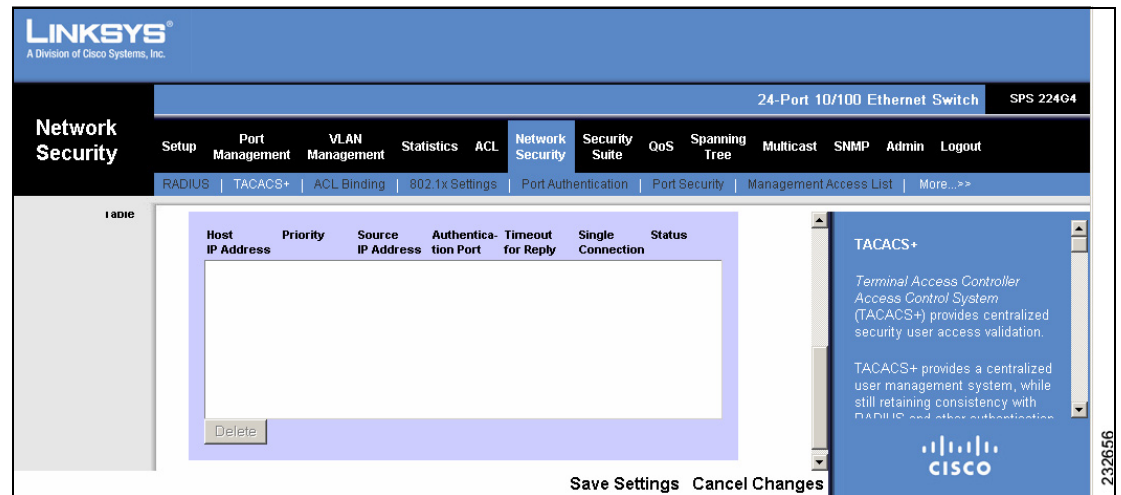
STEP 3 Click **Add To List**. The TACACS+ server configuration is defined, and it is listed in the TACACS+ Table at the bottom of the *TACACS+ Screen*.

STEP 4 Click **Save Settings**. The device is updated with the TACACS+ server configuration.

To delete a TACACS+ server:

- STEP 1** Click **Network Security > TACACS+**. The *TACACS+ Screen* opens. Scroll down to display the TACACS+ table.

Figure 49 TACACS+ Table



- STEP 2** In the TACACS+ Table, select the TACACS+ server entry to delete.
- STEP 3** Click **Delete**. The TACACS+ server configuration is removed from the TACACS+ Table.
- STEP 4** Click **Save Settings**. The device is updated and the TACACS+ server configuration is deleted from the device.

ACL Binding

When an ACL is bound to an interface, all the ACE rules that have been defined are applied to the selected interface. Whenever an ACL is assigned on a port, LAG or, VLAN, flows from that ingress interface that do not match the ACL are matched to the default rule, which is *Drop* unmatched packets.

To bind ACLs to interfaces:

STEP 1 Click **Network Security > ACL Binding**. The *ACL Binding Screen* opens.

Figure 50 ACL Binding Screen

The screenshot shows the Linksys web interface for ACL Binding. The top navigation bar includes 'Setup', 'Port Management', 'VLAN Management', 'Statistics', 'ACL', 'Network Security', 'Security Suite', 'QoS', 'Spanning Tree', 'Multicast', 'SNMP', 'Admin', and 'Logout'. The 'Network Security' section is expanded, showing 'RADIUS', 'TACACS+', 'ACL Binding', '802.1x Settings', 'Port Authentication', 'Port Security', 'Management Access List', and 'More...>>'. The 'ACL Binding Parameters' section has the following fields:

- Interface:** Radio buttons for 'Port' (selected) and 'LAG'. The 'Port' dropdown shows 'e1' and the 'LAG' dropdown shows 'LAG1'.
- ACL Name:** Radio buttons for 'IP Based ACL' (selected) and 'MAC Based ACL'.
- Add to List:** A button to add the configuration to the list.

Below the parameters is a table with the following structure:

Interface	Select ACL

A 'Delete' button is located at the bottom left of the table.

The *ACL Binding Screen* contains the following fields:

- **Unit No.** — Displays the stacking member for which the ACLs are defined.
- **Interface** — Indicates the port or LAG to which the associated ACL is bound.

- **ACL Name** — Indicates the ACL which is bound to the associated interface. The possible values are:
 - *IP Based ACL* — Select an existing IP Based ACL to bind with the interface.
 - *MAC Based ACL* — Select an existing MAC Based ACL to bind with the interface.

STEP 2 Define the relevant fields.

STEP 3 Click **Add To List**. The ACL binding is defined, and it is listed in the table at the bottom of the *ACL Binding Screen*.

To delete an ACL Binding configuration:

STEP 1 Click **Network Security > ACL Binding**. The *ACL Binding Screen* opens.

STEP 2 In the table, select the ACL Binding entry to delete.

STEP 3 Click **Delete**. The ACL Binding configuration is removed from the ACL Binding Table and deleted from the device.

802.1x Settings

The *802.1x Settings Screen* enables configuration of port-based authentication settings.

To define the port-based authentication settings:

- STEP 1** Click **Network Security > 802.1x**. The *802.1x Settings Screen* opens.

Figure 51 802.1x Settings Screen

The screenshot shows the Linksys web interface for a 24-Port 10/100 Ethernet Switch (SPS 224G4). The 'Network Security' tab is selected, and the '802.1x Settings' sub-tab is active. The interface is divided into two main sections: '802.1x Parameters' on the left and '802.1x Table' on the right. The '802.1x Parameters' section includes fields for 'Enable 802.1x' (checkbox), 'Port' (dropdown menu showing 'e1'), 'Status Port Control' (dropdown menu showing 'forceAuthorized'), 'Enable Dynamic VLAN Assignment' (checkbox), 'Enable Periodic Reauthentication' (checkbox), 'Enable Guest VLAN' (checkbox), 'Guest VLAN ID' (text input field showing '0'), and 'Authentication Method' (dropdown menu showing '802.1x Only'). There are 'Setting Timer', 'Update', 'Save Settings', and 'Cancel Changes' buttons at the bottom. The '802.1x Table' section on the right contains a description of the screen and a list of items: '802.1x Parameters' and '802.1x Table'.

The *802.1x Settings Screen* is divided into two areas:

- 802.1x Parameters
- 802.1x Table

802.1x Parameters

The *802.1x Parameters* contains the following fields:

- **Enable 802.1x** — Enables or disables 802.1x on the device.
- **Port** — Indicates the interface to configure the 802.1x settings.
 - *Unit No.* — Indicates the stacking member being managed.
 - *Port* — Indicates interface to configure.

- **Status Port Control** — Specifies the port authorization state. The possible field values are as follows:
 - *ForceAuthorized* — The controlled port state is set to ForceAuthorized (forward traffic).
 - *ForceUnauthorized* — The controlled port state is set to ForceUnauthorized (discard traffic).
 - *Auto* — A port in Auto mode sends EAP packets to the supplicant and will not be authorized unless it is authenticated. The Auto mode is required for selecting Multiple Hosts or Multiple Sessions host authentication in the *Port Authentication* page (see *Port Authentication*).
- **Enable Dynamic VLAN Assignment** — Permits DVA per 802.1x enabled port when host authentication is in multisession mode. When a port is enabled for 802.1 DVA, each authenticated supplicant on the port can be assigned with a different VLAN by the RADIUS server and the port automatically adds itself to the assigned VLAN. The possible field values are:
 - *Checked* — Enables DVA.
 - *Unchecked* — Disables DVA. This is the default value.
- **Enable Periodic Reauthentication** — Permits periodic port reauthentication. The possible field values are:
 - *Checked* — Enables immediate port reauthentication.
 - *Unchecked* — Disables port reauthentication. This is the default value.
- **Enable Guest VLAN** — Enables or disables Guest VLAN on the specific interface. If enabled, Guest VLANs provide a limited network access to unauthorized 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. The possible field values are:
 - *Checked* — Indicates that an unauthorized user can use the Guest VLAN.
 - *Disabled* — Indicates that an unauthorized user cannot use the Guest VLAN.

- **Authentication Method** — Defines the port's authentication method. The possible field values are:
 - *802.1x Only* — Authentication on this port is based on 802.1x frames only. MAC addresses are ignored.
 - *MAC Only* — Authentication on this port is based on MAC addresses only. 802.1x frames are ignored.
 - *MAC & 802.1x* — Authentication on this port based on both MAC addresses and 802.1x frames.

**NOTE**

When the device sends a MAC address as the 802.1x user name or password to a RADIUS server, the characters “.” and “-” are not forwarded to the RADIUS server. Avoid defining the corresponding MAC address with “.” and “-” in the RADIUS server.

STEP 2 Define the relevant fields.

STEP 3 Click **Setting Timer**. The *Setting Timer Screen* opens, in which users configure ports for 802.1x functionality.

Figure 52 Setting Timer Screen

The **Setting Timer** button opens the *Setting Timer Screen* to configure ports for 802.1x functionality.

The *Setting Timer Screen* contains the following fields:

- **Unit No.** — Indicates the stacking member being managed.
- **Port** — Indicates the interface.

- **Reauthentication Period** — Specifies the number of seconds in which the selected port is reauthenticated (Range: 300-4294967295). The field default is 3600 seconds.
- **Quiet Period** — Specifies the number of seconds that the switch remains in the quiet state following a failed authentication exchange (Range: 1-65535). The field default is 60 seconds.
- **Resending EAP** — Specifies the number of seconds that the switch waits for a response to an EAP - request/identity frame, from the supplicant (client), before resending the request. The field default is 30 seconds.
- **Max EAP Request** — 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 number of seconds that lapses before EAP requests are resent to the supplicant (Range: 1-65535). The field default is 30 seconds.
- **Server Timeout** — Specifies the number of seconds that lapses before the switch resends a request to the authentication server (Range: 1-65535). The field default is 30 seconds.

STEP 4 Define the relevant fields.

STEP 5 Click **Save & Close** to save the modifications and close the *Setting Timer Screen* (clicking **Save** keeps the *Setting Timer Screen* open). The defined configuration appears in the 802.1x Table near the bottom of the *802.1x Settings Screen*.

802.1x Table

The displays the 802.1x authentication settings for every interface. Click the **Base Table** link to display only the Status Port Control and Enable Periodic Reauthentication parameters for the interfaces. Click the **More Details** link to display all parameters for the interlaces.

Figure 53 802.1x Table

The screenshot shows the Linksys web interface for a 24-Port 10/100 Ethernet Switch (SPS 224G4). The 'Network Security' tab is selected, and the '802.1x Settings' sub-tab is active. The main content area displays the 'Base Table' with the following data:

Port	Status Port Control	Enable Periodic Reauthentication
e1	forceAuthorized *	Disable
e2	forceAuthorized *	Disable
e3	forceAuthorized *	Disable
e4	forceAuthorized *	Disable
e5	forceAuthorized *	Disable
e6	forceAuthorized *	Disable
e7	forceAuthorized *	Disable
e8	forceAuthorized *	Disable
e9	forceAuthorized *	Disable
e10	forceAuthorized *	Disable
e11	forceAuthorized *	Disable
e12	forceAuthorized *	Disable

Below the table, a footnote states: * Port is down or not present .

The right sidebar contains the '802.1x Settings' section, which explains that the screen enables configuration of port-based authentication settings and is divided into two areas: 802.1x Parameters and 802.1x Table. The '802.1x Parameters' section further states that it contains the following fields:

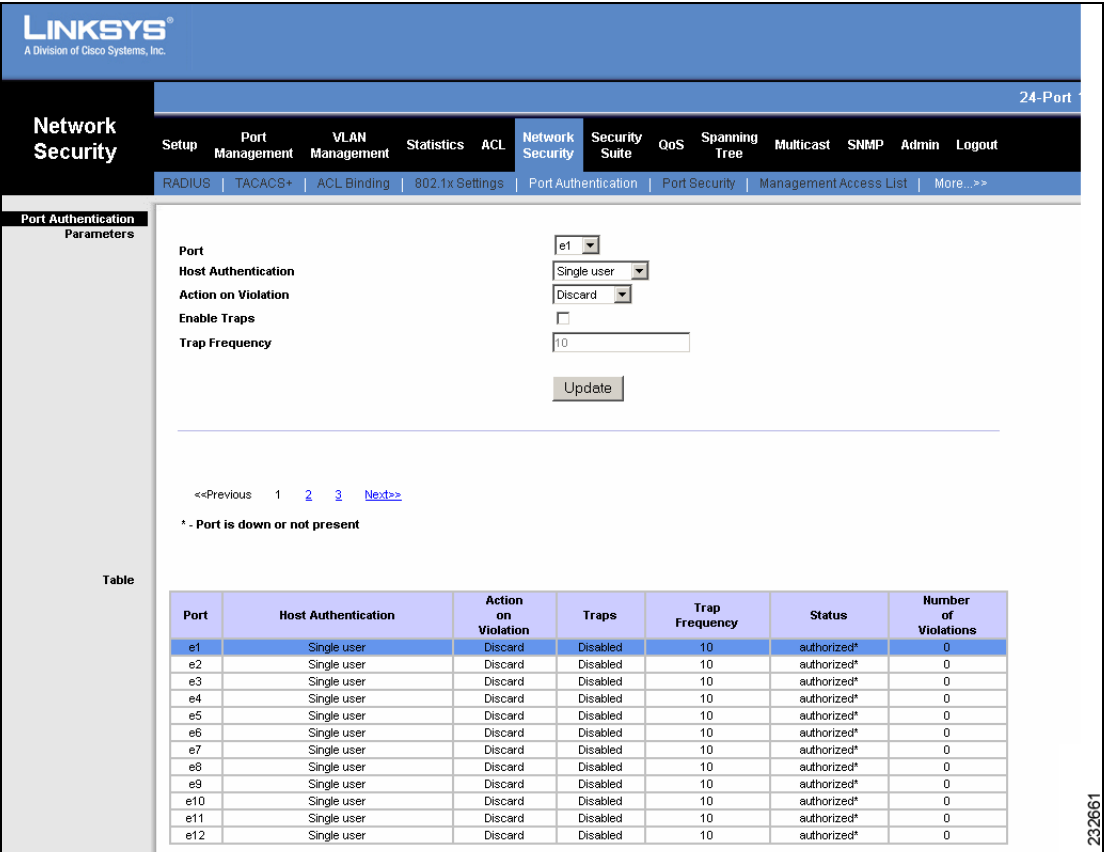
Save Settings Cancel Changes

Port Authentication

The Port Authentication Screen allows administrators to define the ports authentication method for specific ports. Administrators can allow multiple users and sessions on ports if the 802.1x Settings' Status Port Control is defined as Auto. To define the port authorization:

- STEP 1 Click Network Security > Port Authentication. The Port Authentication Screen opens.

Figure 54 Port Authentication Screen



The Port Authentication Screen is divided into two areas:

- Port Parameters
- Port Table

The Port Parameters area contains the following fields:

- **Unit No.** — Indicates the stacking member for which the port authentication details are displayed.
- **Port** — Defines the port number for which advanced port-based authentication is enabled.
- **Host Authentication**— Indicates whether multiple users are enabled on the port. Multiple users must be enabled in order to either disable the ingress-filter, or to use port-lock security on the selected port. Changing the port mode is only relevant if 802.1x authentication is disabled (see *802.1x Settings*). The possible field values are:
 - *Single User* — A single, specific, authorized host can get access to the port. Port security cannot be enabled on a Single User port.
 - *Multiple Host* — Multiple users are enabled on the port. Multiple, specific, authorized hosts can get access to the port. Filtering is based on the source MAC address. If only one of the specified hosts is successfully authorized, all the other specified hosts will be granted network access. If the port is blocked, all specified clients are denied access to the network. Multiple Hosts mode is only available if the *802.1x Settings' Status Port Control* is defined as **Auto**.
 - *Multi-Session* — Enables more than one authorized host to access the port. Filtering is based on the source MAC address. Each specific host must be successfully authorized in order to receive network access. In this mode, packets are not encrypted, and after successful authentication, filtering is based on the source MAC address only. Port security cannot be enabled on a Multi-session port.
- **Action on Violation** — Defines the action to be applied to packets arriving from a host whose MAC address is not the supplicant MAC address. The possible field values are:
 - *Discard* — Discards the packets.
 - *Forward* — Forwards the packet.
 - *Shutdown* — Discards the packets and shuts down the port. The port remains shut down until reactivated, or until the device is reset.

- **Enable Traps** — Indicates if traps are enabled for multiple users or sessions. The possible field values are:
 - *Checked* — Indicates that traps are enabled.
 - *Unchecked* — Indicates that traps are disabled.
- **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 sessions are disabled. The default is 10 seconds.

STEP 2 Define the relevant fields.

STEP 3 Click **Save Settings**. The defined port authentication configuration appears in the Port Table, and the device is updated.

For 24-port devices, the *Port Table* displays the ports on multiple screens. To browse to a specific port entry, click the **Previous**, **1**, **2**, **3**, and **Next** links above the table.

The Port Table displays the authentication parameters of the ports, and contains the following additional parameters:

- **Traps** — Indicates if traps are enabled for multiple sessions. The possible field values are:
 - *True* — Indicates that traps are enabled.
 - *False* — Indicates that traps are disabled.
- **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.
 - *Force Authorized* — 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 only a single client has been authenticated via the port.
 - *Multiple Hosts* — Indicates that the port control is Auto and Multiple Hosts mode is enabled. One client has been authenticated.
 - *Multiple Sessions* — Indicates that the port control is Auto and Multiple Sessions mode is enabled. At least one client has been authenticated.

- **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.

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 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
- Cause the port to be shut down

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.

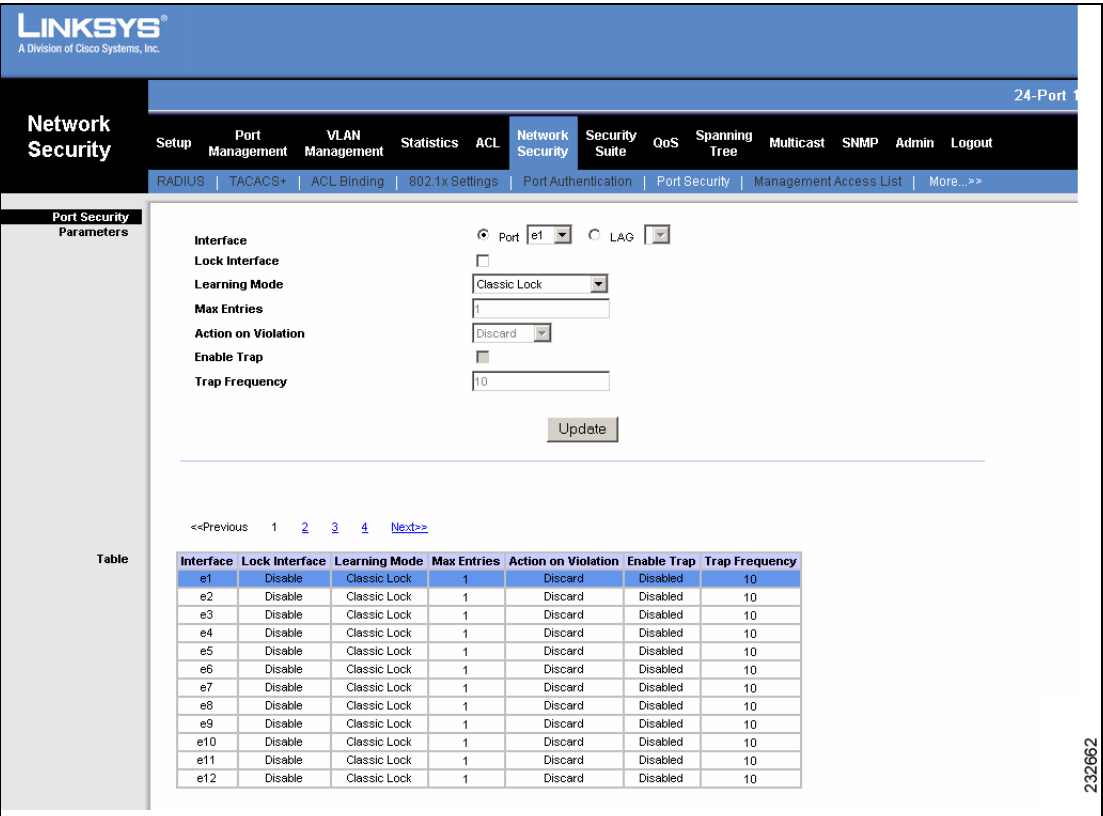
Disabled ports are activated from the *Port Management > Port Configuration Screen* (click the **Detail** button).

Port Security can be enabled only on ports in Multiple User or Multiple Session modes (see *Port Authentication*).

To define port security:

STEP 1 Click **Network Security > Port Security**. The *Port Security Screen* opens.

Figure 55 Port Security Screen



The *Port Security Screen* is divided into two areas:

- Port Security Parameters
- Port Security Table

The Port Security Parameters area contains the following fields:

- **Interface** — Indicates the port or LAG to configure the Port Security.
 - *Unit No.* — Indicates the stacking member being managed.
 - *Port* — Indicates port to configure.
 - *LAG* — Indicates LAG to configure.

- **Lock Interface** — Indicates the port security status. The possible field values are:
 - *Checked* — Indicates that the port is currently locked.
 - *Unchecked* — Indicates that the port is currently unlocked. This is the default value.
- **Learning Mode** — Defines the locked port type. The Learning Mode field is enabled only if Unlocked is selected in the Interface Status 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* — The device learns MAC addresses up to the maximum addresses allowed on the port, after which any new MAC is considered unauthorized. Both relearning and aging MAC addresses are enabled.

In order to change the Learning Mode, the Lock Interface must be set to Unlocked (unchecked). Once the mode is changed, the Lock Interface can be reinstated.

- **Max Entries** — Specifies the number of MAC addresses that can be learned on the port. The Max Entries field is enabled only if *Locked* is selected in the **Locked Interface** field, and if the *Limited Dynamic Lock* mode is selected in the **Learning Mode**. The default is 1.
- **Action on Violation** — Indicates the action to be applied to packets arriving on a locked port. The possible field values are:
 - *Discard* — Discards packets from any unlearned source. This is the default value.
 - *Forward* — Forwards packets from an unknown source without learning the MAC address.
 - *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.

- **Enable 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** — The amount of time (in seconds) between traps. The default value is 10 seconds.

STEP 2 Define the relevant fields.

STEP 3 Click **Save Settings**. The defined port security configuration appears in the Port Security Table, and the device is updated.

For 8-port devices, the Port Security Table displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, and **Next** links above the table.

For 24-port devices, the Port Security Table displays the interface on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, **3**, and **Next** links above the table.

The Port Security Table displays the security parameters of the ports.

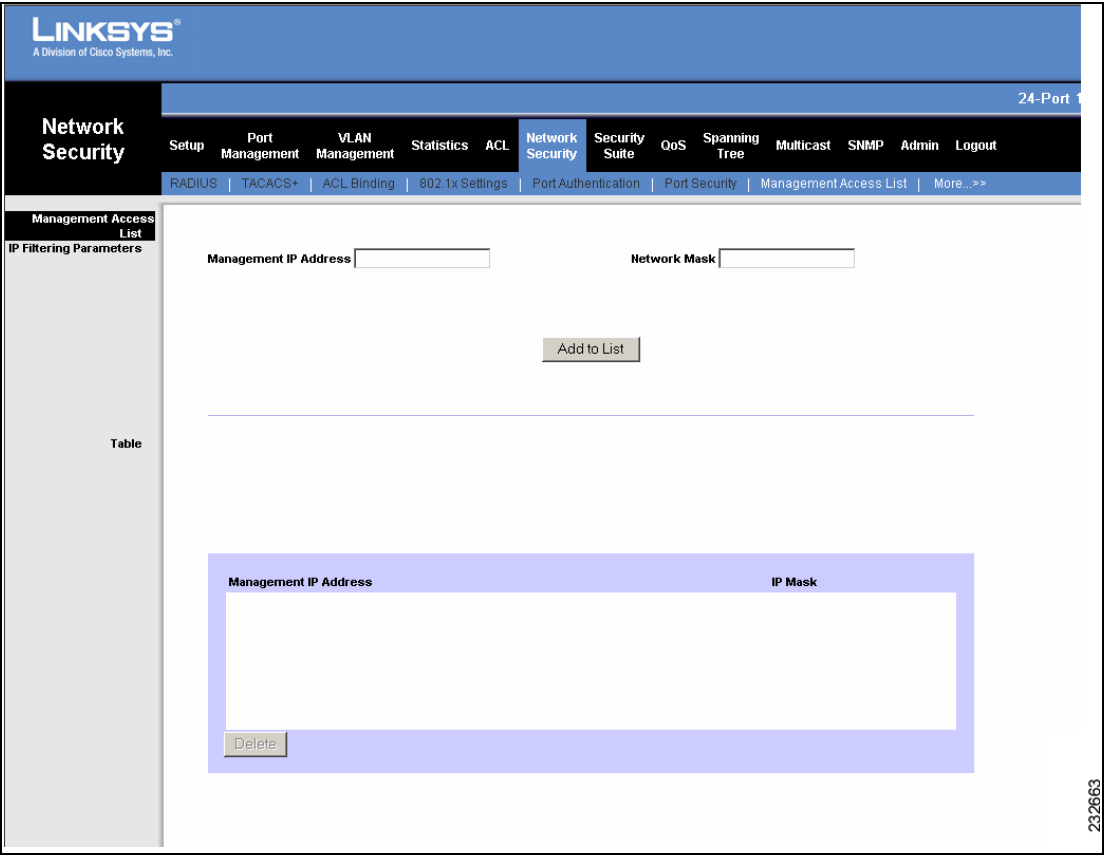
Management Access List

The *Management Access List Screen* enables network administrators to limit management access to the device to specific IP addresses.

To assign management access to specific IP addresses:

- STEP 1
- Click **Network Security > Management Access List**. The *Management Access List Screen* opens.

Figure 56 Management Access List Screen



The *Management Access List Screen* contains the following fields:

- **Management IP Address** — The IP address to be allowed.
- **Wildcard Mask** — Defines the address wildcard mask. Wildcard masks specify which 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 source IP

address 149.36.184.198 and the wildcard mask is 255.36.184.00, the first eight bits of the IP address are ignored, while bits above 36 in the second octet, bits above 184 in the third octet, and the last eight bits in the last octet are used.

STEP 2 Define the relevant fields.

STEP 3 Click **Add To List**. The management access is defined, and the IP address is listed in the table at the bottom of the *Management Access List Screen*.

STEP 4 Click **Save Settings**. The device is updated.

To remove management access rights from an IP address:

STEP 1 Click **Network Security > Management Access List**. The *Management Access List Screen* opens.

STEP 2 In the table, select the IP address to delete.

STEP 3 Click **Delete**. The IP address is removed from the Table.

STEP 4 Click **Save Settings**. The device is updated.

Storm Control

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

Storm Control enables limiting the amount of Multicast, Broadcast, and Unknown Unicast frames (in SPS208 and SPS 224G4 only) accepted and forwarded by the device. When Layer 2 frames are forwarded, Multicast, Broadcast, and Unknown Unicast frames are flooded to all ports on the relevant VLAN. This occupies bandwidth, and loads all nodes connected 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 per port 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 system measures incoming Unknown Unicast frames (addressed to an unknown destination MAC address) separately. The defined Unknown Unicast rate threshold is the maximum rate that all ports are allowed to forward at any single time.

The *Storm Control Screen (SPS 224G4)* provides fields for configuring packet Storm Control.

- STEP 1 Click **Network Security > More > Storm Control**. The *Storm Control Screen (SPS 224G4)* opens.

Figure 57 Storm Control Screen (SPS 224G4)

LINKSYS®
A Division of Cisco Systems, Inc.

24-Port 1

Network Security

SetupPort ManagementVLAN ManagementStatisticsACLNetwork SecuritySecurity SuiteQoSSpanning TreeMulticastSNMPAdminLogout

<<Back...Storm Control

Storm Control

Global Unknown Unicast

Parameters

Table

Unknown Unicast Group Control

☐

Rate Threshold

3500

Port

e1

Broadcast Control

☐

Mode

Broadcast Only

Rate Threshold

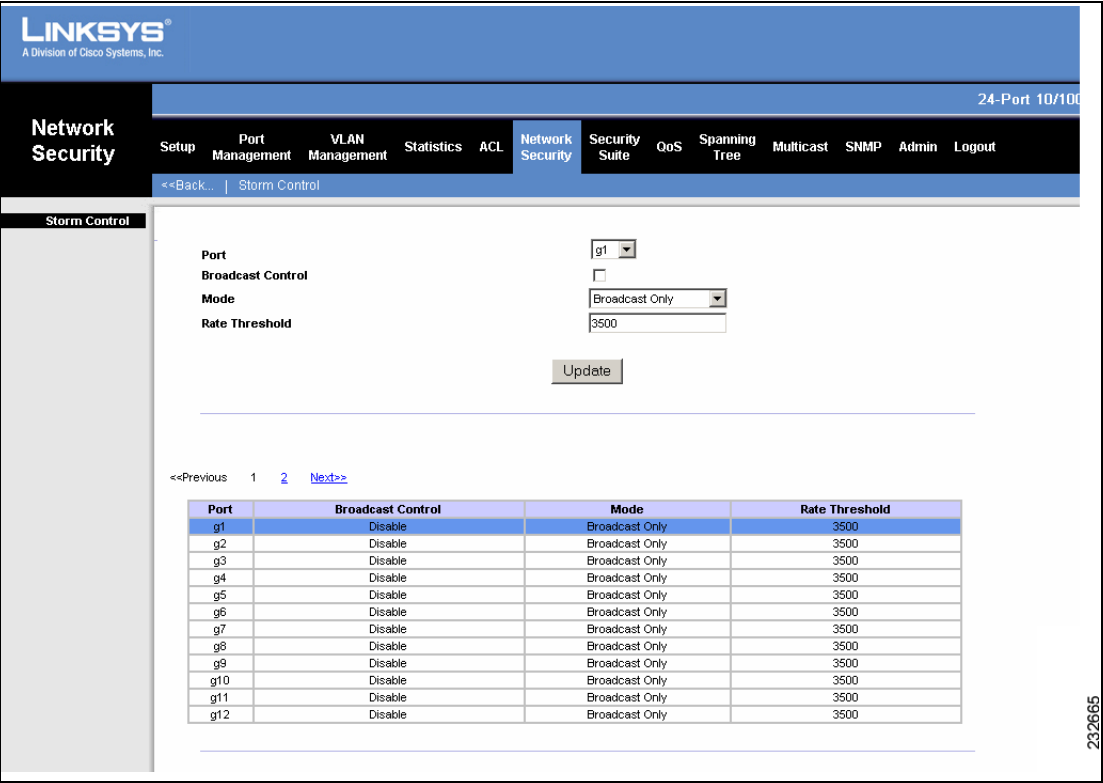
100

Update

<<Previous123Next>>

Port	Broadcast Control	Mode	Rate Threshold
e1	Disable	Broadcast Only	100
e2	Disable	Broadcast Only	100
e3	Disable	Broadcast Only	100
e4	Disable	Broadcast Only	100
e5	Disable	Broadcast Only	100
e6	Disable	Broadcast Only	100
e7	Disable	Broadcast Only	100
e8	Disable	Broadcast Only	100
e9	Disable	Broadcast Only	100
e10	Disable	Broadcast Only	100
e11	Disable	Broadcast Only	100
e12	Disable	Broadcast Only	100

Figure 58 Storm Control Screen (SPS 2024)



The Storm Control Screen (SPS 224G4) is divided into two areas:

- Storm Control Parameters - Global Unknown Unicast (applicable to SPS 208 and SPS 224G4 only) and Port Storm Control
- Storm Control Table

The Storm Control Parameters area contain the following fields:

- **Unknown Unicast Group Control** — Enables or disables the counting of unknown Unicast frames on FE ports globally (applicable to SPS 208 and SPS 224G4 only).
- **Rate Threshold** — The maximum rate (packets per second) at which unknown Unicast packets are forwarded. This rate affects all ports that forward unknown Unicast packets at a single time. The ranges are 3500Kbps – 100Mbps for FE ports (applicable to SPS 208 and SPS 224G4 only).

