

**NETGEAR®**

# **M4100 Series Managed Switch**

**User Manual**

**Version 10.0.2**

April 2015  
202-10967-02

350 East Plumeria Drive  
San Jose, CA 95134  
USA

## **Support**

Thank you for selecting NETGEAR products.

After installing your device, locate the serial number on the label of your product and use it to register your product at <https://my.netgear.com>. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website.

For product updates and web support, visit <http://support.netgear.com>.

Phone (US & Canada only): 1-888-NETGEAR.

Phone (Other Countries): Check the list of phone numbers at <http://support.netgear.com/general/contact/default.aspx>.

Contact your Internet service provider for technical support.

## **Compliance**

For regulatory compliance information, visit <http://www.netgear.com/about/regulatory>.

See the regulatory compliance document before connecting the power supply.

## **Trademarks**

© NETGEAR, Inc., NETGEAR and the NETGEAR logo are trademarks of NETGEAR, Inc. Any non-NETGEAR trademarks are used for reference purposes only.

## **Revision History**

<b>Publication Part Number</b>	<b>Publish Date</b>	<b>Comments</b>
202-10967-01	November 2011	Original publication
202-10967-02	April 2015	Software version 10.0.2

# Contents

## Chapter 1 Get Started

Available Publications and Online Help.....	12
Register Your Product.....	12
Understanding the User Interfaces.....	12
Web Management Interface Overview .....	13
Software Requirements to Use the Web Interface .....	13
Use a Web Browser to Access the Switch and Log In.....	13
Web Interface Buttons and User-Defined Fields.....	14
Interface Naming Conventions .....	14
Online Help.....	15
Web Management Interface Device View.....	16
Using SNMP .....	17

## Chapter 2 Configure System Information

System Configuration.....	20
Configure Initial Management VLAN Settings .....	21
Define System Information .....	22
View the Switch Status.....	24
View the Fan Status .....	24
View the Temperature Status .....	25
View the Device Status .....	26
View Switch Statistics .....	28
View the System CPU Status.....	30
View USB Device Information.....	31
Manage Loopback Interfaces .....	33
View the IPv6 Network Neighbor Table.....	34
Configure an IPv4 Management VLAN .....	35
View or Set the System Time .....	37
Configure SNTP Global Settings.....	38
View the SNTP Global Status.....	40
Configure SNTP Servers .....	43
Configure Summer Time Settings .....	45
Configure DNS.....	47
Configure Host Settings.....	49
Configure Green Ethernet Settings .....	50
Configure Green Ethernet Interface Settings.....	51
Configure Port Green Mode Statistics.....	53
View the Green Mode Statistics Summary .....	55
View the Port Green Mode EEE History .....	57

Configure the DHCP Server.....	58
Exclude an Address from the DHCP Server .....	59
Configure the DHCP Pool.....	60
Configure the DHCP Pool Options .....	63
View DHCP Server Statistics.....	64
View DHCP Bindings Information.....	66
View DHCP Conflicts Information .....	67
Configure the DHCP Relay.....	68
Configure a DHCP L2 Relay VLAN .....	70
Configure the DHCP L2 Relay Interface .....	71
View DHCP L2 Relay Interface Statistics .....	72
Configure UDP Relay Global Settings.....	73
Configure the UDP Relay Interface .....	75
Configure the Basic PoE Settings .....	76
Configure Advanced PoE Settings.....	78
Configure a PoE Port .....	80
Configure SNMP Community Settings .....	83
Configure an SNMP Trap .....	84
Configure Trap Flags.....	86
View All MIBs Supported by the Switch.....	87
Configure SNMP v3 Settings for a User .....	88
LLDP Overview .....	90
Configure LLDP Global Settings .....	90
Configure an LLDP Interface.....	91
View LLDP Statistics.....	92
View LLDP Local Device Information.....	95
View LLDP Remote Device Information .....	96
View LLDP Remote Device Inventory .....	98
Configure LLDP-MED Global Settings.....	99
Configure the LLDP-MED Interface.....	99
View LLDP-MED Local Device Information .....	101
View LLDP-MED Remote Device Information .....	103
View LLDP-MED Remote Device Inventory .....	106
ISDP Settings Overview .....	107
Configure ISDP Global Settings .....	107
Configure Advanced Global ISDP Settings .....	108
Configure the ISDP Interface .....	110
View ISDP Neighbors .....	111
View ISDP Statistics .....	112
Configure Timers.....	114
Configure the Global Timer Settings .....	114
Configure the Timer Schedule .....	115

## Chapter 3 Configure Switching Information

VLAN Overview.....	118
Configure a Basic VLAN.....	118
Configure an Internal VLAN.....	119

Add a VLAN .....	120
Reset VLAN Configuration.....	121
Configure Internal VLAN Settings .....	122
Configure VLAN Trunking .....	123
Configure VLAN Membership .....	125
View VLAN Status.....	127
Configure Port PVID.....	128
Configure a MAC-Based VLAN Group.....	130
Configure a Protocol-Based VLAN Group.....	131
Configure Protocol-Based VLAN Group Membership.....	132
Configure an IP Subnet-Based VLAN .....	134
Configure Port DVLAN.....	135
Configure a Voice VLAN.....	136
Configure GARP Switch Settings .....	137
Configure GARP Port Settings .....	138
Auto-VoIP Overview.....	140
Configure Protocol-Based Port Settings.....	140
Configure OUI-Based Properties .....	141
Configure OUI-Based Port Settings.....	142
Configure the OUI Table.....	143
View the Auto-VoIP Status .....	145
Spanning Tree Protocol Overview.....	145
Configure Spanning Tree Protocol .....	146
Configure Advanced STP Settings .....	148
Configure Common Spanning Tree.....	150
Configure CST Ports .....	152
View Spanning Tree CST Port Status .....	154
Configure an MST Instance .....	156
View MST Port Status .....	158
View Spanning Tree Statistics .....	160
Configure Multicast.....	162
Configure Bridge Multicast Forwarding.....	162
View the MFDB Table .....	163
View MFDB Statistics .....	164
IGMP Snooping Overview .....	165
Configure IGMP Snooping Interface Settings.....	166
Configure IGMP Snooping Settings for VLANs.....	167
Configure IGMP Snooping for a Multicast Router .....	168
Configure IGMP Snooping for a Multicast Router VLAN .....	169
Configure IGMP Snooping Querier.....	170
IGMP Snooping Querier VLAN Configuration.....	172
Configure MLD Snooping.....	174
Configure MLD Snooping for an Interface .....	175
Configure a MLD VLAN .....	176
Configure a Multicast Router .....	177
Configure a Multicast Router VLAN.....	178
Configure the MLD Snooping Querier.....	179
Configure an MLD Snooping Querier VLAN .....	180

Configure MVR .....	182
Configure Advanced MVR Settings .....	183
Configure MVR Groups .....	185
Configure an MVR Interface .....	186
Configure MVR Group Membership.....	187
View MVR Statistics .....	188
Manage MAC Addresses.....	189
View the MAC Address Table .....	190
Configure Dynamic Addresses Aging Interval .....	192
Configure a Static MAC Address.....	193
Configure Port Settings .....	194
Enter a Port Description .....	196
Link Aggregation Group Overview.....	197
Configure LAG Settings .....	197
Configure LAG Membership .....	199

## Chapter 4 Routing

Manage the Routing Table .....	203
Configure Basic Routes .....	203
Configure Advanced Routes .....	205
Configure Route Preferences .....	207
Configure IP Settings .....	208
View IP Statistics.....	210
Configure Advanced IP Settings .....	214
View IP Statistics.....	216
Configure an IP Interface.....	220
Configure a Secondary IP Address.....	222
VLAN Overview.....	223
Use the VLAN Static Routing Wizard .....	224
Configure VLAN Routing .....	225
ARP Overview .....	226
Display ARP Cache Entries.....	227
Configure the Static ARP Cache .....	228
View or Configure the ARP Table .....	229
Configure Router Discovery .....	231

## Chapter 5 Configure Quality of Service

QoS Overview .....	234
Class of Service .....	234
Configure CoS .....	235
Map 802.1p Priorities to Queues.....	236
Map IP DSCP Values to Queues .....	237
Configure CoS Settings for an Interface .....	238
Configure an Interface Queue.....	239
Differentiated Services .....	241
DiffServ Wizard Overview .....	242

Use the DiffServ Wizard .....	242
Configure DiffServ .....	243
Configure the Global Diffserv Mode .....	245
Configure a DiffServ Class .....	247
Configure the Class Match Criteria .....	248
Configure a DiffServ IPv6 Class .....	250
Configure the DiffServ Class Match Criteria .....	252
Configure DiffServ Policy .....	254
Configure DiffServ Policy Attributes .....	255
Configure DiffServ Policy Settings on an Interface .....	257
View Service Statistics .....	258

## Chapter 6 Manage Device Security

Management Security Settings .....	262
Configure Users .....	262
Set the Password for a User .....	263
Enable Password Configuration .....	264
Configure a Line Password .....	265
Configure RADIUS Settings .....	266
Configure a RADIUS Server .....	268
Configure a RADIUS Accounting Server .....	271
TACACS .....	272
Configure Global TACACS Settings .....	273
Configure TACACS Server Settings .....	274
Set Up a Login Authentication List .....	275
Enable an Authentication List .....	276
Configure a Dot1x Authentication List .....	278
Configure an HTTP Authentication List .....	279
HTTPS Authentication List .....	280
View Login Sessions .....	281
Configure Management Access .....	282
Configure HTTP Server Settings .....	282
Configure HTTPS Settings .....	283
Manage Certificates .....	285
Download a Certificate .....	286
Configure SSH .....	287
Manage Host Keys .....	289
Download Host Keys .....	290
Manage Telnet .....	292
Configure a Telnet Authentication List .....	292
Configure Inbound Telnet .....	293
Configure Outbound Telnet .....	294
Configure the Console Port .....	295
Configure Denial of Service Settings .....	297
Port Authentication Overview .....	300
Configure Global 802.1X Settings .....	300
Configure 802.1X Settings .....	302
Configure 802.1X Settings for Port Authentication .....	303

View the Port Summary.....	306
View the Client Summary .....	309
Traffic Control .....	310
Configure MAC Filter Settings .....	310
View the MAC Filter Summary .....	312
Configure the Global Port Security Mode.....	313
Configure Port Security Settings .....	314
Convert a Dynamic MAC Address to a Static Address .....	315
Configure Static MAC Addresses .....	316
Configure a Private Group .....	317
Configure Private Group Membership.....	318
Configure Protected Ports.....	319
Private VLAN Overview .....	321
Configure a Private VLAN Type .....	321
Configure the Private VLAN Association.....	322
Configure the Private VLAN Port Mode .....	323
Configure Private VLAN Host Interface.....	324
Configure Private VLAN Promiscuous Interface Settings.....	325
Storm Control Overview .....	327
Configure Storm Control Global Settings .....	327
View Storm Control Settings for an Interface .....	328
Control DHCP Snooping Settings .....	330
Configure Global DHCP Snooping Settings.....	330
Configure the DHCP Snooping Interface.....	331
Configure DHCP Snooping Static Binding .....	332
Configure DHCP Snooping Dynamic Binding .....	333
Configure Persistent DHCP Snooping .....	334
View DHCP Snooping Statistics .....	335
Configure an IP Source Guard Interface.....	336
Configure IP Source Guard Binding .....	337
Configure Dynamic ARP Inspection .....	339
Configure Dynamic ARC Inspection.....	340
Configure a Dynamic ARC Inspection Interface.....	341
Configure a DAI ACL.....	342
Configure a Dynamic ARP Inspection ACL Rule .....	343
View DAI Statistics .....	343
Access Control List Overview .....	345
Use the ACL Wizard .....	345
Create a MAC ACL .....	347
Configure MAC Rules .....	349
Configure ACL MAC Binding.....	351
View or Delete MAC Bindings.....	353
Configure an IP ACL .....	354
Configure Rules for an IP ACL.....	355
Configure IP Extended Rules.....	358
Configure an IPv6 ACL.....	361
Configure IPv6 Rules .....	362
Configure ACL Interface Bindings .....	365

View or Delete IP ACL Bindings.....	366
View or Delete VLAN ACL Bindings .....	367

## Chapter 7 Monitoring the System

View Port Statistics.....	370
View Detailed Port Statistics.....	371
View EAP Statistics .....	378
Perform a Cable Test .....	379
Logs Overview.....	381
View or Configure Buffered Logs.....	381
Message Format in Logs .....	382
Enable the Command Log .....	383
Configure the Console Log .....	384
Configure the Syslog .....	385
View Trap Logs .....	386
Event Logs .....	388
Configure Persistent Logs .....	389
Port Mirroring Overview .....	391
Configure Port Mirroring.....	391
Configure an RSPAN VLAN .....	393
Configure an RSPAN Source Switch .....	394
Configure an RSPAN Source Interface.....	395
Configure the RSPAN Destination Switch .....	397
sFlow Overview.....	398
Configure sFlow Agent Information.....	398
Configure an sFlow Agent .....	399
Configure the sFlow Receiver .....	400
Configure sFlow Interface Settings .....	402

## Chapter 8 Maintenance

Save Configuration .....	405
Configure Auto Install .....	405
Reboot a Switch.....	406
Reset the Switch to Factory Default Settings.....	407
Reset All User Passwords to Factory Defaults .....	408
Upload Files.....	409
Upload a File from the Switch to the TFTP Server.....	409
Upload an HTTP File .....	411
Upload a USB File .....	412
Download Files.....	413
Download Files .....	413
Download HTTP Files .....	415
Download a File to a USB Device .....	417
File Management Overview.....	418
Copy a File .....	418
Configure Dual Image Settings.....	419
Use the Ping IPv4 Utility.....	420

Use the Ping IPv6 Utility.....	422
Run Traceroute IPv4 .....	423
Configure Traceroute IPv6 Settings .....	425

## **Appendix A Default Settings**

Factory Default Settings .....	427
--------------------------------	-----

## **Appendix B Configuration Examples**

Virtual Local Area Networks .....	431
VLAN Example Configuration .....	432
Access Control Lists .....	433
MAC ACL Sample Configuration.....	433
Standard IP ACL Example Configuration.....	434
Differentiated Services (DiffServ).....	435
Class .....	436
DiffServ Traffic Classes .....	436
Creating Policies .....	437
DiffServ Example Configuration .....	438
802.1X .....	440
802.1X Sample Configuration .....	441
MSTP.....	442
MSTP Sample Configuration.....	444

# Get Started

---

1

This chapter provides an overview of starting your NETGEAR Managed Switch and accessing the user interface. This chapter contains the following sections:

- *Available Publications and Online Help*
- *Register Your Product*
- *Understanding the User Interfaces*
- *Web Management Interface Overview*
- *Use a Web Browser to Access the Switch and Log In*
- *Using SNMP*

---

**Note:** For more information about the topics covered in this manual, visit the support website at [support.netgear.com](http://support.netgear.com).

---

---

**Note:** Firmware updates with new features and bug fixes are made available from time to time at [downloadcenter.netgear.com](http://downloadcenter.netgear.com). Some products can regularly check the site and download new firmware, or you can check for and download new firmware manually. If the features or behavior of your product does not match what is described in this guide, you might need to update your firmware.

---

## Available Publications and Online Help

A number of publications are available for your managed switch at [downloadcenter.netgear.com](http://downloadcenter.netgear.com), including the following publications:

- *M4100 Chassis Hardware Installation Guide.*
- *M4100 Switch Module Installation Guide.*
- *M4100 Software Setup Manual.*
- *M4100 User Manual* (this document). You can also access this document online when you are logged in to the switch. Select **Help > Online Help > User Guide**.
- *M4100 Command Line Interface Manual.*

Refer to the *M4100 Command Line Interface Manual* for information about the command structure. This provides information about the CLI commands used to configure the switch. It provides CLI descriptions, syntax, and default values.

- *M4100 Software Administration Manual.*

When you log into the web management interface, online help is available. See [Online Help](#) on page 15.

## Register Your Product

The first time you log in to the switch, you are given the option of registering with NETGEAR. Registration confirms that your email alerts work, lowers technical support resolution time, and ensures that your shipping address accuracy. NETGEAR would also like to incorporate your feedback into future product development. NETGEAR never sells or rents your email address and you can opt out of communications at any time.

To register with NETGEAR when you are prompted, click the **REGISTER NOW** button.

## Understanding the User Interfaces

The managed switch software includes a set of comprehensive management functions for configuring and monitoring the system by using one of the following methods:

- Web user interface
- Simple Network Management Protocol (SNMP)
- Command-line interface (CLI)

Each of the standards-based management methods allows you to configure and monitor the components of the managed switch software. The method you use to manage the system depends on your network size and requirements, and on your preference.

The *M4100 Series Managed Switch User Manual* (this book) describes how to use the web-based interface to manage and monitor the system.

## Web Management Interface Overview

Your managed switch contains an embedded web server and management software for managing and monitoring switch functions. The managed switch functions as a simple switches without the management software. However, you can use the management software to configure more advanced features that can improve switch efficiency and overall network performance.

Web-based management lets you monitor, configure, and control your switch remotely using a standard web browser instead of using expensive and complicated SNMP software products. From your web browser, you can monitor the performance of your switch and optimize its configuration for your network. You can configure all switch features, such as VLANs, QoS, and ACLs, by using the web-based management interface.

## Software Requirements to Use the Web Interface

To access the switch by using a web browser, the browser must meet the following software requirements:

- HTML version 4.0, or later
- HTTP version 1.1, or later
- Java Runtime Environment 1.6 or later

## Use a Web Browser to Access the Switch and Log In

You can use a web browser to access the switch and log in. You must be able to ping the IP address of the managed switch management interface from your administrative system for web access to be available.

➤ **To use browser-based access to log in to the switch:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

## Web Interface Buttons and User-Defined Fields

The following table shows the command buttons that are used throughout the screens in the web interface:

**Table 1. Web interface command buttons**

Button	Function
<b>ADD</b>	Clicking the <b>ADD</b> button adds the new item configured in the heading row of a table.
<b>APPLY</b>	Clicking the <b>APPLY</b> button sends the updated configuration to the switch. Configuration changes take effect immediately.
<b>CANCEL</b>	Clicking the <b>CANCEL</b> button cancels the configuration on the screen and resets the data on the screen to the previous values of the switch.
<b>DELETE</b>	Clicking the <b>DELETE</b> button removes the selected item.
<b>REFRESH</b>	Clicking the <b>REFRESH</b> button refreshes the screen with the latest information from the device.
<b>LOGOUT</b>	Clicking the <b>LOGOUT</b> button ends the session.

User-defined fields can contain 1 to 159 characters, unless otherwise noted on the configuration web screen. All characters can be used except for the following (unless specifically noted in for that feature):

User-Defined Field Invalid Characters	
\	<
/	>
*	
?	

## Interface Naming Conventions

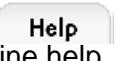
The managed switch supports physical and logical interfaces. Interfaces are identified by their type and the interface number. The physical ports are gigabit interfaces and are numbered on the front panel. You configure the logical interfaces by using the software.

The following table describes the naming convention for all interfaces available on the switch.

**Table 2. Naming conventions for interfaces**

Interface	Description	Example
Physical	The physical ports are gigabit Ethernet interfaces and are numbered sequentially starting from one.	0/1, 0/2, 0/3, and so on
Link aggregation group (LAG)	LAG interfaces are logical interfaces that are used only for bridging functions.	LAG 1, LAG 2, IAG 3, and so on
CPU management interface	This is the internal switch interface responsible for the switch base MAC address. This interface is not configurable and is always listed in the MAC Address Table.	5/1
Routing VLAN interfaces	This is an interface used for routing functionality.	VLAN 1, VLAN 2, VLAN 3, and so on

## Online Help

When you log in to the switch, every screen contains a link to the online help  that contains information to assist in configuring and managing the switch. The online help screens are context sensitive. For example, if the IP Addressing screen is open, the help topic for that screen displays if you click the **Help** button.

You can connect to the online support site at [netgear.com](http://netgear.com) when you are logged in to the switch.

➤ **To access the online support link:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7. Select Help > Online Help > Support.**

To connect to the NETGEAR support site for managed switch, click the **APPLY** button.

## Web Management Interface Device View

The Device View is a Java® applet that displays the ports on the switch. This graphic provides an alternate way to navigate to configuration and monitoring options. The graphic also provides information about device ports, current configuration and status, tables, and feature components.

➤ **To use Device View:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

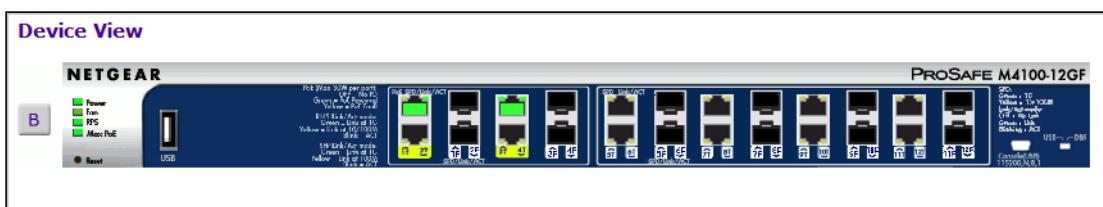
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

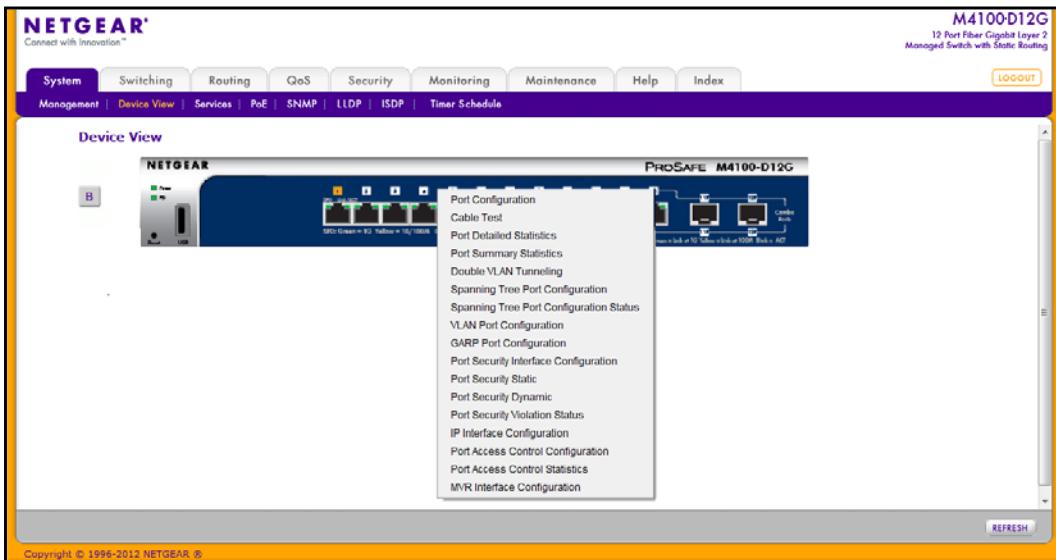
The web management interface menu displays.

7. Select **System > Device View**.



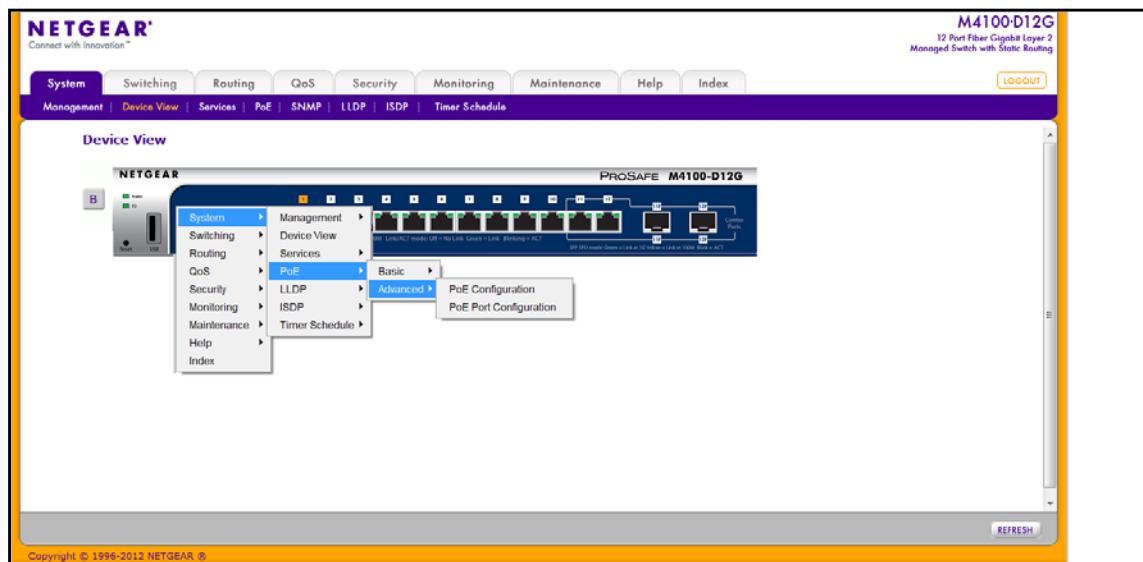
The port coloring indicates whether a port is currently active. Green indicates that the port is enabled; red indicates that an error occurred on the port, or that the link is disabled.

- Click a port to see a menu that displays statistics and configuration options.



You can click a menu option to access the screen that contains the configuration or monitoring options.

If you click the graphic, but do not click a specific port, the main menu displays. This menu contains the same options as the navigation tabs at the top of the screen.



## Using SNMP

The managed switch software supports the configuration of SNMP groups and users that can manage traps that the SNMP agent generates.

The managed switch uses both standard public MIBs for standard functionality and private MIBs that support additional switch functionality. All private MIBs begin with a “-” prefix. The main object for interface configuration is in -SWITCHING-MIB, which is a private MIB. Some interface configurations also involve objects in the public MIB, IF-MIB.

SNMP is enabled by default. The **System > Management > System Information** screen, which is the screen that displays when you log in, displays the information that you need to configure an SNMP manager to access the switch.

Any user can connect to the switch using the SNMP v3 protocol, but for authentication and encryption, the switch supports only one user, which is **admin**; therefore only one profile can be created or modified.

➤ **To configure authentication and encryption settings for the SNMP v3 admin profile:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > SNMP > SNMP v3 > User Configuration**.

The User Configuration screen displays.

8. To enable authentication, select an **Authentication Protocol** option, which is either **MD5** or **SHA**.

9. To enable encryption, select the **DES** option in the **Encryption Protocol** menu. Then, enter an encryption code of eight or more alphanumeric characters in the **Encryption Key** field.

10. Click the **APPLY** button.

Your settings are saved.

To access configuration information for SNMP V1 or SNMP V2, select **System > SNMP > SNMPv1/v2** and select the screen that contains the information to configure.

# Configure System Information

2

This chapter covers the following topics:

- *System Configuration*
- *Configure Initial Management VLAN Settings*
- *Define System Information*
- *View the Switch Status*
- *Manage Loopback Interfaces*
- *View the IPv6 Network Neighbor Table*
- *Configure an IPv4 Management VLAN*
- *View or Set the System Time*
- *Configure DNS*
- *Configure the DHCP Server*
- *Configure the DHCP Pool*
- *Configure UDP Relay Global Settings*
- *Configure the Basic PoE Settings*
- *Configure Advanced PoE Settings*
- *View All MIBs Supported by the Switch*
- *Configure SNMP v3 Settings for a User*
- *LLDP Overview*
- *ISDP Settings Overview*
- *Configure Timers*

## System Configuration

➤ To do the initial system configuration:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

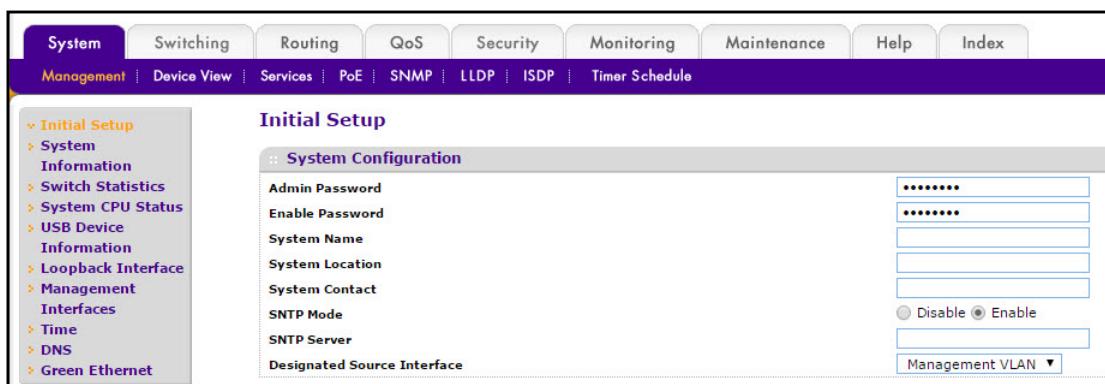
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Management > Initial Setup**.



8. In the **Admin Password** field, enter the new password for the Admin account.

The new password does not display as you type it; only dots are shown to hide the entry. The password is from 8 to 64 alphanumeric characters in length and is case-sensitive.

9. In the **Enable Password** field, enter the new password for the enable mode in the command line interface.

The new password does not display as you type it; only dots are shown to hide the entry. The password is from 8 to 64 alphanumeric characters in length and is case-sensitive.

10. Enter the **System Name**, the name to identify this switch.

You can use a name up to 255 characters in length. The factory default is blank.

11. Enter the **System Location**, the location of the switch.

You can use a location up to 255 characters in length. The factory default is blank.

**12.** Enter the **System Contact**, the name of the contact person for this switch.

You can use a contact name up to 255 characters in length. The factory default is blank.

**13.** In the **SNTP Mode** menu, select **Enable** or **Disable**.

This specifies the state of the SNTP client. The default value is Enable, and the local clock is used to get the time value.

**14.** Specify the address of the **SNTP server**.

Enter a text string of up to 64 characters containing the host name of an SNTP server. The server address can be IPv4, IPv6, or a host name. The host name resolves into an IP address each time an SNTP request is sent to it.

**15.** Select a **Designated Source Interface** from the list.

Possible values are Management VLAN or Service Port. The source interface to be used for SNMP trap, syslog, DNS, TACACS+, RADIUS, sflow and SNTP applications. By default, Management VLAN is used as the source interface.

**Note:** If you configure a management VLAN as the source interface, you must enable routing mode for the selected VLAN.

**16.** Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See *Save Configuration* on page 405.

## Configure Initial Management VLAN Settings

➤ **To configure the initial management VLAN settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7. Select System > Management > Initial Setup**

The Initial Setup screen displays.

**8. Scroll down to display the Management VLAN Configuration section.**

Management VLAN Configuration	
Management VLAN ID	1
Routing Mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IPv4 Address Assignment	<input checked="" type="radio"/> DHCP <input type="radio"/> Static
IP Address	10.130.83.152
Subnet Mask	255.255.255.128
Gateway	0.0.0.0

**9. Specify the Management VLAN ID of the switch.**

The management VLAN is used for management of the switch. The VLAN ID can be any value from 1 to 4093. The default value is VLAN 1.

**10. Select the Routing Mode **Enable** or **Disable** radio button.**

This sets the global IPv4 Routing Mode on the device. The default is Enable.

**11. Select the IPv4 Address Assignment **DHCP** or **Static** radio button.**

This specifies the method for getting IPv4 network parameters (IPv4 address and network mask) for the configured management VLAN interface. The default value for VLAN 1 is Static.

**12. In the **IP Address** field, specify the IP address of the management VLAN interface.**

The factory default value is 169.254.100.100.

**13. In the **Subnet Mask** field, specify the IP subnet mask for the management VLAN interface.**

This is also referred to as the subnet or network mask and defines the portion of the interface's IP address that is used to identify the attached network. The factory default value is 255.255.0.0.

**14. In the **Gateway** field, specify the default gateway for the management VLAN interface.**

The default value is 0.0.0.0.

## Define System Information

➤ **To define system information:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

- Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **System > Management > System Information**.

System Information	
<b>Product Name</b>	M4100-24G-POE+ ProSafe 24-port Gigabit L2+ Managed Switch with PoE+, 10.0.2.2, B1.0.1.1
<b>System Name</b>	<input type="text"/>
<b>System Location</b>	<input type="text"/>
<b>System Contact</b>	<input type="text"/>
<b>Login Timeout</b>	5 (0 to 160) mins
<b>Management Interface</b>	VLAN 1
<b>IPv4 Management VLAN Interface</b>	<a href="#">10.130.84.37/255.255.255.128</a>
<b>Management VLAN ID</b>	1
<b>IPv4 Loopback Interface</b>	
<b>System Date</b>	Jan 1 10:28:38 1970 (UTC+0:00)
<b>System Up Time</b>	0 days 10 hours 28 mins 38 secs
<b>Current SNTP Sync Status</b>	Other
<b>System SNMP OID</b>	1.3.6.1.4.1.4526.100.11.27
<b>System MAC Address</b>	74:44:01:94:DB:F8
<b>Supported Java Plugin Version</b>	1.6
<b>Current SNTP Synchronized Time</b>	SNTP Last Attempt Status Is Not Successful

- Define the following fields:

- System Name.** Enter a name to identify this switch. You can use up to 255 alphanumeric characters. The factory default is blank.
- System Location.** Enter the location of this switch. You can use up to 255 alphanumeric characters. The factory default is blank.
- System Contact.** Enter the contact person for this switch. You can use up to 25 alphanumeric characters. The factory default is blank.
- Login Timeout.** Specify how many minutes of inactivity can occur on a serial port connection before the switch closes the connection. Enter a number between 0 and 160: the factory default is 5. Entering 0 disables the time-out.
- Management Interface**—Select the management interface to be used as source interface for SNMP trap, syslog, DNS, TACACS+, RADIUS, sflow, and SNTP applications. Possible values are as follows:
  - Routing Interface**
  - Routing VLAN**
  - Routing Loopback Interface**

- **Service Port**
- **Different.** Some applications that can be selected in this screen require that the source interface be configured separately. In this case, the Different option is shown.

By default VLAN 1 is used as the source interface.

**9.** Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See [Save Configuration](#) on page 405.

The following table describes the status information the System screen displays.

**Table 3. Status information in the System screen**

Field	Description
Product Name	The product name of this switch.
IPv4 Management VLAN Interface	The IPv4 address and mask assigned to the management VLAN interface.
Management VLAN ID	The management VLAN ID of the switch. Click the displayed Management VLAN ID value to jump to the VLAN screen.
IPv4 Loopback Interface	The IPv4 address and mask assigned to the loopback interface.
System Date	The current date.
System Up time	The time in days, hours, and minutes since the last switch reboot.
Current SNTP Sync Status	Displays the current SNTP sync status.
System SNMP OID	The base object ID for the switch's enterprise MIB.
System Mac Address	Universally assigned network address.
Supported Java plug-in Version	The supported version of Java plug-in.
Current SNTP Synchronized Time	Displays the SNTP synchronized time.

## View the Switch Status

You can view the fan status, temperature status, device status, and switch statistics.

### View the Fan Status

You can view the status of the fans in all units. These fans remove the heat generated by the power, CPU, and other chipsets, and allow the chipsets work normally.

➤ **To view the fan status:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.

2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.

3. Launch a web browser.

4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

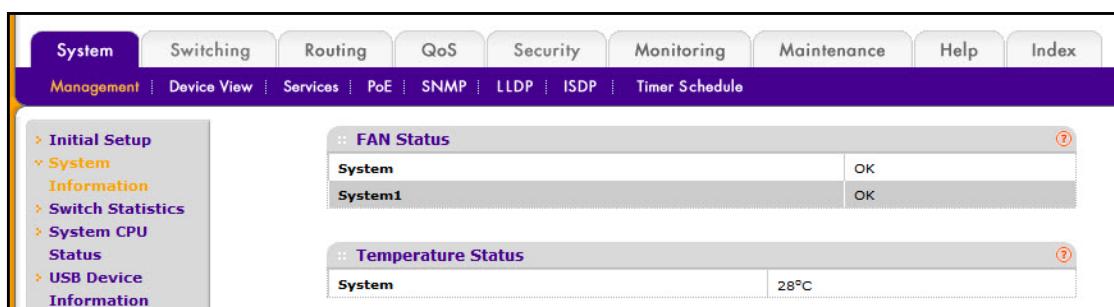
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Management > System Information** and scroll down to the FAN Status.



The following information displays:

- **FAN Status.** OK, Failure, or Not Present.
  - **UNIT ID.** This identifies the switch to which the fan belongs.
  - **System.** The working status of the system fan in each unit.
8. Click the **REFRESH** button to refresh the system information of the switch.

## View the Temperature Status

➤ **To display the temperature status:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.

2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.

3. Launch a web browser.

4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **System > Management > System Information**.  
The System Information screen displays.
8. Scroll down to Temperature Status.  
The screen displays the current temperature of the system sensor of the switch. The maximum temperature of the temperature sensors depends on the actual hardware.
9. To refresh the switch information, click the **REFRESH** button.

## View the Device Status

- **To view the device status:**
1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
  2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
  3. Launch a web browser.
  4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
  5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
  6. Click the **Login** button.  
The web management interface menu displays.
  7. Select **System > Management > System Information**.  
The System Information screen displays.

**8.** Scroll down to Device Status.

Device Status	
Firmware Version	10.0.2.2
Boot Version	B1.0.1.1
CPLD Version	0x0
Serial Number	2TK1215AF000D
AC	OK
Remote	Not Present
PoE Version	1.7.0.3
MAX PoE	OFF

**9.** To refresh the switch information, click the **REFRESH** button.

The following table describes the Device Status information.

**Table 4. Device status**

Field	Description
Firmware Version	The release.version.maintenance number of the code currently running on the switch. For example, if the release was 1, the version was 2, and the maintenance number was 4, the format would be 1.2.4.
Boot Version	The version of the boot code that is in the flash memory to load the firmware into the memory.
CPLD Version	The version of the software for CPLD.
Serial Number	The serial number of this switch.
AC, Remote	Indicates the status of the appropriate power module in each unit. Status can be any of the following: <ul style="list-style-type: none"> <li>• <b>OK.</b> Power module is present and functioning properly.</li> <li>• <b>Not Present.</b> Power module is not present in the slot.</li> <li>• <b>No power.</b> Power module is present but not connected to the power source.</li> <li>• <b>Not powering.</b> Power module is present and connected but the switch uses another power source.</li> <li>• <b>Incompatible.</b> Power module is present but incompatible.</li> <li>• <b>Failed.</b> Power module is present, but power cable is not plugged in or a bad cable is plugged in.</li> </ul>
PoE Version	Version of the PoE controller FW image.
MAX PoE	Indicates the status of maximum PoE power available on the switch as follows: <ul style="list-style-type: none"> <li>• <b>ON.</b> Indicates less than 7W of PoE power available for another device.</li> <li>• <b>OFF.</b> Indicates at least 7W of PoE power available for another device.</li> <li>• <b>N/A.</b> Indicates that PoE is not supported by the unit.</li> </ul>

## View Switch Statistics

➤ To view the switch statistics:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Management > Switch Statistics**.

Switch Statistics	
:: Statistics	
ifIndex	53
Octets Received	3929228
Packets Received Without Errors	33757
Unicast Packets Received	5532
Multicast Packets Received	23710
Broadcast Packets Received	4515
Receive Packets Discarded	0
Octets Transmitted	14036105
Packets Transmitted Without Errors	126647
Unicast Packets Transmitted	5658
Multicast Packets Transmitted	120979
Broadcast Packets Transmitted	10
Transmit Packets Discarded	0
Most Address Entries Ever Used	14
Address Entries in Use	9
Maximum VLAN Entries	1024
Most VLAN Entries Ever Used	2
Static VLAN Entries	2
Dynamic VLAN Entries	0
VLAN Deletes	0
Time Since Counters Last Cleared	1 day 5 hr 41 min 4 sec

8. Click the **CLEAR** button to clear all the counters, resetting all switch summary and detailed statistics to default values. The discarded packets count cannot be cleared.

The following table describes Switch Statistics information.

**Table 5. Switch Statistics**

Field	Description
ifIndex	The ifIndex of the interface table entry associated with the processor of this switch.
Octets Received	The total number of octets of data received by the processor excluding framing bits but including FCS octets.
Packets Received Without Errors	The total number of packets including broadcast packets and multicast packets received by the processor.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets that were discarded even though no errors were detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted Without Errors	The total number of packets transmitted out of the interface.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested that is transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested that are transmitted to a Multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested that are transmitted to the broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets that were discarded even though no errors were detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that were learned by this switch since the most recent reboot.
Address Entries in Use	The number of learned and static entries in the Forwarding Database Address Table for this switch.
Maximum VLAN Entries	The maximum number of virtual LANs (VLANs) allowed on this switch.

**Table 5. Switch Statistics (continued)**

Field	Description
Most VLAN Entries Ever Used	The largest number of VLANs that were active on this switch since the last reboot.
Static VLAN Entries	The number of presently active VLAN entries on this switch that were created statically.
Dynamic VLAN Entries	The number of presently active VLAN entries on this switch that were created by GVRP registration.
VLAN Deletes	The number of VLANs on this switch that were created and then deleted since the last reboot.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

## View the System CPU Status

➤ **To display the CPU status:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7. Select System > Management > System CPU Status.**

The screenshot displays the 'System CPU Status' interface. It includes two main sections: 'CPU Memory Status' and 'CPU Utilization'. The 'CPU Memory Status' section shows 'Total System Memory' as 126416 KBytes and 'Available Memory' as 26780 KBytes. The 'CPU Utilization' section contains a 'Memory Utilization Report' table and a 'CPU Utilization' table. The 'Memory Utilization Report' table shows:

status	bytes
free	27422720
alloc	102027264

The 'CPU Utilization' table shows CPU usage over 5, 60, and 300 seconds for three tasks:

PID	Name	5 Secs	60 Secs	300 Secs
165	hardwareMonitorTask	0.38%	0.30%	0.29%
169	osapiTimer	0.00%	0.10%	0.10%
171	_interrupt_thread	0.00%	0.00%	0.01%

The following information displays:

- **Total System Memory.** The total memory of the switch in KBytes.
- **Available Memory.** The available memory space for the switch in KBytes.
- **CPU Utilization Information.** Memory information, task-related information, and percentage of CPU utilization per task.

## View USB Device Information

You can view USB device details such as manufacturer, vendor, product ID, and status of the USB flash device.

➤ **To display the USB device information:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

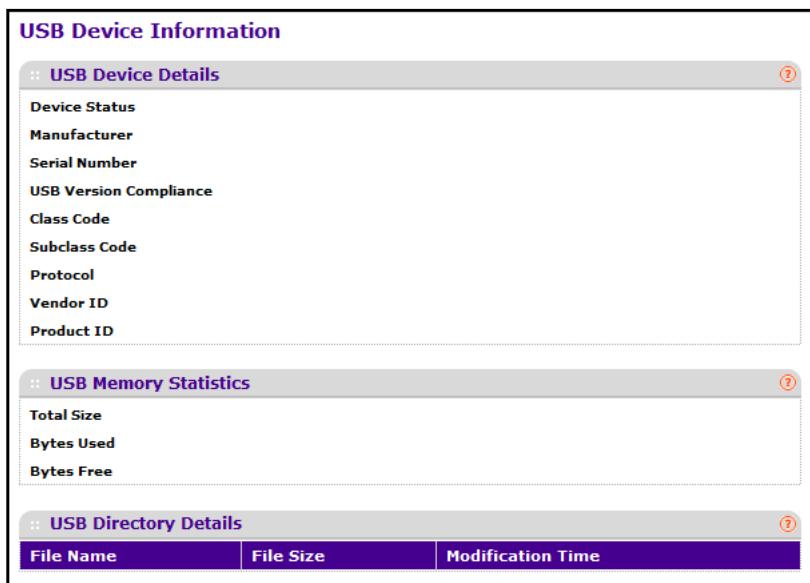
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Management > USB Device Information**.



8. Click the **REFRESH** button to refresh the screen with the latest information.

The following table describes USB Device Details information.

**Table 6. USB device Information**

Field	Description
Device Status	The current status of device. Active if the device is USB plugged in and recognized by the switch. Inactive if the device is not mounted. Invalid if the device is not present or invalid device is plugged in.
Manufacturer	The USB flash drive device manufacturer.
Serial Number	The USB flash drive device serial number.
USB Version Compliance	The USB flash drive device version.
Class Code	The USB flash drive device class.
USB Device Details	
Subclass Code	The USB flash drive device subclass.
Protocol	The USB flash drive device protocol.
Vendor ID	The USB flash drive device vendor ID.

**Table 6. USB device Information (continued)**

Field	Description
Product ID	The USB flash drive device product ID.
USB Memory Statistics	
Total Size	The USB flash device storage size.
Bytes Used	The size of memory used on the USB flash device.
Bytes Free	The size of memory free on the USB flash device.
USB Directory Details	
File Name	The files stored in the USB flash drive.
File Size	The size of the files stored in the USB flash drive.
Modification Time	The last modification time of the file stored in the USB flash drive.

## Manage Loopback Interfaces

You can create, configure, and remove loopback interfaces.

### ➤ To configure a loopback interface

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Management > Loopback Interface**.

Loopback Interface Configuration				
:: IPv4 Loopback Interface Configuration				
	Loopback ID	Primary IP Address	Primary IP Subnet Mask	Loopback Interface Status
<input type="checkbox"/>	<input type="button" value="▼"/>	<input type="text"/>	<input type="text"/>	

8. Use the **Loopback ID** field to select list of currently configured loopback interfaces.
9. Use the **Primary IP Address** field to input the primary IPv4 address for this interface in dotted decimal notation.

This option is visible only when IPv4 loopback is selected.

10. Use the **Primary IP Subnet Mask** field to input the primary IPv4 subnet mask for this interface in dotted decimal notation.

This option is visible only when **IPv4 Loopback** is selected.

The loopback Interface Status indicates whether the link is up or down.

11. To create secondary loopback interfaces, use the **Secondary IP Address** field to input the secondary IP address for this interface in dotted decimal notation.

This input field is visible only when **Add Secondary** is selected. This option is visible when **IPv4 Loopback** is selected.

12. Use the **Secondary Subnet Mask** field to input the secondary subnet mask for this interface in dotted decimal notation.

This input field is visible only when **Add Secondary** is selected. This option is visible when **IPv4 Loopback** is selected.

## View the IPv6 Network Neighbor Table

### ➤ To display the IPv6 Network Neighbor Table:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Management > Management Interfaces > IPv6 Network Neighbor Table**.