- **Port** — Indicates the interface from which storm control is enabled.
 - *Unit No.* — Indicates the stacking member being managed.
 - *Port* — Indicates the port from which storm control is enabled.
- **Broadcast Control** — Indicates if Broadcast control is applied on the specific interface. Broadcast control limits the amount of Broadcast packet types to be forwarded. The possible field values are:
 - *Checked* — Enables Broadcast control.
 - *Unchecked* — Disables Broadcast control.
- **Mode** — Specifies the Broadcast mode currently enabled on the device. The possible field values are:
 - *Multicast & Broadcast* — Counts Broadcast and Multicast traffic together.
 - *Broadcast Only* — Counts only Broadcast traffic.
 - *Unknown Unicast* — Counts only Unknown Unicast traffic (available on GE ports only).
- **Rate Threshold** — The maximum rate (packets per second) at which unknown packets are forwarded. The ranges are 70 Kbps – 100 Mbps for FE ports, and 3.5 Mbps – 100 Mbps for GE ports. The default value is 3.5 Mbps.

The **Update** button adds the configured Storm Control to the Storm Control Table at the bottom of the screen.

STEP 2 Define the relevant fields.

STEP 3 Click **Save Settings**. The Storm Control configuration appears in the Storm Control Table, and the device is updated.

For 24-port devices, the Storm Control Table displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, **3**, and **Next** links above the table.

The Storm Control Table displays the Storm Control configuration configurations for all device interfaces.

Security Suite

The Security Suite configuration options are as follows:

- DHCP Snooping
- DHCP VLANs
- DHCP Trusted Interfaces
- DHCP Database
- ARP Inspection
- ARP Trusted Interfaces
- ARP Inspection List
- ARP VLANs
- IP Source Guard
- IP Source Guard Database

DHCP Snooping

DHCP Snooping enables network administrators to differentiate between trusted interfaces connected to end-users or DHCP Servers and untrusted interfaces located beyond the network firewall.

DHCP Snooping filters untrusted messages. DHCP Snooping creates and maintains a DHCP Snooping Table which contains information received from untrusted packets. Interfaces are untrusted if the packet is received from an interface outside the network or from an interface beyond the network firewall. Trusted interfaces receive packets only from within the network or the network firewall.

The DHCP Snooping Table contains the untrusted interfaces' MAC address, IP address, Lease Time, VLAN ID, and interface information.

The *DHCP Snooping Screen* contains parameters for enabling DHCP Snooping on the device.



NOTE For more information about Insertion of Option 82, see “[DHCP Relay](#),” on page 22.

To define DHCP Snooping on the device:

STEP 1 Click **Security Suite > DHCP Snooping**. The *DHCP Snooping Screen* opens.

Figure 59 DHCP Snooping Screen

The screenshot shows the Linksys web interface for the DHCP Snooping configuration. The top navigation bar includes 'Security Suite' and various other settings like Setup, Port Management, VLAN Management, etc. The left sidebar has 'DHCP Snooping' selected. The main content area has the following fields:

- Enable DHCP Snooping**: ☐ (unchecked)
- Enable Pass Through Option 82**: ☐ (unchecked)
- Enable Verify MAC Address**: ☒ (checked)
- Enable Backup Database**: ☐ (unchecked)
- Database Update Interval**: (0) (sec)

The *DHCP Snooping Screen* contains the following fields:

- **Enable DHCP Snooping** — Enables or disables DHCP Snooping on the device. The possible field values are:
 - *Checked* — Enables DHCP Snooping on the device.
 - *Unchecked* — Disables DHCP Snooping on the device. This is the default value.
- **Enable Pass Through Option 82** — Permits the port to forward packets that contain DHCP Option 82 data. The possible field values are:
 - *Checked* — If DHCP Option 82 with data insertion is enabled, the DHCP relay agent or DHCP Snooping switch can insert information into the DHCP DISCOVER message. The Relay agent information option

specifies the port number from which the client's packet was received. This is the default value.

- *Unchecked* — Disables DHCP Option 82 with data insertion on the device.
- **Enable Verify MAC Address** — Enables or disables MAC address verification. The possible field values are:
 - *Checked* — Verifies that an untrusted port source MAC address matches the MAC address in the packet. This is the default value.
 - *Unchecked* — Disables verification that an untrusted port source MAC address matches the MAC address in the packet.
- **Enable Backup Database** — Enables or disables the DHCP Snooping Database. The possible field values are:
 - *Checked* — Enables storing allotted IP addresses in the DHCP Snooping Database in flash memory.
 - *Unchecked* — Disables storing allotted IP addresses in the DHCP Snooping Database. This is the default value.
- **Database Update Interval** — Indicates how often the DHCP Snooping Database is updated. The possible field range is 600 – 86400 seconds. The field default is 1200 seconds.
- **IP Source Guard** — Indicates if IP Source Guard is enabled on the device. The possible field values are:
 - *Checked* — Enable IP Source Guard on the device. IP source guard stops malignant network users from using unallocated network IP addresses. IP Source Guard ensures that only packets with an IP address stored in the DHCP Database are forwarded. IP address stored in the DHCP Snooping Database are either statically configured by the network administrator or are retrieved using DHCP. IP source guard can be enabled only on DHCP snooping untrusted interface.
 - *Unchecked* — Disables IP Source Guard on the device. This is the default value.
- **Check Availability** — TBD
 - *Retry* — TBD
 - *Frequency* — TBD
 - *Never* — TBD

- STEP 2
- Enable or disable the relevant options.
- STEP 3
- Click **Save Settings**. DHCP Snooping is enabled, and the device is updated.

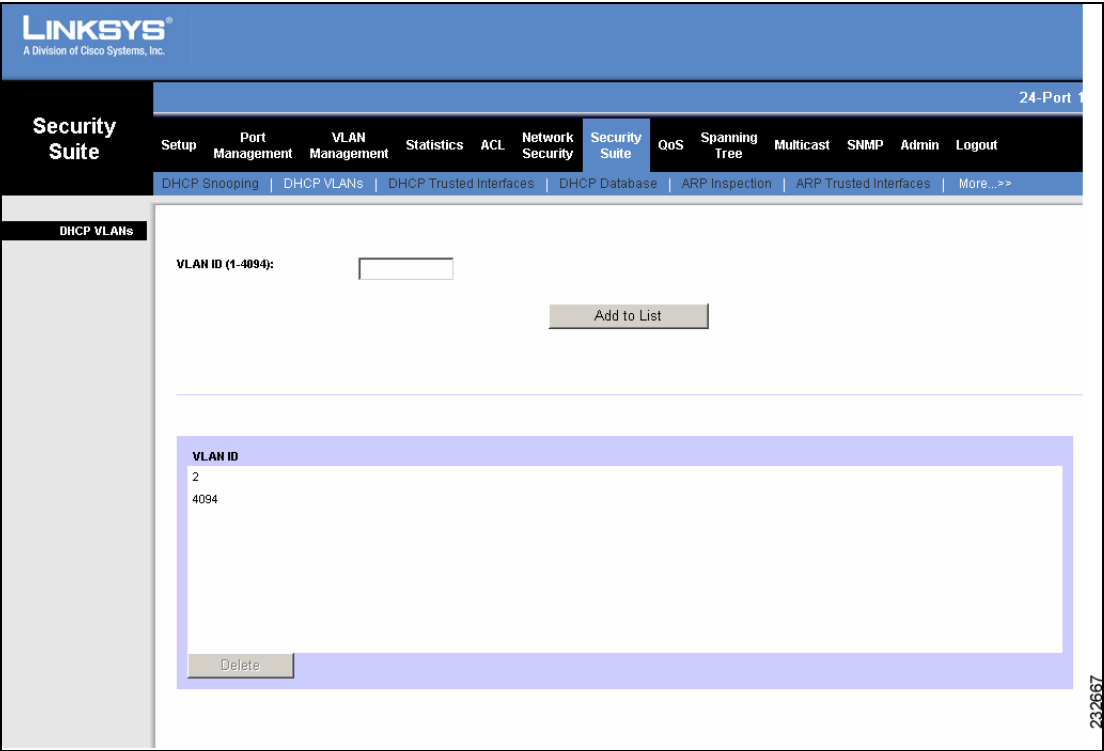
DHCP VLANs

The *DHCP Snooping Enabled VLAN Screen (SPS 224G4)* allows network managers to enable DHCP Snooping on VLANs. DHCP snooping separates ports in the VLAN. To enable DHCP Snooping on VLANs, ensure that DHCP Snooping is enabled on the device.

To enable DHCP Snooping on VLANs:

- STEP 1
- Click **Security Suite > DHCP VLANs**. The *DHCP Snooping Enabled VLAN Screen (SPS 224G4)* opens.

Figure 60 DHCP Snooping Enabled VLAN Screen (SPS 224G4)



The *DHCP Snooping Enabled VLAN Screen (SPS 224G4)* contains the following fields:

- **VLAN ID (1-4093 or 4094)** — The VLAN on which DHCP snooping can be enabled. The possible range is 1-4093 (for SPS-208 and SPS-224G4) or 1-4094 (for SPS-2024).
- **VLAN ID (1-40934094)** — The VLAN on which DHCP snooping can be enabled. The possible range is 1-40934094.
- **VLAN Range** — Indicates a range of VLANs on which to enable DHCP snooping. To add the defined range of VLAN ID numbers, press **Add Range**.

STEP 2 Define the **VLAN ID** and click **Add to List**, or define the **VLAN Range** and click **Add Range**. The VLAN details appear in the **Enabled VLANs Table** and the device is updated.

To delete a DHCP Enabled VLAN from the device:

STEP 1 In the **Enabled VLANs Table**, select the VLAN.

STEP 2 Click **Delete**. The selected VLAN is deleted from the device.

The **Enabled VLANs Table** contains a list of VLANs on which DHCP snooping is enabled.

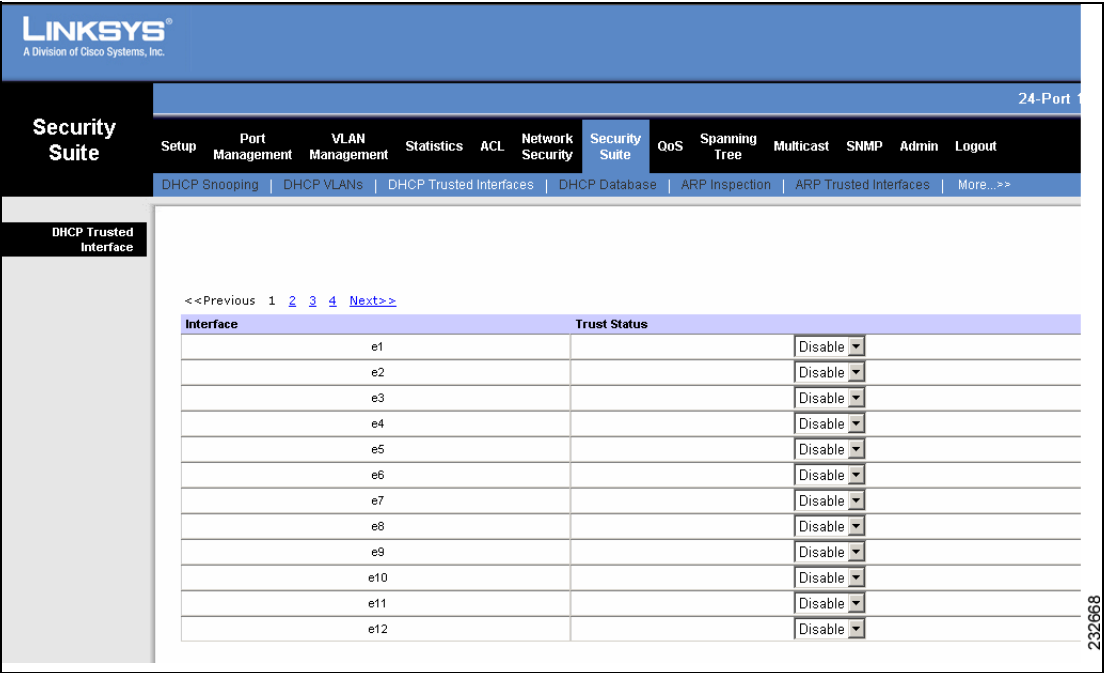
DHCP Trusted Interfaces

The *DHCP Trusted Interface Screen* allows network managers to define Trusted interfaces. Interfaces are untrusted if the packet is received from an interface outside the network or from an interface beyond the network firewall.

To define Trusted interfaces:

- STEP 1
- Click **Security Suite > DHCP Trusted Interfaces**. The *DHCP Trusted Interface Screen* opens.

Figure 61 DHCP Trusted Interface Screen



For 8-port devices, the Trusted Interfaces Table displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, and **Next** links above the table.

For 24-port devices, the Trusted Interfaces Table displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, **3**, and **Next** links above the table.

The *DHCP Trusted Interface Screen* contains the following fields:

- **Unit No.** — Indicates the stacking member for which the Trusted Interface settings are displayed.
- **Interface** — Indicates the port or LAG on which Trust is enabled or disabled.
- **Trust Status** — Enables or disables DHCP Snooping Trust mode on the interface. The possible field values are:
 - *Enable* — Indicates that DHCP Snooping Trust mode is enabled on the interface.
 - *Disable* — Indicates that DHCP Snooping Trust mode is disabled on the interface.

STEP 2 Enable or disable the Trust Status for the relevant interfaces.

STEP 3 Click **Save Settings**. The Trusted Interfaces are defined, and the device is updated.

DHCP Database

The *DHCP Database Screen* contains parameters for querying and adding IP addresses to the DHCP Snooping Database. All changes to the binding storage file are implemented only if the device's system clock is synchronized with the SNTP Server. The DHCP Snooping Database is stored in the device's switch memory.

To query or add IP addresses:

- STEP 1** Click **Security Suite > DHCP Database**. The *DHCP Database Screen* opens.

Figure 62 DHCP Database Screen

LINKSYS®
A Division of Cisco Systems, Inc.

24-Port 1

Security Suite

SetupPort ManagementVLAN ManagementStatisticsACLNetwork SecuritySecurity SuiteQoS Spanning TreeMulticastSNMPAdminLogout

DHCP Snooping | DHCP VLANs | DHCP Trusted Interfaces | DHCP Database | ARP Inspection | ARP Trusted Interfaces | More...>>

DHCP Database
Parameters

Query by:
MAC Address
IP Address
VLAN ID
Interface
Type
Lease Time

☐

☐

☐

☐

☒ Port e1 ☐ LAG Lag1

☒ Dynamic ☐ Static

(Sec)

Infinite ☐

Add to List

Query

<<PreviousNext>>

MAC Address	IP Address	VLAN ID	Interface	Type	Lease Time
-------------	------------	---------	-----------	------	------------

Delete

232689

STEP 2 Select **Query By** and define any of the following fields as a query filter:

- **MAC Address** — Indicates the MAC addresses recorded in the DHCP Database. The Database can be queried by MAC address.
- **IP Address** — Indicates the IP addresses recorded in the DHCP Database. The Database can be queried by IP address.
- **VLAN ID** — Indicates the VLANs recorded in the DHCP Database. The Database can be queried by VLAN.
- **Interface** — Indicates the interface that will be queried in the DHCP Database. The possible field values are:
 - *Unit No.* — Queries the VLAN database by a specific stacking member.
 - *Port* — Queries the VLAN database by a specific port number.
 - *Trunk* — Queries the VLAN database by a specific trunk number.
- **Type** — Indicates the IP address binding type. The possible field values are:
 - *Dynamic* — Indicates the IP address is dynamically defined by the DHCP server.
 - *Static* — Indicates the IP address is static.
- **Lease Time** — Indicates the amount of time the DHCP Snooping entry is active. Addresses whose lease times are expired are ignored by the switch. The possible values are 10 – 4294967295 seconds. Select **Infinite** if the DHCP Snooping entry never expires.

STEP 3 Click **Query**. The results appear in the Query Results table.

To browse to a specific DHCP Snooping entry, click the **First**, **Previous**, **1**, **2**, **Next**, and **Last** links above the table.

ARP Inspection

Classic *Address Resolution Protocol* is a TCP/IP protocol that translates IP addresses into MAC addresses. Classic ARP does the following:

- Permits two hosts on the same network to communicate and send packets.
- Permits two hosts on different networks to communicate via a gateway.
- Permits routers to send packets via a host to a different router on the same network.
- Permits routers to send packets to a destination host via a local host.

ARP Inspection eliminates man-in-the-middle attacks, where false ARP packets are inserted into the subnet. ARP requests and responses are inspected, and their MAC Address to IP Address binding is checked. Packets with invalid ARP Inspection Bindings are logged and dropped. Packets are classified as:

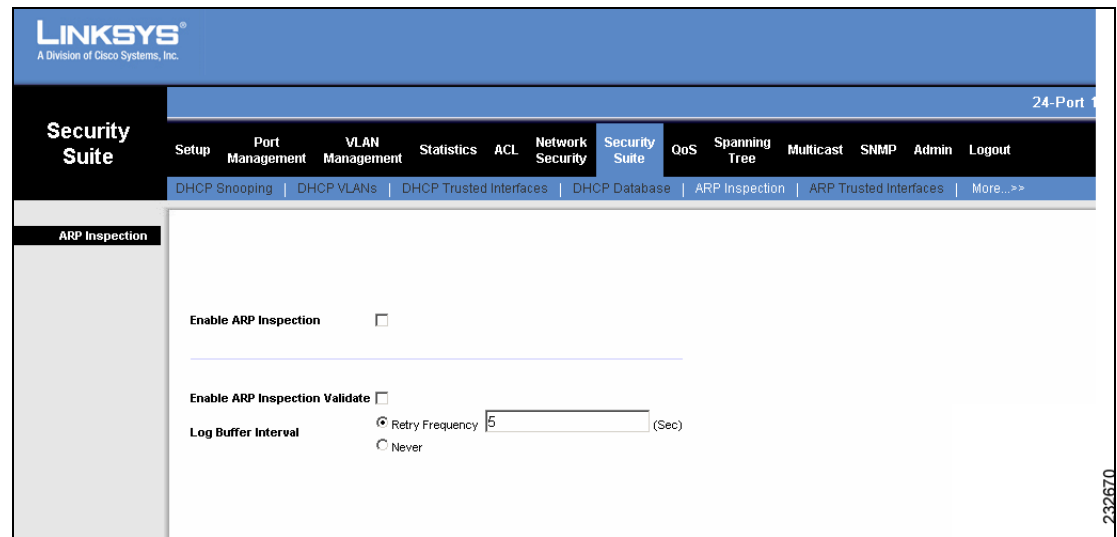
- **Trusted** — Indicates that the interface IP and MAC address are recognized, and recorded in the *ARP Inspection List*. Trusted packets are forward without ARP Inspection.
- **Untrusted** — Indicates that the packet arrived from an interface that does not have a recognized IP and MAC addresses. The packet is checked for:
 - *Source MAC* — Compares the packet's source MAC address against the sender's MAC address in the ARP request. This check is performed on both ARP requests and responses.
 - *Destination MAC* — Compares the packet's destination MAC address against the destination interface's MAC address. This check is performed for ARP responses.
 - *IP Addresses* — Compares the ARP body for invalid and unexpected IP addresses. Addresses include 0.0.0.0, 255.255.255.255, and all IP Multicast addresses. If the packet's IP address was not found in the ARP Inspection List, and DHCP snooping is enabled for a VLAN, a search of the DHCP Snooping Database is performed. If the IP address is found, the packet is valid and is forwarded. ARP inspection is performed only on untrusted interfaces.

The *ARP Inspection Screen* provides parameters or enabling and setting global ARP Inspection parameters, as well as defining ARP Inspection Log parameters.

To enable ARP Inspection:

STEP 1 Click **Security Suite > ARP Inspection**. The *ARP Inspection Screen* opens.

Figure 63 ARP Inspection Screen



The *ARP Inspection Screen* contains the following fields:

- **Enable ARP Inspection** — Enables or disables ARP Inspection on the device. The possible field values are:
 - *Checked* — Enables ARP Inspection on the device.
 - *Unchecked* — Disables ARP Inspection on the device. This is the default value.
- **Enable ARP Inspection Validate** — Enables or disables ARP Inspection Validation on the device. The possible field values are:
 - *Checked* — Enables ARP Inspection Validation on the device.
 - *Unchecked* — Disables ARP Inspection Validation on the device. This is the default value.
- **Log Buffer Interval** — Defines the minimal interval between successive Syslog messages. The possible field values are:
 - *Retry Frequency* — Indicates that ARP SYSLOG messages are generated. The interval between successive Syslog messages is the number of seconds entered into the (Sec) field. The range is 0-86400 seconds. The default value is 5.

- *Never* — Indicates that Syslog messages would not be generated.

- STEP 2** Define the relevant fields.
- STEP 3** Click **Save Settings**. The ARP Inspection configuration is defined, and the device is updated.

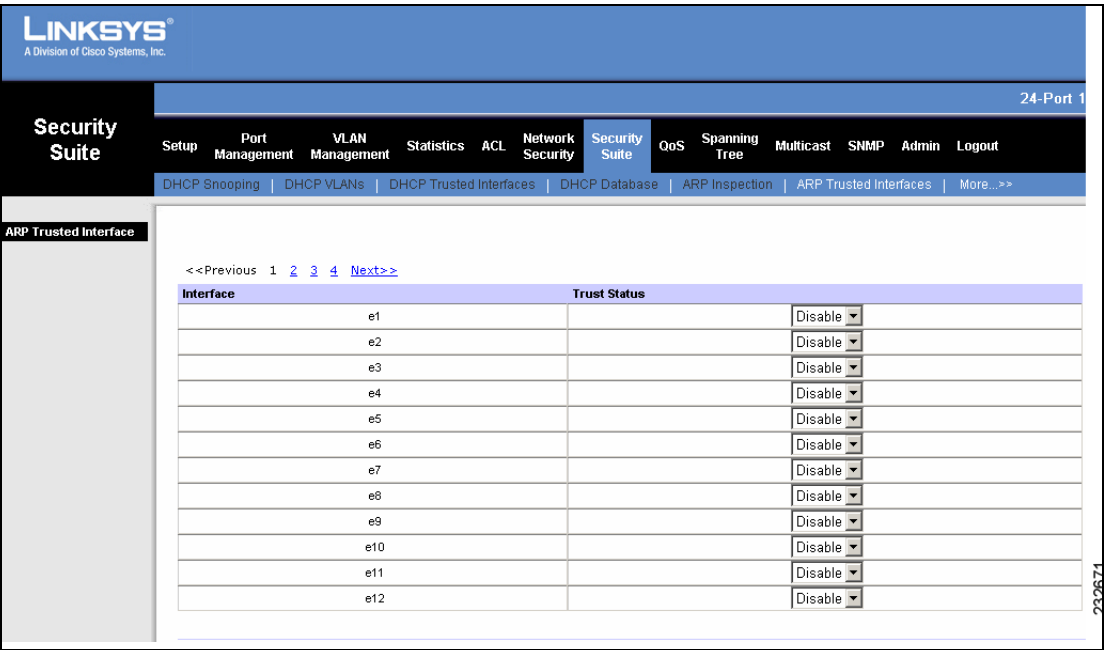
ARP Trusted Interfaces

The *ARP Trusted Interfaces Screen* allows network managers to configure trusted and untrusted interfaces. ARP Inspection is performed on untrusted interfaces only.

To configure ARP Inspection for untrusted interfaces:

- STEP 1** Click **Security Suite > ARP Trusted Interfaces**. The *ARP Trusted Interfaces Screen* opens.

Figure 64 ARP Trusted Interfaces Screen



For 8-port devices, the Trusted Interfaces Table displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, and **Next** links above the table.

For 24-port devices, the Trusted Interfaces Table displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, **3**, and **Next** links above the table.

The *ARP Trusted Interfaces Screen* contains the following fields:

- **Unit No.** — Indicates the stacking member for which the Trusted Interface settings are displayed.
- **Interface** — Indicates the port or LAG on which ARP Inspection Trust is enabled or disabled.
- **Trust Status** — Enables or disables ARP Inspection Trust mode on the interface. The possible field values are:
 - *Enable* — Indicates the port or LAG is a trusted interface, and ARP inspection is not performed on the ARP requests/replies sent to/from the interface.
 - *Disable* — Indicates the port or LAG is not a trusted interface, and ARP inspection is performed on the ARP requests/replies sent to/from the interface. This is the default value.

STEP 2 Enable or disable the Trust Status for the relevant interfaces.

STEP 3 Click **Save Settings**. The Trusted Interfaces are defined, and the device is updated.

ARP Inspection List

The *ARP Inspection List Screen* provides information for creating static ARP Binding Lists. ARP Binding Lists contains the List Name, IP address and MAC address which are validated against ARP requests.

To create an ARP Inspection Binding List:

- STEP 1** Click **Security Suite > More > ARP Inspection List**. The *ARP Inspection List Screen* opens.

Figure 65 ARP Inspection List Screen

The *ARP Inspection List Screen* contains the following fields:

- **List Name** — Select from a list of user-defined ARP Inspection Binding Lists.
- **New List Name** — Defines a new ARP Inspection Binding List. List names can contain up to 32 characters.

- **Delete List Name** — Removes ARP Inspection lists from interfaces. The possible field values are:
 - *Checked* — Removes the specific ARP Inspection Binding List from the selected interface.
 - *Unchecked* — Maintains the current ARP Inspection Binding List assignments.
- **IP Address** — Specifies IP addresses included in ARP Inspection Binding Lists which are checked against ARP requests.
- **MAC Address** — Specifies MAC addresses included in ARP Inspection Binding Lists which are checked against ARP requests.

STEP 2 Define the ARP Inspection Binding List Name.

STEP 3 Add the IP address and MAC address which are validated by the ARP requests.

STEP 4 Click **Add To List**. The ARP Inspection Binding List details appear in the table at the bottom of the *ARP Inspection List Screen*.

STEP 5 Click **Save Settings**. The ARP Inspection Binding configuration is defined, and the device is updated.

To delete an ARP Inspection Binding List from the device:

STEP 1 In the **ARP Inspection List Table**, select the entry.

STEP 2 Click **Delete**. The selected list is deleted from the device.

STEP 3 Click **Save Settings**. The ARP Inspection Binding configuration is modified, and the device is updated.

The ARP Inspection List Table contains a list of ARP Inspection Binding Lists on the device.

ARP VLANs

The *ARP VLANs Screen* contains fields for enabling ARP Inspection on VLANs. In the Enabled VLAN table, users assign static ARP Inspection Lists to enabled VLANs. When a packet passes through an untrusted interface which is enabled for ARP Inspection, the device performs the following checks in order:

- Determines if the packet's IP address and MAC address exist in the static ARP Inspection list. If the addresses match, the packet passes through the interface.
- If the device does not find a matching IP address, but DHCP Snooping is enabled on the VLAN, the device checks the DHCP Snooping database for the IP address-VLAN match. If the entry exists in the DHCP Snooping database, the packet passes through the interface.
- If the packet's IP address is not listed in the ARP Inspection List or the DHCP Snooping database, the device rejects the packet.

To define ARP Inspection on VLANs:

STEP 1 Click **Security Suite > More > ARP VLANs**. The *ARP VLANs Screen* opens.

Figure 66 ARP VLANs Screen

The screenshot shows the 'ARP VLANs' configuration page. At the top, there's a navigation bar with 'Security Suite' and various menu items like Setup, Port Management, VLAN Management, etc. Below this, there's a breadcrumb trail: '<<Back...' | ARP Inspection List | ARP VLANs | IP Source Guard | IP Source Guard DataBase'. The main content area has a left sidebar with 'ARP VLANs' selected. The main form has two input fields: 'VLAN ID' and 'List Name', followed by an 'Add to List' button. Below this is a table titled 'List to VLAN Table' with columns 'VLAN ID' and 'List Name'. At the bottom of the table is a 'Delete' button.

The *ARP VLANs Screen* contains the following fields:

- **VLAN ID** — Indicates the VLAN on which ARP inspection is enabled.
- **List Name** — Assign a static ARP Inspection List to the VLAN. These lists are defined in the *ARP Inspection List Screen*.

STEP 2 To add a bound ARP VLAN to the List To VLAN table, define the VLAN ID and the List Name.

STEP 3 Click **Add To List**. The new ARP-enabled VLAN configuration is added to the *List To VLAN Table*.

The List To VLAN Table contains a list of ARP-enabled VLANs on the device. The List To VLAN Table contains the following fields:

- **VLAN ID** — Indicates the VLAN on which ARP inspection is enabled.
- **List Name** — Indicates the ARP Inspection Lists assigned to this VLAN.

To delete an ARP-enabled VLAN from the device:

STEP 1 In the *List To VLAN Table*, select the entry.

STEP 2 Click **Delete**. The selected VLAN is deleted from the device.

IP Source Guard

IP Source Guard is a security feature that restricts the client IP traffic to those source IP addresses configured in the DHCP Snooping Binding Database and in manually configured IP source bindings. For example, IP Source Guard can help prevent traffic attacks caused when a host tries to use the IP address of its neighbor.

DHCP snooping must be enabled on the device's untrusted interfaces and on the relevant VLAN, in order to activate the IP source guard feature.

- IP Source Guard must be enabled globally in the *IP Source Guard Screen* before it can be enabled on the device interfaces.
- IP Source Guard uses Ternary Content Addressable Memory (TCAM) resources, requiring use of 1 TCAM rule per 1 IP Source Guard address entry. If the number of IP Source Guard entries exceeds the number of available TCAM rules, new IP source guard addresses remain inactive.
- IP Source Guard cannot be configured on a routed port.
- If IP Source Guard and MAC address filtering is enabled on a port, Port Security cannot be activated on the same port.

- If a port is trusted, filtering of static IP addresses can be configured, although IP Source Guard is only active when the port is untrusted.
- If a port's status changes from untrusted to trusted, the static IP address filtering entries remain but become inactive.

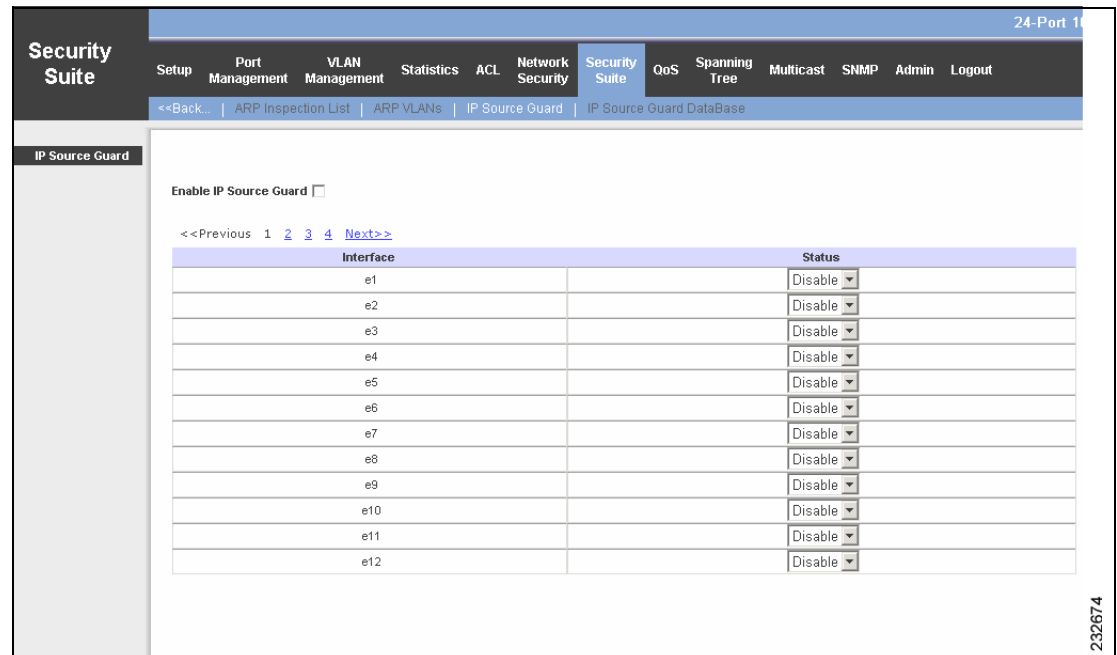
The *IP Source Guard Screen* allows network managers to enable the use of IP Source Guard on the device. IP Source Guard must be enabled for the device before it can be enabled on individual ports or LAGs. The *IP Source Guard Screen* is divided into the following sections:

- **IP Source Guard Global Settings** — Enabling or disabling IP Source Guard on the device.
- **IP Source Guard Interface Table** — Enabling IP Source Guard on DHCP Snooping untrusted interfaces. this permits the transmission of DHCP packets allowed by DHCP Snooping. If source IP address filtering is enabled, packet transmission is permitted as follows:
 - *IPv4 traffic* — Only IPv4 traffic with a source IP address that is associated with the specific port is permitted.
 - *Non IPv4 traffic* — All non-IPv4 traffic is permitted.

To enable IP Source Guard:

- STEP 1** Click **Security Suite > More > IP Source Guard**. The *IP Source Guard Screen* opens.

Figure 67 IP Source Guard Screen



The *IP Source Guard Screen* contain the following fields:

- **Enable IP Source Guard** — Indicates the use of IP Source Guard on the device.
 - *Checked* — Enables IP Source Guard on the device.
 - *Unchecked* — Disables IP Source Guard on the device.

For 8-port devices, the IP Source Guard Interface Table displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, and **Next** links above the table.

For 24-port devices, the IP Source Guard Interface Table displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, **3**, and **Next** links above the table.

The IP Source Guard Interface Table contains the following fields:

- **Interface** — Indicates the port's or LAG's number.
- **Status** — Indicates whether the interface is trusted or untrusted.
 - *Enable* — Indicates that the interface is trusted.
 - *Disable* — Indicates that the interface is untrusted. This is the default value.

STEP 2 Enable or disable IP Source Guard on the device.

STEP 3 Enable or disable IP Source Guard on specific interfaces.

STEP 4 Click **Save Settings**. The IP Source Guard configuration is modified, and the device is updated.

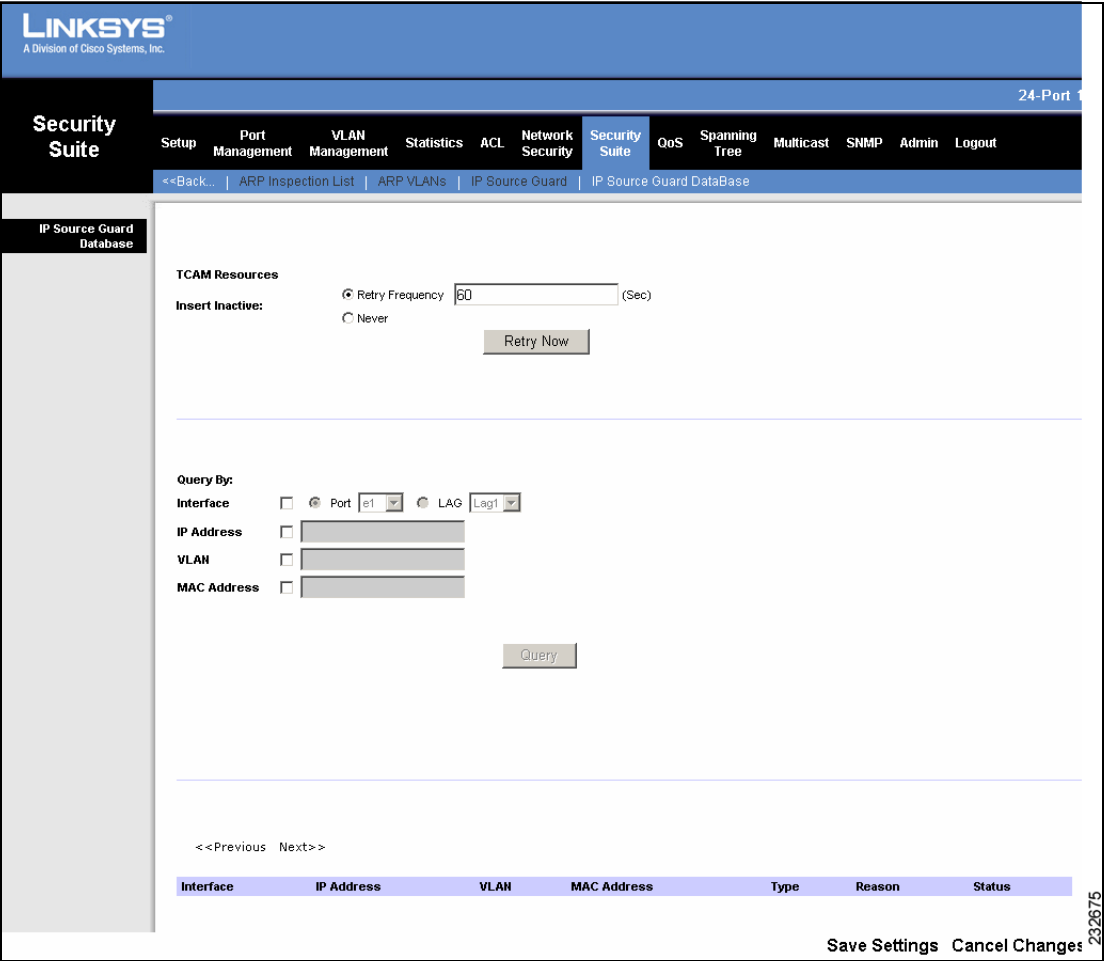
IP Source Guard Database

The *IP Source Guard Database Screen* enables network managers to query and view information about inactive addresses recorded in the IP Source Guard Database.

To query IP addresses in the IP Source Guard Database:

- STEP 1
- Click **Security Suite > More > IP Source Guard Database**. The *IP Source Guard Database Screen* opens.

Figure 68 IP Source Guard Database Screen



STEP 2 In the TCAM Resources section, complete following fields:

STEP 3 Insert Inactive — The IP Source Guard Database uses Ternary Content Addressable Memory (TCAM) resources for managing the database. If there is a shortage of allocated TCAM resources, some IP addresses may become inactive. The device can then try to activate inactive IP addresses in various time intervals:

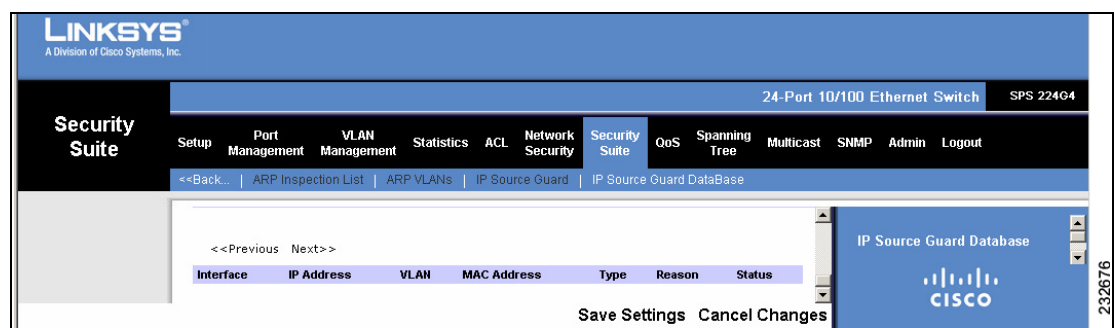
- *Retry Frequency* — Try to activate inactive addresses at a specified interval. The possible values are 10 - 600 seconds. The default value is 60 seconds.
- *Never* — Never try to activate inactive addresses.
- *Retry Now* — Click this button to activate inactive addresses immediately.

STEP 4 In the Query By section, select and define the preferred filter for searching the IP Source Guard Database:

- **MAC Address** — Search the database by MAC address.
- **IP Address** — Search the database by IP address.
- **VLAN** — Search the database by VLAN ID.
- **Interface** — Search the database by interface number. The possible field values are:
 - *Unit No.* — Queries the database by a specific stacking member.
 - *Port* — Queries the database by port number.
 - *LAG* — Queries the VLAN database by LAG number.

STEP 5 Click **Query**. The results appear in the Query Results table.

Figure 69 IP Source Guard Database Screen - Query Results



The Query Results table contains the following fields:

- **Interface** — Displays the interface number.
- **IP Address** — IP address of the inactive address.
- **VLAN** — Indicates if the address is associated with a VLAN.
- **MAC Address** — MAC address of the inactive address.
- **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.
- **Reason** — Displays the reason an IP source address is inactive. The possible field options are:
 - *No Problem*
 - *VLAN*
 - *Trusted Port*
 - *Resource Problem*
- **Status** — Displays the current interface status. The possible field values are:
 - *Active* — Indicates the interface is currently active.
 - *Inactive* — Indicates the interface is currently inactive.

QoS

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

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

QoS Modes

The device provides the following methods for controlling and configuring CoS/ QoS in the device:

- Basic Mode
- Advanced Mode

The device only works in either one of these modes at a single time, or with QoS disabled.

During mode change, some configuration settings revert to their default values

Basic QoS Mode

Basic Mode enables users to categorize frames into classes, according to the ingress interface or a single frame header field value. Each class may be directed to a specific egress queue. Users can also define Queue priority parameters and the ports' bandwidth allocations.

To classify packets, users must apply trust settings which help identify fields for service assignment. Basic Mode supports the following Trust settings:

- **VPT - VLAN Priority Tags** are mapped to priority queues.
 - *802.1p Tag-based* — The IEEE802.1p tag is used to classify packets. The packets are mapped, according to the VPT, to an output queue. Administrators either apply the default VPT mapping (as defined by the 802.1p standard), or may define the mapping according to their own specifications. Mapping is defined on a device-wide basis.

- **802.1p Port-based** — In this mode, users can assign a default queue for forwarding untagged packets. Those packets can then pass in accordance to the priority defined on that queue. Untagged packets can also be converted into tagged packets, with their VPT defined according to the device's active VPT mapping.
- **Layer 3 Predefined Field** — In this method, the DiffServ Code Point (DSCP) of incoming packets are the basis for mapping the packets to the output queues. The DSCP mapping method is applied per device, although it may be enabled or disabled on individual ports. Non-IP packets are classified as Best Effort.

Advanced QoS Mode

In Advanced QoS mode, administrators define forwarding rules which specify flow classifications, and set bandwidth management and queueing assignments to these flows.

After assigning packets to a specific queue, services such as configuring output queues for the scheduling scheme, or CIR, per interface can be applied. Note that packets may egress with a different VPT tag than that with which they ingressed. When using trust VPT this caveat does not exist, and packets egress with the same VPT with which they ingressed.

In Advanced QoS mode, administrators set up policies and assign them to interfaces. Policies are composed of several user-defined configurations, such as:

- **Out of Profile DSCP Assignments** — Assigning the outgoing DSCP tags that takes the place of the incoming DSCP tags.
- **Policy Name** — Creating new policies which can be assigned to interfaces. Policies can be composed of an ACL and QoS rules.
- **Class Map** — Defining class maps, consisting of one IP ACL and/or one MAC ACL.
- **Aggregate Policier** — Applying aggregate policers to multiple classes in the same policy map.
- **Interface To Policy** — Binding QoS policies to interfaces.

Service Types

The following services are available in both Basic and Advanced modes:

- **Minimum Delay** — The queue is assigned to a Strict Priority policy. To reduce delay to its optimum, administrators can assign traffic to the highest priority queue.
- **Best Effort** — Traffic is assigned to the lowest priority queue. By default, the device directs best effort packets through queue no. 1 (*q1*).
- **WRR Scheduling** — Implements Weighted Round Robin (WRR) priority. The queues are mapped to weight values and bandwidth allocations that determine the priority of the traffic passing through the queues. The weights may be assigned to the queues in any order.

Only packets marked with a **Forward** action are assigned to the output queue, based on the specified classification. For packets not matched to a policy classification, **Deny** is the default action.

The following services are available in Advanced mode:

- **Bandwidth Assignments** — Maximum and minimum bandwidth thresholds make sure that the traffic complies with bandwidth availability. The device discards packets that exceed or are less than the allowed bandwidth range.
- **IP DSCP** — Packet DSCP tag values are assigned to traffic queues.
- **Tail Drop** — The tail drop threshold is the length of an output queue which is considered full. If the tail drop is enabled and the queue is congested, the device drops packets until the queue reaches the defined tail drop threshold. Tail drop is configurable only on GE ports.

To optimize the device's QoS performance, administrators can combine the various services in the configuration. The QoS profiles can include the following types of service settings:

- Queue trust mode
- Bandwidth control and maximum/minimum thresholds
- Scheduling
- Traffic shaping on egress interfaces

In Advanced QoS mode, policies can be applied directly to an interface. However, a policy and ACL cannot be simultaneously applied to an interface.

Configuring QoS

The QoS configuration options are as follows:

- CoS Settings
- Queue Settings
- DSCP Settings
- Bandwidth
- Basic Mode
- Advanced Mode

CoS Settings

The *CoS Settings Screen* contains fields for enabling or disabling CoS (Basic or Advanced mode), mapping CoS to queues, and defining the default CoS for each port or LAG.

To define CoS Settings:

STEP 1 Click **QoS > CoS Settings**. The *CoS Settings Screen* opens.

Figure 70 CoS Settings Screen

LINKSYS
A Division of Cisco Systems, Inc.

24-Port

QoS Setup Port Management VLAN Management Statistics ACL Network Security Suite **QoS** Spanning Tree Multicast SNMP Admin Logout

CoS Settings Queue Settings DSCP Settings Bandwidth Basic Mode Advanced Mode

CoS Settings

QoS Mode: Basic

Class of Service	Queue	Restore Defaults
0	2	<input type="checkbox"/>
1	1	<input type="checkbox"/>
2	1	<input type="checkbox"/>
3	2	<input type="checkbox"/>
4	3	<input type="checkbox"/>
5	3	<input type="checkbox"/>
6	4	<input type="checkbox"/>
7	4	<input type="checkbox"/>

Restore Defaults

<<Previous 1 2 3 4 Next>>

Interface	Default CoS
e1	0
e2	0
e3	0
e4	0
e5	0
e6	0
e7	0
e8	0
e9	0
e10	0

232677

The *CoS Settings Screen* has two areas, CoS Settings and CoS Default.

The *CoS Settings* area contains the following fields:

- **QoS Mode** — Indicates if QoS is enabled on the interface. The possible values are:
 - *Disable* — Disables QoS on the device.
 - *Basic* — Enables QoS Basic Mode on the device.
 - *Advanced* — Enables QoS Advanced Mode on the device.
- **Class of Service** — Specifies the CoS priority tag values, where zero is the lowest and 7 is the highest.
- **Queue** — Defines the traffic forwarding queue to which the CoS priority is mapped. Four traffic priority queues are supported, where Queue 4 has the highest priority and Queue 1 has the lowest priority.
- **Queue** — Defines the traffic forwarding queue to which the CoS priority is mapped. Three priority queues are supported.
- **Restore Defaults** — Restores the device factory defaults for mapping CoS values to a forwarding queue.

STEP 2 Enable the QoS mode and, if relevant, change the CoS-Queue priority mapping.

For 24-port devices, the CoS Default Table displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, **3**, **4**, and **Next** links above the table.

Figure 71 CoS Settings Screen — CoS Port Defaults

The screenshot shows the Linksys web interface for a 24-Port 10/100 Ethernet Switch (SPS 22404). The 'QoS' menu is selected, and the 'CoS Settings' sub-menu is active. The 'CoS Default' section displays a table for configuring CoS settings for various interfaces. The table has two columns: 'Interface' and 'Default CoS'. The 'Default CoS' column contains dropdown menus, all currently set to '0'. Navigation links '<<Previous', '1', '2', '3', '4', and 'Next>>' are visible above the table. A 'Save Settings' button and a 'Cancel Changes' button are at the bottom right. A sidebar on the right provides additional information about the CoS Settings screen.

Interface	Default CoS
e1	0
e2	0
e3	0
e4	0
e5	0
e6	0
e7	0
e8	0
e9	0
e10	0
e11	0
e12	0

The *CoS Settings Screen — CoS Port Defaults* contains the following fields:

- **Unit No.** — Indicates the stacking member being managed.
- **Interface** — Port interface to which the CoS configuration applies.
- **Default CoS** — Determines 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.
- **LAG** — LAG to which the port belongs, if relevant. If the port is a member of a LAG, the LAG settings override the port settings.

STEP 3 In the CoS Default Table, define the default CoS levels for the device interfaces.

STEP 4 Click **Save Settings**. The Cos Settings are modified, and the device is updated.

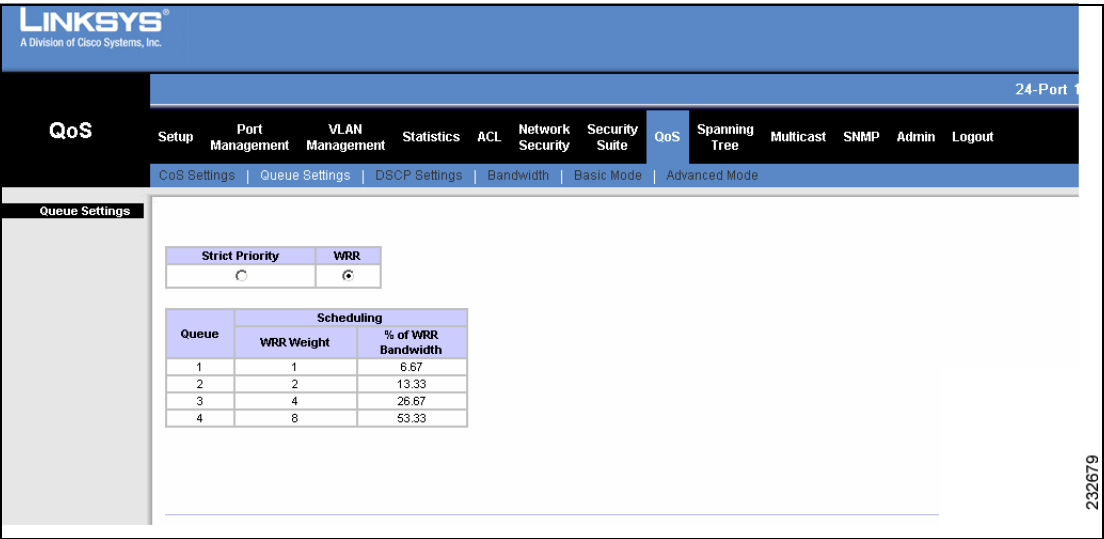
Queue Settings

The *Queue Settings Screen* contains fields for defining the QoS queue forwarding types and scheduling. The queue settings can be defined for the whole device (SPS 208, SPS 224G4) or per queue (SPS 2024). The queue settings are defined for the whole device. The queue settings can be defined per queue.

To define queue scheduling:

- STEP 1** Click **QoS > Queue Settings**. The *Queue Settings Screen* opens.

Figure 72 Queue Settings Screen



The *Queue Settings Screen* contains the following fields:

- **Strict Priority** — Indicates that traffic scheduling on the whole device is based strictly on the queue priority.
- **WRR** — Indicates that traffic scheduling on the whole device is based strictly on the *Weighted Round Robin* (WRR). The predetermined weights 8, 2, 4, and 1 are assigned to queues 4, 3, 2 and 1, respectively.



NOTE WRR and Strict Priority exclude each other and are applied globally to all ports on the device.

- **Queue** — Displays the queue for which the queue settings are displayed. The device supports four queues.
- **WRR Weight** — Indicates the WRR weight assigned to the queue.
- **% of WRR Bandwidth** — Indicates the percentage of bandwidth assigned to the QoS queue.

STEP 2 Select whether traffic scheduling is based on either Strict Priority or WRR.

STEP 3 Click **Save Settings**. The queue scheduling settings are defined, and the device is updated.

DSCP Settings

The *DSCP Settings Screen* contains fields for assigning packet DSCP tag values to traffic queues.

To map DSCP values to queues:

STEP 1 Click **QoS > DSCP Settings**. The *DSCP Settings Screen* opens.

Figure 73 DSCP Settings Screen

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0	1	16	2	32	3	48	4
1	1	17	2	33	3	49	4
2	1	18	2	34	3	50	4
3	1	19	2	35	3	51	4
4	1	20	2	36	3	52	4
5	1	21	2	37	3	53	4
6	1	22	2	38	3	54	4
7	1	23	2	39	3	55	4
8	1	24	2	40	3	56	4
9	1	25	2	41	3	57	4
10	1	26	2	42	3	58	4
11	1	27	2	43	3	59	4
12	1	28	2	44	3	60	4
13	1	29	2	45	3	61	4
14	1	30	2	46	3	62	4
15	1	31	2	47	3	63	4

The *DSCP Settings Screen* contains the following fields:

- **DSCP** — Displays the incoming packet's DSCP value. The following values are reserved and cannot be changed: **3, 11, 19, 27, 35, 43, 51, and 59**.
- **Queue** — Defines the traffic forwarding queue to which the DSCP priority is mapped. Four traffic priority queues are supported.
- **Queue** — Defines the traffic forwarding queue to which the DSCP priority is mapped. In a standalone device, four traffic priority queues are supported. In stacked devices, three priority queues are supported.

STEP 2 Match the DSCP values to the appropriate queues.

STEP 3 Click **Save Settings**. The DSCP Settings are saved and the device is updated.

Bandwidth

The *Bandwidth Screen* allows network managers to define the bandwidth settings for specified egress and ingress interfaces. Modifying queue scheduling affects the queue settings globally.

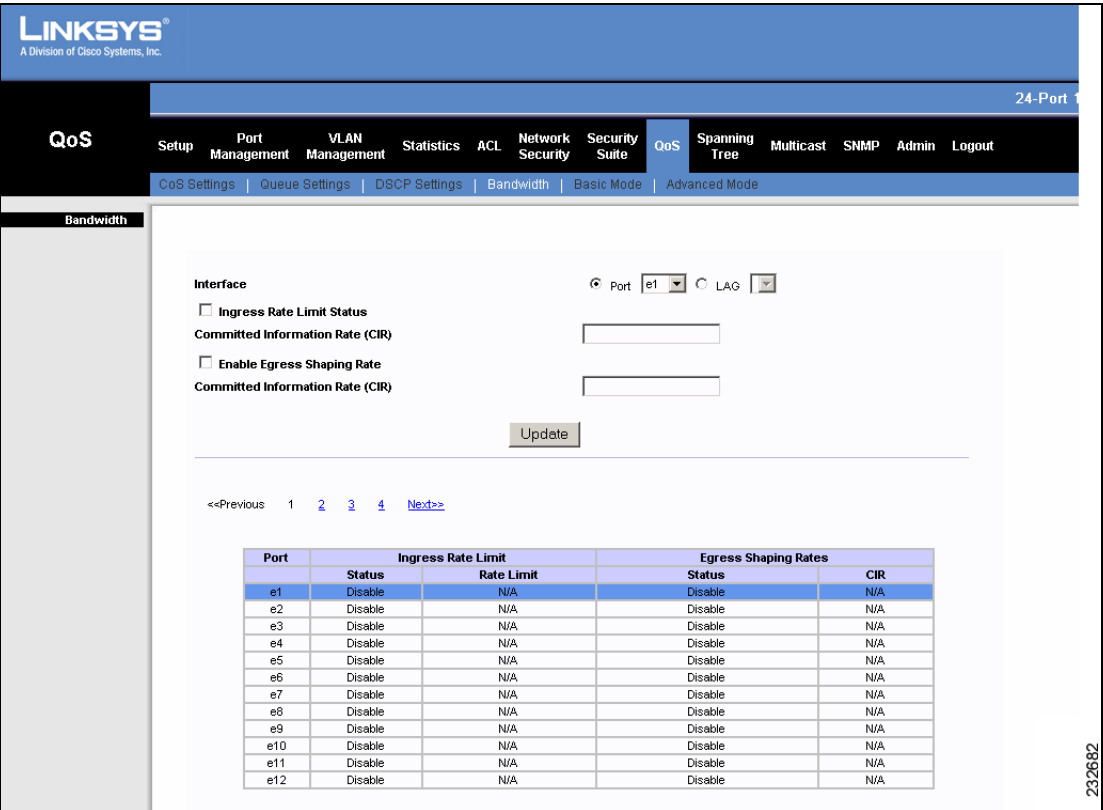
Rate Limits and Shaping are defined per interface:

- Rate Limit sets the maximum bandwidth allowed on an interface.
- Shaping Rate sets the maximum bandwidth allowed on egress interfaces.

To define bandwidth settings:

STEP 1 Click **QoS > Bandwidth**. The *Bandwidth Screen* opens.

Figure 74 Bandwidth Screen



The *Bandwidth Screen* is divided into the following areas:

- Interface Bandwidth Parameters
- Bandwidth Table

The Interface Bandwidth Parameters area contains the following fields:

- **Interface** — Indicates the interface for which this bandwidth information is displayed. The possible field values are:
 - *Port* — Indicates the port for which the bandwidth settings are displayed.
 - *LAG* — Indicates the LAG for which the bandwidth settings are displayed.
- **Ingress Rate Limit Status** — Enables ingress rate limiting on the interface.

- **Committed Information Rate (CIR)** — Defines the traffic rate, when CIR is the traffic shaping type. The possible field value is:
 - For FE ports, 62 Kb - 62.5 Mb.
 - For GE ports, 62 Mb - 1000 Mb.
- **Enable Egress Shaping Rate** — Configures the traffic shaping type for egress interfaces.
Egress Shaping is performed according to the **Token Bucket** Algorithm.
- **Committed Information Rate (CIR)** — Defines the traffic rate, when CIR is the traffic shaping type. The possible field value is 64 Kbps to the maximum port speed.

For 8-port devices, the Bandwidth Table displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, and **Next** links above the table.

For 24-port devices, the Bandwidth Table displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, **3**, and **Next** links above the table.

The Bandwidth Table contains the following fields:

- **Port** — Indicates the interface for which the traffic shaping information is displayed.
- **Ingress Rate Limit** — Displays the Ingress Rate Limit information. The following information is displayed:
 - *Status* — Displays the Enable Ingress Rate Limit status for the selected interface.
 - *Rate Limit* — Displays the Ingress Rate Limit rate for the selected interface.
- **Egress Shaping Rate** — Displays the Egress Shaping Rate information. The following information is displayed:
 - *Status* — Displays the Egress Shaping Rate status for the selected interface.
 - *CIR* — Displays the Egress traffic shaping rate in CIR for the selected interface.

STEP 2 Click **Save Settings**. The Bandwidth settings are saved and the device is updated.

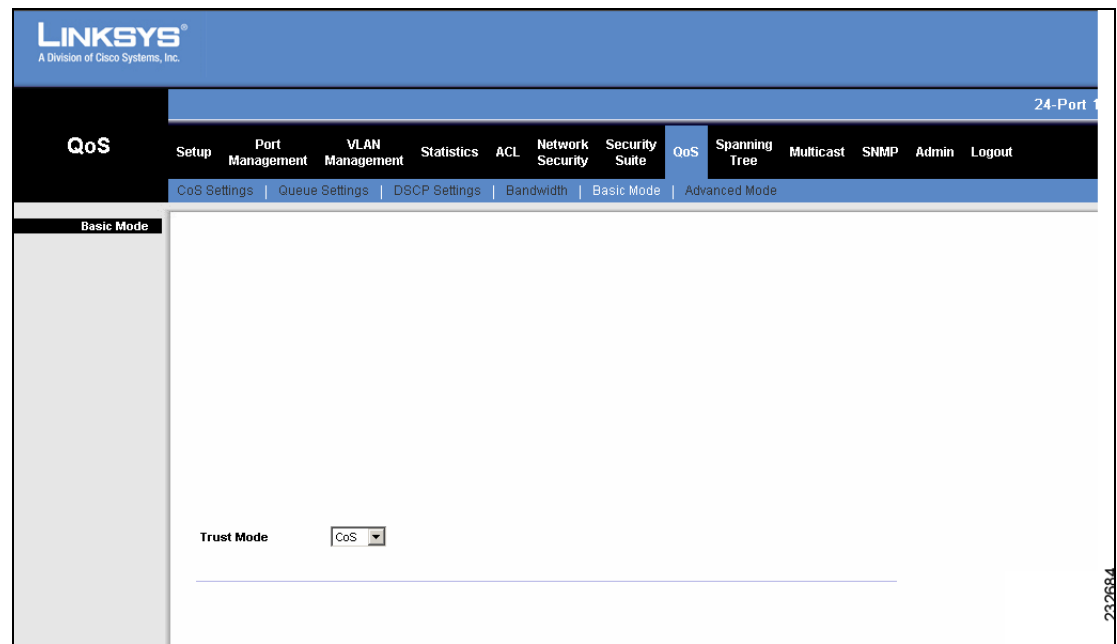
Basic Mode

The *Basic Mode Screen* contains information for enabling Trust on the device. Packets entering a network are classified at the edge of the QoS domain. When the packets are assigned either DSCP or CoS value, Trust can be enabled globally. If a packet's CoS tag and DSCP tag are mapped to different queues, the Trust mode determines the queue to which the packet is assigned.