IPv6 Network Interface Neighbor Table				
IPv6 Network Interface Neighbor Table				
IPv6 Address	MAC Address	isRtr	Neighbor State	Last Updated

The following table displays IPv6 Network Interface Neighbor Table information.

**Table 7. IPv6 Network Interface Neighbor Table**

Field	Description
IPv6 address	The Ipv6 address of a neighbor switch visible to the network interface.
MAC address	The MAC address of a neighbor switch.
IsRtr	True (1) if the neighbor machine is a router, false (2) otherwise.
Neighbor State	The state of the neighboring switch: <ul style="list-style-type: none"><li>• reachable (1). The neighbor is reachable by this switch.</li><li>• stale (2). Information about the neighbor is scheduled for deletion.</li><li>• delay (3). No information was been received from neighbor during delay period.</li><li>• probe (4). Switch is attempting to probe for this neighbor.</li><li>• unknown (6). Unknown status.</li></ul>
Last Updated	The last sysUpTime that this neighbor was updated.

## Configure an IPv4 Management VLAN

For you to manage the device by using the web-based configuration utility, the device management IP address must be defined and known. A management VLAN interface is created by default and it is assigned an IP address if a DHCP server is present. If it fails to get an IP address, a fallback address 169.254.100.100/255.255.0.0 is assigned to it. Management VLAN is used as the default source interface for the syslog, message log, and SNMP client, and so on. The network interface is disabled by default.

The management VLAN is the logical interface used for in-band connectivity with the switch through any of the switch's front panel ports. The configuration parameters associated with the switch's management VLAN do not affect the configuration of the front panel ports through which traffic is switched or routed.

To access the switch over a network, you must first configure it with IP information (IP address, subnet mask). You can configure the IP information using any of the following:

- DHCP
- Terminal interface through the EIA-232 port.

Once you establish in-band connectivity, you can change the IP information using any of the following:

- Terminal interface through the EIA-232 port
- Terminal interface through Telnet
- SNMP-based management
- Web-based management

➤ **To configure the IPv4 management VLAN:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

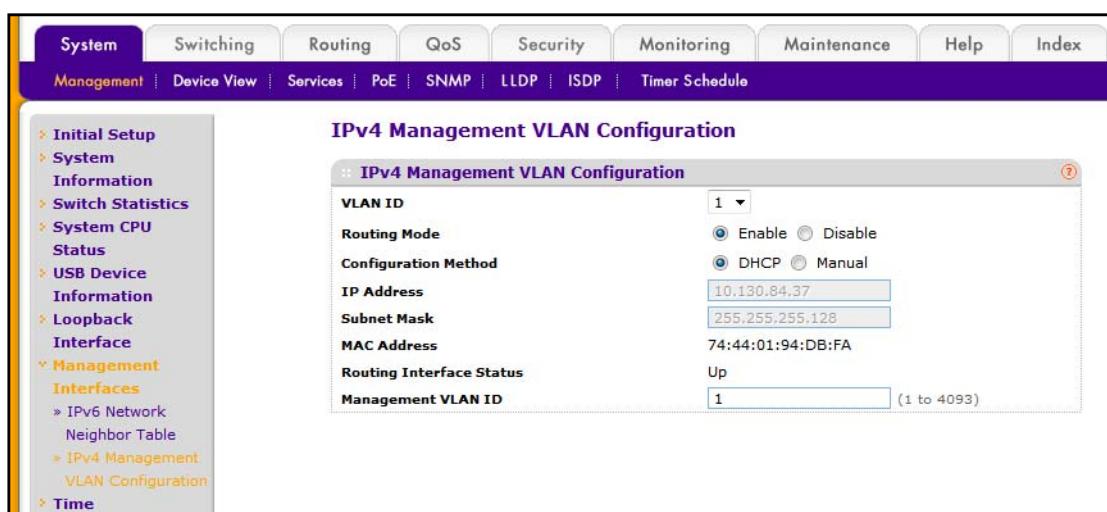
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Management > Management Interfaces > IPv4 Management VLAN Configuration**.



The screen displays the MAC address assigned to the VLAN routing interface and the routing interface status (up or down). These fields display information but cannot be changed.

**8.** From the **VLAN ID** list, select a VLAN.

This list displays all IDs of VLANs configured on this switch.

**9.** In the **Routing Mode** field, select the option to **Enable** or **Disable** the global routing on the selected VLAN interface.

**10.** Select the **Configuration Method**, what the switch does on start-up:

- **DHCP**—Transmit a DHCP request.
- **Manual**—Do nothing.

**11.** Specify the **IP Address** of the interface.

The factory default value is 169.254.100.100.

**12.** Specify the **IP Subnet Mask** for the interface.

The factory default value is 255.255.0.0.

**13.** Specify the **Management VLAN ID** of the switch.

The management VLAN is used for management of the switch. You can enter any value in the range of 1–4093.

**14.** Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See *Save Configuration* on page 405.

## View or Set the System Time

The managed switch software supports the Simple Network Time Protocol (SNTP). You can also set the system time manually.

SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. The managed switch software operates only as an SNTP client and cannot provide time services to other systems.

Time sources are established by strata. Strata define the accuracy of the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock. The device receives time from stratum 1 and above since it is itself a stratum 2 device.

The following is an example of strata:

- **Stratum 0.** A real-time clock is used as the time source, for example, a GPS system.
- **Stratum 1.** A server that is directly linked to a stratum 0 time source is used. Stratum 1 time servers provide primary network time standards.

- **Stratum 2.** The time source is distanced from the stratum 1 server over a network path. For example, a stratum 2 server receives the time over a network link, through NTP, from a stratum 1 server.

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

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

- **T1.** Time that the original request was sent by the client.
- **T2.** Time that the original request was received by the server.
- **T3.** Time that the server sent a reply.
- **T4.** Time that the client received the server's reply.

The device can poll unicast server types for the server time.

Polling for unicast information is used for polling a server for which the IP address is known. SNTP servers that were configured on the device are the only ones that are polled for synchronization information. T1 through T4 are used to determine server time. This is the preferred method for synchronizing device time because it is the most secure method. If this method is selected, SNTP information is accepted only from SNTP servers defined on the device using the SNTP Server Configuration screen.

The device retrieves synchronization information, either by actively requesting information or at every poll interval.

## Configure SNTP Global Settings

You can view and adjust date and time settings. SNTP stands for Simple Network Time Protocol. As its name suggests, it is a less complicated version of Network Time Protocol, that is a system for synchronizing the clocks of networked computer systems, primarily when data transfer is handled through the Internet.

➤ **To configure SNTP global settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

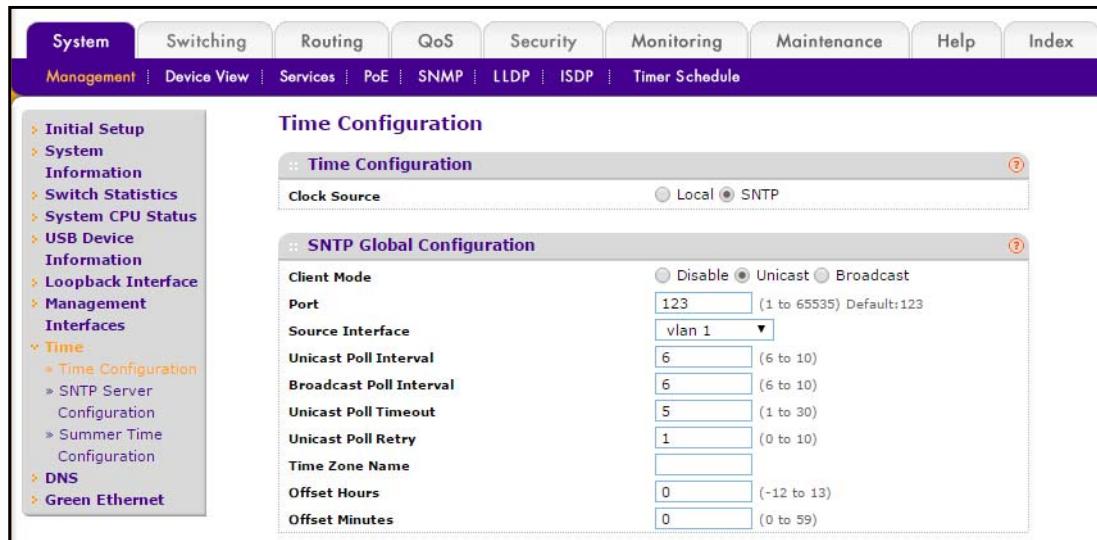
- Click the **Login** button.

The web management interface menu displays.

- Select **System > Management > System Information**.

The System Information screen displays.

- Select **System > Management > Time > Time Configuration**, and select **SNTP** as the **Clock Source**.



- Use **Client Mode** to specify the mode of operation of SNTP Client.

An SNTP client can operate in one of the following modes:

- Disable.** SNTP is not operational. No SNTP requests are sent from the client nor are any received SNTP messages processed.
- Unicast.** SNTP operates in a point-to-point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally, the round-trip delay and local clock offset relative to the server.
- Broadcast.** SNTP operates in the same manner as multicast mode but uses a local broadcast address instead of a multicast address. The broadcast address was a single subnet scope while a multicast address has Internet wide scope.

The default value is Disable.

- Use **Port** to specify the local UDP port to listen for responses or broadcasts.

The allowed range is 1 to 65535. The default value is 123.

- Specify the **Source Interface** to be used for SNTP Client.

Possible values are as follows:

- Routing interface
- Routing VLAN

- Routing loopback interface

By default, VLAN 1 is used as the source interface.

- 12.** Use **Unicast Poll Interval** to specify the number of seconds between unicast poll requests expressed as a power of two when configured in unicast mode.

The allowed range is 6 to 10. The default value is 6.

- 13.** Use **Broadcast Poll Interval** to specify the number of seconds between broadcast poll requests expressed as a power of two when configured in broadcast mode.

Broadcasts received prior to the expiry of this interval are discarded. The allowed range is 6 to 10. The default value is 6.

- 14.** Use **Unicast Poll Timeout** to specify the number of seconds to wait for an SNTP response when configured in unicast mode.

The allowed range is 1 to 30. The default value is 5.

- 15.** Use **Unicast Poll Retry** to specify the number of times to retry a request to an SNTP server after the first time-out before attempting to use the next configured server when configured in unicast mode.

The allowed range is 0 to 10. The default value is 1.

When using SNTP/NTP time servers to update the switch's clock, the time data received from the server is based on Coordinated Universal Time (UTC), that is the same as Greenwich Mean Time (GMT). This cannot be the time zone in which the switch is located.

- 16.** Use **Time Zone Name** to specify the time zone name.

The time zone can affect the display of the current system time. The default value is UTC.

- 17.** Use **Offset Hours** to specify the number of hours difference from UTC. You can configure a time zone specifying the number of offset hours and optionally the number of offset minutes that the switch's time zone is different from UTC.

The allowed range is -24 to 24. The default value is 0.

- 18.** Use **Offset Minutes** to specify the number of minutes that the switch's time zone is different from UTC.

The allowed range is 0 to 59. The default value is 0.

## View the SNTP Global Status

- **To view the SNTP global status:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.

4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **System > Management > Time > Time Configuration**  
The Time Configuration screen displays.
8. Scroll down to view the SNTP Global Status.

SNTP Global Status	
Version	4
Supported Mode	Unicast and Broadcast
Last Update Time	Jan 1 00:00:00 1970 (UTC+0:00)
Last Attempt Time	Jan 1 00:00:00 1970 (UTC+0:00)
Last Attempt Status	Other
Server IP Address	
Address Type	Unknown
Server Stratum	0
Reference Clock Id	
Server Mode	Reserved
Unicast Server Max Entries	3
Unicast Server Current Entries	0
Broadcast Count	0

The following table describes the SNTP Global Status fields.

**Table 8. SNTP Global Status**

Field	Description
Version	Specifies the SNTP version the client supports.
Supported Mode	Specifies the SNTP modes the client supports. Multiple modes can be supported by a client.
Last Update Time	Specifies the local date and time (UTC) the SNTP client last updated the system clock.
Last Attempt Time	Specifies the local date and time (UTC) of the last SNTP request or receipt of an unsolicited message.

**Table 8. SNTP Global Status (continued)**

Field	Description
Last Attempt Status	<p>Specifies the status of the last SNTP request or unsolicited message for both unicast and broadcast modes. If no message was received from a server, a status of Other is displayed. These values are appropriate for all operational modes.</p> <ul style="list-style-type: none"> <li>• Other. None of the following enumeration values.</li> <li>• Success. The SNTP operation was successful and the system time was updated.</li> <li>• Request Timed Out. A directed SNTP request timed out without receiving a response from the SNTP server.</li> <li>• Bad Date Encoded. The time provided by the SNTP server is not valid.</li> <li>• Version Not Supported. The SNTP version supported by the server is not compatible with the version supported by the client.</li> <li>• Server Unsynchronized. The SNTP server is not synchronized with its peers. This is indicated through the leap indicator field on the SNTP message.</li> <li>• Server Kiss Of Death. The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.</li> </ul>
Server IP Address	Specifies the IP address of the server for the last received valid packet. If no message was received from any server, an empty string is shown.
Address Type	Specifies the address type of the SNTP server address for the last received valid packet.
Server Stratum	Specifies the claimed stratum of the server for the last received valid packet.
Reference Clock Id	Specifies the reference clock identifier of the server for the last received valid packet.
Server Mode	Specifies the mode of the server for the last received valid packet.
Unicast Server Max Entries	Specifies the maximum number of unicast server entries that can be configured on this client.
Unicast Server Current Entries	Specifies the number of current valid unicast server entries configured for this client.
Broadcast Count	Specifies the number of unsolicited broadcast SNTP messages that were received and processed by the SNTP client since last reboot.

## Configure SNTP Servers

You can view and modify information for adding and modifying Simple Network Time Protocol (SNTP) servers.

➤ **To configure SNTP servers:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Management > Time > SNTP Server Configuration**.

The screenshot shows two stacked tables. The top table is titled "SNTP Server Configuration" and has columns for Server Type, Address, Port, Priority, and Version. The bottom table is titled "SNTP Server Status" and has columns for Address, Last Update Time, Last Attempt Time, Last Attempt Status, Requests, and Failed Requests.

SNTP Server Configuration				
Server Type	Address	Port	Priority	Version
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

SNTP Server Status					
Address	Last Update Time	Last Attempt Time	Last Attempt Status	Requests	Failed Requests
<input type="text"/>					

8. Enter the appropriate SNTP server information in the available fields:
  - **Server Type.** Specifies whether the address for the SNTP server is an IP address (IPv4) or host name (DNS). The default value is IPv4.
  - **Address.** Specify the address of the SNTP server. This is a text string of up to 64 characters containing the encoded unicast IP address or host name of an SNTP server. Unicast SNTP requests are sent to this address. If this address is a DNS host name, then that host name should be resolved into an IP address each time a SNTP request is sent to it.
  - **Port.** Enter a port number on the SNTP server to which SNTP requests are sent. The valid range is 1–65535. The default is 123.
  - **Priority.** Specify the priority of this server entry in determining the sequence of servers to which SNTP requests are sent. The client continues sending requests to different servers until a successful response is received or all servers are exhausted.

This indicates the order in which to query the servers. A server entry with a precedence of 1 is queried before a server with a priority of 2, and so forth. If more than one server is assigned the same priority, then the requesting order follows the lexicographical ordering of the entries in this table. The allowed range is 1 to 3. The default value is 1.

- **Version.** Enter the NTP version running on the server. The range is 1–4. The default is 4.

**9.** Click the **ADD** button.

**10.** Repeat the previous steps to add additional SNTP servers.

You can configure up to three SNTP servers.

**11.** To remove an SNTP server, select the check box next to the configured server to remove, and then click the **DELETE** button.

The entry is removed, and the device is updated.

**12.** To change the settings for an existing SNTP server, select the check box next to the configured server and enter new values in the available fields, and then click the **APPLY** button.

Configuration changes take effect immediately.

**13.** Click the **REFRESH** button to refresh the screen with the most current data from the switch.

The SNTP Server Status table at the bottom of the screen displays status information about the SNTP servers configured on your switch.

The following table displays SNTP Server Status information.

**Table 9. SNTP server status**

Field	Description
Address	All the existing server addresses. If no server configuration exists, a message saying “No SNTP server exists” flashes on the screen.
Last Update Time	The local date and time (UTC) that the response from this server was used to update the system clock.
Last Attempt Time	The local date and time (UTC) that this SNTP server was last queried.

**Table 9. SNTP server status (continued)**

Field	Description
Last Attempt Status	The status of the last SNTP request to this server. If no packet was received from this server, a status of Other is displayed. <ul style="list-style-type: none"> <li>• <b>Other.</b> None of the following enumeration values.</li> <li>• <b>Success.</b> The SNTP operation was successful and the system time was updated.</li> <li>• <b>Request Timed Out.</b> A directed SNTP request timed out without receiving a response from the SNTP server.</li> <li>• <b>Bad Date Encoded.</b> The time provided by the SNTP server is not valid.</li> <li>• <b>Version Not Supported.</b> The SNTP version supported by the server is not compatible with the version supported by the client.</li> <li>• <b>Server Unsynchronized.</b> The SNTP server is not synchronized with its peers. This is indicated through the leap indicator field on the SNTP message.</li> <li>• <b>Server Kiss Of Death.</b> The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.</li> </ul>
Requests	The number of SNTP requests made to this server since last agent reboot.
Failed Requests	The number of failed SNTP requests made to this server since last reboot.

## Configure Summer Time Settings

➤ **To configure the summer time settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Management > Time > Summer Time Configuration**.

Time Configuration	
:: Summer Time Configuration	
Summer Time	<input checked="" type="radio"/> Disable <input type="radio"/> Recurring <input type="radio"/> Recurring EU <input type="radio"/> Recurring USA <input type="radio"/> Non Recurring
:: Summer Time Status	
Summer Time	Disable
Summer Time In Effect	No

8. Select a Summer Time radio button:

- **Disable.** This option is used to disable Summer Time.
- **Recurring.** This option is used to enable Recurring Summer Time.
- **Recurring EU.** This option is used to enable Recurring EU Summer Time.
- **Recurring USA.** This option is used to enable Recurring USA Summer Time.
- **Non Recurring.** This option is used to configure Non Recurring Summer Time.

The fields described in the following table are visible only when Summer Time is Recurring or Recurring EU or Recurring USA.

**Table 10. Summer Time Recurring configuration**

Field	Description
Begins At	The fields under this are used to configure the Start values for the date and time. <ul style="list-style-type: none"> <li>• Week. This field is used to configure the start week.</li> <li>• Day. This field is used to configure start day.</li> <li>• Month. This field is used to configure start month.</li> <li>• Hours. This field is used to configure start hours.</li> <li>• Minutes. This field is used to configure start minutes.</li> </ul>
Ends At	The fields under this are used to configure the End values for the date and time. <ul style="list-style-type: none"> <li>• Week. This field is used to configure the end week.</li> <li>• Day. This field is used to configure end day.</li> <li>• Month. This field is used to configure end month.</li> <li>• Hours. This field is used to configure end hours.</li> <li>• Minutes. This field is used to configure end minutes.</li> </ul>
Offset	This field is used to configure the recurring offset.
Zone	This field is used to configure the Zone.

The fields in the following table are visible only when Summer Time is Non Recurring.

**Table 11. Summer Time Nonrecurring Configuration**

Field	Description
Begins At	The fields under this are used to configure the Start values for the date and time. <ul style="list-style-type: none"> <li>• Week. This field is used to configure the start week.</li> <li>• Day. This field is used to configure the start day.</li> <li>• Month. This field is used to configure the start month.</li> <li>• Hours. This field is used to configure the start hours.</li> <li>• Minutes. This field is used to configure the start minutes.</li> </ul>
Ends At	The fields under this are used to configure the End values for the date and time. <ul style="list-style-type: none"> <li>• Week. This field is used to configure the end week.</li> <li>• Day. This field is used to configure the end day.</li> <li>• Month. This field is used to configure the end month.</li> <li>• Hours. This field is used to configure the end hours.</li> <li>• Minutes. This field is used to configure the end minutes.</li> </ul>
Offset	This field is used to configure the recurring offset.
Zone	This field is used to configure the Zone.

9. Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See *Save Configuration* on page 405.

## Configure DNS

You can configure the information about DNS servers that the network uses and how the switch operates as a DNS client.

➤ **To configure DNS:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

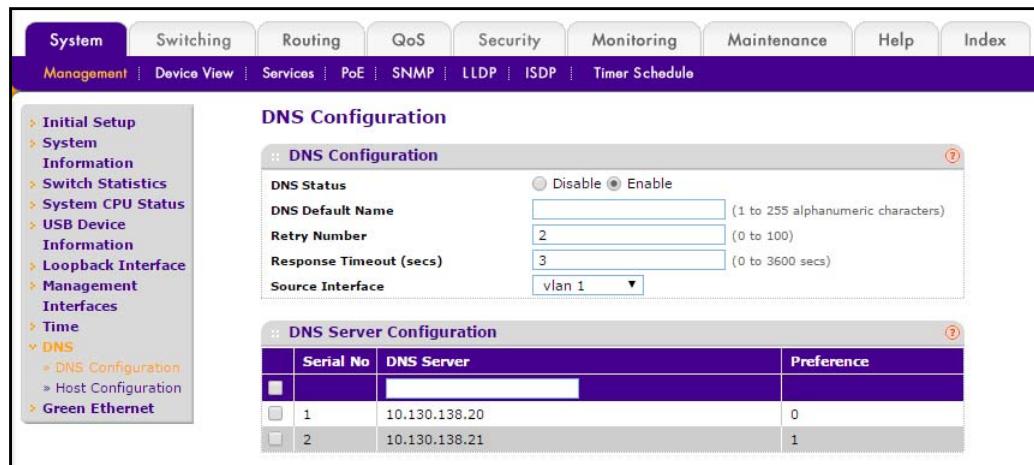
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **System > Management > DNS > DNS Configuration**.



- Specify whether to enable or disable the administrative status of the DNS client.
  - Enable.** Allow the switch to send DNS queries to a DNS server to resolve a DNS domain name. The default value is Enable.
  - Disable.** Prevent the switch from sending DNS queries.
- Enter the DNS default domain name to include in DNS queries.

When the system is performing a lookup on an unqualified host name, this field is provided as the domain name (for example, if the default domain name is netgear.com and you enter test, then test is changed to test.netgear.com to resolve the name). The length of the name must not be longer than 255 characters.

- Use **Retry Number** to specify the number of times to retry sending DNS queries to the DNS server.

This number ranges from 0 to 100. The default value is 2.

- Use **Response Timeout (secs)** to specify the amount of time, in seconds, to wait for a response to a DNS query.

This time-out ranges from 0 to 3600. The default value is 3.

- Specify the **Source Interface** that is used for DNS.

Possible values are as follows:

- Routing interface
- Routing VLAN
- Routing loopback interface

By default, VLAN 1 is used as source interface.

13. To specify the DNS server to which the switch sends DNS queries, enter an IP address in standard IPv4 dot notation in the **DNS Server Address** and click the **ADD** button.

The server appears in the list. You can specify up to eight DNS servers. The precedence is set in the order created.

14. To remove a DNS server from the list, select the check box next to the server and click the **DELETE** button.

If no DNS server is specified, the check box is global and deletes all the DNS servers listed.

15. Click the **APPLY** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

16. To add the specified DNS server to the List of DNS Servers, click the **ADD** button.

Configuration changes take effect immediately.

17. To delete the specified DNS server from the list of DNS servers, click the **DELETE** button.

If no DNS server is specified, then all the DNS Servers are deleted.

## Configure Host Settings

You can manually map host names to IP addresses or view dynamic DNS mappings.

➤ **To configure host settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Management > DNS > Host Configuration.**

The screenshot shows the 'DNS Host Configuration' interface. It consists of two main sections: 'DNS Host Configuration' and 'Dynamic Host Mapping'.  
**DNS Host Configuration:** This section contains a table with columns for 'Host Name (1 to 255 characters)' and 'IP Address'. There is a checkbox next to each row.  
**Dynamic Host Mapping:** This section contains a table with columns for 'Host', 'Total', 'Elapsed', 'Type', and 'Addresses'. There is a checkbox next to each row.

8. Specify the static host name to add.

Its length cannot exceed 255 characters and it is a mandatory field for the user.

9. Specify the IP address in standard IPv4 dot notation to associate with the host name.

10. Click the **ADD** button.

The entry appears in the list.

11. To remove an entry from the static DNS table, select the check box next to the entry and click the **DELETE** button.

12. To change the host name or IP address in an entry, select the check box next to the entry and enter the new information in the appropriate field, and then click the **APPLY** button.

The Dynamic Host Mapping table shows host name-to-IP address entries that the switch learned. The following table describes the dynamic host fields.

**Table 12. DNS Dynamic Host Mapping**

Field	Description
Host	Lists the host name you assign to the specified IP address.
Total	Amount of time since the dynamic entry was first added to the table.
Elapsed	Amount of time since the dynamic entry was last updated.
Type	The type of the dynamic entry.
Addresses	Lists the IP address associated with the host name.

## Configure Green Ethernet Settings

➤ **To configure green Ethernet settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

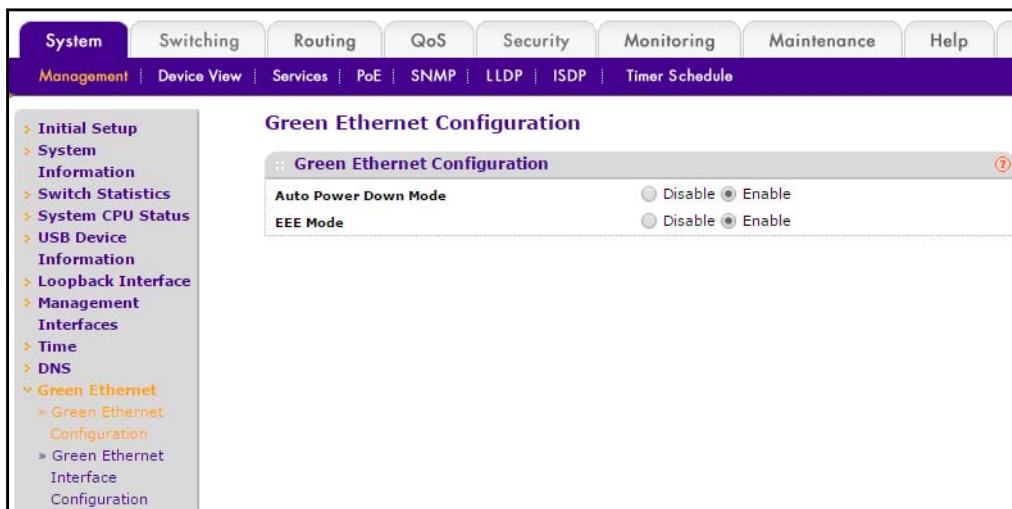
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Management > Green Ethernet > Green Ethernet Configuration**.



8. Select an Auto Power Down Mode **Disable** or **Enable** radio button.

The factory default is Enable. When the port link is down, the PHY automatically goes down for short period of time, and then wakes up to check link pulses. This allows the system to perform autonegotiation and save power consumption when no link partner is present.

9. Select the EE Mode **Disable** or **Enable** radio button.

The default is Enable.

10. Click the **APPLY** button.

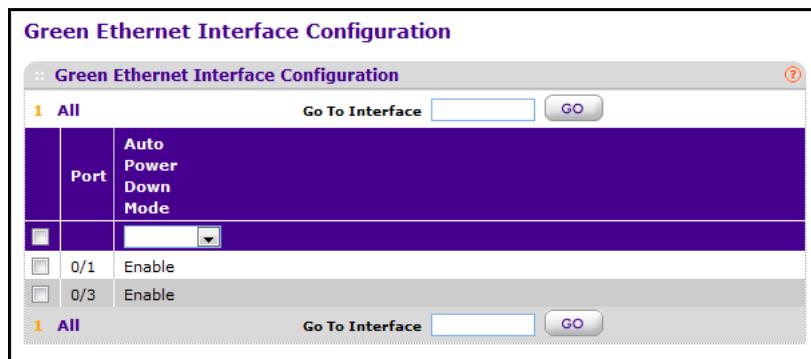
The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See *Save Configuration* on page 405.

## Configure Green Ethernet Interface Settings

➤ **To configure green Ethernet interface settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.

3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
- The Login screen displays.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **System > Management > Green Ethernet > Green Ethernet Interface Configuration**.



8. Specify the **Go To Interface** by entering the Interface in unit/slot/port format and click the **Go** button.  
The entry corresponding to the specified Interface is selected.
9. Select the **Port**.
10. Use the **Auto Power Down Mode** selection to enable or disable this option.

The factory default is enable. When the port link is down the PHY automatically goes down for short period of time, and then wakes up to check link pulses. This allows performing autonegotiation and saving power consumption when no link partner is present.

11. Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See *Save Configuration* on page 405.

## Configure Port Green Mode Statistics

You can configure the Port Green Mode Statistics settings.

➤ **To configure port green mode statistics:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

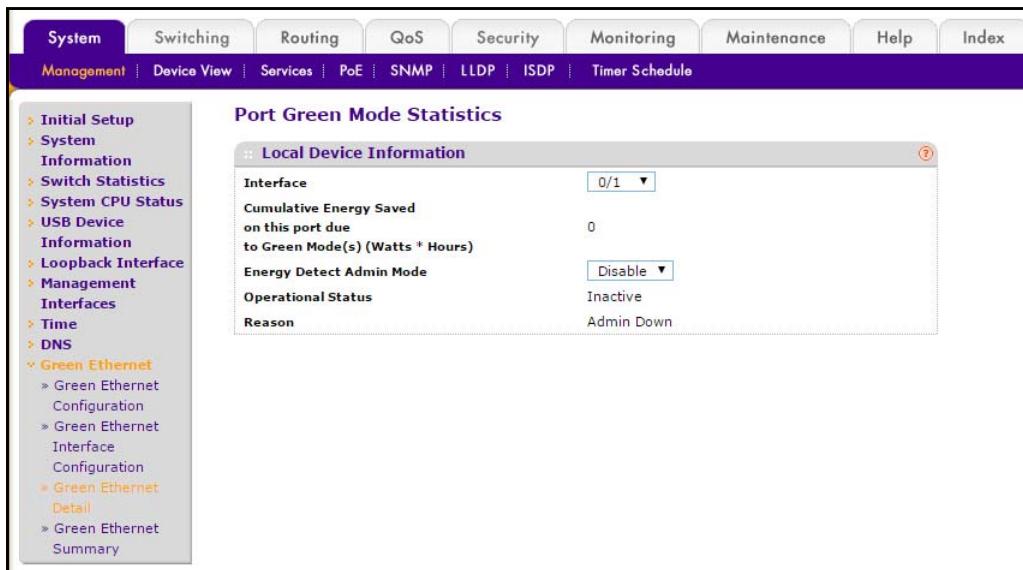
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Management > Green Ethernet > Green Ethernet Detail**.



8. Select the **Interface** for the data is to be displayed or configured.
9. Use the **Energy Detect Admin Mode** selection to enable or disable this option on the port.

With energy detect mode enabled, when the port link is down, the PHY automatically goes down for short period of time, and then wakes up to check link pulses. This allows

performing autonegotiation and saving power consumption when no link partner is present. The default value is Disabled.

**10.** Use the **Short Reach Admin Mode** selection to enable or disable this option on the port.

With short reach mode enabled, PHY is forced to operate in low power mode irrespective of the cable length. The default value is Disabled.

**11.** Use the **EEE Admin Mode** selection to enable or disable this option on the port.

With EEE mode enabled, the port transitions to low power mode during link idle conditions. The default value is Disabled.

**12.** Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See [Save Configuration](#) on page 405.

You can click the **CLEAR** button to clear the configuration and reset the statistics to their default values. You can click the **REFRESH** button to update the screen.

The following table describes the Port Green Mode Statistics nonconfigurable fields.

**Table 13. Port Green Mode Statistics**

Field	Description
Cumulative Energy Saved on this port due to Green Mode(s) (Watts * Hours)	The cumulative energy saved due to all Green Modes enabled on this port in Watts * Hours.
Operational Status	Indicates whether Energy Detect Admin Mode is currently operational (Enabled).
Reason	The reason for the current operational status of Energy Detect Admin Mode.
Operational Status	Indicates whether Short Reach Admin Mode is currently enabled.
Reason	The reason for the current operational status of Short Reach Admin Mode.
Rx Low Power Idle Event Count	This field displays the total number of Rx LPI events since EEE counters were last cleared. The value increments each time the MAC RX enters LP IDLE state.
Rx Low Power Idle Duration (uSec)	The duration of the Rx LPI state in 10us increments. Shows the total duration of Rx LPI since the EEE counters were last cleared.
Tx Low Power Idle Event Count	Shows the total number of Tx LPI events since EEE counters were last cleared. The value increments each time MAC TX enters LP IDLE state.
Tx Low Power Idle Duration (uSec)	This field indicates duration of Tx LPI state in 10us increments. Shows the total duration of Tx LPI since the EEE counters were last cleared.
Tw_sys_tx (uSec)	Integer that indicates the value of Tw_sys that the local system can support.

**Table 13. Port Green Mode Statistics (continued)**

Field	Description
Tw_sys_tx Echo (uSec)	Integer that indicates the remote system's Transmit Tw_sys that was used by the local system to compute the Tw_sys that it wants to request from the remote system.
Tw_sys_rx (uSec)	Integer that indicates the value of Tw_sys that the local system requests from the remote system.
Tw_sys_rx Echo (uSec)	Integer that indicates the remote systems Receive Tw_sys that was used by the local system to compute the Tw_sys that it can support.
Fallback Tw_sys (uSec)	Integer that indicates the value of fallback Tw_sys that the local system requests from the remote system.
Tx_dll_enabled	Data Link Layer Enabled: Initialization status of the EEE transmit Data Link Layer management function on the local system.
Tx_dll_ready	Data Link Layer ready: This variable indicates that the Tx system initialization is complete and is ready to update and receive LLDPDU containing EEE TLV.
Rx_dll_enabled	Status of the EEE capability negotiation on the local system.
Rx_dll_ready	Data Link Layer ready: This variable indicates that the Rx system initialization is complete and is ready to update and receive LLDPDU containing EEE TLV.
Time Since Counters Last Cleared	Time Since Counters Last Cleared (since the time of power-up, or after EEE counters are cleared).

## View the Green Mode Statistics Summary

You can view the Port Green Mode Statistics settings.

➤ **To view the port green mode statistics settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7. Select System > Management > Green Ethernet> Green Ethernet Summary.**

Unit	Green Features supported on this unit
1	Energy-Detect

Interface	Energy Detect Admin Mode	Energy Detect Operational Status
0/1	Disable	Inactive
0/2	Disable	Inactive
0/3	Disable	Inactive
0/4	Disable	Inactive

Click the **REFRESH** button to refresh the screen with the most current data from the switch.

The following table describes the Green Mode Statistics Summary nonconfigurable fields.

**Table 14. Green Mode Statistics Summary**

Field	Description
Current Power Consumption (mWatts)	Estimated power consumption by all ports in mWatts.
Percentage Power Saving (%)	Percentage of power saved on all ports due to Green modes enabled.
Cumulative Energy Saving (W * H)	Cumulative Energy saved in Watts * Hours due to all green modes being enabled.
Unit	Displays the Unit ID.
Green Features supported on this unit	List of Green Features supported on the given unit, that could be one or more of the following: Energy-Detect (Energy Detect), EEE (Energy Efficient Ethernet), LPI-History (EEE Low Power Idle History), LLDP-Cap-Exchg (EEE LLDP Capability Exchange), Pwr-Usg-Est (Power Usage Estimates).
Interface	Interface for which data is displayed or configured.

**Table 14. Green Mode Statistics Summary (continued)**

Field	Description
Energy Detect Admin Mode	Enable or Disable Energy Detect Mode on the port. When this mode is enabled, when the port link is down, the PHY automatically goes down for short period of time, and then wakes up to check link pulses. This allows autonegotiation to be performed power saving consumption when no link partner is present.
Energy Detect Operational Status	Current operational status of the Energy Detect mode.

## View the Port Green Mode EEE History

- To view the port green mode EEE history:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Management > Green Ethernet > Green Ethernet LPI History**.

Sample No.	Time Since The Sample Was Recorded	Percentage Time spent in LPI mode since last sample	Percentage Time spent in LPI mode since last reset
[REDACTED]			

8. Select the **Interface** check box.
9. Specify the **Sampling Interval**.

This is the Interval at which EEE LPI data is collected. This is a global setting and is applied to all interfaces. The range is 30 to 36000. The default value is 3600.

10. In the **Max Samples to keep** field, enter a value.

This is a global setting and is applied to all interfaces. The range is 1 to 168. The default value is 168.

11. Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See *Save Configuration* on page 405.

12. Click the **REFRESH** button to refresh the screen with the most current data from the switch.

The following table describes the Port GreenMode EEE History nonconfigurable fields.

**Table 15. Port GreenMode EEE History**

Field	Description
Percentage LPI time per Stack	Time spent in LPI mode per stack since EEE counters were last cleared.
Sample No.	Sample Index.
Time Since The Sample Was Recorded	Each time the screen is refreshed, this field shows a different time because it reflects the difference between the current time and the time that the sample was recorded.
Percentage Time spent in LPI mode since last sample	Percentage of time spent in LPI mode during the current measurement interval.
Percentage Time spent in LPI mode since last reset	Percentage of time spent in LPI mode since EEE LPI statistics were reset.

## Configure the DHCP Server

➤ **To configure the DHCP server:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Services > DHCP Server > DHCP Server Configuration**.

# Excluded Address	
IP Range From	IP Range To

8. Select the Admin Mode **Disable** or **Enable** radio button.

This specifies whether the DHCP service is enabled or disabled. The default value is Disable.

9. Use **Ping Packet Count** to specify the number of packets a server sends to a pool address to check for duplication as part of a ping operation.

The default value is 2. The valid range is 0, 2 to 10. Setting the value to 0 disables the function.

10. Select the Conflict Logging Mode **Disable** or **Enable** radio button

This specifies whether conflict logging on a DHCP server is enabled. The default value is Enable.

11. Select the BOOTP Automatic Mode **Disable** or **Enable** radio button

This specifies whether BOOTP for dynamic pools is enabled. The default value is Disable.

12. Click the **APPLY** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

## Exclude an Address from the DHCP Server

➤ **To exclude an address from the DHCP server:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.

2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Services > DHCP Server > DHCP Server Configuration**.

	IP Range From	IP Range To
<input type="checkbox"/>		
<input type="checkbox"/>		

8. In the **IP Range From** field, specify an IP address.

You can enter the lowest address in a range, or a single address to exclude.

9. In the **IP Range To** field, specify the highest address in the range.

To exclude a single address, enter the same IP address as specified in the **IP Range From** field, or leave it as 0.0.0.0.

10. Click the **ADD** button.

11. To delete the excluded addresses from the switch, click the **DELETE** button.

## Configure the DHCP Pool

### ➤ To configure the DHCP pool:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.

3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
- The Login screen displays.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **System > Services > DHCP Server > DHCP Pool Configuration**.

8. To add the pool, click the **ADD** button.
9. To delete the pool, click the **DELETE** button.  
The **DELETE** button is not visible if you are logged in as a user with read-only permission.
10. Click the **APPLY** button.  
The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the DHCP Pool Configuration fields.

**Table 16. DHCP Pool configuration**

Field	Description
Pool Name*	For a user with read/write permission, this field shows names of all the existing pools along with an additional option Create. When you select <b>Create</b> the <b>Pool Name</b> list displays. For a user with read-only permission, this list shows only the names of the existing pools.
Pool Name	This field appears when the user with read-write permission selects <b>Create</b> in the <b>Pool Name</b> list. Specifies the name of the pool to be created. Pool Name can be up to 31 characters in length.
Type of Binding	Specifies the type of binding for the pool: <ul style="list-style-type: none"> <li>• Unallocated</li> <li>• Dynamic</li> <li>• Manual</li> </ul>
Network Address	Specifies the subnet address for a DHCP address of a dynamic pool.
Network Mask	Specifies the subnet number for a DHCP address of a dynamic pool. Either Network Mask or Prefix Length can be configured to specify the subnet mask but not both.
Network Prefix Length	Specifies the subnet number for a DHCP address of a dynamic pool. Either Network Mask or Prefix Length can be configured to specify the subnet mask but not both. The valid range is 0 to 32.
Client Name	Specifies the client name for DHCP manual pool.
Hardware Address	Specifies the MAC address of the hardware platform of the DHCP client.
Hardware Address Type	Specifies the protocol of the hardware platform of the DHCP client. The valid types are Ethernet and ieee802. The default value is Ethernet.
Client ID	Specifies the client Identifier for DHCP manual pool.
Host Number	Specifies the IP address for a manual binding to a DHCP client. The host can be set only if at least one client Identifier or hardware address is specified. Deleting Host would delete Client Name, Client ID, Hardware address for the manual pool and set the Pool Type to Unallocated.
Host Mask	Specifies the subnet mask for a manual binding to a DHCP client. Either Host Mask or Prefix Length can be configured to specify the subnet mask but not both.
Host Prefix Length	Specifies the subnet mask for a manual binding to a DHCP client. Either Host Mask or Prefix Length can be configured to specify the subnet mask but not both. The valid range is 0 to 32.

**Table 16. DHCP Pool configuration (continued)**

Field	Description
Lease Time	Can be selected as <b>Infinite</b> to specify the lease time as Infinite, or as <b>Specified Duration</b> and enter a specific lease period. In the case of dynamic binding infinite implies a lease period of 60 days. In the case of manual binding, Infinite implies indefinite lease period. The default value is Specified Duration.
Days	The number of days of the lease period. This field appears only if the user has specified <b>Specified Duration</b> as the Lease time. The default value is 1. The valid range is 0 to 59.
Hours	The number of hours of lease period. This field appears only if you specified <b>Specified Duration</b> as the lease time. The valid range is 0 to 22.
Minutes	The number of minutes in the lease period. This field appears only if you specified <b>Specified Duration</b> as the lease time. The valid range is 0 to 86399.
Default Router Addresses	The list of default router addresses for the pool. You can specify up to 8 default router addresses in order of preference.
DNS Server Addresses	The list of DNS server addresses for the pool. You can specify up to 8 DNS server addresses in order of preference.
NetBIOS Name Server Addresses	The list of NetBIOS name server addresses for the pool. You can specify up to 8 NetBIOS name server addresses in order of preference.
NetBIOS Node Type	The NetBIOS node type for DHCP clients: <ul style="list-style-type: none"> <li>• b-node Broadcast</li> <li>• p-node Peer-to-Peer</li> <li>• m-node Mixed</li> <li>• h-node Hybrid</li> </ul>
Next Server Address	The next server address for the pool.
Domain Name	The domain name for a DHCP client. The domain name can be up to 255 characters in length.
Bootfile	The name of the default boot image for a DHCP client. The file name can be up to 128 characters in length.

## Configure the DHCP Pool Options

➤ **To configure the DHCP pool options:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Services > DHCP Server > DHCP Pool Options**.

Pool Name	Option Code	Option Type	Option Value

8. In the **Pool Name** field, select the Pool Name.
9. **Option Code** specifies the Option Code configured for the selected pool.
10. Use **Option Type** to specify the Option Type against the Option Code configured for the selected pool:
  - ASCII
  - Hex
  - IP Address
11. **Option Value** specifies the Value against the Option Code configured for the selected pool.
12. To add a new Option Code for the selected pool, click the **ADD** button.
13. To delete the Option Code for the selected pool, click the **DELETE** button.

## View DHCP Server Statistics

➤ **To view DHCP server statistics:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

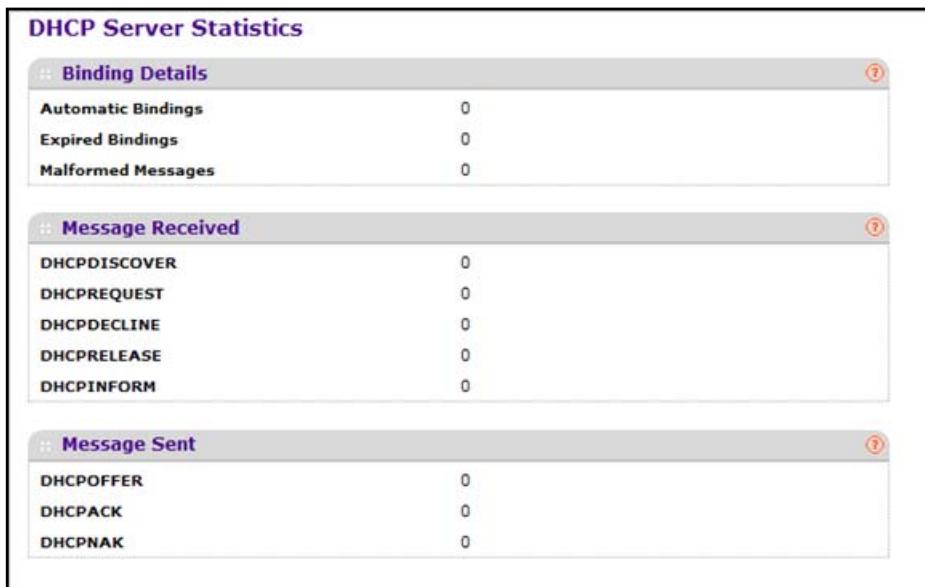
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Services > DHCP Server > DHCP Server Statistics**.



The following table describes the DHCP Server Statistics fields.

**Table 17. DHCP server statistics**

Field	Description
Automatic Bindings	Specifies the number of Automatic Bindings on the DHCP server.
Expired Bindings	Specifies the number of Expired Bindings on the DHCP server.
Malformed Messages	Specifies the number of the malformed messages.
DHCPDISCOVER	Specifies the number of DHCPDISCOVER messages received by the DHCP server.
DHCPPREQUEST	Specifies the number of DHCPPREQUEST messages received by the DHCP server.
DHCPDECLINE	Specifies the number of DHCPDECLINE messages received by the DHCP server.
DHCPRERELEASE	Specifies the number of DHCPRERELEASE messages received by the DHCP server.
DHCPIINFORM	Specifies the number of DHCPIINFORM messages received by the DHCP server.
DHCPOFFER	Specifies the number of DHCPOFFER messages sent by the DHCP server.

**Table 17. DHCP server statistics (continued)**

Field	Description
DHCPACK	Specifies the number of DHCPACK messages sent by the DHCP server.
DCHPNAK	Specifies the number of DCHPNAK messages sent by the DHCP server.