To define the Trust configuration:

STEP 1 Click **QoS > Basic Mode**. The *Basic Mode Screen* opens.

Figure 75 Basic Mode Screen



The *Basic Mode Screen* contains the following fields:

- **Trust Mode** — Displays the trust mode. If a packet's CoS tag and DSCP tag are mapped to different queues, the Trust Mode determines the queue to which the packet is assigned. Possible values are:
 - *CoS* — Sets trust mode to CoS on the device. The CoS mapping determines the packet queue.
 - *DSCP* — Sets trust mode to DSCP on the device. The DSCP mapping determines the packet queue.

STEP 2 Define the Trust Mode.

STEP 3 Click **Save Settings**. The Trust settings are saved and the device is updated.

Advanced Mode

Advanced QoS mode provides administrators with a complete set of QoS configuration components.

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

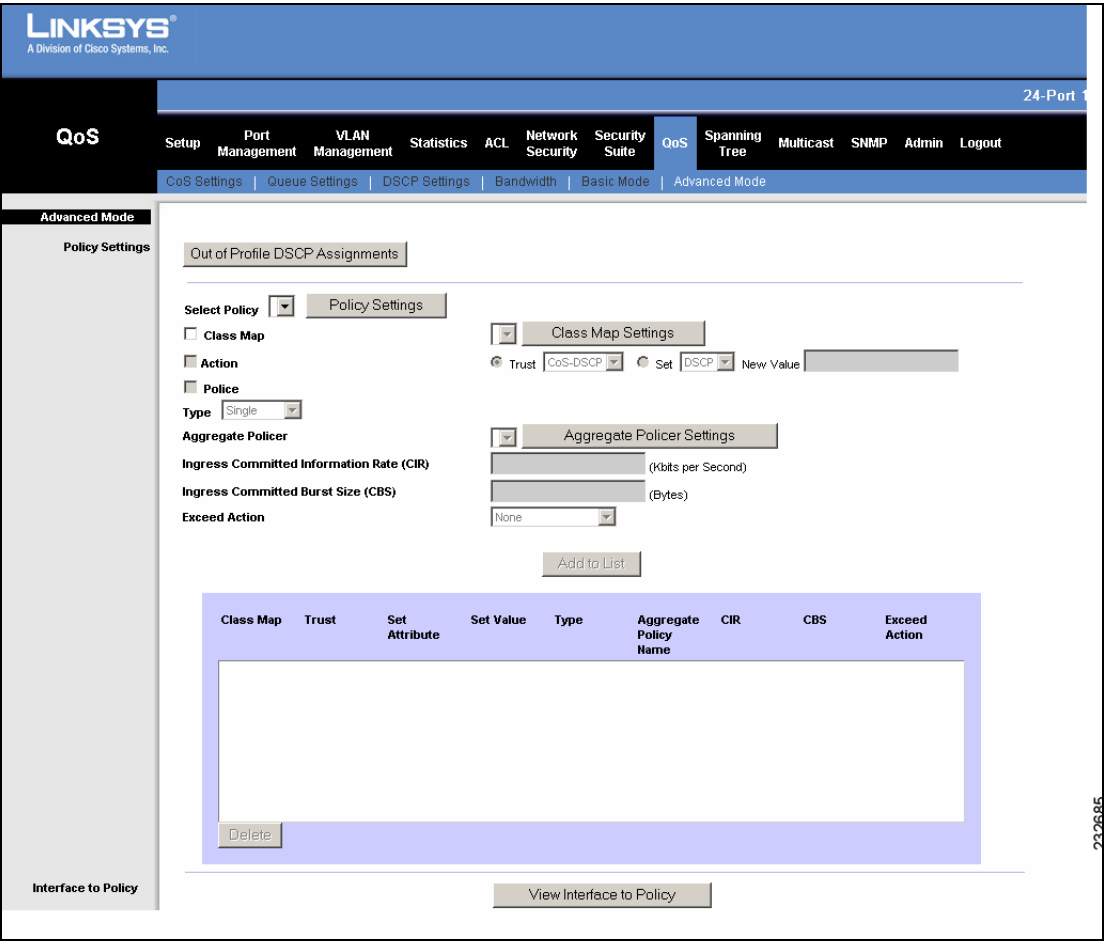
The *Advanced Mode Screen* contains parameters for setting up policies and assigning them to interfaces. The Advanced Mode Screen also provides access to the following QoS configuration options:

- Out of Profile DSCP Assignments
- Policy Name
- Class Map
- Aggregate Policer
- Interface To Policy

To define the Advanced QoS Mode configuration:

STEP 1 Click **QoS > Advanced Mode**. The *Advanced Mode Screen* opens.

Figure 76 Advanced Mode Screen - Policy Settings



The *Advanced Mode Screen* is divided into the following areas:

- Policy Settings
- Policy Table
- Interface To Policy

The Policy Settings area contains the following command:

- **Out of Profile DSCP Assignments** — Opens the *Out of Profile DSCP Assignments Screen*, in which users define the Differentiated Services Code Point (DSCP) tag to use in place of the incoming DSCP tags. For more information, see Out of Profile DSCP Assignments later in this section. For more information, see Out of Profile DSCP Assignments.
- **Select Policy** — Selects the active policy name.
 - *Policy Settings* — Click this button to create and configure policies in the *Policy Name Screen*. For more information, see Policy Name later in this section. For more information, see Policy Name.
- **Class Map** — Defines the name of the active class map.
 - *Class Map Settings* — Click this button to create and configure class maps in the *New Class Map Screen*. For more information, see Class Map later in this section. For more information, see Class Map.
- **Action** — Defines the action attached to the class rule. The possible field values are:
 - **Trust** — Enables CoS-DSCP Trust Mode for the class. This command is used to distinguish the QoS trust behavior for given traffic. When a given type is trusted, the QoS mechanism maps a packet to a queue using the received or default value and the relevant map, as defined on the QoS Settings. By designating trust, it is possible to trust only incoming traffic with certain DSCP values.
 - **Set** — Defines the Trust configuration manually. The possible field values are:
 - *DSCP* — In the **New Value** box, the possible values are 0-63.
 - *CoS* — In the **New Value** box, the possible values are 0-7.



NOTE The CoS setting will not affect regular IP traffic. This setting affects only non-IP traffic, unless the outgoing port is Gigabit port.

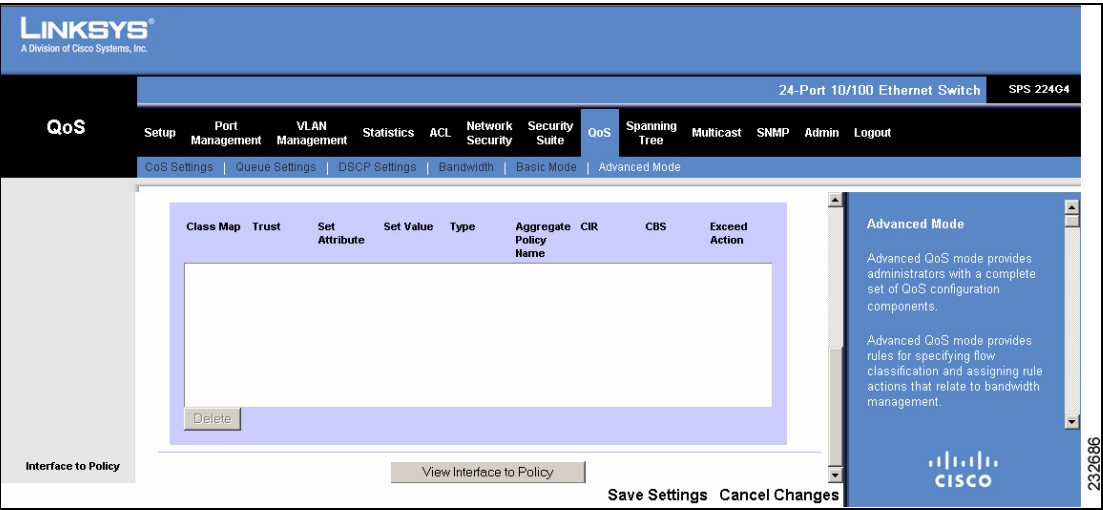
- **Police** — Enables Policer functionality.

- **Type** — Policer type for the policy. Possible values are:
 - *Aggregate* — Configures the class to use a configured aggregate policer selected from the drop-down menu. An aggregate policer is defined if the policer is shared with multiple classes. Traffic from two different ports can be configured for policing purposes. An aggregate policer can be applied to multiple classes in the same policy map, but cannot be used across different policy maps.
 - *Single* — Configures the class to use manually configured information rates and exceed actions.
- **Aggregate Policer** — Specifies the Aggregate Policer Name.
 - Aggregate Policer Settings — Click this button to create and configure aggregate policers in the *New Aggregate Policer Screen*. For more information, see Aggregate Policer later in this section. For more information, see Aggregate Policer.
- **Ingress Committed Information Rate (CIR)** — Defines the CIR in Kbps. This field is only relevant when the Police Type is *Single*.
- **Ingress Committed Burst Size (CbS)** — Defines the CbS in bytes. This field is only relevant when the Police Type is *Single*.
- **Exceed Action** — Action assigned to incoming packets exceeding the CIR. This field is only relevant when the Police value is Single. Possible values are:
 - *Drop* — Drops packets exceeding the defined CIR value.
 - *Out Of Profile DSCP* —Remarks packet's DSCP values exceeding the defined CIR value.
 - *None* —Forwards packets exceeding the defined CIR value.

STEP 2 Define the relevant fields.

STEP 3 Click **Add To List**. The policy profile is defined and is displayed in the Policy Table below the Policy Settings.

Figure 77 Advanced Mode Table



- In addition to the Policy Settings, the Policy Table contains the following fields:
- **Trust** — Displays the Trust mode attached to the rule.
 - **Set Attribute** — Indicates the defined Trust mode. The possible field values are *DSCP* and *CoS*.
 - **Set Value** — Indicates the Trust value.
 - If the Trust mode is DSCP, the possible DSCP values are 0-63.
 - If the Trust mode is CoS, the possible priority values are 0-7.
 - **Aggregate Policy Name** — Displays the Aggregate Policer Name.
 - **CIR** — Displays the Ingress Committed Information Rate in kbps.
 - **CBS** — Displays the Ingress Committed Burst Size in bytes.

To modify policy settings:

- STEP 1** Click **QoS > Advanced Mode**. The *Advanced Mode Screen* opens.
- STEP 2** In the Policy Table below the Policy Settings, click a policy to modify.
- STEP 3** Define the relevant fields.
- STEP 4** Click **Update**. The policy profile is defined and is displayed in the Policy Table.

To delete a policy from the device:

- STEP 1
- In the Policy Table, select the entry.
- STEP 2
- Click **Delete**. The selected policy is deleted from the device.

The Interface To Policy area contains the following field:

- **View Interface To Policy** — Opens the *Interface To Policy Screen*, where QoS policies are bound with specific interfaces. For more information, see Interface To Policy later in this section. For more information, see Interface To Policy.

Out of Profile DSCP Assignments

In the *Out of Profile DSCP Assignments Screen*, administrators rewrite the outgoing Differentiated Services Code Point (DSCP) tag to use in place of the incoming DSCP tags.

To rewrite the DSCP tags:

- STEP 1
- Click **QoS > Advanced Mode**. The *Advanced Mode Screen* opens.
- STEP 2
- In the Policy Settings area, click **Out of Profile DSCP Assignments**. The *Out of Profile DSCP Assignments Screen* opens.

Figure 78 Out of Profile DSCP Assignments Screen

Out of Profile DSCP Assignments							
DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out	DSCP In	DSCP Out
0	0	16	16	32	32	48	48
1	1	17	17	33	33	49	49
2	2	18	18	34	34	50	50
3	3	19	19	35	35	51	51
4	4	20	20	36	36	52	52
5	5	21	21	37	37	53	53
6	6	22	22	38	38	54	54
7	7	23	23	39	39	55	55
8	8	24	24	40	40	56	56
9	9	25	25	41	41	57	57
10	10	26	26	42	42	58	58
11	11	27	27	43	43	59	59
12	12	28	28	44	44	60	60
13	13	29	29	45	45	61	61
14	14	30	30	46	46	62	62
15	15	31	31	47	47	63	63

CloseSave & CloseSave

The *Out of Profile DSCP Assignments Screen* contains the following fields:

- **DSCP In** — Indicates the DSCP value in the incoming packet.
- **DSCP Out** — Indicates the DSCP value in the outgoing packet.

STEP 3 Define the DSCP mappings.

STEP 4 Click **Save & Close** to save the modifications and close the *Out of Profile DSCP Assignments Screen* (clicking **Save** keeps the *Out of Profile DSCP Assignments Screen* open). The device is updated.

Policy Name

In the *Policy Name Screen*, administrators create new policies which can be assigned to interfaces.

To create a new policy:

STEP 1 Click **QoS > Advanced Mode**. The *Advanced Mode Screen* opens.

STEP 2 In the Add Alarms area, click **Policy Settings**. The *Policy Name Screen* opens.

Figure 79 Policy Name Screen

Policy Name

Policy Name

Add to List

#	Policy Name
---	-------------

Delete

Close Save & Close Save

232688

The *Policy Name Screen* is divided into the following areas:

- Policy Name Parameter
- Policy Name Table

The Policy Name Parameter area contains the following field:

- **Policy Name** — Defines a new policy name.

STEP 3 Define the new Policy Name.

STEP 4 Click **Add To List**. The new policy name is defined and is displayed in the Policy Name Table in the bottom half of the *Policy Name Screen*.

STEP 5 Click **Save & Close** to save the new policy and close the *Policy Name Screen* (clicking **Save** keeps the *Policy Name Screen* open). The device is updated.

To delete a policy name from the device:

STEP 1 In the Policy Name Table, select the entry.

STEP 2 Click **Delete**. The selected policy name is deleted from the device.

Class Map

The *New Class Map Screen* contains parameters for defining class maps. One IP ACL and/or one MAC ACL comprise a class map. Class maps are configured to match packet criteria. For example, Class Map A can be assigned to packets based only on an IP-based ACL or a MAC-based ACL. Class Map B can be assigned to packets based on both an IP-based and a MAC-based ACL.

Class maps are matched to packets on a first-fit basis, which makes their order in the Class Map Table very important.

To add class maps:

STEP 1 Click **QoS > Advanced Mode**. The *Advanced Mode Screen* opens.

STEP 2 In the Add Alarms area, click **Class Map Settings**. The *New Class Map Screen* opens.

Figure 80 New Class Map Screen

The *New Class Map Screen* is divided into the following areas:

- Add Class Map Parameters
- Class Map Table

The Add Class Map Parameters area contains the following fields:

- **Class Map Name** — Defines a new Class Map name.
- **Preferred ACL** — Defines if packets are first matched to an IP based ACL or a MAC based ACL. The possible field values are:
 - *IP Based* — Matches packets to IP based ACLs first, then matches packets to MAC based ACLs.
 - *MAC Based* — Matches packets to MAC based ACLs first, then matches packets to IP based ACLs.
- **IP ACL** — Defines the IP based ACL to match with packets.
- **Match** — Criteria used to match IP addresses and /or MAC addresses with an ACL's address. The possible field values are:
 - *And* — Both the MAC-based and the IP-based ACL must match a packet.
 - *Or* — Either the MAC-based or the IP-based ACL must match a packet.

- **MAC ACL** — Defines the MAC based ACL to match with packets.

- STEP 3** Create class maps in order of preference for first-fit execution. Define the relevant fields.
- STEP 4** Click **Add To List**. The new class map is defined and is displayed in the Class Map Table in the bottom half of the *New Class Map Screen*.
- STEP 5** Click **Save & Close** to save the new class map and close the *New Class Map Screen* (clicking **Save** keeps the *New Class Map Screen* open). The device is updated.

To delete a class map from the device:

- STEP 1** In the Class Map Table, select the entry.
- STEP 2** Click **Delete**. The selected class map is deleted from the device.
-

Aggregate Policer

A policy is a collection of classes, each of which is a combination of a class map and a QoS action to apply to matching traffic. Classes are applied in a first-fit manner within a policy.

Before configuring policies for classes whose match criteria are defined in a class map, a class map must first be defined, or the name of the policy map to be created, added to, or modified must first be specified. Class policies can be configured in a policy map only if the classes have defined match criteria.

An aggregate policer can be applied to multiple classes in the same policy map, but an aggregate policer cannot be used across different policy maps. Define an aggregate policer if the policer is shared with multiple classes. Policers in one port cannot be shared with other policers in another device. Traffic from two different ports can be aggregated for policing purposes.

To define aggregate policers:

- STEP 1** Click **QoS > Advanced Mode**. The *Advanced Mode Screen* opens.
- STEP 2** In the Add Alarms area, click **Aggregate Policer Settings**. The *New Aggregate Policer Screen* opens.

Figure 81 New Aggregate Policer Screen

The *New Aggregate Policer Screen* is divided into the following areas:

- Aggregate Policer Parameters
- Aggregate Policer Table

The Aggregate Policer Parameters area contains the following fields:

- **Aggregate Policer Name**— Specifies the Aggregate Policer Name.
- **Ingress Committed Information Rate (CIR)** — Defines the Committed Information Rate (CIR) in bits per second.
- **Ingress Committed Burst Size (CbS)** — Defines the Committed Burst Size (CbS) in bytes per second.
- **Exceed Action** — Action assigned to incoming packets exceeding the CIR. Possible values are:
 - *Drop* — Drops packets exceeding the defined CIR value.
 - *Remark DSCP*—Remarks packet's DSCP values exceeding the defined CIR value.
 - *None* — Forwards packets exceeding the defined CIR value.

STEP 3 Define the relevant fields.

-
- STEP 4** Click **Add To List**. The new aggregate policer is defined and is displayed in the Aggregate Policer Table in the bottom half of the *New Aggregate Policer Screen*.
- STEP 5** Click **Save & Close** to save the new aggregate policer and close the *New Aggregate Policer Screen* (clicking **Save** keeps the *New Aggregate Policer Screen* open). The device is updated.
-

To delete an aggregate policer from the device:

-
- STEP 1** In the Aggregate Policer Table, select the entry.
- STEP 2** Click **Delete**. The selected aggregate policer is deleted from the device.
-

Interface To Policy

The *Interface To Policy Screen* displays QoS policies which are bound to specific interfaces.

-
- STEP 1** Click **QoS > Advanced Mode**. The *Advanced Mode Screen* opens.
- STEP 2** In the Interface To Policy area, click **View Interface To Policy**. The *Interface To Policy Screen* opens.

Figure 82 Interface To Policy Screen

LINKSYS
A Division of Cisco Systems, Inc.

24-Port

QoS

Setup Port Management VLAN Management Statistics ACL Network Security Security Suite QoS Spanning Tree Multicast SNMP Admin Logout

CoS Settings Queue Settings DSCP Settings Bandwidth Basic Mode Advanced Mode

Interface To Policy

<<Previous 1 2 3 4 Next>>

Interface	Policy Name
e1	None
e2	None
e3	None
e4	None
e5	None
e6	None
e7	None
e8	None
e9	None
e10	None
e11	None
e12	None

Back

232691

The *Interface To Policy Screen* contains the following fields:

- **Interface** — Displays the interface to which the entry refers.
- **Policy Name** — Defines a Policy bound to the interface.

STEP 3 Bind policies to relevant interfaces.

STEP 4 Click **Save Settings**. The Interface To Policy settings are saved and the device is updated.

Spanning Tree

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

Loops occur when alternate 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 device supports the **Classic STP** Spanning Tree version, which provides a single path between end stations, avoiding and eliminating loops.

The device supports the following Spanning Tree versions:

- **Classic STP** — Provides a single path between end stations, avoiding and eliminating loops.
- **Rapid STP (RSTP)** — Detects and uses network topologies that provide faster convergence of the spanning tree, without creating forwarding loops.
- **Multiple STP (MSTP)** — Provides full connectivity for packets allocated to any VLAN. Multiple STP is based on the RSTP. In addition, Multiple STP transmits packets assigned to different VLANs through different MST regions. MST regions act as a single bridge.

The Spanning Tree configuration options are as follows:

- STP Status
- Global STP
- STP Port Settings
- RSTP Port Settings
- MSTP Properties
- MSTP Instance Settings
- MSTP Interface Settings

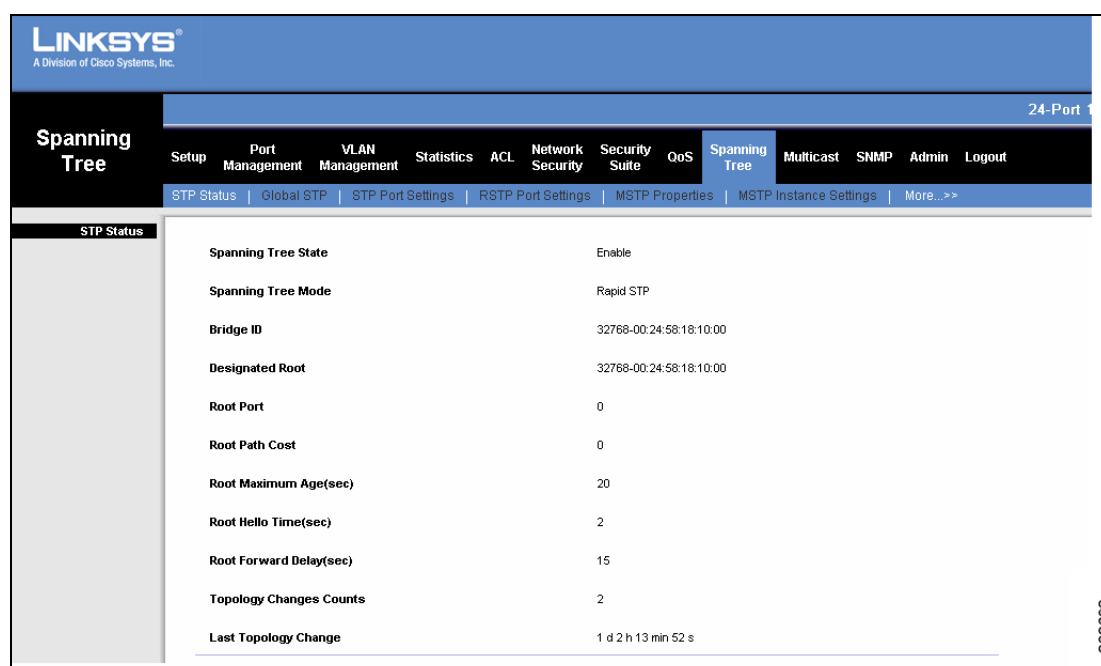
STP Status

The *STP Status Screen* describes the current Spanning Tree information and status globally on the device.

To view STP status and information:

STEP 1 Click **Spanning Tree > STP Status**. The *STP Status Screen* opens.

Figure 83 STP Status Screen



The *STP Status Screen* contains the following fields:

- **Spanning Tree State** — Indicates if STP is enabled on the device. The possible field values are:
 - *Enable* — Indicates whether STP is enabled on the device.
 - *Disable* — Indicates whether STP is disabled on the device.
- **Spanning Tree Mode** — Indicates the STP mode that is enabled on the device.
- **Bridge ID** — Identifies the bridge priority and MAC address.
- **Designated Root** — Identifies the bridge priority and MAC address of the root bridge.

- **Root Port** — Indicates the port number that offers the lowest cost path from this bridge to the Root Bridge. It is significant when the Bridge is not the Root.
- **Root Path Cost** — The cost of the path from this bridge to the root.
- **Root Maximum Age (sec)** — Indicates the device Maximum Age Time. The Maximum Age Time indicates the amount of time in seconds a bridge waits before sending configuration messages. The default max age is 20 seconds. The range is 6 to 40 seconds.
- **Root Hello Time (sec)** — Indicates 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. The range is 1 to 10 seconds.
- **Root Forward Delay (sec)** — Indicates the device forward delay time. The Forward Delay Time indicates the amount of time in seconds a bridge remains in both learning and listening states before forwarding packets. The default is 15 seconds. The range is 4 to 30 seconds.

For example, if the value = 15 seconds, the device can remain in the listening state for 15 seconds and then in the learning state for 15 seconds before forwarding the packets.

- **Topology Changes Counts** — Indicates the total amount of STP topology 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 occurred. The time is displayed in a day hour minute second format, for example, 2 days 5 hours 10 minutes and 4 seconds:

Global STP

The *Global STP Screen* contains parameters for enabling Spanning Tree on the device.

To define the device STP configuration:

STEP 1 Click **Spanning Tree > Global STP**. The *Global STP Screen* opens.

Figure 84 Global STP Screen

LINKSYS®
A Division of Cisco Systems, Inc.

Spanning Tree

Setup Port Management VLAN Management Statistics ACL Network Security Security Suite QoS Spanning Tree Multicast SNMP Admin Logout

STP Status Global STP STP Port Settings RSTP Port Settings MSTP Properties MSTP Instance Settings More...>>

Global STP

Global Settings

Spanning Tree State: Enable

STP Operation Mode: Rapid STP

BPDU Handling: Flooding

Path Cost Default Values: Long

Bridge Settings

Priority: 32768

Hello Time: 2 (Sec)

Max Age: 20 (Sec)

Forward Delay: 15 (Sec)

232693

The *Global STP Screen* is divided into two areas:

- Global Settings
- Bridge Settings

The Global Settings area contains the following fields:

- **Spanning Tree State** — Indicates if STP is enabled on the device. The possible field values are:
 - *Enable* — Enables STP on the device.
 - *Disable* — Disables STP on the device.
- **Spanning Tree Mode** — Indicates 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 Bridge Protocol Data Units (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.
 - *Flooding* — Floods BPDU packets when spanning tree is disabled on an interface. This is the default value.
 - *Bridging* — Indicates the both REP and STP BPDU packets are bridged with all the VLAN rules and configurations.
- **Path Cost Default Values** — Specifies the method used to assign default path costs to STP ports. The possible field values are:
 - *Short* — Specifies that the default path costs are per the short default cost method. The possible range is 1 through 65535.
 - *Long* — Specifies that the default path costs are per the long default cost method. The possible range is 1 through 200,000,000. This is the default value.

The Bridge Settings area contains the following fields:

- **Priority** — 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 bridge priority value is provided in increments of 4096. For example, 4096, 8192, 12288, etc. The range is 0 to 65535. The default value is 32768.



NOTE The Hello Time, Max Age and Forward Delay fields are applicable to the Root Bridge and must be set individually. After each field is set, save the configuration.

- **Hello Time** — Specifies the device Hello Time. The Hello Time indicates the amount of time in seconds a root bridge waits between configuration messages. The range is 1 to 10 seconds. The default is 2 seconds.

- **Max Age** — Specifies the device Maximum Age Time. The Maximum Age Time indicates the amount of time in seconds a bridge waits before sending configuration messages. The range is 6 to 40 seconds. The default max age is 20 seconds.
- **Forward Delay** — Specifies the device forward delay time. The Forward Delay Time indicates the amount of time in seconds a bridge remains in a learning state before forwarding packets. The range is 4 to 30 seconds. The default is 15 seconds.

STEP 2 Define the relevant fields.

STEP 3 Click **Save Settings**. The device STP configuration is saved and the device is updated.

STP Port Settings

Network administrators can assign STP settings to specific interfaces using the *STP Port Settings Screen*.

To define interface STP configurations:

- STEP 1** Click **Spanning Tree > STP Port Settings**. The *STP Port Settings Screen* opens.

Figure 85 STP Port Settings Screen

LINKSYS®
A Division of Cisco Systems, Inc.

24-Port

Spanning Tree

SetupPort ManagementVLAN ManagementStatisticsACLNetwork SecuritySecurity SuiteQoSSpanning TreeMulticastSNMPAdminLogout

STP StatusGlobal STPSTP Port SettingsRSTP Port SettingsMSTP PropertiesMSTP Instance SettingsMore...>>

STP Port Settings

Interface

Port e1LAG

Enable STP☒

Port Fast☐

Port StateDisable

Speed100M

Path Cost2000000

Default Path Cost☐

Root Guard☐

Priority128

Designated Bridge IDN/A

Designated Port IDN/A

Designated CostN/A

Forward TransitionsN/A

Update

<<Previous1234Next>>

Port	STP	Port Fast	Port State	Port Role	Speed	Path Cost	Root Guard	Priority	Designated Bridge ID	Designated Port ID	Designated Cost	Forward Transitions
e1	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e2	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e3	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e4	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e5	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e6	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e7	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e8	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e9	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e10	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e11	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e12	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A

The *STP Port Settings Screen* is divided into two areas:

- STP Port Parameters
- STP Port Table

The STP Port Parameters area contains the following fields:

- **Interface** — Define the port or LAG of this STP configuration. The possible field values are:
 - *Unit No.* — Indicates the stacking member on which this STP configuration is defined.
 - *Port* — Indicates the port on which this STP configuration is defined.
 - *LAG* — Indicates the LAG on which this STP configuration is defined.
- **Enable STP** — Enable or disable STP on the port. The possible field values are:
 - *Checked* — Indicates that STP is enabled on the port.
 - *Unchecked* — Indicates that STP is disabled on the port.
- **Port Fast** — Enable or disable Fast Link 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. The possible field values are:
 - *Checked* — Indicates that Fast Link is enabled on the port.
 - *Unchecked* — Indicates that Fast Link is disabled on the port.
- **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:
 - *Disable* — Indicates that STP is currently disabled on the port or if the port is not active. The port forwards traffic while learning MAC addresses.
 - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses.
 - *Listening* — Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.

- *Learning* — Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
- *Forwarding* — Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **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 used for forwarding traffic.
- **Default Path Cost** — When checked, returns the path cost to its default value.
- **Root Guard** — Enables or disables Root Guard, which prevents devices outside the network core from being assigned the spanning tree root. The possible field values are:
 - *Enable* — Indicates that Root Guard is enabled on the selected port or LAG.
 - *Disable* — Indicates that Root Guard is disabled on the selected port or LAG. This is the default value.
- **Priority** — Priority value of the port. The priority value influences the port choice when a bridge has two paths to the root. The priority value is between 0-240. The priority value is provided in increments of 16.
- **Designated Bridge ID** — Displays the bridge priority and the MAC Address of the designated bridge.
- **Designated Port ID** — Displays the designated port's priority and interface.
- **Designated Cost** — Displays the cost of the designated port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
- **Forward Transitions** — Displays the number of times the port has changed from the **Blocking** state to **Forwarding** state.

STEP 2 Define the relevant fields.

STEP 3 Click **Update**. The interface STP configuration is defined and is displayed in the STP Port Table.

STEP 4 Click **Save Settings**. The STP configuration is saved and the device is updated.

Figure 86 STP Port Table

Port	STP	Port Fast	Port State	Port Role	Speed	Path Cost	Root Guard	Priority	Designated Bridge ID	Designated Port ID	Designated Cost	Forward Transitions
e1	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e2	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e3	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e4	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e5	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e6	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e7	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e8	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e9	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e10	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e11	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A
e12	Enable	Disable	Disable	Disable	100M	2000000	Disable	128	N/A	N/A	N/A	N/A

For 8-port devices, the STP Port Table displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, and **Next** links above the table.