## View DHCP Bindings Information

➤ **To view the DHCP Bindings information:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **System > Services > DHCP Server > DHCP Bindings Information**.

IP Address	Hardware Address	Lease Time Left	Type
------------	------------------	-----------------	------

8. Select one of the following:
  - **All Dynamic Bindings** to specify all dynamic bindings.
  - **Specific Dynamic Binding** to specify a dynamic binding.

The following table describes the DHCP Bindings Information fields.

**Table 18. DHCP Bindings Information**

Field	Description
IP Address	Specifies the Client's IP Address.
Hardware Address	Specifies the Client's Hardware Address.
Lease Time Left	Specifies the Lease time left in Days, Hours and Minutes (dd:hh:mm). format.
Type	Specifies the Type of Binding: Dynamic or Manual.

## View DHCP Conflicts Information

➤ **To view the DHCP conflicts information:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **System > Services > DHCP Server > DHCP Conflicts Information**.

8. Select one of the following:
  - **All Address Conflicts** to specify all address conflicts.

- **Specific Address Conflict** to specify a dynamic binding.

The following table describes the DHCP Conflicts Information fields.

**Table 19. DHCP conflicts information**

Field	Description
IP Address	Specifies the IP Address of the host as recorded on the DHCP server.
Detection Method	Specifies the manner in which the IP address of the hosts were found on the DHCP server.
Detection Time	Specifies the time when the conflict was detected in N days NNh:NNm:NNs format with respect to the system up time.

## Configure the DHCP Relay

➤ **To configure the DHCP relay:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7.** Select **System > Services > DHCP Relay**.

- 8.** Use **Maximum Hop Count** to enter the maximum number of hops a client request can take before being discarded.

The range is 1 to 16. The default value is 4.

- 9.** Select the Admin Mode **Disable** or **Enable** radio button.

When you select **Enable**, DHCP requests are forwarded to the IP address you entered in the **Server Address** on the UDP Relay Global Configuration screen.

- 10.** Use **Minimum Wait Time** to enter a Minimum Wait Time in seconds.

This value is compared to the time stamp in the client's request packets, that should represent the time since the client was powered up. Packets are forwarded only when the time stamp exceeds the minimum wait time. The range is 0 to 100.

- 11.** Select the Circuit ID Option Mode **Disable** or **Enable** radio button.

This specifies the Circuit ID Option mode. If you select **Enable**, Relay Agent options are added to requests before they are forwarded to the server and removed from replies before they are forwarded to clients.

The following table describes the DHCP Relay Status fields.

**Table 20. DHCP Relay Status**

Field	Description
Requests Received	The total number of DHCP requests received from all clients since the last time the switch was reset.
Requests Relayed	The total number of DHCP requests forwarded to the server since the last time the switch was reset.
Packets Discarded	The total number of DHCP packets discarded by this Relay Agent since the last time the switch was reset.

## Configure a DHCP L2 Relay VLAN

➤ **To configure a DHCP L2 Relay VLAN:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **System > Services > DHCP L2 Relay > DHCP L2 Relay Global Configuration**.

The screenshot shows the 'DHCP L2 Relay Configuration' page. At the top, there is a link to 'DHCP L2 Relay Global Configuration'. Below it, there is an 'Admin Mode' section with 'Disable' and 'Enable' radio buttons, currently set to 'Disable'. Underneath is the 'DHCP L2 Relay VLAN Configuration' section, which contains a table with two rows. The columns are labeled 'VLAN ID', 'Admin Mode', 'Circuit ID Mode', and 'Remote ID String'. Row 1 has a checked checkbox in the VLAN ID column, '1' in the Admin Mode dropdown, 'Disable' in the Circuit ID Mode dropdown, and an empty Remote ID String field. Row 2 has an unchecked checkbox in the VLAN ID column, '2' in the Admin Mode dropdown, 'Disable' in the Circuit ID Mode dropdown, and an empty Remote ID String field.

VLAN ID	Admin Mode	Circuit ID Mode	Remote ID String
1	Disable	Disable	
2	Disable	Disable	

8. Use **Admin Mode** to enable or disable the DHCP L2 Relay on the switch.  
The default is Disable.  
**VLAN ID** shows the VLAN ID configured on the switch.
9. Use **Admin Mode** to enable or disable the DHCP L2 Relay on the selected VLAN.
10. Use **Circuit ID Mode** to enable or disable the Circuit ID suboption of DHCP Option-82.
11. Use **Remote ID String** to specify the Remote ID when Remote ID mode is enabled.

## Configure the DHCP L2 Relay Interface

➤ To configure the DHCP L2 Relay Interface:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Configuration**.

The screenshot shows a table titled "DHCP L2 Relay Configuration" with the following data:

DHCP L2 Relay Configuration		Go To Interface	
1	LAGS All	GO	
	Interface	Admin Mode	82 Option Trust Mode
1	0/1	Disable	Disable
2	0/2	Disable	Disable
3	0/3	Disable	Disable
4	0/4	Disable	Disable
5	0/5	Disable	Disable
6	0/6	Disable	Disable
7	0/7	Disable	Disable
8	0/8	Disable	Disable
9	0/9	Disable	Disable
10	0/10	Disable	Disable
11	0/11	Disable	Disable
12	0/12	Disable	Disable

8. Use **Admin Mode** to enable or disable the DHCP L2 Relay on the selected interface.

The default is disable.

9. Use **82 Option Trust Mode** to enable or disable an interface to be trusted for DHCP L2 Relay (Option-82) received.

## View DHCP L2 Relay Interface Statistics

➤ To view the DHCP L2 Relay Interface Statistics:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **System > Services > DHCP L2 Relay > DHCP L2 Relay Interface Statistics**.

DHCP L2 Relay Interface Statistics				
:: DHCP L2 Relay Interface Statistics				
1 LAGS All				
Interface	Untrusted Server Messages With Opt82	Untrusted Client Messages With Opt82	Trusted Server Messages Without Opt82	Trusted Client Messages Without Opt82
0/1	0	0	0	0
0/2	0	0	0	0
0/3	0	0	0	0
0/4	0	0	0	0
0/5	0	0	0	0
0/6	0	0	0	0
0/7	0	0	0	0
0/8	0	0	0	0
0/9	0	0	0	0
0/10	0	0	0	0
0/11	0	0	0	0
0/12	0	0	0	0
1 LAGS All				

The following table describes the DHCP L2 Relay Interface Statistics fields.

**Table 21. DHCP L2 Relay Interface Statistics**

Field	Description
Interface	The interface from which the DHCP messages are received.
UntrustedServerMsgsWithOpt82	The number of DHCP messages with option82 received from an untrusted server.
UntrustedClientMsgsWithOpt82	The number of DHCP messages with option82 received from an untrusted client.
TrustedServerMsgsWithoutOpt82	The number of DHCP messages without option82 received from a trusted server.
TrustedClientMsgsWithoutOpt82	The number of DHCP messages without option82 received from a trusted client.

## Configure UDP Relay Global Settings

➤ **To configure the UDP Relay global settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Services > UDP Relay> UDP Relay Global Configuration.**

UDP Relay Configuration				
Admin Mode		<input checked="" type="radio"/> Disable	<input type="radio"/> Enable	(?)
UDP Relay Global Configuration				
	Server Address	UDP Port	UDP Port Other Value	Hit Count
<input type="checkbox"/>				

8. Use **Admin Mode** to enable or disable the UDP Relay on the switch.

The default value is Disable.

9. Use **Server Address** to specify the UDP relay server address in x.x.x.x format.

10. Use **UDP Port** to specify the UDP Destination Port. These ports are supported:

- **DefaultSet.** Relay UDP port 0 packets. This is specified if no UDP port is selected when you are creating the Relay server.
- **dhcp.** Relay DHCP UDP port 67 packets.
- **domain.** Relay DNS UDP port 53 packets.
- **isakmp.** Relay ISAKMP UDP port 500 packets.
- **mobile-ip.** Relay Mobile IP UDP port 434 packets.
- **nameserver.** Relay IEN-116 Name Service UDP port 42 packets.
- **netbios-dgm.** Relay NetBIOS datagram server UDP port 138 packets.
- **netbios-ns.** Relay NetBIOS name server UDP port 137 packets.
- **ntp.** Relay Network Time protocol UDP port 123 packets.
- **pim-auto-rp.** Relay PIM auto RP UDP port 496 packets.
- **rip.** Relay RIP UDP port 520 packets.
- **tacacs.** Relay TACACS UDP port 49 packet.
- **tftp.** Relay TFTP UDP port 69 packets.
- **time.** Relay time service UDP port 37 packets.
- **Other.** If this option is selected, the UDP Port Other Value is enabled. This option permits you to enter your own UDP port in **UDP Port Other Value**.

11. Use **UDP Port Other Value** to specify a UDP Destination Port that lies between 0 and 65535.

12. To create an entry in UDP Relay Table with the specified configuration, click the **ADD** button.

13. To remove all entries or a specified one from the UDP Relay Table, click the **DELETE** button.

The Hit Count field displays the number of UDP packets hitting the UDP port.

## Configure the UDP Relay Interface

➤ **To configure the UDP Relay Interface:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Services > UDP Relay > UDP Relay Interface Configuration**.

UDP Relay Interface Configuration						
UDP Relay Interface Configuration						
Interface	Server Address	UDP Port	UDP Port Other Value	Discard	Hit Count	
1	169.254.100.100	1	1	1	1	1

8. Use **Interface** to select an Interface to be enabled for the UDP Relay.
9. Use **Server Address** to specify the UDP relay server address in x.x.x.x format.
10. Use **UDP Port** to specify UDP Destination Port.

The following ports are supported:

- **DefaultSet**. Relay UDP port 0 packets. This is specified if no UDP port is selected when you are creating a Relay server.
- **dhcp**. Relay DHCP UDP port 67 packets.
- **domain**. Relay DNS UDP port 53 packets.
- **isakmp**. Relay ISAKMP UDP port 500 packets.
- **mobile-ip**. Relay Mobile IP UDP port 434 packets
- **nameserver**. Relay IEN-116 Name Service UDP port 42 packets.
- **netbios-dgm**. Relay NetBIOS datagram server UDP port 138 packets.
- **netbios-ns**. Relay NetBIOS name server UDP port 137 packets.
- **ntp**. Relay Network Time Protocol UDP port 123 packets.
- **pim-auto-rp**. Relay PIM auto RP UDP port 496 packets.

- **rip.** Relay RIP UDP port 520 packets.
- **tacacs.** Relay TACACS UDP port 49 packet.
- **tftp.** Relay TFTP UDP port 69 packets.
- **time.** Relay time service UDP port 37 packets.
- **Other.** If this option is selected, the UDP Port Other Value is enabled. This option permits you to enter your own UDP port in **UDP Port Other Value**.

- 11.** Use **UDP Port Other Value** to specify UDP Destination Port that lies between 0 and 65535.
- 12.** Use **Discard** to enable or disable dropping of matched packets.

Enable can be selected only when you enter 0.0.0.0 as the IP address. Discard mode can be set to Disable when you add a new entry with a non-zero IP address.

- 13.** To create an entry in the UDP Relay Table with the specified configuration, click the **ADD** button.
- 14.** To remove all entries or a specified one from the UDP Relay Interface Configuration Table, click the **DELETE** button.

The **Hit Count** field displays the number of UDP packets hitting the UDP port.

## Configure the Basic PoE Settings

➤ **To display the Basic PoE Configuration:**

- 1.** Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
- 2.** Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
- 3.** Launch a web browser.
- 4.** Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

- 5.** Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- 6.** Click the **Login** button.

The web management interface menu displays.

**7.** Select **System > PoE > Basic > PoE Configuration**.

The screenshot shows the 'PoE Configuration' screen with the following details:

- Unit Selection:** Unit 1
- Firmware Version:** 1.1.0.2
- Power Status:** On
- Total Power (Main AC):** 150 Watt
- Total Power (RPS):** 0 Watt
- Power Source:** Main AC
- Threshold Power:** 135000 mW
- Consumed Power:** 14200 mW
- System Usage Threshold:** 90 (1% to 99%)
- Power Management Mode:** Dynamic
- Traps:** Enable (radio button selected)

The **Unit Selection** list displays the current PoE unit.

- 8.** To change the PoE unit, select another unit from the menu.
- 9.** To set the **System Usage Threshold**, enter a number from 1 to 99.

This sets the threshold level at which a trap is sent if consumed power is greater than the threshold power.

- 10.** Use **Power Management Mode** to describe or control the power management algorithm used by the PSE to deliver power to the requesting PDs.

Select **Static** to indicate that the power allocated for each port depends on the type of power threshold configured on the port. Select **Dynamic** to indicate that the power consumption on each port is measured and calculated in real time.

- 11.** Select the Traps **Enable** or **Disable** radio button.

**Enable** activates the PoE traps. **Disable** deactivates the PoE traps. The default setting is enabled.

- 12.** Click the **APPLY** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table shows the nonconfigurable fields in the PoE Configuration screen.

**Table 22. PoE Configuration**

Field	Description
Units	Displays the Current PoE Unit. You can change the PoE Unit by selecting another unit ID listed here.
Firmware Version	Version of the PoE controller's FW image.

**Table 22. PoE Configuration (continued)**

Field	Description
Power Status	Indicates the power status.
Total Power (Main AC)	Displays the total power provided by the MAIN AC power source.
Total Power (RPS)	Displays the total power provided by the redundant power source.
Power Source	Current source of system power (Main AC or RPS).
Threshold Power	System can power up one port, if consumed power is less than this power. That is, consumed power can be between Nominal & Threshold Power values. The threshold power value is effected by changing System Usage Threshold.
Consumed Power	Total amount of power that is currently being delivered to all ports.

## Configure Advanced PoE Settings

➤ **To configure advanced PoE settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **System > PoE > Advanced > PoE Configuration**.

The screenshot shows the 'PoE Configuration' interface. At the top, there's a 'Unit Selection' section with a dropdown menu set to '1'. Below it is the main 'PoE Configuration' section. Key settings shown include:

- Firmware Version:** 1.1.0.2
- Power Status:** On
- Total Power (Main AC):** 150 Watt
- Total Power (RPS):** 0 Watt
- Power Source:** Main AC
- Threshold Power:** 135000 mW
- Consumed Power:** 12900 mW
- System Usage Threshold:** 90 (1% to 99%)
- Power Management Mode:** Dynamic (selected)
- Traps:** Enable (radio button selected)

The **Unit** list displays the current PoE unit.

8. To change the PoE unit, select another unit from the menu.
9. In the **System Usage Threshold** field, enter a number from 1 to 99.

This sets the threshold level at which a trap is sent if consumed power is greater than the threshold power.

10. Select the Power Management Mode **Dynamic** or **Static** radio button.

This setting describes or controls the power management algorithm used by the PSE to deliver power to the requesting PDs.

- **Dynamic.** The power consumption on each port is measured and calculated in real time.
- **Static.** The power allocated for each port depends on the type of power threshold configured on the port.

11. Select the Traps **Enable** or **Disable** radio button.

Enable activates the PoE traps. Disable deactivates the PoE traps. The default setting is enabled.

12. Click the **APPLY** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the PoE Configuration nonconfigurable fields.

**Table 23. Advanced PoE Configuration**

Field	Description
Units	Displays the Current PoE Unit. You can change the PoE Unit by selecting another unit ID listed here.
Firmware Version	Version of the PoE controller's FW image.
Power Status	Indicates the power status.
Total Power (Main AC)	Displays the total power provided by the MAIN AC power source.
Total Power (RPS)	Displays the total power provided by the redundant power source.
Power Source	Current source of system power (Main AC or RPS).
Threshold Power	System can power up one port, if consumed power is less than this power. That is, consumed power can be between Nominal and Threshold Power values. The threshold power value is effected by changing System Usage Threshold.
Consumed Power	Total amount of a power that is currently being delivered to all ports.

## Configure a PoE Port

➤ **To configure a PoE port:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > PoE > Advanced > PoE Port Configuration**.

PoE Port Configuration																
PoE Port Configuration																
	Port	Admin Mode	High Power	Max Power	Port Priority	High Power Mode	Power Limit Type	Power Limit (Watts)	Detection Type	Class	Timer Schedule	Output Voltage (Volts)	Output Current (mA)	Output Power (Watts)	Status	Fault Status
Q/2	Enable	Yes	22.0	Low	802.3at	User	20.000	auto	Unknown	None	0	0	0.000	Searching	No Error	
Q/4	Enable	Yes	22.0	Low	802.3at	User	20.000	auto	Unknown	None	0	0	0.000	Searching	No Error	
Q/5	Enable	Yes	22.0	Low	802.3at	User	20.000	auto	Unknown	None	0	0	0.000	Searching	No Error	
Q/6	Enable	Yes	22.0	Low	802.3at	User	20.000	auto	Unknown	None	0	0	0.000	Searching	No Error	
Q/7	Enable	Yes	22.0	Low	802.3at	User	20.000	auto	Unknown	None	0	0	0.000	Searching	No Error	
Q/8	Enable	Yes	22.0	Low	802.3at	User	20.000	auto	Unknown	None	0	0	0.000	Searching	No Error	
Q/9	Enable	Yes	22.0	Low	802.3at	User	20.000	auto	Unknown	None	0	0	0.000	Searching	No Error	
Q/10	Enable	Yes	22.0	Low	802.3at	User	20.000	auto	Unknown	None	0	0	0.000	Searching	No Error	
Q/11	Enable	Yes	22.0	Low	802.3at	User	20.000	auto	Unknown	None	0	0	0.000	Searching	No Error	
Q/12	Enable	Yes	22.0	Low	802.3at	User	20.000	auto	Unknown	None	0	0	0.000	Searching	No Error	

8. For **Admin Mode**, select **Enable** or **Disable** to determine the ability of the port to deliver power.
9. Use **Port Priority** to determine which ports can deliver power when the total power delivered by the system crosses a specific threshold.

If the switch is not able to supply power to all connected devices, priority is used to determine which ports can supply power. The lowest numbered port that is one of the ports of the same priority has a higher priority. Select the priority order from the following list:

- **Low.** Low priority
- **Medium.** Medium priority
- **High.** High priority
- **Critical.** Critical priority

10. Select the **High Power Mode** from the following options:
- **Disabled** indicates that a port is powered in the IEEE 802.3af mode.
  - **Legacy** indicates that a port is powered using high-inrush current, used by legacy PD's whose power requirements are more than 15W from power-up.
  - **Pre-802.3at** indicates a port is powered in the IEEE 802.3af mode initially and then switched to the high-power IEEE 802.3at mode before 75 msec. This mode must be selected if the PD is NOT performing Layer 2 Classification or the PSE is performing 2-Event Layer 1 Classification.
  - **802.3at** indicates that a port is powered in the IEEE 802.3at mode. For example, if the class detected by PSE is not class4, then the PSE port does not power up the PD.
11. The **Power Limit Type** describes or controls the maximum power that a port can deliver.

Select the type from the following list:

- **Class.** The port power limit is equal to the class of the PD attached.
- **User.** The port power limit is equal to the value specified by Power Limit.
- **None.** The port draws up to class 0 maximum power in the case of low power mode and up to class 4 maximum power in the case of high power mode.

12. Select the **Power Limit** to define the maximum power in watts that can be delivered by a port.
13. The **Detection Type** describes a PD detection mechanism performed by the PSE port.
  - **pre-ieee**. Only legacy detection is done.
  - **ieee**. 4 Point Resistive Detection is done.
  - **auto**. 4 Point Resistive Detection followed by Legacy Detection is done.
  - **4point** and **Legacy** indicates that the resistive 4 point detection scheme is used and when it fails to detect a connected PD, legacy capacitive detection is used.
14. The **Timer Schedule** defines the timer schedule assigned to the port.  
Select **None** to remove the timer schedule assignment.
15. Click **Reset** to forcibly reset the PSE port.
16. Click the **APPLY** button.

The updated configuration file is sent to the switch. Configuration changes take effect immediately.

The following table describes the PoE Port Configuration nonconfigurable fields.

**Table 24. PoE Port Configuration**

Field	Description
Port	The interface.
High Power	Enabled when particular port supports High Power Mode.
Max Power	The maximum power in Watts that can be provided by the port.
Class	The Class defines the range of power a PD is drawing from the system. Class definitions: 0 – 0.44-12.95 (watts) 1 – 0.44-3.83 (watts) 2 – 0.44-6.48 (watts) 3 – 0.44-12.95 (watts) 4 – 0.44-25.5 (watts)
Output Voltage	Current voltage being delivered to device in volts.
Output Current	Current being delivered to device in mA.
Output Power	Current power being delivered to device in Watts.

**Table 24. PoE Port Configuration (continued)**

Field	Description
Status	The status is the operational status of the port PD detection. <ul style="list-style-type: none"> <li>• <b>Disabled.</b> No power being delivered.</li> <li>• <b>DeliveringPower.</b> Power is being drawn by the device.</li> <li>• <b>Fault.</b> Indicates a problem with the port.</li> <li>• <b>Test.</b> The port is in test mode.</li> <li>• <b>otherFault.</b> The port is idle due to an error condition.</li> <li>• <b>Searching.</b> The port is not in one of the above states.</li> </ul>
Fault Status	Describes the error description when the PSE port is in fault status. No Error indicates that the PSE port is not in any error state. MPS Absent indicates that the PSE port has detected an absence of main power supply. Short indicates that the PSE port has detected a short circuit condition. Overload indicates that the PD connected to the PSE port had tried to provide more power than is permissible by the hardware. Power Denied indicates that the PSE port was denied power because of a shortage of power or due to administrative action.

## Configure SNMP Community Settings

By default, two SNMP Communities exist that use the SNMP V1 and SNMP V2 protocol:

- Private, with Read/Write privileges and status set to **Enable**.
- Public, with read-only privileges and status set to **Enable**.

These are well-known communities. You can change the default settings or add other communities. Only the defined communities can access the switch using the SNMP V1 and SNMP V2 protocols. Only those communities with read/write access can be used to change the configuration using SNMP.

For information about using SNMP v3, see *Configure SNMP v3 Settings for a User* on page 88.

➤ **To configure SNMP community settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

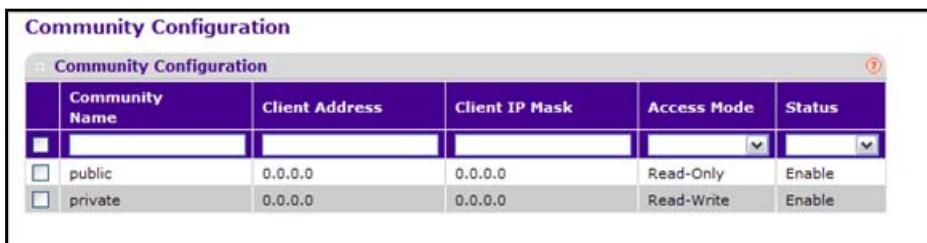
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > SNMP > SNMP V1/V2 > Community Configuration**.



The screenshot shows a table titled "Community Configuration" with the following data:

Community Name	Client Address	Client IP Mask	Access Mode	Status
public	0.0.0.0	0.0.0.0	Read-Only	Enable
private	0.0.0.0	0.0.0.0	Read-Write	Enable

8. In the **Community Name** list, select an existing community name or select **Create** to create a new one.

A valid entry is a case-sensitive string of up to 16 characters.

9. To denote a range of IP addresses that SNMP clients can use to access this device, complete the **Client Address** field and the **Client IP Mask** field.

If either the Client Address or IP Mask value is 0.0.0.0, access is allowed from any IP address. Otherwise, every client's address is ANDed with the mask, as is the Client Address, and, if the values are equal, access is allowed. For example, if the Client Address and Client IP Mask parameters are 192.168.1.0/255.255.255.0, then any client whose address is 192.168.1.0 through 192.168.1.255 (inclusive) is allowed access. To allow access from only one station, use a Client IP Mask value of 255.255.255.255, and use that machine's IP address for the Client Address.

10. In the **Access Mode** list, select **Read/Write** or **Read Only** to specify the access level for this community.

11. Use **Status** to specify the status of this community by selecting **Enable** or **Disable**.

If you select enable, the community name must be unique among all valid community names or the set request is rejected. If you select **Disable**, the community name becomes invalid.

12. To add the currently selected community to the switch, click the **ADD** button.

13. To delete the currently selected Community Name, click the **DELETE** button.

## Configure an SNMP Trap

➤ **To configure an SNMP trap:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

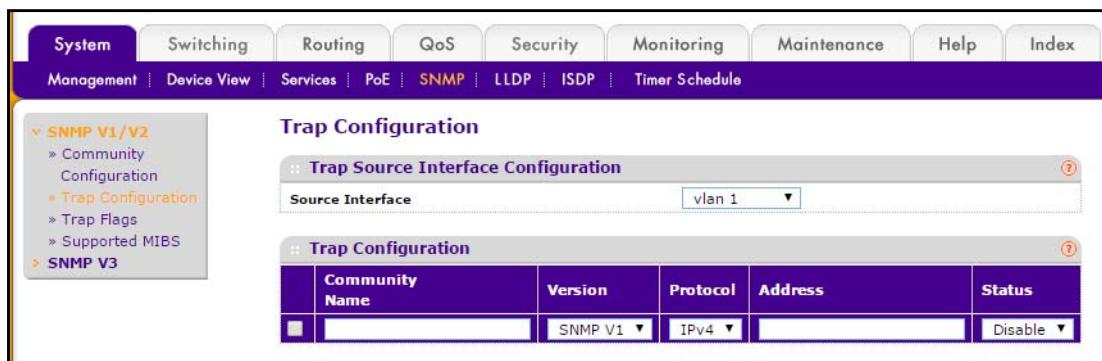
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > SNMP > SNMP V1/V2 > Trap Configuration**.



This screen displays an entry for every active trap receiver.

8. Specify the Source Interface to be used for SNMP Trap manager.

Possible values are as follows:

- Routing interface
- Routing VLAN
- Routing loopback interface

By default, VLAN 1 is used as source interface.

9. To add a host that receives SNMP traps, enter trap configuration information in the available fields described below, and then click the **ADD** button.

- **Community Name.** Enter the community string for the SNMP trap packet to be sent to the trap manager. This can be up to 16 characters and is case-sensitive.
- **Version.** Select the trap version to be used by the receiver:
  - **SNMP V1.** Uses SNMP V1 to send traps to the receiver.
  - **SNMP V2.** Uses SNMP V2 to send traps to the receiver.
- **Protocol.** Select the protocol to be used by the receiver. Select **IPv4** if the receiver's address is IPv4 address or **IPv6** if the receiver's address is IPv6.
- **Address.** Enter the IPv4 address in x.x.x.x format or the IPv6 address in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx format or a host name starting with a letter to receive SNMP traps from this device. Length of address can not exceed 158 characters.

- **Status.** Select the receiver's status from the menu:
    - **Enable.** Send traps to the receiver.
    - **Disable.** Do not send traps to the receiver.
- 10.** To modify information about an existing SNMP recipient, select the check box next to the recipient, change the desired fields, and then click the **APPLY** button.  
Configuration changes take effect immediately.
- 11.** To delete a recipient, select the check box next to the recipient and click the **DELETE** button.

## Configure Trap Flags

You can enable or disable traps. When the condition identified by an active trap is encountered by the switch, a trap message is sent to any enabled SNMP Trap Receivers, and a message is written to the trap log.

➤ **To configure trap flags:**

- 1.** Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
- 2.** Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
- 3.** Launch a web browser.
- 4.** Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

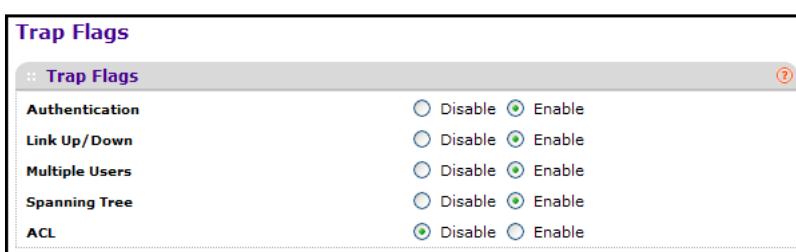
- 5.** Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- 6.** Click the **Login** button.

The web management interface menu displays.

- 7.** Select **System > SNMP > SNMP V1/V2 > Trap Flags.**



- 8.** Use **Authentication** to enable or disable activation of authentication failure traps by selecting the corresponding radio button.

The factory default is enabled.

9. Use **Link Up/Down** to enable or disable activation of link status traps by selecting the corresponding radio button.  
The factory default is enabled.
10. Use **Multiple Users** to enable or disable activation of multiple user traps by selecting the corresponding radio button.  
The factory default is enabled. This trap is triggered when the same user ID is logged in to the switch more than once at the same time either through Telnet or the serial port.
11. Use **Spanning Tree** to enable or disable activation of spanning tree traps by selecting the corresponding radio button.  
The factory default is enabled.
12. Use **ACL** to enable or disable activation of ACL traps by selecting the corresponding radio button.  
The factory default is disabled.
13. Use **PoE** to enable or disable activation of PoE traps by selecting the corresponding radio button.  
The factory default is enabled. Indicates whether PoE traps are sent.
14. Click the **APPLY** button.  
The updated configuration is sent to the switch. Configuration changes take effect immediately.

## View All MIBs Supported by the Switch

➤ **To view supported MIBs:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.

## 7. Select System > SNMP > SNMP V1/V2 > Supported MIBs.

SNMP Supported MIBs	
Name	Description
RFC 1907 - SNMPv2-MIB	The MIB module for SNMPv2 entities
RFC 2819 - RMON-MIB	Remote Network Monitoring Management Information Base
Broadcom-REF-MIB	Broadcom Reference
SNMP-COMMUNITY-MIB	This MIB module defines objects to help support coexistence between SNMPv1, SNMPv2, and SNMPv3.
SNMP-FRAMEWORK-MIB	The SNMP Management Architecture MIB
SNMP-MPD-MIB	The MIB for Message Processing and Dispatching
SNMP-NOTIFICATION-MIB	The Notification MIB Module
SNMP-TARGET-MIB	The Target MIB Module
SNMP-USER-BASED-SM-MIB	The management information definitions for the SNMP User-based Security Model.
SNMP-VIEW-BASED-ACM-MIB	The management information definitions for the View-based Access Control Model for SNMP.
USM-TARGET-TAG-MIB	SNMP Research, Inc.
FASTRPATH-POWER-ETHERNET-MIB	Fastpath Power Ethernet Extensions MIB
POWER-ETHERNET-MIB	Power Ethernet MIB
sfFlow-MIB	sfFlow MIB
FASTRPATH-ISDP-MIB	Industry Standard Discovery Protocol MIB
LAG-MIB	The Link Aggregation module for managing IEEE 802.3ad
RFC 1213 - RFC1213-MIB	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
RFC 1493 - BRIDGE-MIB	Definitions of Managed Objects for Bridges (dot1d)
RFC 2674 - P-BRIDGE-MIB	The Bridge MIB Extension module for managing Priority and Multicast Filtering, defined by IEEE 802.1D-1998.
RFC 2674 - Q-BRIDGE-MIB	The VLAN Bridge MIB module for managing Virtual Bridged Local Area Networks
RFC 2737 - ENTITY-MIB	Entity MIB (Version 2)
RFC 2863 - IF-MIB	The Interfaces Group MIB using SMIv2
RFC 3635 - Etherlike-MIB	Definitions of Managed Objects for the Ethernet-like Interface Types
FASTRPATH-SWITCHING-MIB	FASTRPATH Switching - Layer 2
FASTRPATH-INVENTORY-MIB	Unit and Slot configuration.
FASTRPATH-PORTSECURITY-PRIVATE-MIB	Port Security MIB.
IEEE 802.1QAB/D13	LLDP basic MIB
IEEE8021-PAE-MIB	Port Access Entity module for managing IEEE 802.1X.
FASTRPATH-RADIUS-AUTH-CLIENT-MIB	Broadcom FastPath Radius MIB
RADIUS-ACC-CLIENT-MIB	RADIUS Accounting Client MIB
RADIUS-AUTH-CLIENT-MIB	RADIUS Authentication Client MIB
FASTRPATH-CAPTIVE-PORTAL-MIB	FastPath Captive Portal MIB
FASTRPATH-NGMT-SECURITY-MIB	The Broadcom Private MIB for FastPath Mgmt Security
IANA-ADDRESS-FAMILY-NUMBERS-MIB	The MIB module defines the AddressFamilyNumbers textual convention.
RFC 1724 - RIPv2-MIB	RIP Version 2 MIB Extension
RFC 1850 - OSPF-MIB	OSPF Version 2 Management Information Base
RFC 1850 - OSPF-TRAP-MIB	The MIB module to describe traps for the OSPF Version 2 Protocol.
RFC 2287 - VRRP-MIB	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
FASTRPATH-ROUTING-MIB	FASTRPATH Routing - Layer 3
FASTRPATH-QOS-MIB	FASTRPATH Flex QoS Support
FASTRPATH-QOS-ACL-MIB	FASTRPATH Flex QoS ACL
FASTRPATH-QOS-COS-MIB	FASTRPATH Flex QoS COS
FASTRPATH-QOS-AUTOVOIP-MIB	FASTRPATH Flex QoS VOIP
RFC 3289 - DIFFSERV-DSCP-TC	Management Information Base for the Textual Conventions used in DIFFSERV-MIB
RFC 3289 - DIFFSERV-MIB	Management Information Base for the Differentiated Services Architecture
FASTRPATH-QOS-DIFFSERV-EXTENSIONS-MIB	FASTRPATH Flex QoS DiffServ Private MIBs' definitions
FASTRPATH-QOS-DIFFSERV-PRIVATE-MIB	FASTRPATH Flex QoS DiffServ Private MIBs' definitions
RFC 2932 - IPROUTE-MIB	IPv4 Multicast Routing MIB
draft-ietf-magma-mprmd-mib-03	MGRD MIB, includes IGMPv3 and MLDv2.
RFC 5060 - PIM-STD-MIB	Protocol Independent Multicast MIB
RFC 5240 - PIM-BSR-MIB	Bootstrap Router mechanism for PIM routers
DVMRP-STD-MIB	Distance-Vector Multicast Routing Protocol MIB
IANA-RTPROTO-MIB	IANA IP Route Protocol and IP MRroute Protocol Textual Conventions
FASTRPATH-NSP-MIB	The MIB module defines objects to configure Non Stop Forwarding.
RFC 2465 - IPv6-MIB	Management Information Base for IP Version 6: Textual Conventions and General Group
RFC 2466 - IPv6-ICMP-MIB	Management Information Base for IP Version 6: ICMPv6 Group
RFC 3419 - TRANSPORT-ADDRESS-MIB	Textual Conventions for Transport Addresses
FASTRPATH-ROUTINGS-MIB	The Broadcom Private MIB for FastPath Ipv6 Routing

In the **Name** field, the screen displays the RFC number if applicable and the name of the MIB.

## Configure SNMP v3 Settings for a User

### ➤ To configure SNMP v3 settings for a user:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > SNMP > SNMP V3 > User Configuration**.

The screenshot shows the 'User Configuration' page with two main sections:

- User Names:** A table with one row for 'User Name' set to 'admin'.
- User Configuration:** A table with three rows:
  - SNMP v3 Access Mode:** Set to 'Read/Write'.
  - Authentication Protocol:** Radio buttons for 'None', 'MD5', and 'SHA'; 'None' is selected.
  - Encryption Protocol:** Radio buttons for 'None' and 'DES'; 'None' is selected.

8. Use **User Name** to specify the user account to be configured.

9. Select the **SNMP v3 Access Mode**.

This indicates the SNMP v3 access privileges for the user account. The admin account always has Read/Write access, and all other accounts use Read Only access.

10. Use **Authentication Protocol** to specify the SNMP v3 Authentication Protocol setting for the selected user account. The valid Authentication Protocols are None, MD5 or SHA:

- If you select **None**, the user cannot access the SNMP data from an SNMP browser.
- If you select **MD5** or **SHA**, the user login password are used as the SNMP v3 authentication password, and you must therefore specify a password, and it must be eight characters long.

11. Use **Encryption Protocol** to specify the SNMP v3 Encryption Protocol setting for the selected user account. The valid Encryption Protocols are None or DES:

- If you select the **DES Protocol**, you must enter a key in the **Encryption Key** field.
- If **None** is specified for the Protocol, the Encryption Key is ignored.

12. Enter the **Encryption Key**.

If you selected **DES** in the **Encryption Protocol** field, enter the SNMP v3 Encryption Key here; otherwise, this field is ignored. Valid keys are 0 to 15 characters long. The **APPLY** check box must be selected for you to change the Encryption Protocol and Encryption Key.

13. Click the **APPLY** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

## LLDP Overview

The IEEE 802.1AB-defined standard, Link Layer Discovery Protocol (LLDP), allows stations on an 802 LAN to advertise major capabilities and physical descriptions. This information is viewed by a network manager to identify system topology and detect bad configurations on the LAN.

LLDP is a one-way protocol; there are no request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function. The transmit and receive functions can be enabled or disabled separately per port. By default, both transmit and receive are disabled on all ports. The application is responsible for starting each transmit and receive state machine appropriately, based on the configured status and operational state of the port.

The Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) is an enhancement to LLDP with the following features:

- Auto-discovery of LAN policies such as VLAN, Layer 2 Priority, and DiffServ settings, enabling plug and play networking.
- Device location discovery for creation of location databases.
- Extended and automated power management of Power over Ethernet endpoints.
- Inventory management, enabling network administrators to track their network devices and determine their characteristics (manufacturer, software and hardware versions, serial or asset number).

## Configure LLDP Global Settings

You can specify LLDP parameters that are applied to the switch.

➤ **To configure LLDP global settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7.** Select **System > LLDP > Global Configuration**.

Global Configuration	
Transmit Interval	30 (5 to 32768 secs)
Transmit Hold Multiplier	4 (2 to 10 secs)
Re-Initialization Delay	2 (1 to 10 secs)
Notification Interval	5 (5 to 3600 secs)

- 8.** Use **Transmit Interval** to specify the interval in seconds to transmit LLDP frames.  
The range is from 5 to 32768 secs. The default value is 30 seconds.
- 9.** Use **Transmit Hold Multiplier** to specify the multiplier on Transmit Interval to assign TTL.  
The range is from 2 to 10 secs. The default value is 4.
- 10.** Use **Re-Initialization Delay** to specify the delay before re-initialization.  
The range is from 1 to 10 secs. The default value is 2 seconds.
- 11.** Use **Notification Interval** to specify the interval in seconds for transmission of notifications.  
The range is from 5 to 3600 secs. The default value is 5 seconds.
- 12.** Click the **APPLY** button.  
The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See *Save Configuration* on page 405.

## Configure an LLDP Interface

➤ **To configure an LLDP interface:**

- 1.** Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
- 2.** Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
- 3.** Launch a web browser.
- 4.** Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
- 5.** Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
- 6.** Click the **Login** button.  
The web management interface menu displays.

7. Select **System > LLDP > Interface Configuration**.

LLDP Interface Configuration										
:: Interface Configuration										
1 All						Go To Port	GO			
			Operational TLV(s)						Transmit Management Information	
Port	Link Status	Transmit	Receive	Notify		Port Description	System Name	System Description	System Capabilities	
<input type="checkbox"/>	0/1	Up	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/2	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/3	Up	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/4	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/5	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/6	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/7	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/8	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/9	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/10	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/11	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	0/12	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable

8. Use **Go To Port** to enter the Port in unit/slot/port format and click the **Go** button.  
The entry corresponding to the specified port is selected.
9. Use **Port** to specify the list of ports on which LLDP - 802.1AB can be configured.
10. **Link Status** indicates whether the Link is up or down.
11. Use **Transmit** to specify the LLDP - 802.1AB transmit mode for the selected interface.
12. Use **Receive** to specify the LLDP - 802.1AB receive mode for the selected interface.
13. Use **Notify** to specify the LLDP - 802.1AB notification mode for the selected interface.
14. Specify optional TLVs:
- Use **Port Description** to include the port description TLV in LLDP frames.
  - Use **System Name** to include the system name TLV in LLDP frames.
  - Use **System Description** to include the system description TLV in LLDP frames.
  - Use **System Capabilities** to include the system capability TLV in LLDP frames.
15. Use **Transmit Management Information** to specify whether the management address is transmitted in LLDP frames for the selected interface.

## View LLDP Statistics

➤ **To view LLDP statistics:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.

2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > LLDP > Statistics**.

**LLDP Statistics**

Last Update		0 Days 00:01:33	
Total Inserts	1	Total Deletes	0
Total Drops	0	Total Ageouts	0

Interface	Transmit Total	Receive Total	Discards	Errors	Ageouts	TLV Discards	TLV Unknowns	TLV MED	TLV 802.1	TLV 802.3
0/1	173	175	0	0	0	0	0	0	0	0
0/2	0	0	0	0	0	0	0	0	0	0
0/3	0	0	0	0	0	0	0	0	0	0
0/4	0	0	0	0	0	0	0	0	0	0
0/5	0	0	0	0	0	0	0	0	0	0
0/6	0	0	0	0	0	0	0	0	0	0
0/7	0	0	0	0	0	0	0	0	0	0
0/8	0	0	0	0	0	0	0	0	0	0
0/9	0	0	0	0	0	0	0	0	0	0
0/10	0	0	0	0	0	0	0	0	0	0
0/11	0	0	0	0	0	0	0	0	0	0
0/12	0	0	0	0	0	0	0	0	0	0

The following table describes the LLDP Statistics fields.

**Table 25. LLDP statistics**

Field	Description
Last Update	Specifies the time when an entry was created, modified, or deleted in the tables associated with the remote system.
Total Inserts	Specifies the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) was inserted into tables associated with the remote systems.

**Table 25. LLDP statistics (continued)**

<b>Field</b>	<b>Description</b>
Total Deletes	Specifies the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) was deleted from tables associated with the remote systems.
Total Drops	Specifies the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) could not be entered into tables associated with the remote systems because of insufficient resources.
Total Age outs	Specifies the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) was deleted from tables associated with the remote systems because the information timeliness interval has expired.
Interface	Specifies the unit/slot/port for the interfaces.
Transmit Total	Specifies the number of LLDP frames transmitted by the LLDP agent on the corresponding port.
Receive Total	Specifies the number of valid LLDP frames received by this LLDP agent on the corresponding port, while the LLDP agent is enabled.
Discards	Specifies the number of LLDP TLVs discarded for any reason by the LLDP agent on the corresponding port.
Errors	Specifies the number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
Age outs	Specifies the number of age-outs that occurred on a given port. An age-out is the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) was deleted from tables associated with the remote entries because information timeliness interval had expired.
TLV Discards	Specifies the number of LLDP TLVs discarded for any reason by the LLDP agent on the corresponding port.
TLV Unknowns	Specifies the number of LLDP TLVs received on the local ports that were not recognized by the LLDP agent on the corresponding port.
TLV MED	Specifies the total number of LLDP-MED TLVs received on the local ports.
TLV 802.1	Specifies the total number of LLDP TLVs received on the local ports that are of type 802.1.
TLV 802.3	Specifies the total number of LLDP TLVs received on the local ports that are of type 802.3.

## View LLDP Local Device Information

➤ **To view LLDP local device information:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > LLDP > Local Device Information**.

LLDP Local Device Information	
:: LLDP Interface Selection	
Interface:	0/1
:: Local Device Information	
Chassis ID Subtype	MAC Address
Chassis ID	20:4E:7F:5B:8A:6C
Port ID Subtype	Local
Port ID	0/1
System Name	
System Description	M4100-12GF ProSafe 12-port Gigabit Fiber L2+ Managed Switch with PoE+, 10.15.17.33, B1.0.0.6
Port Description	
System Capabilities Supported	bridge, router
System Capabilities Enabled	bridge
Management Address Type	IPv4
Management Address	10.130.181.160

8. Use **Interface** to specify the list of all the ports on which LLDP - 802.1AB frames can be transmitted.

The following table describes the LLDP Local Device Information fields.

**Table 26. LLDP Local Device Information**

Field	Description
Chassis ID Subtype	Specifies the string that describes the source of the chassis identifier.
Chassis ID	Specifies the string value used to identify the chassis component associated with the local system.

**Table 26. LLDP Local Device Information**

Field	Description
Port ID Subtype	The string that describes the source of the port identifier.
Port ID	The string that describes the source of the port identifier.
System Name	The system name of the local system.
System Description	The description of the selected port associated with the local system.
Port Description	The description of the selected port associated with the local system.
System Capabilities Supported	The system capabilities of the local system.
System Capabilities Enabled	The system capabilities of the local system that are supported and enabled.
Management Address Type	The type of the management address.
Management Address	The advertised management address of the local system.

## View LLDP Remote Device Information

You can view information about remote devices connected to the port.

➤ **To view LLDP remote device information:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7.** Select **System > LLDP > Remote Device Information**.

**8.** Use **Interface** to select the local ports that can receive LLDP frames.

The following table describes the LLDP Remote Device Information fields.

**Table 27. LLDP remote device information**

Field	Description
Remote ID	The Remote ID.
Chassis ID	The chassis component associated with the remote system.
Chassis ID Subtype	The source of the chassis identifier.
Port ID	The port component associated with the remote system.
Port ID Subtype	The source of the port identifier.
System Name	The system name of the remote system.
System Description	The description of the given port associated with the remote system.
Port Description	The description of the given port associated with the remote system.
System Capabilities Supported	The system capabilities of the remote system.
System Capabilities Enabled	The system capabilities of the remote system that are supported and enabled.
Time to Live	The Time To Live value in seconds of the received remote entry.
Management Address Type	The type of the management address.
Management Address	<ul style="list-style-type: none"> <li>• Management Address specifies the advertised management address of the remote system.</li> <li>• Type specifies the type of the management address.</li> </ul>

## View LLDP Remote Device Inventory

➤ To view LLDP remote device inventory:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **System > LLDP > LLDP > Remote Device Inventory**.

LLDP Remote Device Inventory					
:: LLDP Remote Device Inventory					
<input type="text" value="Search By Interface"/> <input type="button" value="GO"/> <span style="float: right;">?</span>					
Port	Remote Device ID	Management Address	MAC Address	System Name	Remote Port ID
0/12	3	10.27.34.158	00-06-02-05-06-03		1/0/16

The following table describes the LLDP Remote Device Inventory fields.

**Table 28. LLDP remote device inventory**

Field	Description
Port	Specifies the list of all the ports on which LLDP frame is enabled.
Remote Device ID	Specifies the remote device ID.
Management Address	Specifies the advertised management address of the remote system.
MAC Address	Specifies the MAC address associated with the remote system.
System Name	Specifies model name of the remote device.
Remote Port ID	Specifies the port component associated with the remote system.