For 24-port devices, the STP Port Table displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, **3**, and **Next** links above the table.

In addition to the STP Port Parameters, the STP Port Table contains the following fields:

- **Port** — Indicates the port or LAG of this STP configuration.
- **STP** — Indicates if STP is enabled or disabled on this port or LAG.
- **Port 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* — 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* — The port is not participating in the Spanning Tree.

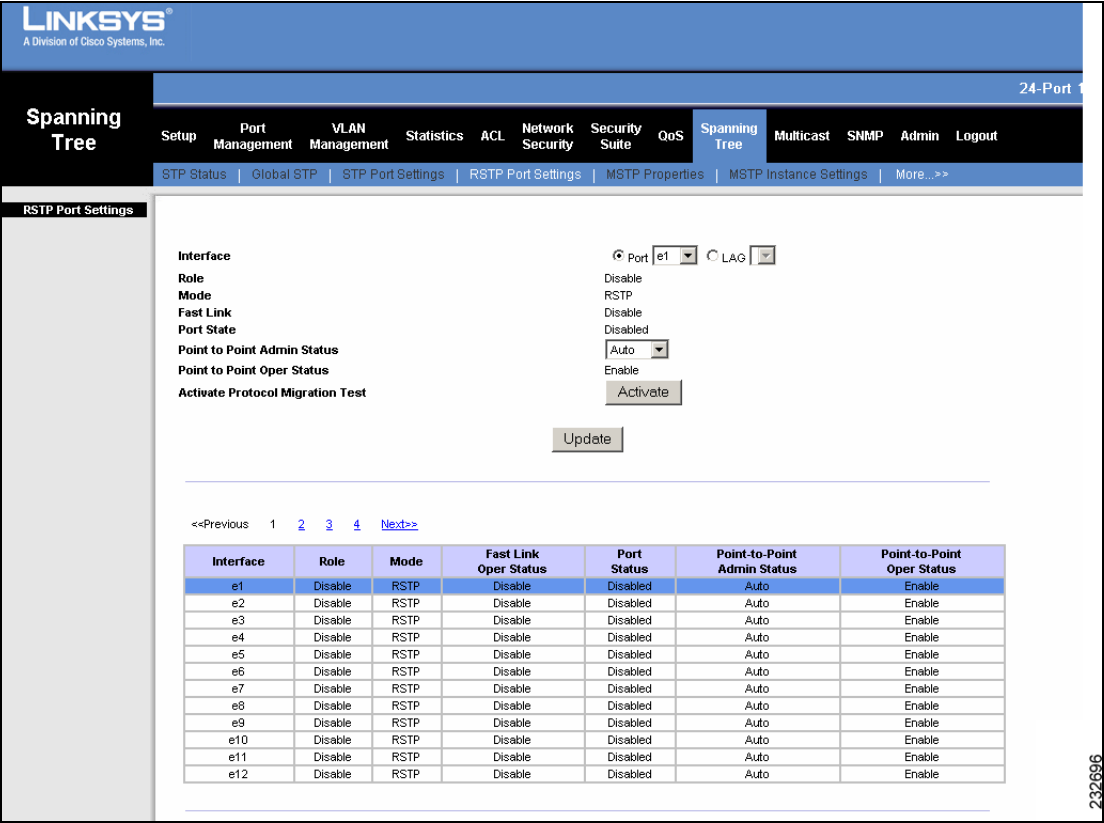
RSTP Port Settings

While the classic spanning tree 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.

To define RSTP on interfaces:

STEP 1 Click **Spanning Tree > RSTP Port Settings**. The *RSTP Port Settings Screen* opens.

Figure 87 RSTP Port Settings Screen



The *RSTP Port Settings Screen* is divided into two areas:

- RSTP Port Parameters
- RSTP Port Table

The RSTP Port Parameters area contains the following fields:

- **Interface** — Define the port or LAG of this RSTP configuration. The possible field values are:
 - *Unit No.* — Indicates the stacking member on which this RSTP configuration is defined.
 - *Port* — Indicates the port on which this RSTP configuration is defined.
 - *LAG* — Indicates the LAG on which this RSTP configuration is defined.
- **Role** — Indicates the port role assigned by the STP algorithm in order to provide STP paths. The possible field values are:
 - *Root* — Provides the lowest cost path to forward packets to root switch.
 - *Designated* — Indicates that the port or LAG via 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. Backup ports also occur when a LAN has two or more connections connected to a shared segment.
 - *Disable* — Indicates the port is not participating in the Spanning Tree.
- **Mode** — Indicates the current Spanning Tree mode. The possible field values are:
 - *STP* — Indicates that Classic STP is detected on the interface.
 - *Rapid STP* — Indicates that Rapid STP is detected on the interface.
 - *Multiple STP* — Indicates that Multiple STP is detected on the interface.
- **Fast Link** — Indicates if Fast Link is enabled or disabled for the port or LAG. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state. The possible field values are:
 - *Enable* — Fast Link is enabled.
 - *Disable* — Fast Link is disabled.
 - *Auto* — Fast Link mode is enabled a few seconds after the interface becomes active.

- **Port State** — Indicates the RSTP status on the specific port. The possible field values are:
 - *Disabled* — Indicates that STP is currently disabled on the port or if the port is not active. The port forwards traffic while learning MAC addresses.
 - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses.
 - *Listening* — Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.
 - *Learning* — Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
 - *Forwarding* — Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Point-to-Point Admin Status** — Indicates whether a point-to-point link is established on the port. Ports defined as Full Duplex are considered Point-to-Point port links. The possible field values are:
 - *Enable* — Device establishes point-to-point, full duplex links.
 - *Disable* — Device establishes shared, half duplex links.
 - *Auto* — Device automatically determines the state.
- **Point-to-Point Oper Status** — Indicates the Point-to-Point operating state.
- **Activate Protocol Migration Test** — Click the *Activate* button to run a Protocol Migration Test. The test identifies the STP mode of the interface connected to the selected interface.

The *RSTP Port Table* contains a list of the interface RSTP configurations on the device.

Figure 88 RSTP Port Table

Interface	Role	Mode	Fast Link Oper Status	Port Status	Point-to-Point Admin Status	Point-to-Point Oper Status
e1	Disable	RSTP	Disable	Disabled	Auto	Enable
e2	Disable	RSTP	Disable	Disabled	Auto	Enable
e3	Disable	RSTP	Disable	Disabled	Auto	Enable
e4	Disable	RSTP	Disable	Disabled	Auto	Enable
e5	Disable	RSTP	Disable	Disabled	Auto	Enable
e6	Disable	RSTP	Disable	Disabled	Auto	Enable
e7	Disable	RSTP	Disable	Disabled	Auto	Enable
e8	Disable	RSTP	Disable	Disabled	Auto	Enable
e9	Disable	RSTP	Disable	Disabled	Auto	Enable
e10	Disable	RSTP	Disable	Disabled	Auto	Enable
e11	Disable	RSTP	Disable	Disabled	Auto	Enable
e12	Disable	RSTP	Disable	Disabled	Auto	Enable

For 8-port devices, the RSTP Port Table displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, and **Next** links above the table.

For 24-port devices, the RSTP Port Table displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, **3**, and **Next** links above the table.

- STEP 2** In the RSTP Port Table, select the interface.
- STEP 3** Define the point-to-point status of the interface.
- STEP 4** Click **Update**. The interface RSTP configuration is defined and is displayed in the RSTP Port Table.
- STEP 5** Click **Save Settings**. The RSTP configuration is saved and the device is updated.

MSTP Properties

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

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.

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

To define MSTP on the device:

STEP 1 Click **Spanning Tree > MSTP Properties**. The *MSTP Properties Screen* opens.

Figure 89 MSTP Properties Screen

The screenshot displays the Linksys web interface for configuring MSTP properties. The top navigation bar includes links for Setup, Port Management, VLAN Management, Statistics, ACL, Network Security, Security Suite, QoS, Spanning Tree, Multicast, SNMP, Admin, and Logout. The 'Spanning Tree' menu is expanded, showing 'MSTP Properties' as the selected option. The 'MSTP Properties' section contains the following fields:

Field	Value
Region Name	00:24:58:18:10:00
Revision	0
Max Hops	20
IST Master	32768-00:24:58:18:10:00

The *MSTP Properties Screen* contains the following fields:

- **Region Name** — Provides a user-defined STP region name.
- **Revision** — Defines 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 field range 0-65535.

- **Max Hops** — Indicates 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 field default is 20 hops.
- **IST Master** — Identifies the region's master. The IST Master is the specified instance root.

STEP 2 Define the relevant fields.

STEP 3 Click **Save Settings**. The device MSTP configuration is saved and the device is updated.

MSTP Instance Settings

MSTP maps VLANs into STP instances. Packets assigned to various VLANs are transmitted along different paths within 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 MSTP Instances settings using the *MSTP Instance Settings Screen*.

To define the MSTP instance settings on the device:

- STEP 1** Click **Spanning Tree > MSTP Instance Settings**. The *MSTP Instance Settings Screen* opens.

Figure 90 MSTP Instance Settings Screen

The screenshot displays the Linksys web interface for configuring MSTP Instance Settings. The top navigation bar includes 'Spanning Tree' and other settings like 'Setup', 'Port Management', 'VLAN Management', etc. The left sidebar shows 'MSTP Instance Settings' as the active section. The main content area is titled 'VLAN Instance Configuration' and contains the following fields:

- Instance ID:** A dropdown menu set to '1'.
- Included VLAN:** A dropdown menu set to '1'.
- Instance Settings:**
 - Bridge Priority:** A text input field containing '32768'.
 - Designated Root Bridge ID:** A text input field containing '32768-00:24:58:18:10:00'.
 - Root Port:** A text input field containing '0'.
 - Root Path Cost:** A text input field containing '0'.
 - Bridge ID:** A text input field containing '32768-00:24:58:18:10:00'.
 - Remaining Hops:** A text input field containing '20'.

The *MSTP Instance Settings Screen* contains the following fields:

- **VLAN Instance Configuration** — Opens the VLAN Instance Configuration Screen, in which administrators can map VLANs to MSTP Instances. See VLAN Instance Configuration following this section. See VLAN Instance Configuration.
- **Instance ID** — Specifies the instance being defined. The possible values are 1-7.

- **Included VLAN** — Displays the VLANs mapped to the selected instance. Each VLAN belongs to one instance.
- **Bridge Priority** — Specifies the priority for this instance. The field range is 0-61440. The default value is 32768.
- **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 path cost to the root of this instance.
- **Bridge ID** — Indicates the bridge ID of the selected instance.
- **Remaining Hops** — Indicates the number of hops remaining to the next destination.

STEP 2 Define the relevant fields.

STEP 3 Click **Save Settings**. The MSTP instance configuration is saved and the device is updated.

VLAN Instance Configuration

The *VLAN Instance Configuration Screen* enables mapping VLANs to MSTP Instances.

To map VLANs to MSTP Instance IDs:

STEP 1 Click **Spanning Tree > MSTP Instance Settings**. The *VLAN Instance Configuration Screen* opens.

STEP 2 Click **VLAN Instance Configuration**. The *VLAN Instance Configuration Screen* opens.

Figure 91 VLAN Instance Configuration Screen

VLAN Instance Configuration

VLAN	Instance ID (0-7)
VLAN 1	<input type="text" value="0"/>
VLAN 2	<input type="text" value="0"/>
VLAN 3	<input type="text" value="0"/>
VLAN 4	<input type="text" value="0"/>
VLAN 5	<input type="text" value="0"/>
VLAN 6	<input type="text" value="0"/>
VLAN 7	<input type="text" value="0"/>
VLAN 8	<input type="text" value="0"/>
VLAN 9	<input type="text" value="0"/>
VLAN 10	<input type="text" value="0"/>
VLAN 11	<input type="text" value="0"/>
VLAN 12	<input type="text" value="0"/>
VLAN 13	<input type="text" value="0"/>
VLAN 14	<input type="text" value="0"/>
VLAN 15	<input type="text" value="0"/>
VLAN 16	<input type="text" value="0"/>
VLAN 17	<input type="text" value="0"/>
VLAN 18	<input type="text" value="0"/>
VLAN 19	<input type="text" value="0"/>
VLAN 20	<input type="text" value="0"/>
VLAN 21	<input type="text" value="0"/>

232700

The *VLAN Instance Configuration Screen* contains the following fields:

- **VLAN** — Indicates the VLAN for which the MSTP instance ID is defined.
- **Instance ID (0-7)** — Indicates the MSTP instance ID assigned to the VLAN. The possible field range is 0-7.

STEP 3 Click **Save & Close** to save the modified Instance-to-VLAN mapping and close the *VLAN Instance Configuration Screen* (clicking **Save** keeps the *VLAN Instance Configuration Screen* open). The device is updated.

MSTP Interface Settings

Network Administrators can define MSTP Instances settings for interfaces using the *MSTP Interface Settings Screen*.

To define the MSTP interface settings:

- STEP 1
- Click **Spanning Tree > MSTP Interface Settings**. The *MSTP Interface Settings Screen* opens.

Figure 92 MSTP Interface Settings Screen

LINKSYS®
A Division of Cisco Systems, Inc.

24-Port

Spanning Tree

SetupPort ManagementVLAN ManagementStatisticsACLNetwork SecuritySecurity SuiteQoSSpanning TreeMulticastSNMPAdminLogout

<<Back... | MSTP Interface Settings

MSTP Interface Settings

Instance ID1

InterfacePort e1LAG

STP Port StateEnable

Port StateN/A

TypeN/A

RoleN/A

Interface Priority128

Path Cost2000000Use Default

Designated Bridge IDN/A

Designated Port IDN/A

Designated CostN/A

Forward TransitionsN/A

Remain HopsN/A

Update

<<Previous1234Next>>

Port	STP Port State	Port State	Type	Role	Interface Priority	Path Cost	Designated Bridge ID	Designated Port ID	Designated Cost	Forward Transitions	Remain Hops
e1	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e2	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e3	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e4	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e5	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e6	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e7	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e8	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e9	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e10	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e11	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e12	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A

The *MSTP Interface Settings Screen* is divided into two areas:

- MSTP Interface Parameters
- MSTP Interface Table

The MSTP Interface Parameters area contains the following fields:

- **Instance ID** — Lists the MSTP instances configured on the device. Possible field range is 0-7.
- **Interface** — Define the port or LAG of this MSTP configuration. The possible field values are:
 - *Unit No.* — Indicates the stacking member on which this MSTP configuration is defined.
 - *Port* — Indicates the port on which this MSTP configuration is defined.
 - *LAG* — Indicates the LAG on which this MSTP configuration is defined.
- **STP Port Status** — Enables or disables STP on the interface. The possible field values are:
 - *Enable* — Indicates that STP is enabled on the interface.
 - *Disable* — Indicates that STP is disabled on the interface.
- **Port State** — Indicates the MSTP status on the specific port. The possible field values are:
 - *Disabled* — Indicates that STP is currently disabled on the port or if the port is not active. The port forwards traffic while learning MAC addresses.
 - *Blocking* — Indicates that the port is currently blocked and cannot forward traffic or learn MAC addresses.
 - *Listening* — Indicates that the port is in Listening mode. The port cannot forward traffic nor can it learn MAC addresses.
 - *Learning* — Indicates that the port is in Learning mode. The port cannot forward traffic, however it can learn new MAC addresses.
 - *Forwarding* — Indicates that the port is in Forwarding mode. The port can forward traffic and learn new MAC addresses.
- **Type** — Indicates if the port is a point-to-point port, or a port connected to a hub. The possible field values are:
 - *Boundary Port* — Indicates the port is a boundary port. A Boundary port attaches MST bridges to LAN in an outlying region. If the port is a boundary port, it 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.
 - *Internal* — Indicates the port is an internal port.
- **Role** — Indicates the port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:
 - *Root* — Provides the lowest cost path to forward packets to root device.
 - *Designated* — Indicates the port or LAG via which the designated device is attached to the LAN.
 - *Alternate* — Provides an alternate path to the root device from the root interface.
 - *Backup* — Provides a backup path to the designated port path toward the Spanning Tree leaves. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur 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 current Spanning Tree mode. The possible field values are:
 - *Classic STP* — Indicates that Classic STP is enabled on the port.
 - *Rapid STP* — Indicates that Rapid STP is enabled on the port.
- **Interface Priority** — Defines the interface priority for specified instance. The default value is 128.
- **Path Cost** — Defines the port contribution to the Spanning Tree instance. Click **Use Default** to set the path cost to the default value (depends on the port speed and the **Path Cost Default Values** method defined in the *Global STP Screen*).
- **Designated Bridge ID** — Indicates the bridge ID number (priority + MAC address) that connects the link or shared LAN to the root.
- **Designated Port ID** — Indicates the Port ID number (priority + port number) on the designated bridge that connects the link or the shared LAN to the root.
- **Designated Cost** — Displays the cost of the designated 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.
- **Remain Hops** — Indicates the hops remaining to the next destination.

STEP 2 Define the relevant fields.

STEP 3 Click **Save Settings**. The MSTP interface configuration is saved and the details appear in the MSTP Interface Table on the bottom half of the screen. The device is updated.

Figure 93 MSTP Interface Table

The screenshot shows the Linksys web interface for a 24-Port 10/100 Ethernet Switch (SPS 224G4). The 'Spanning Tree' tab is selected, and the 'MSTP Interface Settings' screen is displayed. The table below shows the MSTP Interface Table with 12 interfaces (e1 to e12). The table is divided into two sections: MSTP Interface Parameters and MSTP Interface Table. The interface also shows navigation links like <<Previous, 1, 2, 3, 4, Next>>.

Port	STP Port State	Port State	Type	Role	Interface Priority	Path Cost	Designated Bridge ID	Designated Port ID	Designated Cost	Forward Transitions	Remain Hops
e1	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e2	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e3	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e4	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e5	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e6	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e7	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e8	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e9	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e10	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e11	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A
e12	Enable	N/A	N/A	N/A	128	2000000	N/A	N/A	N/A	N/A	N/A

Save Settings Cancel Changes

For 8-port devices, the MSTP Interface Table displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, and **Next** links above the table.

For 24-port devices, the MSTP Interface Table displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, **3**, and **Next** links above the table.

Multicast

Multicasting is a broadcast technique used in real-time applications such as videoconferencing and multimedia streaming. Multicast forwarding allows a single packet to be forwarded to multiple destinations. Layer 2 Multicast service is based on a Layer 2 switch receiving a single packet addressed to a specific Multicast address. Multicast forwarding creates copies of the packet, and transmits the packets to the relevant ports. The Internet Group Management Protocol (IGMP) allows hosts to notify their local switch or router that they want to receive transmissions assigned to a specific Multicast group.

Multicast forwarding enables transmitting packets from either a specific Multicast group to a source, or from a non-specific source to a Multicast group.

The device supports IGMPv1 and IGMPv2.

The device supports IGMPv1, IGMPv2, and IGMPv3.

The Multicast configuration options are as follows:

- IGMP Snooping
- IGMP Querier
- Bridge Multicast
- Bridge Multicast Forward All

IGMP Snooping

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.

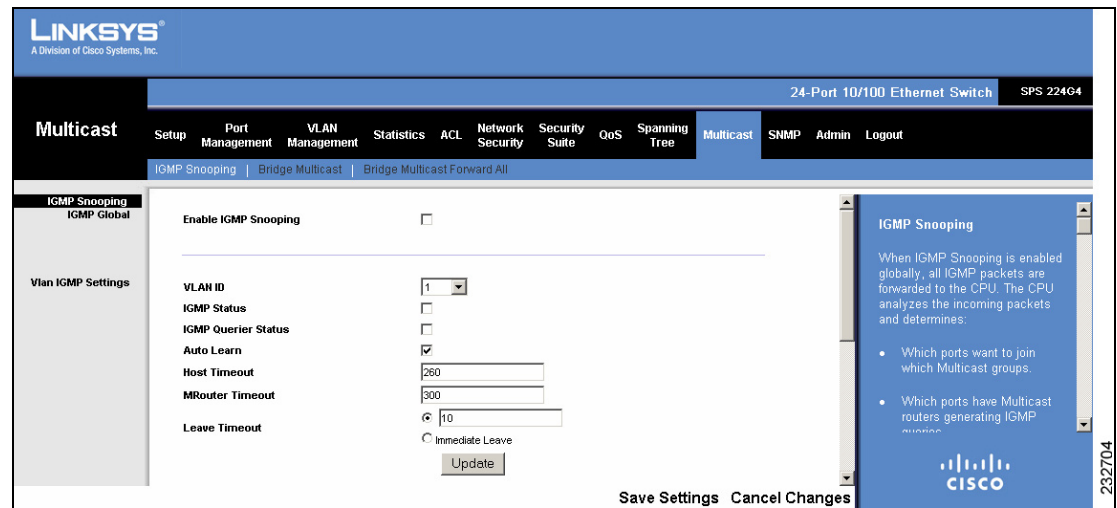
Ports requesting to join a specific Multicast group issue an IGMP report, specifying that the Multicast group is accepting members. This results in the creation of the Multicast filtering database.

For IGMP Snooping to work normally, at least one IGMP Query Router, sending IGMP Host Membership Query messages, must be connected to the network.

To define the IGMP Snooping configuration on the device:

STEP 1 Click **Multicast > IGMP Snooping**. The *IGMP Snooping Screen* opens.

Figure 94 IGMP Snooping Screen



The *IGMP Snooping Screen* is divided into the following areas:

- IGMP Global
- VLAN IGMP Settings
- VLAN IGMP Table

IGMP Global

The IGMP Global area contains the following field:

- **Enable IGMP Snooping** — 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 IGMP Settings

The VLAN IGMP Settings area contains the following fields:

- **VLAN ID** — Specifies the VLAN ID.
- **IGMP Status** — Indicates if IGMP snooping is enabled on the VLAN. The possible field values are:
 - *Checked* — Enables IGMP Snooping on the VLAN.
 - *Unchecked* — Disables IGMP Snooping on the VLAN.
- **IGMP Querier Status** — Indicates if IGMP Querier is enabled on the VLAN. The IGMP Snooping Querier is used to support the L2 multicast domain of snooping switches in the absence of a multicast router. The possible field values are:
 - *Checked* — Enables IGMP Querier on the VLAN.
 - *Unchecked* — Disables IGMP Querier on the VLAN.
- **Auto Learn** — Indicates if Auto Learn is enabled on the VLAN. If Auto Learn is enabled, the devices automatically learn where other Multicast groups are located. The possible field values are:
 - *Checked* — Enables auto learn.
 - *Unchecked* — Disables auto learn.
- **Host Timeout** — Indicates the amount of time the device waits to receive a message before timing out. The possible range is 60-2,147,483,647 seconds. The default time is 260 seconds.
- **MRouter Timeout** — Indicates the amount of the time the device waits to receive a message from the Multicast router before it times out. The possible range is 60-2,147,483,647 seconds. The default value is 300 seconds.
- **Leave Timeout** — Indicates the amount of time the device 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 possible range is 0-2,147,483,647 seconds. The default timeout is 10 seconds.

STEP 2 Select the VLAN ID.

STEP 3 Define the relevant fields.

STEP 4 Click **Update**. The IGMP Snooping configuration is defined and is displayed in the VLAN IGMP Table.

STEP 5 Click **Save Settings**. The IGMP Snooping configuration is saved and the device is updated.

The VLAN IGMP Table displays all of the device's VLANs' IGMP Snooping configurations.

Figure 95 IGMP Snooping Table

LINKSYS®
A Division of Cisco Systems, Inc.

24-Port 10/100 Ethernet Switch SPS 224G4

Multicast

Setup Port Management VLAN Management Statistics ACL Network Security Suite OoS Spanning Tree Multicast SNMP Admin Logout

IGMP Snooping Bridge Multicast Bridge Multicast Forward All

Vlan IGMP Table

<<Previous Next>>

VLAN ID	IGMP Snooping Status	IGMP Querier Status	Auto Learn	Host Timeout	MRouter Timeout	Leave Timeout
1	Disabled	Disabled	Enabled	260	300	10 (Sec)
2	Disabled	Disabled	Enabled	260	300	10 (Sec)
1000	Disabled	Disabled	Enabled	260	300	10 (Sec)
1001	Disabled	Disabled	Enabled	260	300	10 (Sec)
1002	Disabled	Disabled	Enabled	260	300	10 (Sec)
1003	Disabled	Disabled	Enabled	260	300	10 (Sec)
1004	Disabled	Disabled	Enabled	260	300	10 (Sec)
1005	Disabled	Disabled	Enabled	260	300	10 (Sec)
1006	Disabled	Disabled	Enabled	260	300	10 (Sec)
1007	Disabled	Disabled	Enabled	260	300	10 (Sec)
1008	Disabled	Disabled	Enabled	260	300	10 (Sec)
1009	Disabled	Disabled	Enabled	260	300	10 (Sec)
1010	Disabled	Disabled	Enabled	260	300	10 (Sec)
1011	Disabled	Disabled	Enabled	260	300	10 (Sec)

Save Settings Cancel Changes

IGMP Snooping

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.

CISCO

232746

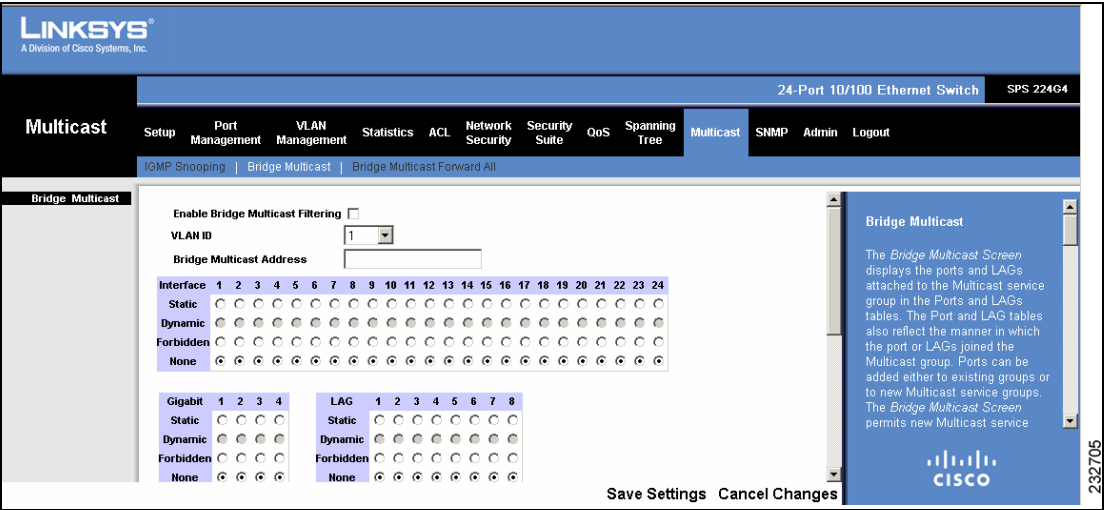
Bridge Multicast

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

To define Multicast groups:

STEP 1 Click **Multicast > Bridge Multicast**. The *Bridge Multicast Screen* opens.

Figure 96 Bridge Multicast Screen



The *Bridge Multicast Screen* is divided into two areas:

- Configuring Multicast
- Multicast Table

The *Bridge Multicast Screen* contains the following fields:

- **Enable Bridge Multicast Filtering** – Indicates if Multicast Filtering is enabled on the device. IGMP Snooping and MLD Snooping cannot be supported when bridge multicast filtering is disabled. When Multicast filtering is disabled, all multicast addresses are flooded to all ports. The possible field values are:
 - *Checked* — Enables Multicast Filtering on the device. Multicast Filtering must be enabled to enable both IGMP Snooping and MLD Snooping.
 - *Unchecked* — Disables Multicast Filtering on the device. This is the default value.
- **Unit No.** — Indicates the stacking member on which this Multicast Group configuration is defined.
- **VLAN ID** — Identifies a VLAN to be configured to a Multicast service.
- **Bridge Multicast Address** — Identifies the Multicast group MAC address.
- **Enable Bridge Multicast Filtering** — Enables or disables Bridge Multicast Filtering on the device.

The interface Multicast configuration options are as follows:

- **Interface** — Indicates the interface with the configuration options below.
- **Static** — Indicates the interface is user-defined.
- **Dynamic** — Indicates the interface is configured dynamically.
- **Forbidden** — Indicates the interface is not included the Multicast group, even if IGMP Snooping designated the interface to join a Multicast group.
- **None** — The interface is not configured for Multicast service.

STEP 2 Select the VLAN ID.

STEP 3 Enter the Bridge Multicast Address for the Multicast group.

STEP 4 Add ports and/or LAGs to the Multicast group by selecting *Static* or *Dynamic*. Ports marked as *Forbidden* or *None* do not belong to a Multicast group.

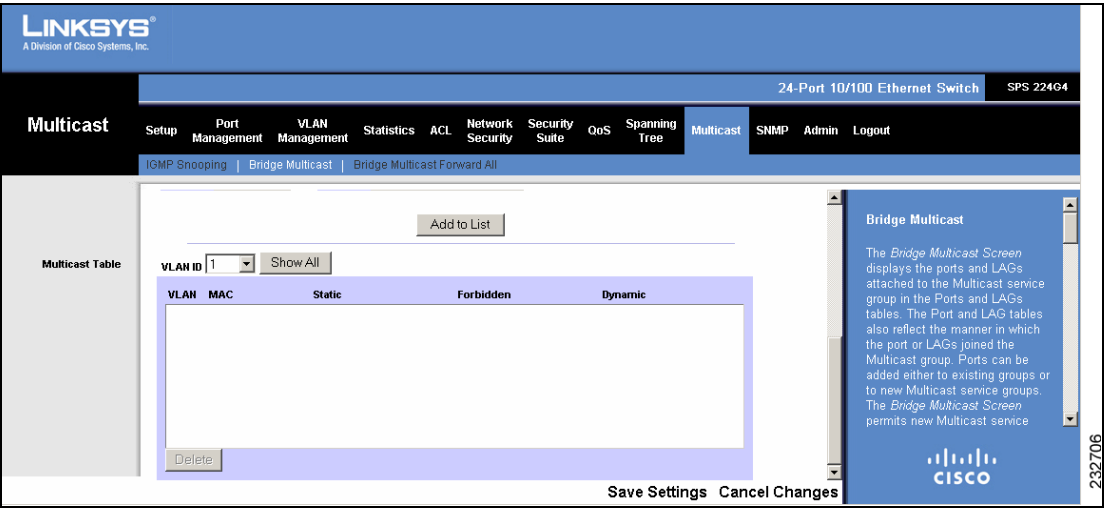
STEP 5 Click **Add to List**. The configured Multicast group is displayed in the Multicast Table at the bottom of the screen.

- STEP 6** Click **Show All** to display all the Multicast addresses on all VLANs in the Multicast Table at the bottom of the screen.
- STEP 7** Click **Save Settings**. The Multicast group configuration is saved and the device is updated.

The **Add to List** button adds the configured Multicast group to the table at the bottom of the screen.