## Configure LLDP-MED Global Settings

You can specify LLDP-MED parameters that are applied to the switch.

➤ **To configure LLDP-MED global settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **System > LLDP > LLDP-MED > Global Configuration**.



The **Device Class** field displays the local device's MED classification. There are four different kinds of devices; three of them represent the actual end points (classified as Class I Generic [IP Communication Controller and so on], Class II Media [Conference Bridge and so on], Class III Communication [IP Telephone and so on]). The fourth device is a Network Connectivity Device, which is typically a LAN switch or router, IEEE 802.1 Bridge, IEEE 802.11 Wireless Access Point, and so on.

8. Use **Fast Start Repeat Count** to specify the number of LLDP PDUs that are transmitted when the protocol is enabled.

The range is from 1 to 10. The default value is 3.

## Configure the LLDP-MED Interface

➤ **To configure the LLDP-MED interface:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.

2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > LLDP > LLDP-MED > Interface Configuration**.

The screenshot shows a table titled "LLDP-MED Interface Configuration" with 13 columns. The columns are: Interface, Link Status, Med Status, Operational Status, Notification Status, MED Capabilities, Network Policy, Location Identification, Extended Power via MDI-PSE, Extended Power via MDI-PD, and Inventory Information. There are 13 rows, each representing a port (0/1 to 0/12). The "Link Status" column shows values like "Up" or "Down". The "Med Status" column shows values like "Enable" or "Disable". The "Operational Status" column shows values like "Disable" or "Enable". The "Notification Status" column shows values like "Enable" or "Disable". The "MED Capabilities" column shows values like "Enable" or "Disable". The "Network Policy" column shows values like "Enable" or "Disable". The "Location Identification" column shows values like "Enable" or "Disable". The "Extended Power via MDI-PSE" column shows values like "Disable" or "Enable". The "Extended Power via MDI-PD" column shows values like "Disable" or "Enable". The "Inventory Information" column shows values like "Enable" or "Disable".

The screen displays the link status (whether the port is up or down) and the operational status (whether LLDP-MED TLVs are transmitted or not on this interface).

8. Use **Go To Port** to enter the port in unit/slot/port format and click the **Go** button.  
The entry corresponding to the specified port is selected.
9. Use **Interface** to specify the list of ports on which LLDP-MED - 802.1AB can be configured.
10. Use **MED Status** to specify whether LLDP-MED mode is enabled or disabled on this interface.
11. Use **Notification Status** to specify the LLDP-MED topology notification mode of the interface.
12. Use **Transmit Type Length Values** to specify which optional type length values (TLVs) in the LLDP-MED are transmitted in the LLDP PDUs frames for the selected interface.

The following values are available:

- **MED Capabilities.** Transmit the capabilities TLV in LLDP frames.
- **Network Policy.** Transmit the network policy TLV in LLDP frames.
- **Location Identification.** Transmit the location TLV in LLDP frames.
- **Extended Power via MDI - PSE.** Transmit the extended PSE TLV in LLDP frames.
- **Extended Power via MDI - PD.** Transmit the extended PD TLV in LLDP frames.
- **Inventory Information.** To transmit the inventory TLV in LLDP frames.

## View LLDP-MED Local Device Information

➤ **To view LLDP-MED local device information:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **System > LLDP > LLDP-MED > Local Device Information.**

**LLDP-MED Local Device Information**

:: LLDP-MED Interface Selection					
Interface:	0/1				
:: Network Policies Information					
Media Application Type	VLAN ID	Priority	DSCP	Unknown Bit Status	Tagged Bit Status
:: Inventory Information					
Hardware Revision	0x0				
Firmware Revision	1				
Software Revision	10.14.19.6				
Serial Number	23				
Manufacturer Name	Broadcom Corporation				
Model Name	GSM7212P				
Asset Id					
:: Location Information					
Sub Type	Location Information				
Coordinate Based					
Civic Address					
ELIN					
:: Extended PoE					
Device Type	Power Source	Power Priority	Power Value		
PSE	Unknown	High	0 Watts		

8. Use **Interface** to select the ports on which LLDP-MED frames can be transmitted.

The following table describes the LLDP-MED Local Device Information fields.

**Table 29. LLDP-MED local device information**

Field	Description		
<b>Network Policy Information:</b> Specifies if the network policy TLV is present in the LLDP frames.			
	Media Application Type	The application type. Types of applications are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streammingvideo, and videosignalling.  Each application type that is received has a VLAN ID, priority, DSCP, tagged bit status, and unknown bit status. A port can receive one or many such application types.  Only when a network policy TLV was transmitted, is this information be displayed	
<b>Inventory:</b> Specifies if the inventory TLV is present in LLDP frames.			

**Table 29. LLDP-MED local device information (continued)**

Field	Description	
Local Device Information: Specifies if the local device information TLV is present in LLDP frames.	Hardware Revision	The hardware version.
	Firmware Revision	The Firmware version.
	Software Revision	The Software version.
	Serial Number	The serial number.
	Manufacturer Name	The manufacturers name.
	Model Name	The model name.
	Asset ID	The asset ID.
<b>Location Information: Specifies if the location TLV is present in LLDP frames.</b>		
Location Information	Sub Type	The type of location information.
	Location Information	The location information as a string for a given type of location ID.

## View LLDP-MED Remote Device Information

➤ **To view LLDP-MED remote device information:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **System > LLDP > LLDP-MED > Remote Device Information**.

The screenshot displays the 'LLDP-MED Remote Device Information' configuration page. It includes several sections:

- LLDP-MED Interface Selection:** Shows 'Interface' set to 0/1 and 'Remote ID' set to 1.
- Capability Information:** Lists 'Supported Capabilities', 'Enabled Capabilities', and 'Device Class'.
- Network Policies Information:** A table with columns: Media Application Type, VLAN ID, Priority, DSCP, Unknown Bit Status, and Tagged Bit Status.
- Inventory Information:** Lists hardware, firmware, software, serial number, manufacturer, model name, and asset id.
- Location Information:** Sub Type and Location Information.
- Extended PoE:** Device Type, Power Source, Power Priority, and Power Value.

8. Use **Interface** to select the ports on which LLDP-MED is enabled.

The following table describes the LLDP-MED Remote Device Information fields.

**Table 30. LLDP-MED remote device information**

Field	Description	
<b>Capability Information:</b> Specifies the supported and enabled capabilities that were received in MED TLV on this port.		
	Supported Capabilities	Specifies supported capabilities that were received in MED TLV on this port.
	Enabled Capabilities	Specifies enabled capabilities that were received in MED TLV on this port.
	Device Class	The device class as advertised by the device remotely connected to the port.
<b>Network Policy Information:</b> Specifies if the network policy TLV is received in the LLDP frames on this port.		

**Table 30. LLDP-MED remote device information (continued)**

Field	Description
Media Application Type	The application type. Types of applications are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streamingvideo, and videoesignalling. Each application type that is received has the VLAN ID, priority, DSCP, tagged bit status, and unknown bit status. A port can receive one or many such application types. Only when a network policy TLV was received on this port, is this information displayed.
	VLAN Id
	Priority
	DSCP
	Unknown Bit Status
	Tagged Bit Status
<b>Inventory Information: Specifies if the inventory TLV is received in LLDP frames on this port.</b>	
Hardware Revision Firmware Revision Software Revision Serial Number Manufacturer Name Model Name Asset ID	The hardware version of the remote device.
	The Firmware version of the remote device.
	The Software version of the remote device.
	The serial number of the remote device.
	The manufacturers name of the remote device.
	The model name of the remote device.
	The asset ID of the remote device.
<b>Location Information: Specifies if the location TLV is received in LLDP frames on this port.</b>	
Sub Type Location Information	The type of location information.
	The location information as a string for given type of location ID.
<b>Extended POE: Specifies if the remote device is a PoE device.</b>	
Device Type	The remote device's PoE device type connected to this port.
<b>Extended POE PSE: Specifies if the extended PSE TLV is received in LLDP frame on this port.</b>	
Available Source Priority	The remote port's PSE power value in tenths of watts.
	The remote port's PSE power source.
	The remote port's PSE power priority.
<b>Extended POE PD: Specifies if the extended PD TLV is received in LLDP frame on this port.</b>	

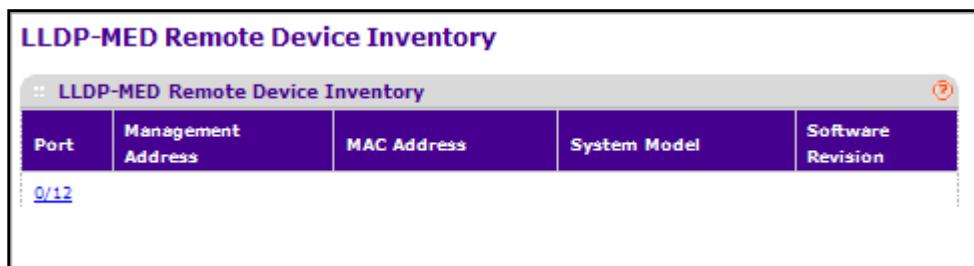
**Table 30. LLDP-MED remote device information (continued)**

Field	Description
Required	The remote port's PD power requirement.
	The remote port's PD power source.
	The remote port's PD power priority.

## View LLDP-MED Remote Device Inventory

➤ **To view LLDP-MED remote device inventory:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **System > LLDP > LLDP-MED > Remote Device Inventory**.



The following table describes the LLDP-MED Remote Device Inventory fields.

**Table 31. LLDP-MED remote device inventory**

Field	Definition
Port	The list of all the ports on which LLDP-MED is enabled.
Management Address	The advertised management address of the remote system.

**Table 31. LLDP-MED remote device inventory**

Field	Definition
MAC Address	The MAC address associated with the remote system.
System Model	The model name of the remote device.
Software Revision	The software version of the remote device.

## ISDP Settings Overview

You can configure ISDP global settings and the ISDP interface.

### Configure ISDP Global Settings

➤ **To configure ISDP global settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **System > ISDP > Basic > Global Configuration**.

Global Configuration	
<b>Admin Mode</b>	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
<b>Timer</b>	30 (5 to 254 secs)
<b>Hold Time</b>	180 (10 to 255 secs)
<b>Version 2 Advertisements</b>	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
<b>Neighbors table last time changed</b>	2 Days 01:15:07
<b>Device ID</b>	2ER1084000005
<b>Device ID Format Capability</b>	Serial Number, Host Name
<b>Device ID Format</b>	Serial Number

8. Use **Admin Mode** to specify whether the ISDP service is to be Enabled or Disabled.  
The default value is Enabled.
9. Use **Timer** to specify the period of time between sending new ISDP packets.  
The range is 5 to 254 seconds. The default value is 30 seconds.
10. Use **Hold Time** to specify the hold time for ISDP packets that the switch transmits.  
The hold time specifies how long a receiving device should store information sent in the ISDP packet before discarding it. The range 10 to 255 seconds. The default value is 180 seconds.
11. Select the **Version 2 Advertisements** **Disable** or **Enable** radio button.  
This enables or disables the sending of ISDP version 2 packets from the device. The default value is Enable.
12. Click the **APPLY** button.  
Your settings are saved.

The following table describes the ISDP Basic Global Configuration fields.

**Table 32. ISDP Basic Global Configuration**

Field	Description
Neighbors table last time changed	Specifies the last time the neighbors table changed.
Device ID	Displays the device ID of this switch.
Device ID format capability	Displays the device ID format capability.
Device ID format	Displays the device ID format.

## Configure Advanced Global ISDP Settings

➤ **To configure global ISDP settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **System > ISDP > Advanced > Global Configuration**.

The screenshot shows the 'Global Configuration' page with the following settings:

- Admin Mode:** Radio button selected for 'Enable'.
- Timer:** Value set to 30 (5 to 254 secs).
- Hold Time:** Value set to 180 (10 to 255 secs).
- Version 2 Advertisements:** Radio button selected for 'Enable'.
- Neighbors table last time changed:** Value set to 2 Days 01:15:37.
- Device ID:** Value set to 2ER1084000005.
- Device ID Format Capability:** Value set to Serial Number, Host Name.
- Device ID Format:** Value set to Serial Number.

- Select the Admin Mode **Enable** radio button.

The default value is Enable.

- In the **Timer** field, specify the period of time between sending new ISDP packets.

The range is 5 to 254 seconds. The default value is 30 seconds.

- In the **Hold Time** field, specify the hold time for ISDP packets that the switch transmits.

The hold time specifies how long a receiving device should store information sent in the ISDP packet before discarding it. The range 10 to 255 seconds. The default value is 180 seconds.

- Select the **Version 2 Advertisements Disable or Enable** radio button.

This setting controls the sending of ISDP version 2 packets from the device. The default value is Enable.

- Click the **APPLY** button.

Your settings are saved.

The following table describes the ISDP Advanced Global Configuration fields.

**Table 33. ISDP Advanced Global Configuration**

Field	Description
Neighbors table last time changed	Displays when the Neighbors table last changed.
Device ID	Displays the device ID of this switch.
Device ID format capability	Displays the device ID format capability.
Device ID format	Displays the device ID format.

## Configure the ISDP Interface

➤ **To configure the ISDP Interface:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **System > ISDP > Advanced > Interface Configuration.**

The screenshot shows a table titled "ISDP Interface Configuration" with the sub-section "Interface Configuration". The table has two sections: "1 All" at the top and "1 All" at the bottom. The columns are "Port" and "Admin Mode". The "Port" column lists ports 0/1 through 0/12. The "Admin Mode" column shows "Enable" for all ports. There are "Go To Port" and "GO" buttons at the top and bottom of each section.

Port	Admin Mode
0/1	Enable
0/2	Enable
0/3	Enable
0/4	Enable
0/5	Enable
0/6	Enable
0/7	Enable
0/8	Enable
0/9	Enable
0/10	Enable
0/11	Enable
0/12	Enable

8. Select the check box for the port on which the admin mode is configured.
9. In the **Admin Mode** list, select **Enable** or **Disable**.  
The default value is **Enable**.
10. Click the **APPLY** button.  
Your settings are saved.

## View ISDP Neighbors

➤ **To view ISDP neighbors:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

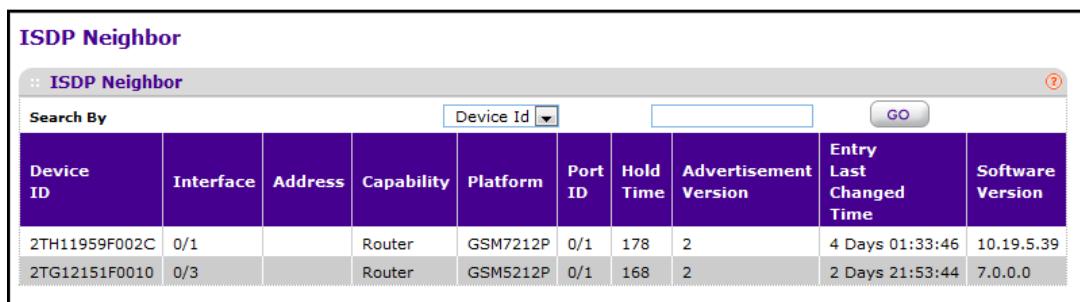
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > ISDP > Advanced > Neighbor**.



The screenshot shows a table titled "ISDP Neighbor" with the sub-section "ISDP Neighbor". The table has columns for Device ID, Interface, Address, Capability, Platform, Port ID, Hold Time, Advertisement Version, Entry Last Changed Time, and Software Version. Two rows of data are displayed:

Device ID	Interface	Address	Capability	Platform	Port ID	Hold Time	Advertisement Version	Entry Last Changed Time	Software Version
2TH11959F002C	0/1		Router	GSM7212P	0/1	178	2	4 Days 01:33:46	10.19.5.39
2TG12151F0010	0/3		Router	GSM5212P	0/1	168	2	2 Days 21:53:44	7.0.0.0

The following table describes the ISDP Neighbor fields.

**Table 34. ISDP Neighbor**

Field	Description
Device ID	The device ID of the ISDP neighbor.
Interface	The interface on which the neighbor is discovered.
Address	Displays the address of the neighbor.

**Table 34. ISDP Neighbor**

Field	Description
Capability	Displays the capability of the neighbor. These are supported: <ul style="list-style-type: none"> <li>• Router</li> <li>• Trans Bridge</li> <li>• Source Route</li> <li>• Switch</li> <li>• Host</li> <li>• IGMP</li> <li>• Repeater</li> </ul>
Platform	Display the model type of the neighbor. 0 to 32
Port ID	Display the port ID of the neighbor.
Hold Time	Displays the hold time for ISDP packets that the neighbor transmits.
Advertisement Version	Displays the ISDP version sending from the neighbor.
Entry Last Changed Time	Displays the time since last entry was changed.
Software Version	Displays the software version of the neighbor.

## View ISDP Statistics

➤ **To view ISDP statistics:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7. Select System > ISDP > Advanced > Statistics.**

ISDP Statistics	
ISDP Statistics	
ISDP Packets Received	60333
ISDP Packets Transmitted	13196
ISDPv1 Packets Received	0
ISDPv1 Packets Transmitted	0
ISDPv2 Packets Received	60333
ISDPv2 Packets Transmitted	13196
ISDP Bad Header	0
ISDP Checksum Error	0
ISDP Transmission Failure	0
ISDP Invalid Format	0
ISDP Table Full	0
ISDP IP Address Table Full	0

The following table describes the ISDP Statistics fields.

**Table 35. ISDP statistics**

Field	Description
ISDP Packets Received	Displays the ISDP packets received including ISDPv1 and ISDPv2 packets.
ISDP Packets Transmitted	Displays the ISDP packets transmitted including ISDPv1 and ISDPv2 packets.
ISDPv1 Packets Received	Displays the ISDPv1 packets received.
ISDPv1 Packets Transmitted	Displays the ISDPv1 packets transmitted.
ISDPv2 Packets Received	Displays the ISDPv2 packets received.
ISDPv2 Packets Transmitted	Displays the ISDPv2 packets transmitted.
ISDP Bad Header	Displays the ISDP bad packets received.
ISDP Checksum Error	Displays the number of the checksum error.
ISDP Transmission Failure	Displays the number of the transmission failure.
ISDP Invalid Format	Displays the number of the invalid format ISDP packets received.
ISDP Table Full	Displays the table size of the ISDP table.
ISDP Ip Address Table Full	Displays the table size of the ISDP IP address table.

## Configure Timers

You can configure global timer settings and set up timer schedules.

### Configure the Global Timer Settings

➤ **To configure the timer global settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

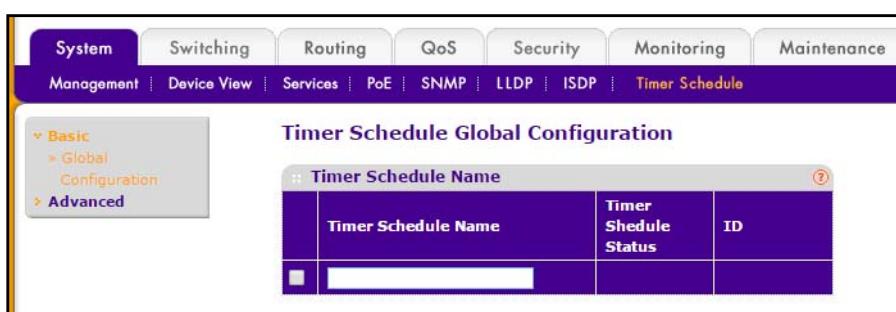
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **System > Timer Schedule > Basic > Global Configuration**.



The screen displays the timer schedule status as active or inactive.

8. In the **Timer Schedule Name** field, type the name of a timer schedule.
9. To add a new timer schedule, click the **ADD** button.

Your change takes effect immediately.

10. To delete a timer schedule, select it and click the **DELETE** button.

Your change takes effect immediately.

## Configure the Timer Schedule

- To configure the timer schedule:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **System > Timer Schedule > Advanced > Schedule Configuration**.

8. To select a timer schedule or create a new schedule, specify the following settings:
  - **Timer Schedule Name**.
  - **Timer Schedule Type (Absolute or Periodic)**.
  - **Timer Schedule Entry**.
9. To configure the timer schedule, complete these fields:
  - **Time Start**. The time when the schedule operation is started. This field is the required field. If no time is specified, the schedule does not start running.
  - **Time End**. The time of the day when the schedule operation is terminated.
  - **Date Start**. The schedule start date. If no date is specified, the schedule starts running immediately.
  - **Date Stop**. The schedule termination date. If no end date selected, the schedule operates indefinitely.

- 10.** Use the **Recurrence Pattern** to show with what period the event repeats. If recurrence is not needed (a timer schedule should be triggered just once), then set **Date Stop** as equal to **Date Start**. The following recurrence values are available:

- **Daily.** The timer schedule works with daily recurrence.

The Every WeekDay selection means that the schedule is triggered every day from Monday to Friday. The Every Day(s) selection means that the schedule is triggered every defined number of days. If the number of days is not specified, then the schedule is triggered every day.

- **Weekly.** The timer schedule works with weekly recurrence.

- **Every Week (s).** Define the number of weeks when the schedule is triggered. If number of weeks is not specified, then the schedule is triggered every week.
- **WeekDay.** Specify the days of week when the schedule operates.

- **Monthly.** The timer schedule works with monthly recurrence.

Show the day of the month when the schedule is triggered. The Every Month(s) selection means that the schedule is triggered every defined number of months.

- 11.** Click the **APPLY** button.

The updated configuration is sent to the switch and takes effect immediately.

# Configure Switching Information

3

This chapter covers the following topics:

- *VLAN Overview*
- *Auto-VoIP Overview*
- *Spanning Tree Protocol Overview*
- *Configure Multicast*
- *Configure Multicast*
- *Configure MLD Snooping*
- *Configure MVR*
- *Manage MAC Addresses*
- *Configure Port Settings*
- *Link Aggregation Group Overview*

## VLAN Overview

Adding Virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical segments, which provides better administration, security, and management of multicast traffic.

By default, all ports on the switch are in the same broadcast domain. VLANs electronically separate ports on the same switch into separate broadcast domains so that broadcast packets are not sent to all the ports on a single switch. When you use a VLAN, users can be grouped by logical function instead of physical location.

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station can omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet can either reject it or insert a tag using its default VLAN ID. A given port can handle traffic for more than one VLAN, but it can support only one default VLAN ID.

## Configure a Basic VLAN

You can define VLAN groups stored in the VLAN membership table. Each switch in the managed switch family supports up to 1024 VLANs. Two VLANs are created by default, VLAN 1 and VLAN 2:

- VLAN 1 is the default VLAN of which all ports are members.
- VLAN 2 is the default Auto VoIP VLAN.

➤ **To configure a basic VLAN:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > VLAN > Basic > VLAN Configuration**.