The **Show All** button displays all the Multicast addresses on all VLANs in the table at the bottom of the screen.

Figure 97 Multicast Table



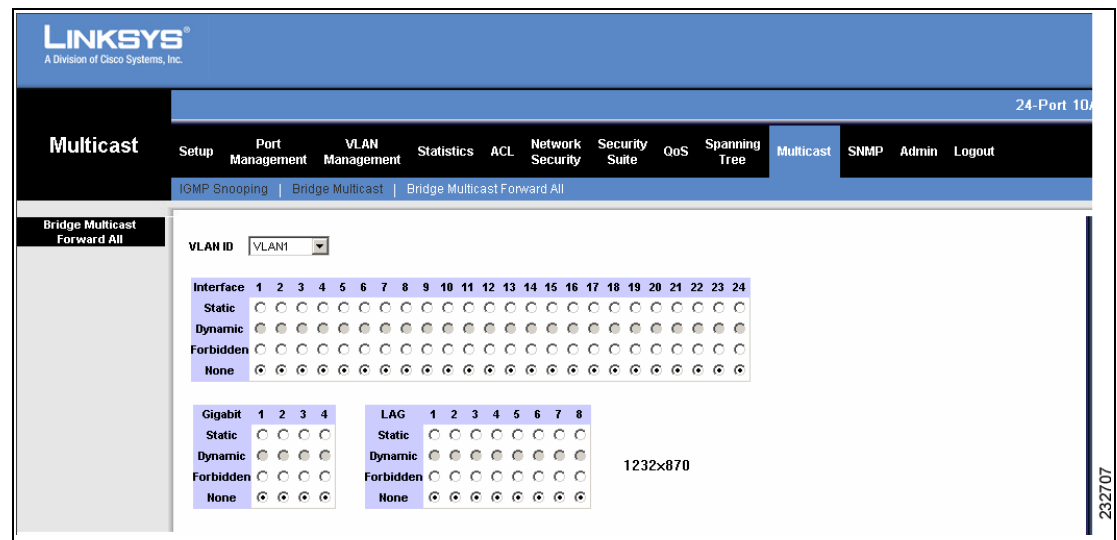
Bridge Multicast Forward All

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

To define Multicast packet forwarding to Multicast routers:

- STEP 1** Click **Multicast > Bridge Multicast Forward All**. The *Bridge Multicast Forward All Screen* opens.

Figure 98 Bridge Multicast Forward All Screen



The *Bridge Multicast Forward All Screen* contains the following fields:

- **VLAN ID** — Displays the VLAN for which Multicast parameters are displayed.

The configuration options are as follows:

- **Static** — Indicates the interface is user-defined.
- **Dynamic** — Indicates the interface is configured dynamically.
- **Forbidden** — Indicates the interface is not included the Multicast group, even if IGMP Snooping designated the interface to join a Multicast group.
- **None** — The interface is not configured for Multicast service.

-
- STEP 2** Select the VLAN ID.
 - STEP 3** Add ports and/or LAGs to the Multicast group by selecting *Static* or *Dynamic*. Interfaces marked as *Forbidden* or *None* do not belong to a Multicast group.
 - STEP 4** Click **Save Settings**. The Multicast Forwarding configuration is saved and the device is updated.
-

SNMP

The Simple Network Management Protocol (SNMP) provides a method for managing network devices. The device supports SNMP v1, v2, and v3.

- **SNMP v1 and v2**

SNMP agents maintain a list of variables that are used to manage the device. The variables are defined in the Management Information Base (MIB). The MIB presents the variables controlled by the agent. 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.

- **SNMP v3**

SNMP v3 also applies access control and a new traps mechanism to SNMPv1 and SNMPv2 PDUs. In addition, User Security Model (USM) is defined for SNMPv3 and includes:

- **Authentication** — Provides data integrity and data origin authentication.
- **Privacy** — Protects against disclosure message content. Cipher Block-Chaining (CBC) is used for encryption. Either authentication is enabled on an 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 the 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 (OID). OIDs are used by the system to manage device features. SNMP v3 supports the following features:
 - Security
 - Feature Access Control
 - Traps

The SNMP configuration options are as follows:

- Global Parameters
- Views
- Group Profile
- Group Membership
- Communities
- Notification Filter
- Notification Recipient

Global Parameters

The *Global Parameters Screen* contains parameters for defining SNMP authentication and notification parameters.

To define SNMP authentication and notification parameters on the device:

STEP 1 Click **SNMP > Global Parameters**. The *Global Parameters Screen* opens.

Figure 99 SNMP Global Parameters Screen

The screenshot displays the Linksys web interface for configuring SNMP. The top navigation bar includes links for Setup, Port Management, VLAN Management, Statistics, ACL, Network Security, Security Suite, QoS, Spanning Tree, Multicast, and SNMP (which is currently selected). Below this, a sub-menu shows 'Global Parameters' as the active option. The main configuration area is split into two panels. The left panel, titled 'Global Parameters', contains a section for 'SNMPv3' with a 'Local Engine ID' text box (containing 'EngineID not Configured') and a 'Use Default' checkbox. The right panel, titled 'Notifications', contains two checked checkboxes: 'SNMP Notifications' and 'Authentication Notifications'. A vertical text '232709' is visible on the far right edge of the interface.

The *Global Parameters Screen* contains the following fields:

- **Local Engine ID** — Indicates the local device engine ID. The field value is a hexadecimal string. Each byte in hexadecimal character strings consists of two hexadecimal digits. The Engine ID must be defined before SNMPv3 is

enabled. Select a default Engine ID that is comprised of Enterprise number and the default MAC address, and verify that the Engine ID is unique for the administrative domain. This prevents two devices in a network from having the same Engine ID.

- **Use Default** — When checked, 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. To locate the IANA Enterprise number refer to the Vendor web site.
 - Fifth octet — Set to 3 to indicate the MAC address that follows.
 - Last 6 octets — MAC address of the device.

The possible values are:

- *Checked* — Use the default Engine ID.
- *Unchecked* — Use a user-defined Engine ID.
- **SNMP Notifications** — Indicates if the device can send SNMP notifications. The possible field values are:
 - *Checked* — Enables SNMP notifications.
 - *Unchecked* — Disables SNMP notifications.
- **Authentication Notifications** — Indicates if SNMP Authentication failure notification is enabled on the device. The possible field values are:
 - *Checked* — Enables the device to send authentication failure notifications.
 - *Unchecked* — Disables the device from sending authentication failure notifications.

STEP 2 Define the relevant fields.

STEP 3 Click **Save Settings**. The SNMP authentication and notification configuration is saved and the device is updated.

Views

SNMP Views provide access or block access to device features or feature aspects. Feature access is granted via the MIB name, or MIB Object ID.

To define SNMP views:

STEP 1 Click **SNMP > Views**. The *Views Screen* opens.

Figure 100 SNMP Views Screen

The screenshot shows the Linksys SNMP Views configuration screen. The navigation menu includes Setup, Port Management, VLAN Management, Statistics, ACL, Network Security, Security Suite, QoS, Spanning Tree, Multicast, SNMP, Admin, and Logout. The SNMP sub-menu is expanded, showing Global Parameters, Views, Group Profile, Group Membership, Communities, Notification Filter, and More... The Views screen is divided into two main sections: Views Parameters and Views Table.

Views Parameters:

- View Name:** Default (selected)
- New View Name:** (empty field)
- Object ID Subtree:** Select from List (selected)
- View Type:** Included (selected)
- Insert:** 1.3.6.1.2.1.1 (text field)
- Buttons:** Up, Down, Add to List

Views Table:

Object ID Subtree	View Type
1	Included
1.3.6.1.6.3.13	Excluded
1.3.6.1.6.3.16	Excluded
1.3.6.1.6.3.18	Excluded
1.3.6.1.6.3.12.1.2	Excluded
1.3.6.1.6.3.12.1.3	Excluded
1.3.6.1.6.3.15.1.2	Excluded

Buttons: Delete

The *Views Screen* is divided into two areas:

- Views Parameters
- Views Table

The Views Parameters area contains the following fields:

- **View Name** — Indicates the user-defined views. The default options are as follows:
 - *Default* — Indicates the default SNMP view for read and read/write views.

- *DefaultSuper* — Indicates the default SNMP view for administrator views.
- *User Defined*— Lists all user-defined SNMP views.
- **New View Name** — User-specified new View Name.
- **Object ID Subtree** — Indicates the device feature OID that is included or excluded in the selected SNMP view. The options to select the Subtree are as follows:
 - *Select from List* — Select the Subtree from the provided list.
 - *Insert* — Type an OID in the box.
- **View Type** — Indicates if the defined OID branch will be *Included* or *Excluded* in the selected SNMP view.

STEP 2 Define the relevant fields.

STEP 3 Click **Add to List**. The Views configuration is displayed in the Views Table at the bottom of the screen.

The **Add to List** button adds the Views configuration to the Views Table at the bottom of the screen.

To modify an SNMP view:

STEP 4 Select the SNMP View in the Views Table.

STEP 5 Define the relevant fields.

STEP 6 Click **Update**. The SNMP View configuration is updated in the Views Table. The device is updated.

To delete an SNMP view from the device:

STEP 1 In the Views Table, select the entry.

STEP 2 Click **Delete**. The selected SNMP view configuration is deleted from the device.

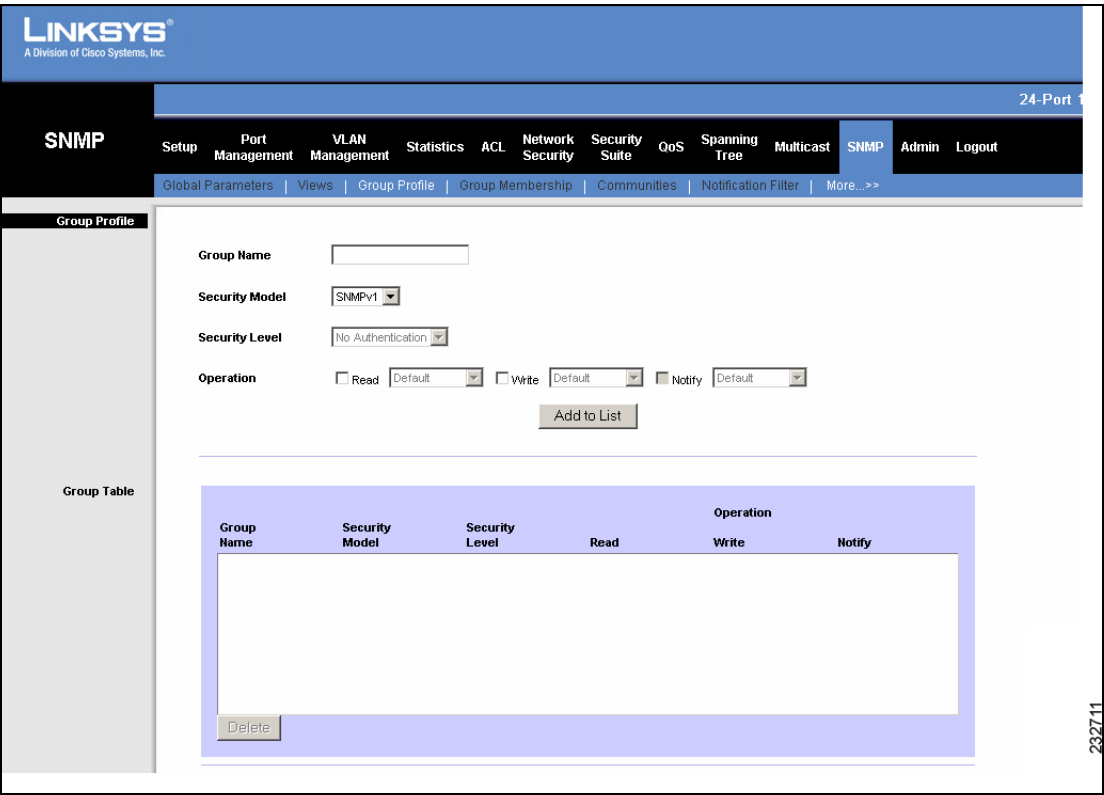
Group Profile

The *Group Profile Screen* 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 features aspects.

To create and configure SNMP group profiles:

STEP 1 Click **SNMP > Group Profile**. The *Group Profile Screen* opens.

Figure 101 SNMP Group Profile Screen



The *Group Profile Screen* is divided into two areas:

- Group Parameters
- Group Table

The Group Parameters area contains the following fields:

- **Group Name** — Indicates 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.
 - *SNMPv2* — SNMPv2 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 the SNMP messages origin is authenticated.
 - *Privacy* — Encrypts SNMP message.
- **Operation** — Defines the group access rights. The possible field values are:
 - *Read* — The management access is restricted to read.
 - *Write* — The management access is write and changes can be made to the assigned SNMP view.
 - *Notify* — Sends SNMP traps to group members.

The options for Read, Write, and Notify operations are as follows:

- *Default* — Defines the default group access rights.
- *DefaultSuper* — Defines the default group access rights for administrator.

STEP 2 Define the relevant fields.

STEP 3 Click **Add to List**. The group profile is displayed in the Log Table at the bottom of the screen.

To modify an SNMP group profile:

-
- STEP 1** Select the group profile in the Log Table.
 - STEP 2** Define the relevant fields.
 - STEP 3** Click **Update**. The SNMP group profile is updated in the Log Table. The device is updated.
-

To delete an SNMP group profile from the device:

-
- STEP 1** In the Group Table, select the entry.
 - STEP 2** Click **Delete**. The selected SNMP group profile is deleted from the device.

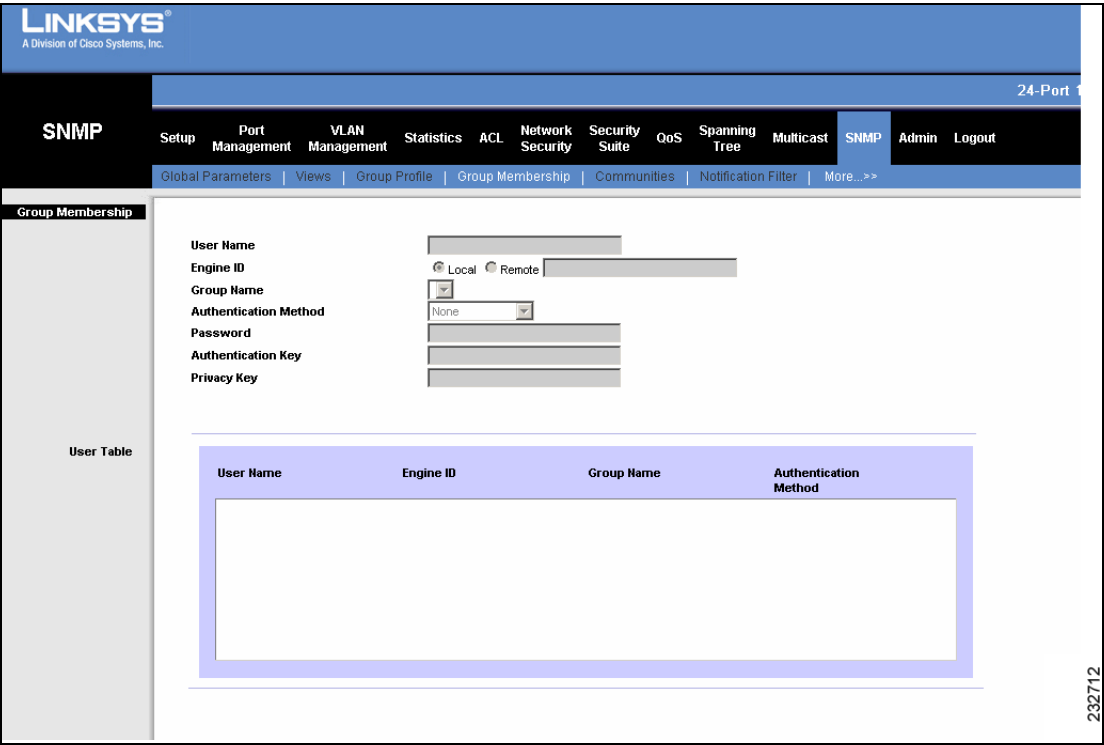
Group Membership

The *Group Membership Screen* provides information for assigning SNMP access control privileges to SNMP group members.

To add members to SNMP groups:

- STEP 1** Click **SNMP > Group Membership**. The *Group Membership Screen* opens.

Figure 102 SNMP Group Membership Screen



The *Group Membership Screen* is divided into two areas:

- Group Member Parameters
- User Table

The Group Member Parameters area contains the following fields:

- **User Name** — Defines the group member's user name.
- **Engine ID** — Indicates either the local or remote SNMP entity to which the user is connected.
 - *Local* — Indicates that the user is connected to a local SNMP entity.
 - *Remote* — Indicates that the user is connected to a remote SNMP entity, and can receive inform messages.
- **Group Name** — Contains a list of user-defined SNMP groups. SNMP groups are defined in the SNMP Group Profile page.
- **Authentication Method** — Indicates the Authentication method used. The possible field values are:
 - *None* — Indicates that no authentication method is used.
 - *MD5 Password* — An 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.
 - *MD5 Key* — Users are authenticated using the HMAC-MD5 algorithm.
 - *SHA Key* — Users are authenticated using the HMAC-SHA-96 authentication level.
- **Password** — Defines the local user password. Local user passwords can contain up to 159 characters.
- **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 for HMAC-MD5-96 and 20 bytes are defined for HMAC-SHA-96. If both privacy and authentication are required, 32 bytes are defined for HMAC-MD5-96 and 36 bytes are defined for HMAC-SHA-96. Each byte in hexadecimal character strings is two hexadecimal digits.
- **Privacy Key** — Defines the Privacy Key (LSB). If only authentication is required, 16 bytes are defined. Each byte in hexadecimal character strings is two hexadecimal digits. Each byte can be separated by a period or colon.

STEP 2 Define the relevant fields.

STEP 3 Click **Add to List**. The new group member is displayed in the User Table at the bottom of the screen.

The **Add to List** button adds the group member to the User Table at the bottom of the screen.

To modify an SNMP group member:

STEP 1 Select the group member in the User Table.

STEP 2 Define the relevant fields.

STEP 3 Click **Update**. The SNMP group member is updated in the User Table. The device is updated.

To delete an SNMP group member from the device:

STEP 1 In the User Table, select the entry.

STEP 2 Click **Delete**. The selected SNMP group member is deleted from the device.

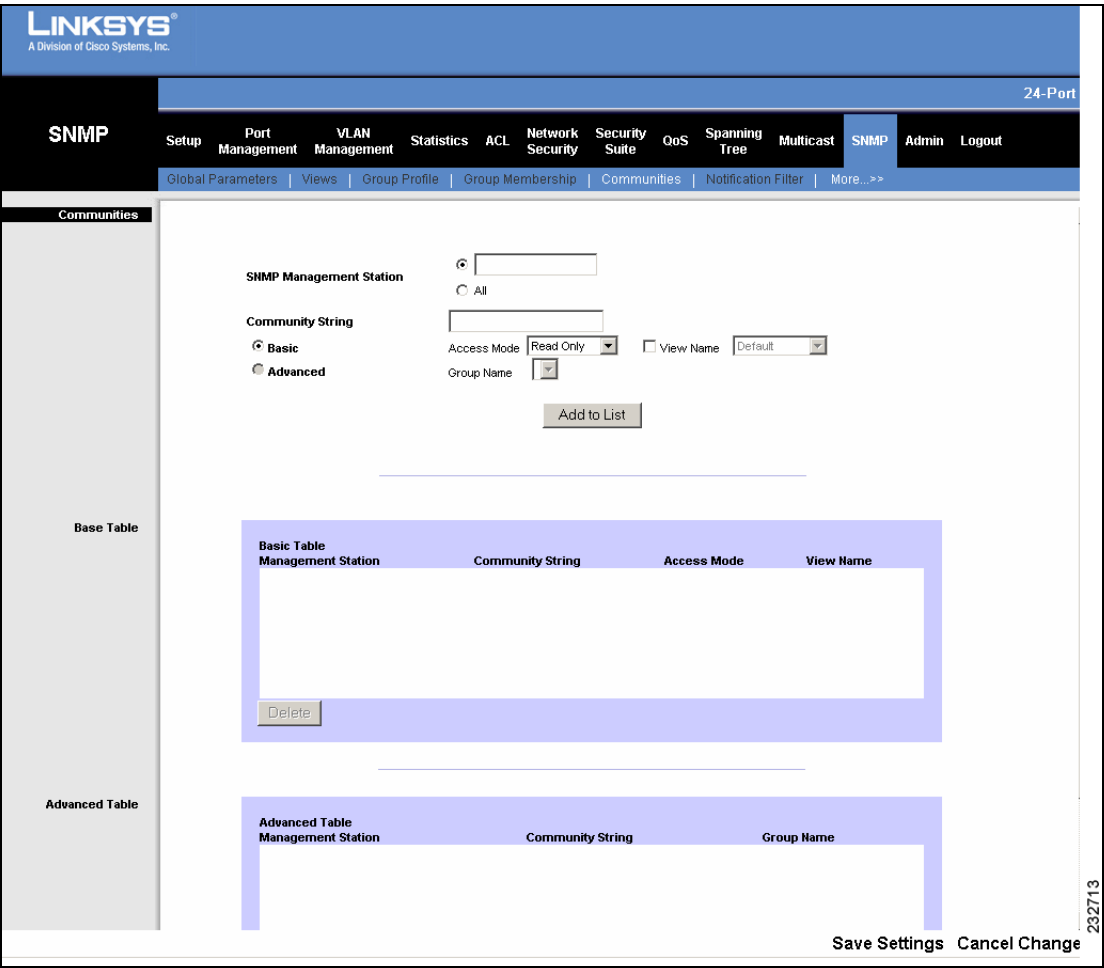
Communities

The Access rights are managed by defining communities in the *Communities Screen*. 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:

- STEP 1** Click **SNMP > Communities**. The *Communities Screen* opens.

Figure 103 SNMP Communities Screen



The *Communities Screen* contains the following areas:

- Communities Parameters
- Basic Table

- Advanced Table

The Communities Parameters area contains the following fields:

- **SNMP Management Station** — Defines the management station IP address for which the advanced SNMP community is defined. There are two definition options:
 - Define the management station IP address.
 - Select **All**, which includes all management station IP addresses.
- **Community String** — Defines the password used to authenticate the management station to the device.
- **Basic** — Enables SNMP Basic mode for a selected community and contains the Access Mode and View Name fields.
- **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. The possible values are:
 - *Default* — View that defines the default group access rights.
 - *DefaultSuper* — View that defines the default group access rights for administrator.
 - If additional SNMP views have been defined, they also appear in this list.
- **Advanced** — Enables SNMP Advanced mode for a selected community and contains the following field:
 - *Group Name* — Assigns the SNMP community to a specific group.

STEP 2 Define the relevant fields.

STEP 3 Click **Add to List**. The new community is displayed in either the Basic Table or Advanced Table at the bottom of the screen.

Figure 104 SNMP Communities Screen - Basic and Advanced Tables

The screenshot displays the Linksys SNMP Communities configuration interface. The top navigation bar includes links for Setup, Port Management, VLAN Management, Statistics, ACL, Network Security, Security Suite, QoS, Spanning Tree, Multicast, and SNMP (selected). The left sidebar shows 'Base Table' and 'Advanced Table' sections. The main content area features two tables for configuring SNMP communities. The 'Basic Table' has columns for Management Station, Community String, Access Mode, and View Name. The 'Advanced Table' has columns for Management Station, Community String, and Group Name. Both tables have a 'Delete' button at the bottom. At the bottom right, there are 'Save Settings' and 'Cancel Change' buttons.

The Basic Table area contains the following fields:

- **Management Station** — Displays the management station IP address for which the SNMP community is defined.
- **Community String** — Displays the password used to authenticate the management station to the device.
- **Access Mode** — Displays the access rights of the community.
- **View Name** — Displays the view name assigned to the community.

The Advanced Table area contains the following fields:

- **Management Station** — Displays the management station IP address for which the SNMP community is defined.

- **Community String** — Displays the password used to authenticate the management station to the device.
- **Group Name** — Displays the group to which this community belongs.

To modify an SNMP community:

-
- STEP 1** Select the community in the Basic or Advanced Table.
 - STEP 2** Define the relevant fields.
 - STEP 3** Click **Update**. The SNMP community is updated in the respective Table. The device is updated.
-

To delete an SNMP community from the device:

-
- STEP 1** Select the community in the Basic or Advanced Table.
 - STEP 2** Click **Delete**. The selected SNMP community is deleted from the device.
-

Notification Filter

The *Notification Filter Screen* permits network managers to filter traps based on OIDs. Each OID is linked to a device feature or a feature aspect.

To add a notification filter:

STEP 1 Click **SNMP > Notification Filter**. The *Notification Filter Screen* opens.

Figure 105 Notification Filter Screen

The screenshot displays the Linksys SNMP Notification Filter configuration page. The top navigation bar includes links for Setup, Port Management, VLAN Management, Statistics, ACL, Network Security, Security Suite, QoS, Spanning Tree, Multicast, and SNMP (which is currently selected). Below this, a sub-navigation bar lists various SNMP-related options: Global Parameters, Views, Group Profile, Group Membership, Communities, Notification Filter (selected), and More... The main content area is titled 'Notification Filter' and contains the following elements:

- Filter Name:** A text input field.
- New Filter Name:** A text input field.
- New Object Identifier Tree:** A section with a 'Select from List' radio button and a tree view. The tree view shows a hierarchy: 'system' (selected), 'interfaces', 'ip', 'icmp', and 'tcp'. There are 'Up' and 'Down' buttons next to the tree view.
- Object ID:** A text input field containing the value '1.3.6.1.2.1.1'.
- Filter Type:** A dropdown menu currently set to 'Included'.
- Add to List:** A button to add the current filter configuration to the list.
- Filter Table:** A table with two columns: 'Object ID Subtree' and 'Filter Type'. It is currently empty.
- Delete:** A button located at the bottom left of the table area.

The *Notification Filter Screen* contains the following areas:

- Filter Parameters
- Filter Table

The Filter Parameters area contains the following fields:

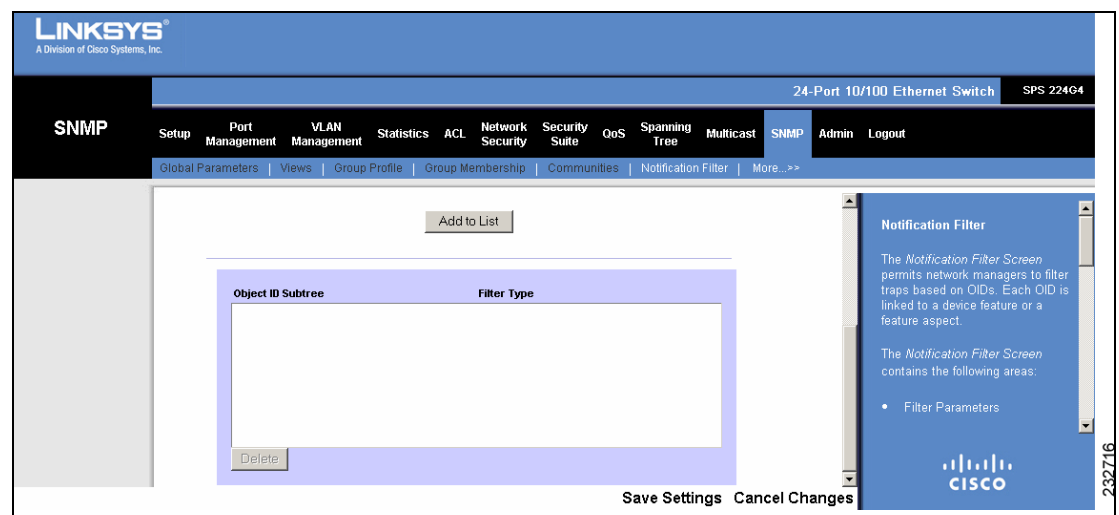
- **Filter Name** — Contains a list of user-defined notification filters. Filter names with special characters cannot be used to define a filter name *,?,<,>|,\,/, :.
- **New Filter Name** — Defines a new filter name.
- **New Object Identifier Tree** — Displays the OID for which notifications are sent or blocked. Object IDs are selected from either of the following configuration options:
 - *Select from List* — Select the OID from the provided list.
 - *Object ID* — Type an OID in the box.
- **Filter Type** — Indicates whether informs or traps are sent regarding the OID to the trap recipients.
 - *Included* — Sends OID traps or informs.
 - *Excluded* — Restricts sending OID traps or informs.

STEP 2 Define the relevant fields.

STEP 3 Click **Add to List**. The new filter is displayed in the Filter Table at the bottom of the screen.

The **Add to List** button adds the filter to the Filter Table at the bottom of the screen.

Figure 106 Notification Filter Table



To modify an SNMP notification filter:

-
- STEP 1** Select the filter in the Filter Table.
 - STEP 2** Define the relevant fields.
 - STEP 3** Click **Update**. The SNMP notification filter is updated in the Filter Table. The device is updated.
-

To delete an SNMP notification filter from the device:

-
- STEP 1** Select the filter in the Filter Table.
 - STEP 2** Click **Delete**. The selected filter is deleted from the device.
-

Notification Recipient

The *Notification Recipient Screen* allows managers to define the users who receive traps, and the trap types that the users receive.

To define a notification recipient:

- STEP 1
- Click **SNMP > More > Notification Recipient**. The *Notification Recipient Screen* opens.

Figure 107 Notification Recipient Screen

LINKSYS®
A Division of Cisco Systems, Inc.

24-Port

SNMP

SetupPort ManagementVLAN ManagementStatisticsACLNetwork SecuritySecurity SuiteQoSSpanning TreeMulticastSNMPAdminLogout

<<Back... | Notification Recipient

Notification Recipient

Recipient IP

Notification Type

Community String

Notification Version

User Name

Security Level

UDP Port

Filter Name

Timeout

Retries

Traps

SNMPv1

NoAuthentication

162

15 (sec)

3

Add to List

SNMPv1,2 Notification Recipient

Recipients	Notification Type	Community String	Notification Version	UDP Port	Filter Name	Timeout	Retries

Delete

232717

The *Notification Recipient Screen* contains the following areas:

- Notification Recipient Parameters
- SNMPv1,2 Notification Recipient Table
- SNMPv3 Notification Recipient Table

The Notification Recipient Parameters area contains the following fields:

- **Recipient IP** — Indicates the IP address to whom the traps are sent.
- **Notification Type** — Defines the notification sent. The possible field values are:
 - *Traps* — Indicates traps are sent.
 - *Informs* — Indicates informs are sent.

Either SNMPv1,2 or SNMPv3 can be enabled at any one time, but not both at the same time.

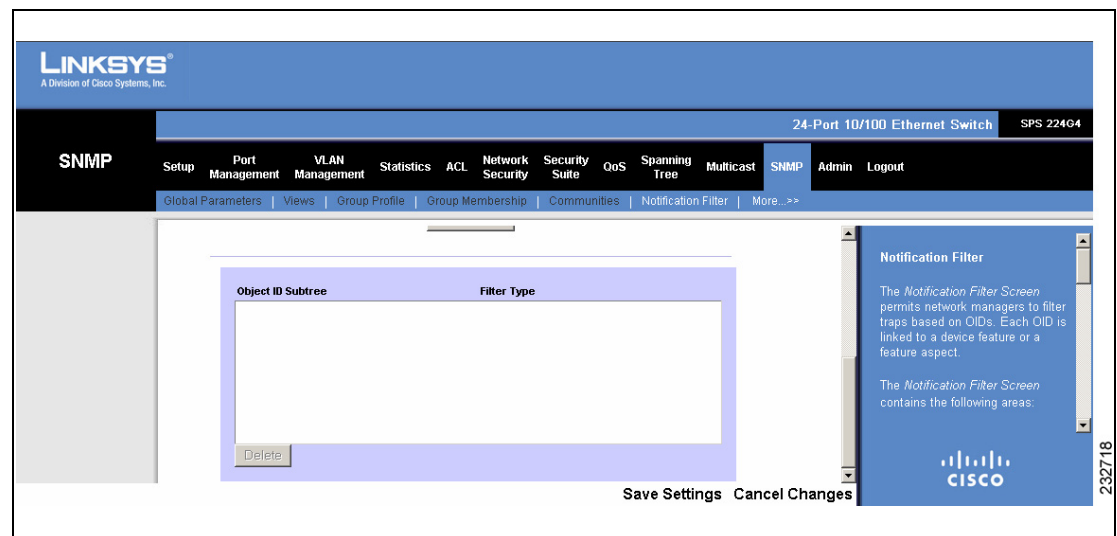
- **SNMPv1,2** — Enables SNMPv1,2 as the Notification Recipient.
- **Community String** — Identifies the community string of the trap manager.
- **Notification Version** — Determines the trap type. The possible field values are:
 - *SNMP V1* — Indicates SNMP Version 1 traps are sent.
 - *SNMP V2* — Indicates SNMP Version 2 traps are sent.
- **SNMPv3** — Enables SNMPv3 as the Notification Recipient.
- **User Name** — Defines the user to whom SNMP notifications are sent.
- **Security Level** — Defines the means by which the packet is authenticated. The possible field values are:
 - *No Authentication* — Indicates the packet is neither authenticated nor encrypted.
 - *Authentication* — Indicates the packet is authenticated.
 - *Privacy* — Indicates the packet is both authenticated and encrypted.
- **UDP Port** — Displays the UDP port used to send notifications. The default is 162.
- **Filter Name** — Indicates the SNMP filter (defined in the *Notification Filter Screen*) that specifies the traps which this user receives.
- **Timeout** — Indicates the amount of time (seconds) the device waits before re-sending an inform request. The range is 1-300 seconds. The default is 15 seconds.
- **Retries** — Indicates the number of times the device re-sends an inform request. The range is 0-255 times. The default is 3 times.

STEP 2 Define the relevant fields.

STEP 3 Click **Add to List**. The new notification recipient is displayed in either the SNMPv1,2 Table or the SNMPv3 Table at the bottom of the screen.

The **Add to List** button adds the notification recipient to either the SNMPv1,2 Table or the SNMPv3 Table at the bottom of the screen.

Figure 108 Notification Recipient Table



To modify an SNMP notification recipient:

STEP 1 Select the recipient in either the SNMPv1,2 Table or the SNMPv3 Table.

STEP 2 Define the relevant fields.

STEP 3 Click **Update**. The SNMP notification recipient is updated in the respective Table. The device is updated.

To delete an SNMP notification filter from the device:

STEP 1 Select the recipient in either the SNMPv1,2 Table or the SNMPv3 Table.

STEP 2 Click **Delete**. The selected filter is deleted from the device.

Admin

The Admin features include screens and utilities that enable network administrators to register users, run diagnostics, software backup and upgrade, and device monitoring.

The Admin configuration options are as follows:

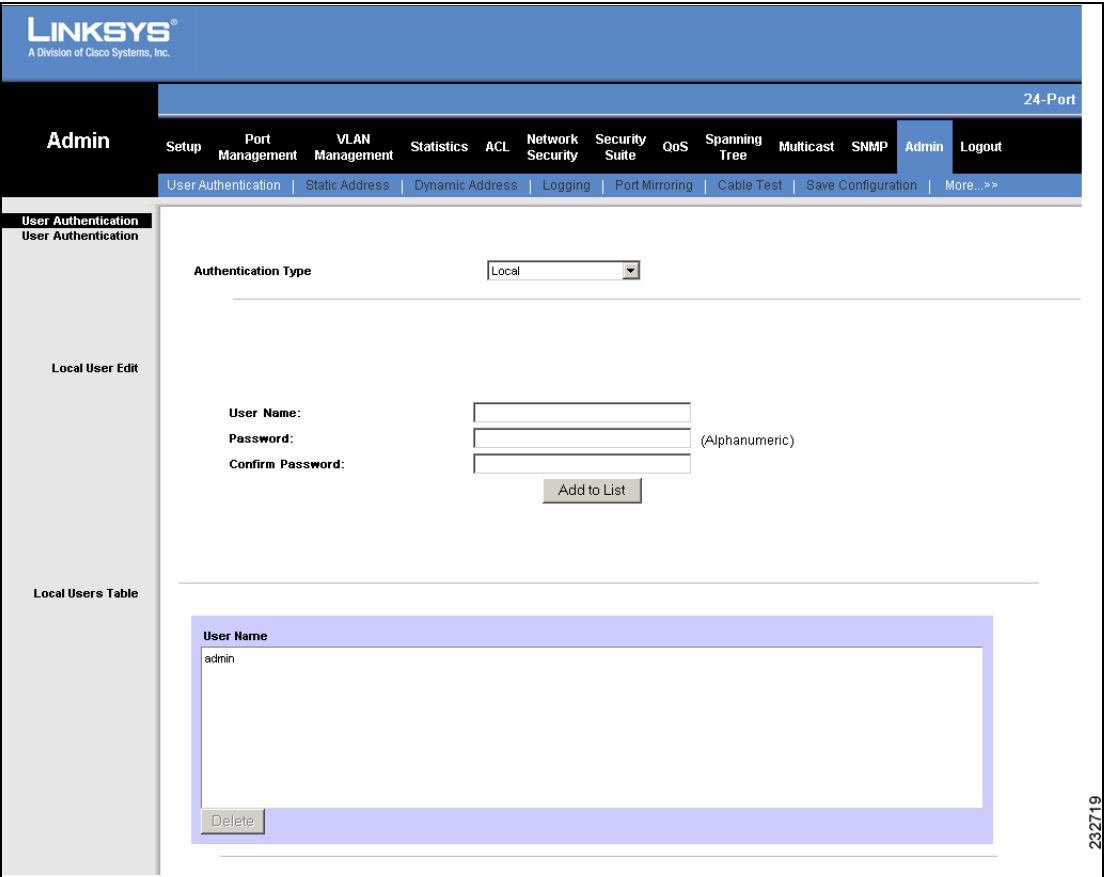
- User Authentication
- Static Address
- Dynamic Address
- Logging
- Port Mirroring
- Cable Test
- Saving or Upgrading a Configuration
- Firmware Upgrade
- Reboot
- Factory Default
- Server Logs
- Memory Logs
- Flash Logs

User Authentication

The *User Authentication Screen* is used to define user names and passwords.
To define a user configuration:

STEP 1 Click **Admin > User Authentication**. The *User Authentication Screen* opens.

Figure 109 User Authentication Screen



The *User Authentication Screen* contains the following areas:

- User Authentication Parameters
- Local Users Edit
- Local Users Table

The User Authentication Parameters area contains the following field:

- **Authentication Type** — Defines the possible authentication types. Any one or combination of these types can be selected. If the first method returns an error (not a failure), the device applies the second method, and so on. To ensure successful authentication in case other methods result in errors, specify **None** as the last method to try. The possible authentication types are as follows:
 - *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.
 - *TACACS+* — Authenticates the user at the TACACS+ server.
 - *None* — Assigns no authentication method to the authentication profile.

The Local Users Edit area contains the following fields:

- **User Name** — Specifies the user name.
- **Password** — Specifies the new password. The password is not displayed. As it entered an “*” corresponding to each character is displayed in the field. (Range: 1-15 characters).
- **Confirm Password** — Confirms the new password. The password entered into this field must be exactly the same as the password entered in the **Password** field.

STEP 1 Define the relevant fields.

STEP 2 Click **Add to List**. The new user configuration is displayed in the Local Users Table at the bottom of the screen.

To modify a user configuration:

-
- STEP 1** Select the user in the Local Users Table.
 - STEP 2** Define the relevant fields.
 - STEP 3** Click **Update**. The user is updated in the Local Users Table.
 - STEP 4** Click **Save Settings**. The user configuration is saved and the device is updated.
-

To delete a user from the device:

-
- STEP 1** Select the user in the Local Users Table.
 - STEP 2** Click **Delete**. The selected user is deleted from the Local Users Table.
 - STEP 3** Click **Save Settings**. The selected user is deleted from the device and the device is updated.
-

Static Address

A static MAC address can be assigned to a specific interface on this switch. Static MAC addresses are bound to the assigned interface and cannot be moved. When a static MAC address is seen on another interface, the address will be ignored and will not be written to the address table.

Packets addressed to destinations stored in the Static databases are immediately forwarded to the defined port. Static addresses are configured manually.

To define static MAC addresses to interfaces:

STEP 1 Click **Admin > Static Address**. The *Static Address Screen* opens.

Figure 110 Static Address Screen

The screenshot shows the Linksys web interface for configuring static MAC addresses. The top navigation bar includes 'Admin' and 'Logout'. The left sidebar has 'Static Address' selected. The main configuration area includes fields for 'Interface' (Port e1 or LAG LAG1), 'MAC Address', 'VLAN ID' (1), 'VLAN NAME', and 'Status' (Permanent). An 'Add to List' button is present. Below the configuration area is a table with columns 'VLAN ID', 'MAC Address', 'Interface', and 'Status'. A 'Delete' button is at the bottom left of the table.

VLAN ID	MAC Address	Interface	Status
---------	-------------	-----------	--------

The *Static Address Screen* contains the following areas:

- Static Address Parameters
- Static Address Table

The Static Address Parameters area contains the following fields:

- **Interface** — Displays the interface to which the address entry refers:
 - *Unit No.* — Indicates the stacking member to which the address entry refers.
 - *Port* — The specific port number to which the address entry refers.
 - *LAG* — The specific LAG number to which the address entry refers.
- **MAC Address** — Specifies the MAC address assigned to this interface.
- **VLAN ID** — Displays the VLAN ID number associated with this interface.
- **VLAN Name** — Displays the VLAN name associated with this interface.
- **Status** — Displays defined actions for the MAC address entry. The possible field values are:
 - *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. The default timeout is 300 seconds.
 - *Secure* — The MAC Address is defined for locked ports.

STEP 2 Define the relevant fields.

STEP 3 Click **Add to List**. The new static address entry is displayed in the Static Address Table at the bottom of the screen.

The **Add to List** button adds the static address to the Static Address Table.

To modify a static address entry:

STEP 1 Select the address in the Static Address Table.

STEP 2 Define the relevant fields.

STEP 3 Click **Update**. The address entry is updated in the Static Address Table. The device is updated.

To delete a static address from the device:

-
- STEP 1** Select the address in the Static Address Table.
- STEP 2** Click **Delete**. The selected address entry is deleted from the device.
-

Dynamic Address

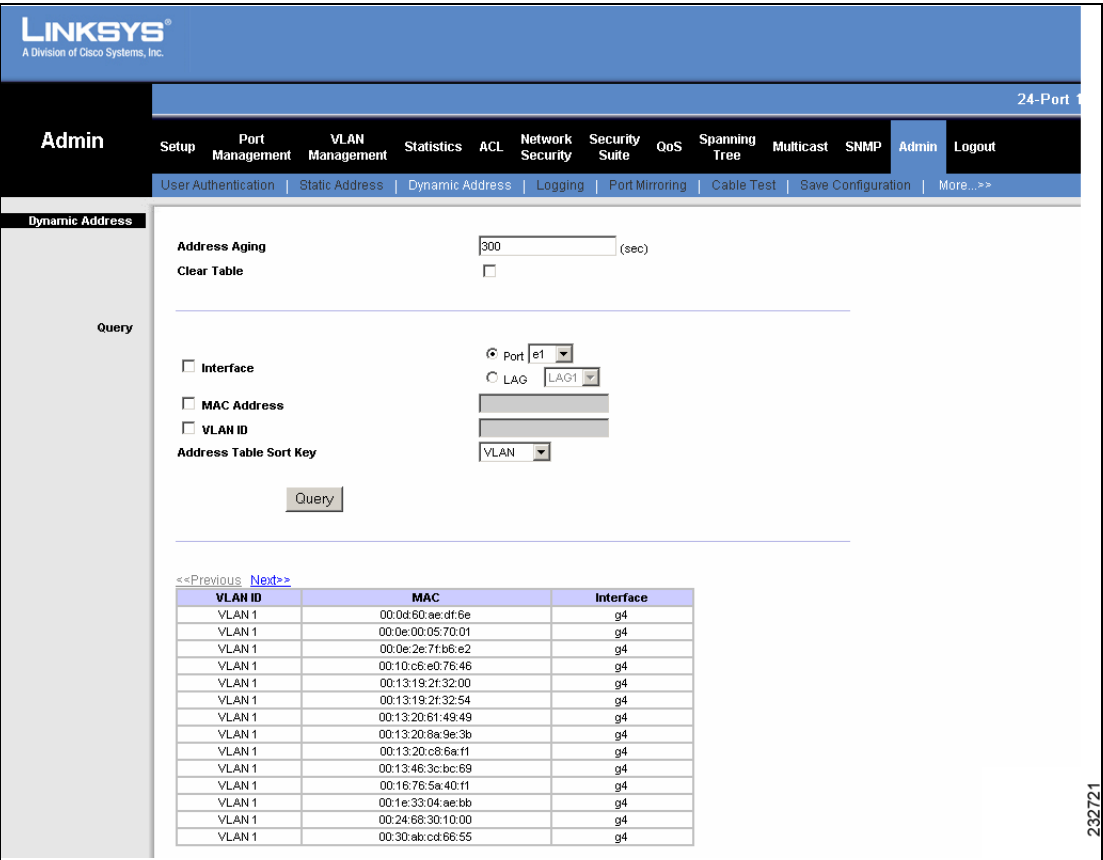
The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

The *Dynamic Address Screen* 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 learn dynamic MAC addresses on a specific interface:

STEP 1 Click **Admin > Dynamic Address**. The *Dynamic Address Screen* opens.

Figure 111 Dynamic Address Screen



The *Dynamic Address Screen* contains the following areas:

- General Parameters
- Query Parameters
- Query Results Table

The General Parameters area contains the following fields:

- **Address Aging** — Specifies the amount of time the MAC address remains in the Dynamic MAC Address table before it is timed out, if no traffic from the source is detected. The default value is 300 seconds.
- **Clear Table** — If checked, clears the MAC address table.

The Query Parameters area contains the following fields:

- **Interface** — Specifies the interface for dynamic MAC addresses are queried. The possible field values are:
 - *Unit No.* — Indicates the stacking member on which the MAC addresses are learned.
 - *Port* — Indicates the port number on which the MAC addresses are learned.
 - *LAG* — Indicates the LAG number on which the MAC addresses are learned.
- **MAC Address** — Specifies a MAC address to query.
- **VLAN ID** — Identifies the VLAN by number.
- **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.

STEP 2 Define the relevant query filter fields.

STEP 3 Click **Query**. The Dynamic MAC Address Table is queried, and the discovered MAC addresses are displayed in the Query Results Table.

Logging

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 or 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 logging.

In the *Logging Screen*, network administrators define the levels of event severity that are recorded to the system event logs.

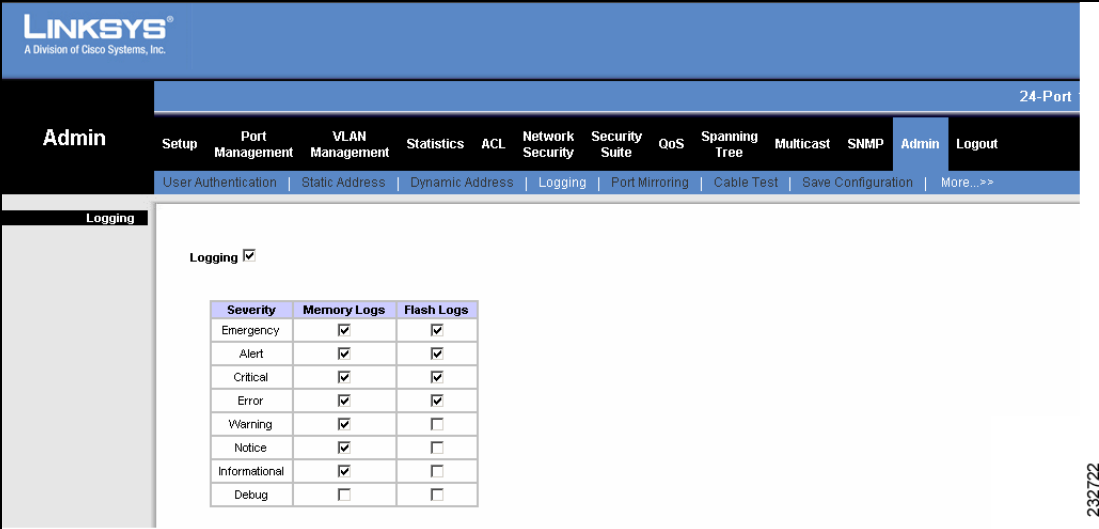
The event severity levels are listed on this page in descending order from the highest severity to the lowest. When a severity level is selected to appear in a log, all higher severity events will automatically be selected to appear in the log. Conversely, when a security level is not selected, no lower severity events will appear in the log.

For example, if Warning is selected, all severity levels higher and including Warning will appear in the log. Additionally, no events with a lower severity level than Warning will be listed.

To define the levels of event security that are recorded to the system logs:

STEP 1 Click **Admin > Logging**. The *Logging Screen* opens.

Figure 112 Logging Screen



LINKSYS®
A Division of Cisco Systems, Inc.

24-Port

Admin Setup Port Management VLAN Management Statistics ACL Network Security Security Suite QoS Spanning Tree Multicast SNMP Admin Logout

User Authentication Static Address Dynamic Address Logging Port Mirroring Cable Test Save Configuration More...>>

Logging

Logging ☒

Severity	Memory Logs	Flash Logs
Emergency	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Alert	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Critical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Error	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Warning	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Notice	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Informational	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Debug	<input type="checkbox"/>	<input type="checkbox"/>

232722

The *Logging Screen* contains the following fields:

- **Logging** — Enables system logging globally on the device. Console logs are enabled by default. The possible values are:
 - *Checked* — Logging is enabled.
 - *Unchecked* — Logging is disabled.
- **Emergency** — The system is not functioning.
- **Alert** — The system needs immediate attention.
- **Critical** — The system is in a critical state.
- **Error** — A system error has occurred.

- **Warning** — A system warning has occurred.
- **Notice** — The system is functioning properly, but system notice has occurred.
- **Informational** — Provides device information.
- **Debug** — Provides detailed information about the log. If a Debug error occurs, contact Customer Tech Support.

Logging can be performed in Memory and in Flash. Memory Logs are deleted at reboot. Flash Logs are available after reboot.

STEP 2 Define the required severity levels.

STEP 3 Click **Save Settings**. The system logging configuration is saved and the device is updated.

Port Mirroring

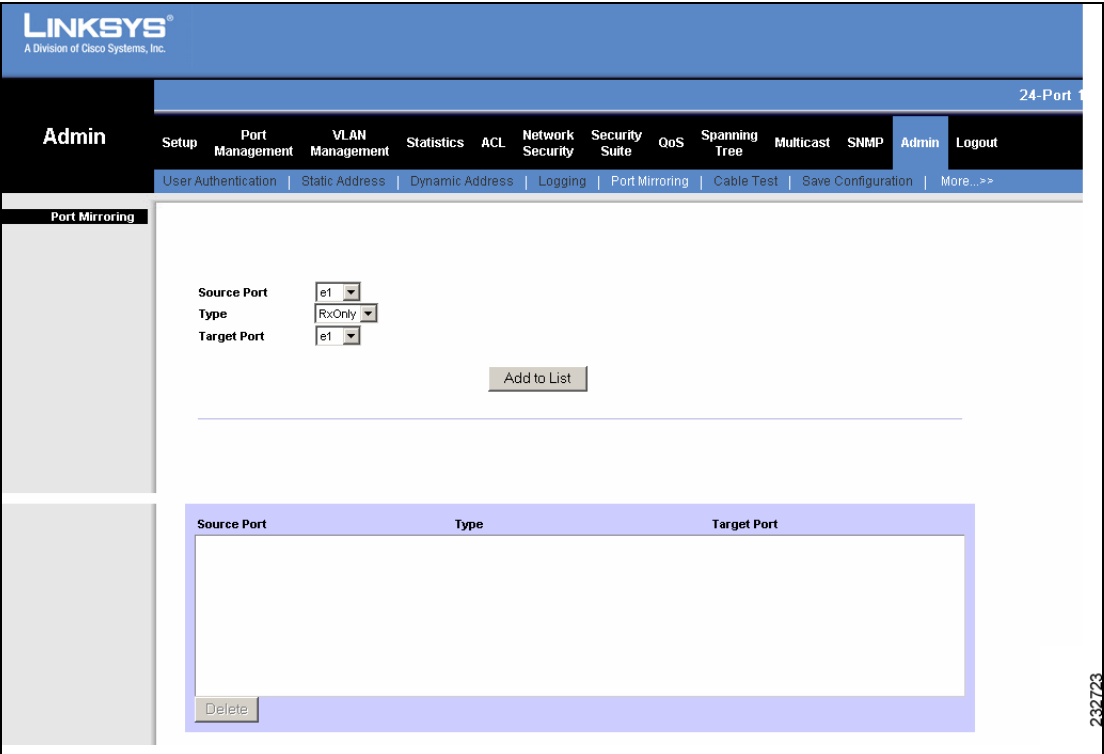
Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port. Port mirroring can be used as diagnostic tool and/or a debugging feature. Port mirroring also enables switch performance monitoring.

Network administrators configure port mirroring by selecting a specific port to copy all packets, and different ports from which the packets are copied.

To enable port mirroring:

- STEP 1** Click **Admin > Port Mirroring**. The *Port Mirroring Screen* opens.

Figure 113 Port Mirroring Screen



The *Port Mirroring Screen* contains the following areas:

- Port Mirroring Parameters
- Port Mirroring Table

The Port Mirroring Parameters contains the following fields:

- **Source Port** — Defines the port from which traffic is analyzed and copied. The possible values are:
 - *Unit No.* — Indicates the stacking member that contains the port being copied.
 - *Port* — Indicates the port being copied.
- **Type** — Indicates the port mode configuration for port mirroring. The possible field values are:
 - *RxOnly* — Defines the port mirroring on received packets only. This is the default value.
 - *TxOnly* — Defines the port mirroring on transmitted packets only.
 - *Both* — Defines the port mirroring on both received and transmitted packets.
- **Target Port** — Defines the port to which traffic is mirrored. A single target port can be specified. The possible values are:
 - *Unit No.* — Indicates the stacking member that contains the port to which traffic is mirrored.
 - *Port* — Indicates the port to which traffic is mirrored.

STEP 2 Define the relevant fields.

STEP 3 Click **Add to List**. The new port mirroring entry is displayed in the Port Mirroring Table at the bottom of the screen.

The **Add to List** button adds the port mirroring entry to the Port Mirroring Table.

To modify a port mirroring entry:

STEP 1 Select the entry in the Port Mirroring Table.

STEP 2 Define the relevant fields.

STEP 3 Click **Update**. The port mirroring entry is updated in the Port Mirroring Table.

STEP 4 Click **Save Settings**. The port mirroring configuration is updated in the device.

To delete a port mirroring definition from the device:

-
- STEP 1** Select the entry in the Static Address Table.
 - STEP 2** Click **Delete**. The selected port mirroring entry is deleted from the Static Address Table.
 - STEP 3** Click **Save Settings**. The port mirroring configuration is deleted from the device.
-

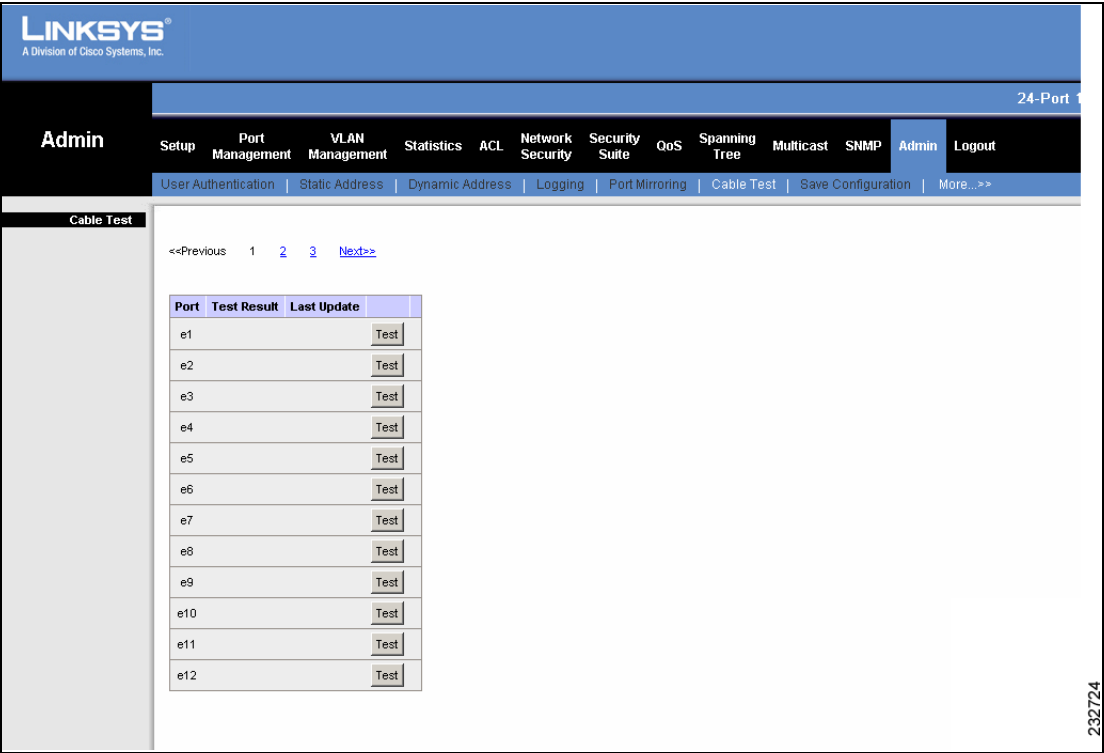
Cable Test

The *Cable Test Screen* 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 that 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. When cables are tested, the ports are in the down state, with the exception of the Approximated Cable Length test.

To test cables:

STEP 1 Click **Admin > Cable Test**. The *Cable Test Screen* opens.

Figure 114 Cable Test Screen



For 24-port devices, the Cable Test Screen displays the interfaces on multiple screens. To browse to a specific interface entry, click the **Previous**, **1**, **2**, **3**, and **Next** links above the table.

The *Cable Test Screen* contains the following fields:

- **Unit No.** — Indicates the stacking member on which cable tests are performed.
- **Port** — Specifies 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 or cut in the middle.
 - *Short Cable* — Indicates that a short has occurred in the cable.
 - *OK* — Indicates that a cable passed the test.
- **Last Update** — Indicates the last time the port was tested.

For testing on GE ports, an **Advanced** button opens the *Copper Cable Extended Feature Screen*.

Figure 115 Advanced Cable Test Screen - GE Ports

Copper Cable Extended Feature						
Cable Status		Unknown Test Result				
Speed		1000 MB/s				
Link Status		Up				
Pair	Distance to Fault	Status	Cable Length	Channel	Polarity	Pair Skew
1-2			Between 80-110in	B	normal	0 ns
3-6			Between 80-110in	A	normal	8 ns
4-5			Between 80-110in	D	normal	0 ns
7 8			Between 80-110in	C	normal	0 ns

Done

232745

The *Copper Cable Extended Feature Screen* contains the following fields.

- **Cable Status** — Displays the cable status.
- **Speed** — Indicates the speed at which the cable is transmitting packets.
- **Link Status** — Displays the current link status.

- **Pair** — The pair of cables under test.
- **Distance to Fault** — Indicates the distance between the port and where the cable error occurred.
- **Status** — Displays the pair status, Green (OK) or Red (not OK).
- **Cable length** — Displays the cable length.
- **Channel** — Displays the cable's channel.
- **Polarity** — Automatic polarity detection and correction permits on all RJ-45 ports for automatic adjustment of wiring errors.
- **Pair Skew** — Reaction or transmission time in nanoseconds for the selected cable pair and given cable length.

STEP 2 Click the **Test** button for the relevant port. The test results appear.

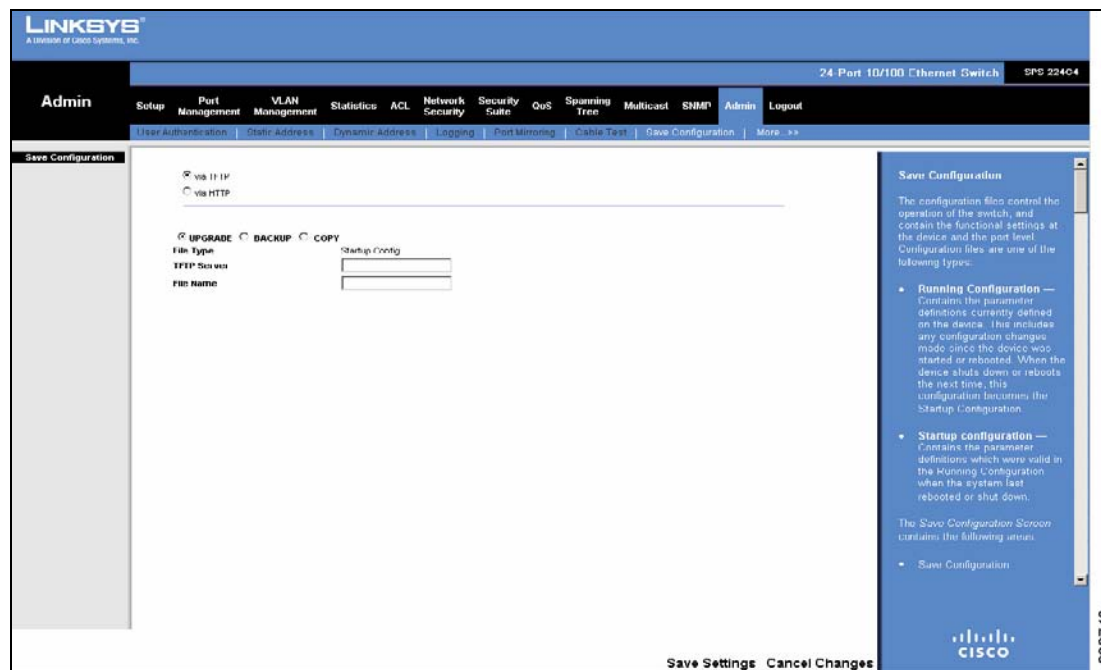
Saving or Upgrading a Configuration

The configuration files control the operation of the switch, and contain the functional settings at the device and the port level. Configuration files are one of the following types:

- **Factory Default** — Contains preset default parameter definitions which are downloaded with a new or upgraded version.
- **Running Configuration** — Contains the parameter definitions currently defined on the device. This includes any configuration changes made since the device was started or rebooted. When the device shuts down or reboots the next time, this configuration becomes the Startup Configuration.
- **Startup configuration** — Contains the parameter definitions which were valid in the Running Configuration when the system last rebooted or shut down.
- **Backup configuration** — Contains a copy of the system configuration for protection against system shutdown, or for maintenance of a specific operating state.

STEP 1 Click **Admin > Save Configuration**. The screen opens.

Figure 116 Save Configuration Screen



The *Save Configuration Screen* contains the following areas:

- **Save Configuration:** Allows you to upgrade, back up, or copy a configuration file.
- **Auto Configuration**

The *Save Configuration* section contains the following fields:

- **via TFTP** — Specifies that the configuration file is saved via a TFTP Server.
- **via HTTP** — Specifies that the configuration file is loaded via an HTTP Server.

STEP 2 If **via TFTP** is selected, select among **Upgrade**, **Backup**, or **Copy**.

- **Upgrade** — Specifies that the source is a configuration file on the TFTP server and the destination is defined in the File Type field. This is an upgrade procedure.
- **Backup** — Specifies that the source is the Running Configuration on the device and the destination is a configuration file on the TFTP server. This is a backup procedure.

- **Copy** — Indicates the device configuration file to copy and the intended usage of the copied file.

If **Upgrade** is selected, the following fields are available:

- **File Type** — Defines the configuration file type. The possible value is:
 - *Running Config* — Contains the parameter definitions currently defined on the device. This includes any configuration changes made since the device was started or rebooted. When the device shuts down or reboots the next time, this configuration becomes the startup configuration.
 - *Startup Config* — Contains the parameter definitions which were valid when the Running Configuration was saved. The Startup Configuration is used when the system restarts or starts after shutdown.
 - *Backup Config* — Contains a copy of the system configuration for protection against system shutdown, or for maintenance of a specific operating state.
- **TFTP Server** — Defines the TFTP Server IP Address to which the Configuration file is uploaded or from which it is downloaded.
- **File Name** — Defines the name of the configuration file that is used for either upgrading or backup.

If **Backup** is selected, the following fields are available:

- **File Type** — Displays the configuration file type. The possible value is:
 - *Startup Config* — Contains the parameter definitions which were valid when the Running Configuration was saved. The Startup Configuration is used when the system restarts or starts after shutdown.
- **TFTP Server** — Defines the TFTP Server IP Address to which the Configuration file is uploaded or from which it is downloaded.
- **File Name** — Displays the name of the configuration file that is used for either upgrading or backup.

If **Copy** is selected, the following fields are available:

- **Source File Type** — Indicates the type of configuration file to copy from the device. The possible value is:
 - *Running Config* — Contains the parameter definitions currently defined on the device, including any configuration changes made since the

device was started or rebooted. When the changes are saved in the device, this configuration becomes the startup configuration.

- *Startup Config* — Contains the parameter definitions which were valid in the Running Configuration when the system last rebooted or shut down.
- *Backup Config* — Contains a copy of the system configuration for protection against system shutdown, or for maintenance of a specific operating state.
- **Destination File Type** — Defines the intended usage of the copied configuration file on the destination device. The possible value is:
 - *Startup Config* — Contains the parameter definitions which were valid when the Running Configuration was saved. The Startup Configuration is used when the system restarts or starts after shutdown.
 - *Running Config* — Contains the parameter definitions defined on the device when this file was saved. This includes any configuration changes made between the device reboot and the creation of this file.
 - *Backup Config* — Contains a copy of the system configuration for protection against system shutdown, or for maintenance of a specific operating state.

STEP 3 If via HTTP is selected, select among **Upgrade**, **Backup**, or **Copy**.

- **Upgrade** — Specifies that the source is a configuration file on the HTTP server and the destination is defined in the File Type field. This is an upgrade procedure.
- **Backup** — Specifies that the source is the Running Configuration on the device and the destination is a configuration file on the HTTP server. This is a backup procedure.

If **Upgrade** is selected, the following fields are available:

- **File Type** — Defines the configuration file type. The possible value is:
 - *Running Config* — Contains the parameter definitions currently defined on the device. This includes any configuration changes made since the device was started or rebooted. When the device shuts down or reboots the next time, this configuration becomes the startup configuration.
 - *Startup Config* — Contains the parameter definitions which were valid when the Running Configuration was saved. The Startup Configuration is used when the system restarts or starts after shutdown.

- *Backup Config* — Contains a copy of the system configuration for protection against system shutdown, or for maintenance of a specific operating state.
- **HTTP Server** — Defines the HTTP Server IP Address to which the Configuration file is uploaded or from which it is downloaded.
- **File Name** — Defines the name of the configuration file that is used for either upgrading or backup.

If **Backup** is selected, the following fields are available:

- **File Type** — Displays the configuration file type. The possible value is:
 - *Startup Config* — Contains the parameter definitions which were valid when the Running Configuration was saved. The Startup Configuration is used when the system restarts or starts after shutdown.
- **TFTP Server** — Defines the HTTP Server IP Address to which the Configuration file is uploaded or from which it is downloaded.
- **File Name** — Displays the name of the configuration file that is used for either upgrading or backup.
- **Source File** — Defines the file name when using the HTTP Server to load the configuration file.

STEP 4 Define the required saved configuration.

- **Source File** — Defines the file name when using the HTTP Server to load the configuration file.

STEP 5 Define the auto configuration.

STEP 6 Click **Save Settings**. The defined configuration file modes are saved and the device is updated.

Enabling DHCP Option 67

DHCP option 67 provides configuration file downloads to the device as part of the procedure to renew the IP address in a TCP/IP network. Once DHCP load configuration is enabled, on the next DHCP renew, if there is a new configuration available on the server it will be downloaded and the system automatically reboots to apply the new configuration.

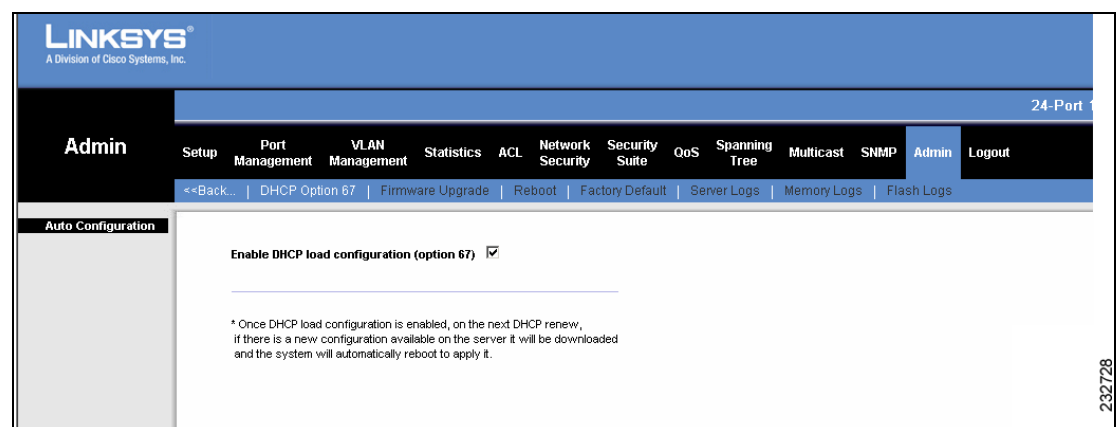
If DHCP load configuration is enabled, when pressing the Renew DHCP Address button if there is a new configuration available on the server it is downloaded and the system automatically reboots to apply it. If the device was configured with additional attributes over the configuration file, these settings are deleted. To prevent this, clear the Enable DHCP load configuration option. In an automatic DHCP renewal procedure (not manual), the device configuration is not overwritten

- **Backup configuration** — Contains a copy of the system configuration for protection against system shutdown, or for maintenance of a specific operating state.

To define configuration files:

STEP 1 Click **Admin > DHCP Option 67**. The *Auto Configuration Screen* opens.

Figure 117 Auto Configuration Screen



The *Auto Configuration* section contains the following field:

- **Enable DHCP load configuration (option 67)** — Indicates if DHCP Option 67 is enabled. The possible field values are:
 - *Checked* — Enables DHCP Option 67 on the device.
 - *Unchecked* — Disables DHCP Option 67 on the device.

- **.Source File** — Defines the file name when using the HTTP Server to load the configuration file.

STEP 2 Define the auto configuration.

STEP 3 Click **Save Settings**. The defined configuration file mode is saved and the device is updated.

Firmware Upgrade

The *Firmware Upgrade Screen* contains parameters for downloading system files.

The Active Image file for each unit in a stacking configuration can be individually selected.

To define firmware upgrade files:

STEP 1 Click **Admin > More > Firmware Upgrade**. The *Firmware Upgrade Screen* opens.

Figure 118 Firmware Upgrade Screen

The *Firmware Upgrade Screen* contains the following fields:

- **via TFTP** — Specifies that the upgrade is downloaded from a TFTP Server.
- **via HTTP** — Specifies that the upgrade is downloaded from an HTTP Server.

STEP 2 If **via TFTP** is selected, choose among **Upgrade**, **Backup**, and **Copy**:

- **Upgrade** — Defines the screen functionality as a Firmware upgrade.
- **Backup** — Defines the screen functionality as a Firmware backup.
- **Copy** — Defines the screen functionality as a Firmware copy. Allows to copy the firmware from the master unit to a unit or all units.

If **Upgrade** is selected, the following fields are available:

- **File Type** — Defines the destination file type to which to the file is downloaded. The possible field values are:
 - *Software Image* — Downloads the Image file.
 - *Boot Code* — Downloads the Boot file.
- **TFTP Server** — Defines the TFTP Server IP Address from which files are downloaded.
- **File Name** — Defines the file to be downloaded when using TFTP.
- **Current Active Image** — Indicates the Image file which is currently active on the device.
- **Active Image After Reset** — Defines the Image file which is active 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.

If **Backup** is selected, the following fields are available:

- **File Type** — Displays the destination file type to which to the file is copied.
- **TFTP Server** — Defines the TFTP Server IP Address to which backup files are stored.
- **File Name** — Displays the file to be uploaded when using TFTP.
- **Master Only** — Specifies to upgrade only the Master.
- **All Units** — Specifies to upgrade all stackable units, including the Master.

STEP 3 If **via HTTP** is selected, enter the following information:

- **Source File** — Defines the file name to be downloaded when using HTTP.

STEP 4 Define the required firmware upgrade settings.

STEP 5 Click **Save Settings** to save the Firmware Upgrade configuration.

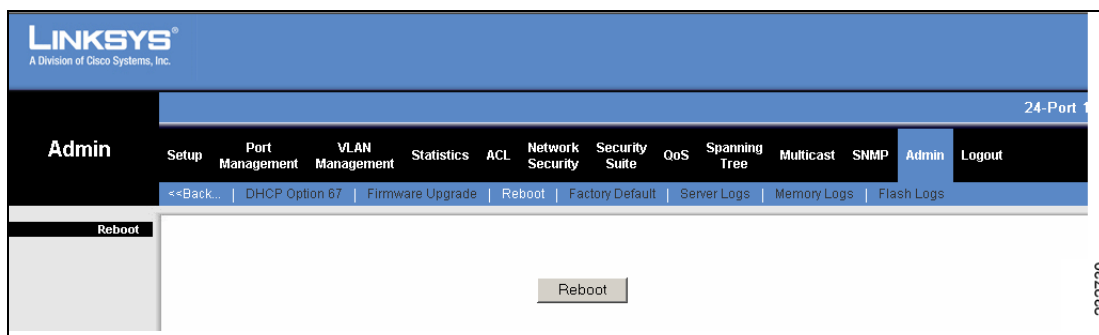
Reboot

In the *Reboot Screen*, the user resets the device. To retain the device's current configuration, copy the Running Configuration file to the Startup Configuration file in the *Saving or Upgrading a Configuration Screen* before resetting the device.

To reset the device:

STEP 1 Click **Admin > More > Reboot**. The *Reboot Screen* opens.

Figure 119 Reboot Screen



The *Reboot Screen* contains the following button:

- **Reboot** — Resets the device.

STEP 2 Click **Reboot** to restart and reset the device.

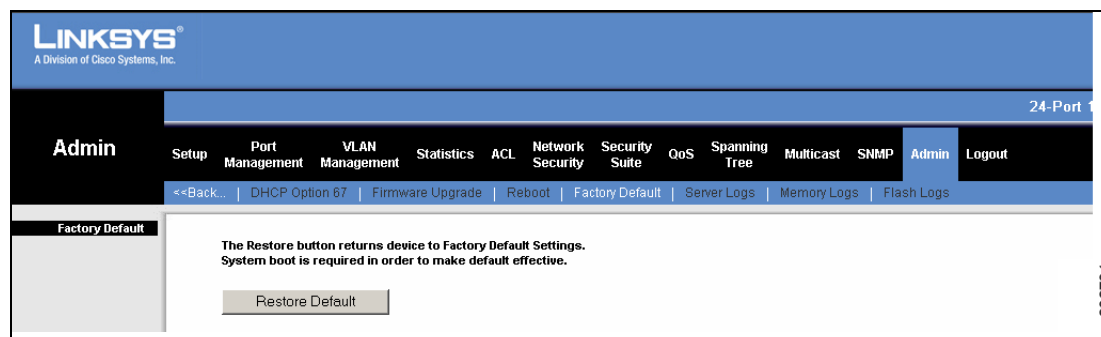
Factory Default

The *Factory Default Screen* allows network managers to reset the device to the factory defaults shipped with the switch. Restoring factory defaults results in erasing the configuration file.

To reset the device to the factory default configuration:

STEP 1 Click **Admin > More > Factory Default**. The *Factory Default Screen* opens.

Figure 120 Factory Default Screen



The *Factory Default Screen* contains the following command:

- **Restore Default** — The device is restored to the factory default configuration after system reset. In Stacking mode, unit no. 1 becomes the Master, and the stacking members are reset.

STEP 2 Click **Restore Default** to restore the device to the factory default configuration.

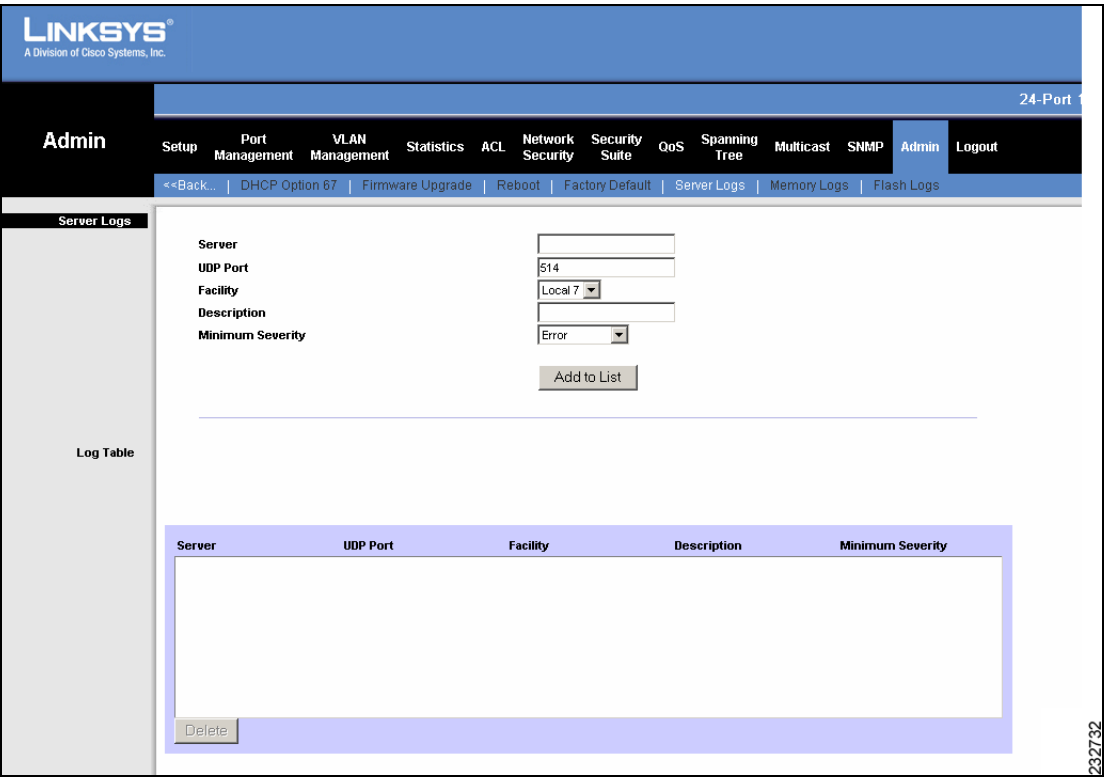
Server Logs

The *Server Logs Screen* 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 remote log servers:

- STEP 1** Click **Admin > More > Server Logs**. The *Server Logs Screen* opens.

Figure 121 Server Logs Screen



The *Server Logs Screen* contains the following areas:

- Log Parameters
- Log Table

The Log Parameters contains the following fields:

- **Server** — Specifies the server IP to which logs can be sent.
- **UDP Port** — Defines the UDP port to which the server logs are sent. The possible range is 1 to 65535. The default value is 514.
- **Facility** — Defines a user-defined application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility 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 from a Notice severity and higher are sent to the remote server. The possible values are:
 - *Emergency* — The system is not functioning.
 - *Alert* — The system needs immediate attention.
 - *Critical* — The system is in a critical state.
 - *Error* — A system error has occurred.
 - *Warning* — A system warning has occurred.
 - *Notice* — The system is functioning properly, but system notice has occurred.
 - *Informational* — Provides device information.
 - *Debug* — Provides detailed information about the log. If a Debug error occurs, contact Customer Tech Support.

STEP 2 Define the relevant fields.

STEP 3 Click **Add to List**. The new Server Log configuration is displayed in the Log Table at the bottom of the screen.

The **Add to List** button adds the Server Log configuration to the Log Table.

To modify a Server Log entry:

-
- STEP 1** Select the entry in the Log Table.
 - STEP 2** Define the relevant fields.
 - STEP 3** Click **Update**. The Server Log configuration is updated in the Log Table. The device is updated.
-

To delete a Server Log configuration from the device:

-
- STEP 1** Select the entry in the Log Table.
 - STEP 2** Click **Delete**. The selected Server Log configuration is deleted from the device.
-

Memory Logs

The *Memory Logs Screen* contains all system log entries in chronological order that are saved in RAM (Cache). After restart, these log entries are deleted.

To view the memory log:

STEP 1 Click **More > Admin > More > Memory Logs**. The *Memory Logs Screen* opens.

Figure 122 Memory Logs Screen

Log Index	Log Time	Severity	Description	
1	2147483516	20-Aug-2008 10:11:56	Informational	%AAA-I-DISCONNECT: http connection for user admin, source 10.6.70.12 destination 10.6.24.2 TERMINATED
2	2147483517	20-Aug-2008 10:10:38	Informational	%AAA-I-CONNECT: User CLI session for user admin over console , source 0.0.0.0 destination 0.0.0.0 ACCEPTED
3	2147483518	20-Aug-2008 10:10:37	Warning	%AAA-W-REJECT: New console connection for user unknown, source 0.0.0.0 destination 0.0.0.0 REJECTED
4	2147483519	20-Aug-2008 10:03:39	Informational	%AAA-I-CONNECT: New http connection for user admin, source 10.6.70.12 destination 10.6.24.2 ACCEPTED
5	2147483520	20-Aug-2008 10:02:04	Informational	%BOOTP_DHCP_CL-I-DHCPRENEWED: The device has been renewed the configuration on interface Vlan1 , IP 10.6.24.2, mask 255.255.255.224, DHCP server 10.6.22.25
6	2147483521	20-Aug-2008 10:02:04	Warning	%BOOTP_DHCP_CL-W-FLNMEMPTY: No option 67 in the DHCP packet. Unable to start out of configuration.
7	2147483522	20-Aug-2008 09:45:32	Informational	%AAA-I-CONNECT: New http connection for user admin, source 10.6.150.49 destination 10.6.24.2 ACCEPTED
8	2147483523	20-Aug-2008 09:41:42	Informational	%AAA-I-CONNECT: New http connection for user admin, source 10.6.150.49 destination 10.6.24.2 ACCEPTED
9	2147483524	20-Aug-2008 09:41:32	Informational	%AAA-I-DISCONNECT: http connection for user admin, source 10.6.150.49 destination 10.6.24.2 TERMINATED
10	2147483525	20-Aug-2008 09:05:49	Informational	%AAA-I-CONNECT: New http connection for user admin, source 10.6.150.49 destination 10.6.24.2 ACCEPTED
11	2147483526	20-Aug-2008 09:05:31	Informational	%AAA-I-DISCONNECT: http connection for user admin, source 10.6.150.49 destination 10.6.24.2 TERMINATED
12	2147483527	20-Aug-2008 08:53:56	Informational	%AAA-I-CONNECT: New http connection for user admin, source 10.6.150.49 destination 10.6.24.2 ACCEPTED

The *Memory Logs Screen* may display log entries in multiple tables. To browse to a specific log entry, click the **Previous** and **Next** links above the table.

The *Memory Logs Screen* contains the following fields:

- **Log Index** — Displays the log number.
- **Log Time** — Displays the time at which the log was generated.
- **Severity** — Displays the log severity.
- **Description** — Displays the log message text.

To clear the Memory Log, click the **Clear Log** button. All log entries are cleared.

Flash Logs

The *Flash Logs Screen* 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 Flash Log is available after reboot.

To view the Flash Log:

STEP 1 Click **Admin > More > Flash Logs**. The *Flash Logs Screen* opens.

Figure 123 Flash Logs Screen

The screenshot shows the Linksys Flash Logs screen. The top navigation bar includes 'Admin' and 'Logout'. Below the navigation bar, there's a section for 'Flash Logs' with a table of log entries. The table has four columns: Log Index, Log Time, Severity, and Description. The log entries are as follows:

Log Index	Log Time	Severity	Description
1	2147471579 01-Oct-2006 01:05:08	Emergency	%SWCOS-F-PCLSERVDELBDARP: Delete not existed VLAN 1 ***** FATAL ERROR ***** Reporting Task: POLI. Software Version: 1.0.2 (date 06-Aug-2008 time 14:18 :48) 0x14510c 0x142770 0x414204 0x345860 0x348818 0x606710 0x607170 0x87e 2bc 0x43545c 0x472190 ***** END OF FATAL ERROR *****
2	2147472790 01-Oct-2006 03:25:08	Emergency	%SWCOS-F-PCLSERVDELBDARP: Delete not existed VLAN 1 ***** FATAL ERROR ***** Reporting Task: POLI. Software Version: 1.0.2 (date 06-Aug-2008 time 14:18 :48) 0x14510c 0x142770 0x414204 0x345860 0x348818 0x606710 0x607170 0x87e 2bc 0x43545c 0x472190 ***** END OF FATAL ERROR *****
3	2147474979 01-Oct-2006 01:05:36	Emergency	%SNMP-F-FTLERR: SNMP Package: SnmpCen Routine: 25 Location: 10 Error: Application returned a bad key: IP address type not supported error: variable = 125, field = udpEndpointLocalAddress, value = 0 ***** FATAL ERROR ***** (warning: SYS LOGG_log_fatal should be used to log fatal errors, not SYSLOGG_log) Reporting Task: SNMP. Software Version: 1.0.2 (date 09-Jul-2008 time 12:45:39) 0x14510 c 0x142770 0x412d9c 0x344fbc 0x348054 0x348498 0x31411c 0x315680 0x2faa 8c 0x2fada8 0x2e8a14 0x2d1e34 0x2d4030 0x2dd164 0x2e581c 0x2e5890 0x2e75f c 0x2e76c4 0x312808 0x471e48 ***** END OF FATAL ERROR *****
4	2147477168 01-Oct-2006 01:07:57	Emergency	%SNMP-F-FTLERR: SNMP Package: SnmpCen Routine: 25 Location: 10 Error: Application returned a bad key: IP address type not supported error: variable = 125, field = udpEndpointLocalAddress, value = 0 ***** FATAL ERROR ***** (warning: SYS LOGG_log_fatal should be used to log fatal errors, not SYSLOGG_log) Reporting Task: SNMP. Software Version: 1.0.2 (date 09-Jul-2008 time 12:45:39) 0x14510 c 0x142770 0x412d9c 0x344fbc 0x348054 0x348498 0x31411c 0x315680 0x2faa 8c 0x2fada8 0x2e8a14 0x2d1e34 0x2d4030 0x2dd164 0x2e581c 0x2e5890 0x2e75f c 0x2e76c4 0x312808 0x471e48 ***** END OF FATAL ERROR *****
5	2147479357 01-Oct-2006 01:05:26	Emergency	%SNMP-F-FTLERR: SNMP Package: SnmpCen Routine: 25 Location: 10 Error: Application returned a bad key: IP address type not supported error: variable = 125, field = udpEndpointLocalAddress, value = 0 ***** FATAL ERROR ***** (warning: SYS LOGG_log_fatal should be used to log fatal errors, not SYSLOGG_log) Reporting Task: SNMP. Software Version: 1.0.2 (date 09-Jul-2008 time 12:45:39) 0x14510 c 0x142770 0x412d9c 0x344fbc 0x348054 0x348498 0x31411c 0x315680 0x2faa 8c 0x2fada8 0x2e8a14 0x2d1e34 0x2d4030 0x2dd164 0x2e581c 0x2e5890 0x2e75f c 0x2e76c4 0x312808 0x471e48 ***** END OF FATAL ERROR *****
6	2147481546 01-Oct-2006 01:17:19	Emergency	%SNMP-F-FTLERR: SNMP Package: SnmpCen Routine: 25 Location: 10 Error: Application returned a bad key: IP address type not supported error: variable = 125, field = udpEndpointLocalAddress, value = 0 ***** FATAL ERROR ***** (warning: SYS LOGG_log_fatal should be used to log fatal errors, not SYSLOGG_log) Reporting Task: SNMP. Software Version: 1.0.2 (date 09-Jul-2008 time 12:45:39) 0x14510 c 0x142770 0x412d9c 0x344fbc 0x348054 0x348498 0x31411c 0x315680 0x2faa 8c 0x2fada8 0x2e8a14 0x2d1e34 0x2d4030 0x2dd164 0x2e581c 0x2e5890 0x2e75f c 0x2e76c4 0x312808 0x471e48 ***** END OF FATAL ERROR *****

The *Flash Logs Screen* may display log entries in multiple tables. To browse to a specific log entry, click the **Previous** and **Next** links above the table.

The *Flash Log Screen* contains the following fields:

- **Log Index** — Displays the log number.
- **Log Time** — Displays the time at which the log was generated.
- **Severity** — Displays the log severity.
- **Description** — Displays the log message text.

To clear the Flash Log, click the **Clear Log** button. All log entries are cleared.

Logout

The Logout command enables network administrators to log out of the device management application in an orderly manner.

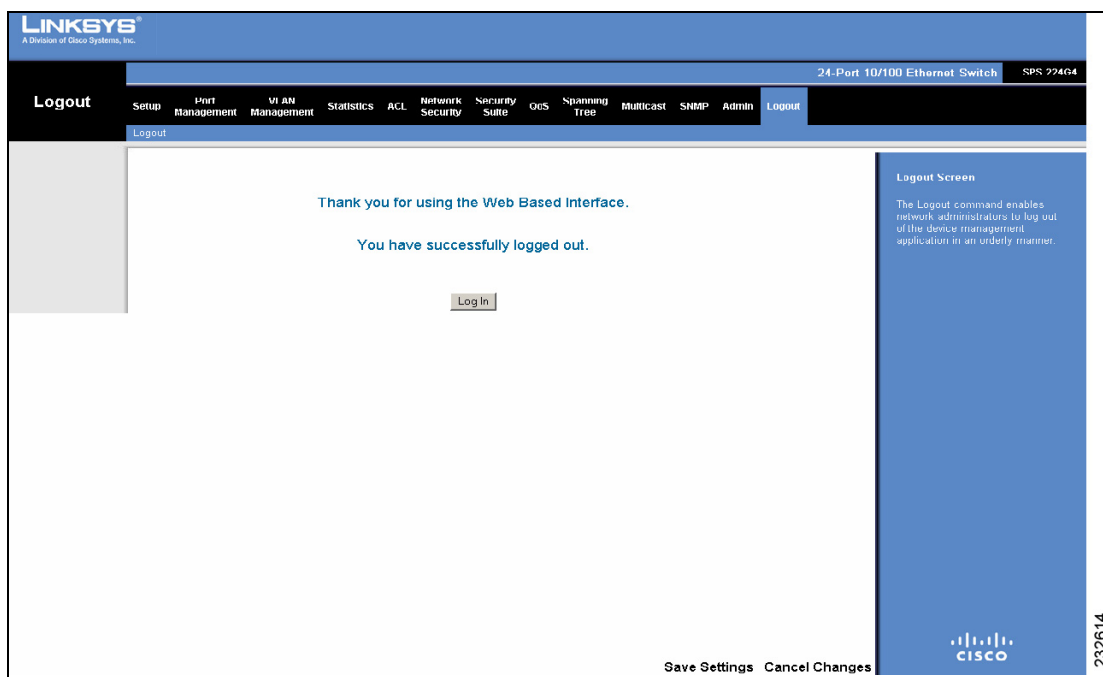
Logout

The Logout command enables network administrators to log out of the device management application in an orderly manner.

To log out of the device management application:

STEP 1 Click **Logout**. The *Logout Screen* opens.

Figure 124 Logout Screen



The *Logout Screen* notifies whether logout was successful.

Where to Go From Here

Product Resources

Website addresses in this document are listed without **http://** in front of the address because most current web browsers do not require it. If you use an older web browser, you may have to add **http://** in front of the web address.

Resource	Link
Cisco Partner Central (requires partner registration and login)	www.cisco.com/web/partners/sell/smb/
Cisco Small Medium Business Product Information	www.cisco.com/go/smallbiz

Related Documentation

For additional information about the Ethernet switches, see the *SPS208G/SPS224G4/SPS2024 Ethernet Switches Command Line Interface Reference Guide*.

Additional Information

Regulatory Compliance and Safety Information

Regulatory Compliance and Safety Information for this product is available on Cisco.com at the following location:

www.cisco.com/go/smallbiz

Warranty

Warranty information that applies to this product is available on Cisco.com at the following location:

www.cisco.com/go/smallbiz

End User License Agreement (EULA)

Licensing information that applies to this product is available on Cisco.com at the following location:

www.cisco.com/go/smallbiz



Support Contacts

Support contact information for this product is available on Cisco.com at the following location:

www.cisco.com/go/smallbiz