The screenshot shows the 'VLAN Configuration' page with the following sections:

- Reset:** Contains a 'Reset Configuration' checkbox.
- Internal VLAN Configuration:** Shows an 'Internal VLAN Allocation Base' set to 4093 and an 'Internal VLAN Allocation Policy' set to Ascending.
- VLAN Configuration:** A table listing VLANs with columns: VLAN ID, VLAN Name, VLAN Type, and Make Static. The table contains two rows:
 

	VLAN ID	VLAN Name	VLAN Type	Make Static
<input checked="" type="checkbox"/>	1	default	Default	Disable
<input checked="" type="checkbox"/>	2		Dynamic (AUTO VoIP)	Disable

8. Specify the **Reset Configuration** setting.

If you select this check box and click the **APPLY** button, all VLAN configuration parameters are reset to their factory default values. Also, all VLANs except for the default VLAN are deleted. The factory default values are as follows:

- All ports are assigned to the default VLAN of 1.
- All ports are configured with a PVID of 1.
- All ports are configured to an Acceptable Frame Types value of Admit All Frames.
- All ports are configured with ingress filtering disabled.
- All ports are configured to transmit only untagged frames.
- GVRP is disabled on all ports and all dynamic entries are cleared.

## Configure an Internal VLAN

This section displays the allocation base and the allocation mode of internal VLANs. The internal VLAN is reserved by a port-based routing interface and is invisible to the end user. Once these internal VLANs are allocated by port-based routing interface, they cannot be assigned to a routing VLAN interface.

➤ **To configure an internal VLAN:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **Switching > VLAN > Basic > VLAN Configuration**.

The screenshot shows the 'VLAN Configuration' page with two main sections:

- Internal VLAN Configuration:** Contains fields for 'Internal VLAN Allocation Base' (set to 4093) and 'Internal VLAN Allocation Policy' (set to Ascending).
- VLAN Configuration:** A table with columns: VLAN ID, VLAN Name, VLAN Type, and Make Static. It lists two entries:
 

	VLAN ID	VLAN Name	VLAN Type	Make Static
1	1	default	Default	Disable
2	2		Dynamic (AUTO VoIP)	Disable

- Use **Internal VLAN Allocation Base** to specify the VLAN allocation base for the routing interface.

The default base of the internal VLAN is 1 to 4093.

- Use the optional **Internal VLAN Allocation Policy** field to specify a policy for the internal VLAN allocation.

Two policies are supported: ascending and descending.

## Add a VLAN

➤ **To add a VLAN:**

- Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
- Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
- Launch a web browser.
- Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

- Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

**7.** Select **Switching > VLAN > Basic > VLAN Configuration**.

The screenshot shows the 'VLAN Configuration' page. At the top is a 'Reset' section with a 'Reset Configuration' button. Below it is the 'Internal VLAN Configuration' section, which includes an 'Internal VLAN Allocation Base' field set to 4093 and an 'Internal VLAN Allocation Policy' radio button group where 'Ascending' is selected. The main area is the 'VLAN Configuration' table:

	VLAN ID	VLAN Name	VLAN Type	Make Static
<input type="checkbox"/>	1	default	Default	Disable
<input type="checkbox"/>	2		Dynamic (AUTO VoIP)	Disable

**8.** Use **VLAN ID** to specify the VLAN Identifier for the new VLAN.

The range of the VLAN ID is 1 to 4093.

**9.** Use the optional **VLAN Name** field to specify a name for the VLAN.

It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of Default.

**10.** To add a new VLAN to the switch, click the **ADD** button.

**11.** To delete a selected VLAN from the switch, click the **DELETE** button.

The following table describes the nonconfigurable information displayed on the screen.

**Table 36. VLAN Configuration**

Field	Description
VLAN Type	This field identifies the type of the VLAN that you are configuring. You cannot change the type of the default VLAN (VLAN ID = 1): it is always type 'Default'. When you create a VLAN, using this screen, its type is always Static. A VLAN that is created by GVRP registration initially has a type of Dynamic. When configuring a dynamic VLAN, you can change its type to 'Static'.

## Reset VLAN Configuration

➤ **To reset VLAN configuration:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > VLAN > Advanced > VLAN Configuration**.

The screenshot shows the 'VLAN Configuration' page with three main sections:

- Internal VLAN Configuration:** Shows 'Internal VLAN Allocation Base' set to 4093 and 'Internal VLAN Allocation Policy' set to Ascending.
- VLAN Configuration:** A table with columns: VLAN ID, VLAN Name, VLAN Type, and Make Static. It shows one entry: VLAN ID 1, VLAN Name default, VLAN Type Default, and Make Static set to Disable.

8. Select or clear the **Reset Configuration** check box.

If you select this check box and confirm your selection on the next screen, all VLAN configuration parameters are reset to their factory default values. Also, all VLANs except for the default VLAN are deleted. The factory default values are as follows:

- All ports are assigned to the default VLAN of 1.
- All ports are configured with a PVID of 1.
- All ports are configured to an Acceptable Frame Types value of Admit All Frames.
- All ports are configured with ingress filtering disabled.
- All ports are configured to transmit only untagged frames.
- GVRP is disabled on all ports and all dynamic entries are cleared.

## Configure Internal VLAN Settings

You can view the allocation base and the allocation mode of internal VLAN. The internal VLAN is reserved by port-based routing interface and invisible to the end user. Once these internal VLANs are allocated by port-based routing interface, they cannot be assigned to a routing VLAN interface.

➤ **To configure internal VLAN settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.

2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > VLAN > Advanced > VLAN Configuration**.

The screenshot shows the 'VLAN Configuration' page with two main sections:

- Internal VLAN Configuration:** Contains fields for 'Internal VLAN Allocation Base' (set to 4093) and 'Internal VLAN Allocation Policy' (set to Ascending).
- VLAN Configuration:** A table with columns: VLAN ID, VLAN Name, VLAN Type, and Make Static. It shows one entry: VLAN ID 1, VLAN Name default, VLAN Type Default, and Make Static set to Disable.

8. Use **Internal VLAN Allocation Base** to specify the VLAN allocation base for the routing interface.

The default base of the internal VLAN is 1 to 4093.

9. Use the optional **Internal VLAN Allocation Policy** field to specify a policy for the internal VLAN allocation.

There are two policies supported: ascending and descending.

## Configure VLAN Trunking

You can configure switchport mode settings on interfaces. The switchport mode defines the purpose of the port based on the type of device it connects to and constrains the VLAN configuration of the port accordingly. Assigning the appropriate switchport mode helps simplify VLAN configuration and minimize errors.

### ➤ To configure VLAN Trunking:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.

2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > VLAN > Advanced > VLAN Trunking Configuration**.

Interface	Switchport Mode	Native VLAN Tagging	Access VLAN ID	Native VLAN ID	Trunk Allowed VLANs
0/1	General	Disable	1	1	1-4093
0/2	General	Disable	1	1	1-4093
0/3	General	Disable	1	1	1-4093

8. Select the interface to configure:
  - Select the **Unit ID** field to display physical port information for the selected unit.
  - Use **LAG** to display LAG only.
  - Use **All** to display all physical ports.
  - Use **Go To Interface** to select an interface by entering its number.
  - Select the **Interface** check box.
9. Select from the menu to configure the switchport mode of the interface as one of the following:
  - **Access** mode is suitable for ports connected to end stations or end users. Access ports participate only in one VLAN. They accept both tagged and untagged packets, but always transmit untagged packets.
  - **General** mode enables custom configuration of a port. The user configures the General port VLAN attributes, such as membership, PVID, tagging, ingress filter, and so on, using the settings on the Port Configuration screen. By default, all ports are initially configured in **General** mode.
  - **Trunk** mode is intended for ports that are connected to other switches. Trunk ports can participate in multiple VLANs and accept both tagged and untagged packets.
10. Select from the menu to configure the **Access VLAN ID**.

This is the access VLAN for the port, and is valid only when the port switchport mode is **Access**.

**11.** Select from the menu to configure the **Native VLAN ID**.

This is the native VLAN for the port, and is valid only when the port switchport mode is **Trunk**.

**12.** Configure the **Trunk Allowed VLANs**, the set of VLANs of which the port can be a member when configured in **Trunk** mode.

By default, this list contains all possible VLANs, even if they are not yet created. VLAN IDs are in the range 1 to 4093. Use a hyphen (-) to specify a range, or a comma (,) to separate VLAN IDs in a list. Spaces are not permitted. A zero value clears allowed VLANs. An **All** value sets all VLANs in the range 1 to 4093.

**13.** Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See *Save Configuration* on page 405.

The following table describes the nonconfigurable data that the Switchport Configuration screen displays.

**Table 37. Switchport Mode Configuration**

Field	Description
Native VLAN Tagging	<ul style="list-style-type: none"> <li>When VLAN tagging is enabled, if the trunk port receives untagged frames, it forwards them on the native VLAN with no VLAN tag.</li> <li>When VLAN tagging is disabled, if the trunk port receives untagged frames, it includes the native VLAN ID in the VLAN tag when forwarding.</li> </ul>

## Configure VLAN Membership

➤ **To configure VLAN membership:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **Switching > VLAN > Advanced > VLAN Membership**.

VLAN Membership	
VLAN ID	1
Group Operation	
Untag All	
VLAN Name	default
VLAN Type	Default
Unit 1	
Port	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
	U U
25 26 27 28	U U U U
Unit 2	
LAG	

- Use **VLAN ID** to select the VLAN ID.
- Use **Group Operation** to select all the ports and configure them:
  - Untag All**. Select all the ports on which all frames transmitted for this VLAN are untagged. All the ports are included in the VLAN.
  - Tag All**. Select the ports on which all frames transmitted for this VLAN are tagged. All the ports are included in the VLAN.
  - Remove All**. Select all the ports that can be dynamically registered in this VLAN through GVRP. This selection excludes all ports from the selected VLAN.
- Use **Port List** to add the ports you selected to this VLAN.

Each port has three modes:

- T (Tagged)**. Select the ports on which all frames transmitted for this VLAN are tagged. The ports that are selected are included in the VLAN.
- U (Untagged)**. Select the ports on which all frames transmitted for this VLAN are untagged. The ports that are selected are included in the VLAN.
- BLANK (Autodetect)**. Select the ports that can be dynamically registered in this VLAN through GVRP. This selection has the effect of excluding a port from the selected VLAN.

**Table 38. VLAN Membership**

Field	Definition
VLAN Name	The name for the VLAN that you selected. It can be up to 32 alphanumeric characters long, including blanks. VLAN ID 1 always has a name of Default.
VLAN Type	The type of the VLAN you selected. The VLAN type: <ul style="list-style-type: none"><li>• <b>Default</b> (VLAN ID = 1). Always present</li><li>• <b>Static</b>. A VLAN you configured</li><li>• <b>Dynamic</b>. A VLAN created by GVRP registration that you did not convert to static, and that GVRP can therefore remove</li></ul>

## View VLAN Status

You can view the status of all currently configured VLANs.

➤ **To view the VLAN status:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > VLAN > Advanced > VLAN Status**.

VLAN Status				
:: VLAN Status				
VLAN ID	VLAN Name	VLAN Type	Routing Interface	Member Ports
1	default	Default		0/1 - 0/12, lag 1 - lag 12
2	Auto VoIP	AUTO VoIP		0/1 - 0/12, lag 1 - lag 12

The following table describes the nonconfigurable information displayed on the screen.

**Table 39. Advanced VLAN Status**

Field	Definition
VLAN ID	The VLAN Identifier (VID) of the VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	The name of the VLAN. VLAN ID 1 is always named ‘Default’.
VLAN Type	The type of the VLAN you selected. The VLAN type: <ul style="list-style-type: none"> <li>• <b>Default</b> (VLAN ID = 1). Always present</li> <li>• <b>Static</b>. A VLAN you configured</li> <li>• <b>Dynamic</b>. A VLAN created by GVRP registration that you did not convert to static, and that GVRP can therefore remove</li> </ul>
Routing Interface	The interface associated with the VLAN, in the case that VLAN routing is configured for this VLAN.
Member Ports	The ports that are included in the VLAN.

## Configure Port PVID

The Port PVID Configuration screen lets you assign a port VLAN ID (PVID) to an interface. There are certain requirements for a PVID:

- All ports must use a defined PVID.
- If no other value is specified, the default VLAN PVID is used.
- To change the ports default PVID, you must first create a VLAN that includes the port as a member.
- Use the Port VLAN ID (PVID) Configuration screen to configure a virtual LAN on a port.

➤ **To configure port PVID:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7. Select **Switching > VLAN > Advanced > Port PVID Configuration**.**

<b>Port PVID Configuration</b>							
:: PVID Configuration			Go To Interface <input type="text"/> GO				
	1	2	LAGS	All			
	Interface	Configured PVID	Current PVID	Acceptable Frame Types	Configured Ingress Filtering	Current Ingress Filtering	Port Priority
<input type="checkbox"/>	1/0/1	1	1	Admit All	Disable	Disable	0
<input type="checkbox"/>	1/0/2	1	1	Admit All	Disable	Disable	0
<input type="checkbox"/>	1/0/3	1	1	Admit All	Disable	Disable	0
<input type="checkbox"/>	1/0/4	1	1	Admit All	Disable	Disable	0
<input type="checkbox"/>	1/0/5	1	1	Admit All	Disable	Disable	0
<input type="checkbox"/>	1/0/6	1	1	Admit All	Disable	Disable	0
<input type="checkbox"/>	1/0/7	1	1	Admit All	Disable	Disable	0
<input type="checkbox"/>	1/0/8	1	1	Admit All	Disable	Disable	0
<input type="checkbox"/>	1/0/9	1	1	Admit All	Disable	Disable	0

**8. Click **ALL** to display information for all physical ports and LAGs.**

**9. Select the check box next to the interfaces to configure.**

You can select multiple interfaces to apply the same setting to the selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.

**10. Use **Interface** to select the interface.**

**11. Use **PVID** to specify the VLAN ID you want assigned to untagged or priority tagged frames received on this port.**

The factory default is 1.

**12. In the **Acceptable Frame Types** field, select **VLAN only** or **Admit All**.**

This specifies the types of frames that can be received on this port.

- **VLAN only.** Untagged frames or priority tagged frames received on this port are discarded.
- **Admit All.** Untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.

**13. Specify the **Ingress Filtering** setting:**

- When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the port VLAN ID specified for the port that received this frame.
- When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.

**14. Use **Port Priority** to specify the default 802.1p priority assigned to untagged packets arriving at the port.**

The possible value is from 0 to 7.

## Configure a MAC-Based VLAN Group

The MAC-based VLAN feature allows incoming untagged packets to be assigned to a VLAN and thus classifies traffic based on the source MAC address of the packet.

You define MAC to VLAN mapping by configuring an entry in the MAC to VLAN table. An entry is specified through a source MAC address and the desired VLAN ID. The MAC to VLAN configurations are shared across all ports of the device (for example, system-wide table has MAC address to VLAN ID mappings).

When untagged or priority tagged packets arrive at the switch and entries exist in the MAC to VLAN table, the source MAC address of the packet is looked up. If an entry is found, the corresponding VLAN ID is assigned to the packet. If the packet is already priority tagged, it maintains this value; otherwise the priority is set to zero. The assigned VLAN ID is verified against the VLAN table. If the VLAN is valid ingress processing on the packet continues; otherwise, the packet is dropped. This implies that the user is allowed to configure a MAC address mapping to a VLAN that has not been created on the system.

➤ **Configure a MAC-based VLAN group:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > VLAN > Advanced > MAC Based VLAN**.

Mac Based VLAN Group Configuration		
:: MAC Based VLAN Configuration		
	MAC Address	VLAN ID
<input type="checkbox"/>	00:00:00:00:00:00	
<input type="checkbox"/>	D4:B2:9D:3C:90:43	150

8. The **MAC Address** fields display valid MAC addresses that can be bound to a VLAN ID.

These fields are configurable only when a MAC Based VLAN is created.

9. Use **VLAN ID** to specify a VLAN ID in the range of 1 to 4093.
10. To add a MAC address to VLAN mapping, click the **ADD** button.
11. To delete a MAC address to VLAN mapping, click the **DELETE** button.

## Configure a Protocol-Based VLAN Group

You can use a protocol-based VLAN to define filtering criteria for untagged packets. By default, if you do not configure any port- (IEEE 802.1Q) or protocol-based VLANs, untagged packets are assigned to VLAN 1. You can override this behavior by defining either port-based VLANs or protocol-based VLANs, or both. Tagged packets are always handled according to the IEEE 802.1Q standard, and are not included in protocol-based VLANs.

If you assign a port to a protocol-based VLAN for a specific protocol, untagged frames received on that port for that protocol are assigned the protocol-based VLAN ID. Untagged frames received on the port for other protocols are assigned the Port VLAN ID, either the default PVID (1) or a PVID that you specifically assigned to the port using the Port VLAN Configuration screen.

You define a protocol-based VLAN by creating a group. Each group has a one-to-one relationship with a VLAN ID, can include one to three protocol definitions, and can include multiple ports. When you create a group, you choose a name and a Group ID is assigned automatically.

➤ **To configure a protocol-based VLAN group:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7. Select **Switching > VLAN > Advanced > Protocol Based VLAN Group Configuration.****

<b>Protocol Based VLAN Group Configuration</b>					
:: <b>Protocol Based VLAN Group Configuration</b>					
	<b>Group ID</b>	<b>Group Name</b>	<b>Protocol</b>	<b>VLAN ID</b>	<b>Ports</b>
<input type="checkbox"/>	1	IPX	IPX	150	1/0/7 - 1/0/9

**8. Use **Group Name** to assign a name to a new group.**

You can enter up to 16 characters.

**9. Use **Protocol(s)** to select the protocols to be associated with the group.**

There are three configurable protocols: IP, IPX, ARP.

- **IP.** IP is a network layer protocol that provides a connectionless service for the delivery of data.
- **ARP.** Address Resolution Protocol (ARP) is a low-level protocol that dynamically maps network layer addresses to physical medium access control (MAC) addresses.
- **IPX.** The Internetwork Packet Exchange (IPX) is a connectionless datagram network-layer protocol that forwards data over a network.

**10. Use **VLAN ID** to select the VLAN ID.**

It can be any number in the range of 1 to 4093. All the ports in the group assign this VLAN ID to untagged packets received for the protocols you included in this group.

**11. To add a new protocol-based VLAN group to the switch, click the **ADD** button.**

**12. To remove the protocol-based VLAN group identified by the value in the Group ID field, click the **DELETE** button.**

The following table describes the nonconfigurable information displayed on the screen.

**Table 40. Protocol-Based VLAN Group Configuration**

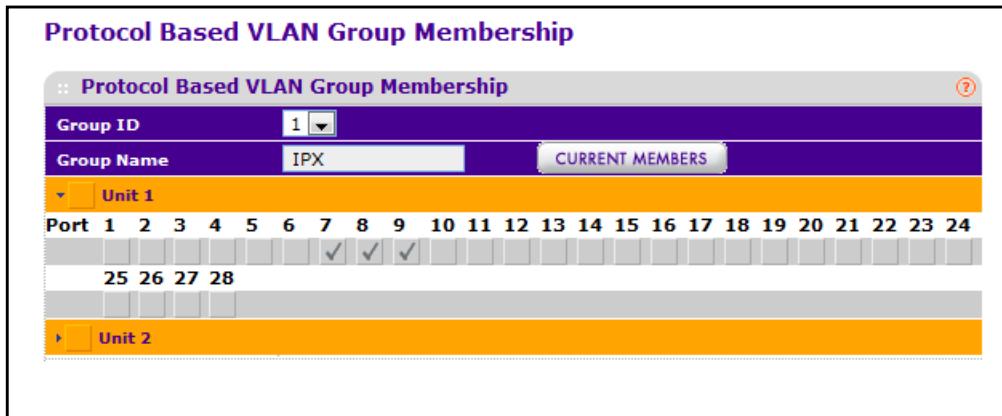
<b>Field</b>	<b>Description</b>
Group ID	A number used to identify the group created by the user. Group IDs are automatically assigned when a group is created by the user.
Ports	Display all the member ports that belong to the group.

## Configure Protocol-Based VLAN Group Membership

➤ **To display the protocol-based VLAN group membership:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.

3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
- The Login screen displays.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Switching > VLAN > Advanced > Protocol Based VLAN Group Membership**.



8. Use **Group ID** to select the protocol-based VLAN group ID.
9. Use **Port List** to add the ports you selected to this protocol-based VLAN group.  
A given interface can belong to only one group for a given protocol. If you already added a port to a group for IP, you cannot add it to another group that also includes IP, although you could add it to a new group for IPX.

The following table describes the nonconfigurable information displayed on the screen.

**Table 41. Protocol-Based VLAN Group Membership**

Field	Description
Group Name	This field identifies the name for the protocol-based VLAN you selected. It can be up to 32 alphanumeric characters long, including blanks.
Current Members	This button can be click to show the current numbers in the selected protocol-based VLAN group.

## Configure an IP Subnet-Based VLAN

IP Subnet to VLAN mapping is defined by configuring an entry in the IP Subnet to VLAN table. An entry is specified through a source IP address, network mask, and the desired VLAN ID. The IP subnet to VLAN configurations are shared across all ports of the device.

➤ **To configure an IP subnet-based VLAN:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Switching > VLAN > Advanced > IP Subnet Based VLAN**.

IP Subnet Based VLAN Configuration			
:: IP Subnet Based VLAN Configuration			
	IP Address	Subnet Mask	VLAN ID
<input type="checkbox"/>			
<input type="checkbox"/>	192.168.10.0	255.255.255.0	200

8. Use **IP Address** to specify a valid IP address bound to the VLAN ID.  
Enter the IP address in dotted decimal notation.
9. Use **Subnet Mask** to specify a valid subnet mask of the IP address.  
Enter the subnet mask in dotted decimal notation.
10. Use **VLAN ID** to specify a VLAN ID in the range of (1 to 4093).
11. To add a new IP subnet-based VLAN, click the **ADD** button.
12. To delete the IP subnet-based VLAN selected, click the **DELETE** button.

## Configure Port DVLAN

➤ **To configure port DVLAN:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Switching > VLAN > Advanced > Port DVLAN Configuration**.

The screenshot shows the 'Port DVLAN Configuration' interface. It has two main sections: 'Global Configuration' and 'DVLAN Configuration'. In the 'Global Configuration' section, the 'Global EtherType' dropdown is set to '802.1Q Tag'. In the 'DVLAN Configuration' section, there are tabs for '1', '2', 'LAGS', and 'All'. The 'All' tab is selected. It contains a table with columns 'Interface' and 'Admin Mode'. The table lists ports 1/0/1 through 1/0/6, all of which have their 'Admin Mode' set to 'Disable'. There is also a 'Go To Interface' input field and a 'GO' button.

Interface	Admin Mode
1/0/1	Disable
1/0/2	Disable
1/0/3	Disable
1/0/4	Disable
1/0/5	Disable
1/0/6	Disable

8. Use **Interface** to select the physical interface.  
Select **All** to set the parameters for all ports to same values.
9. Select the Administrative Mode **Disable** or **Enable** radio button.  
The default value is Disable.
10. Use the 2-byte hex Global EtherType as the first 16 bits of the DVlan tag.
  - **802.1Q Tag**. Commonly used tag representing 0x8100
  - **vMAN Tag**. Commonly used tag representing 0x88A8
  - **Custom Tag**. Configure the EtherType in any range from 0 to 65535

## Configure a Voice VLAN

You can configure the parameters for a voice VLAN. Only a user with Read/Write access privileges can change the data on this screen.

➤ **To configure a voice VLAN:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > VLAN > Advanced > Voice VLAN Configuration**.

	Interface	Interface Mode	Value	CoS Override Mode	Operational State
1	1/0/1	Disable	0	Disable	Disable
2	1/0/2	Disable	0	Disable	Disable
3	1/0/3	Disable	0	Disable	Disable
4	1/0/4	Disable	0	Disable	Disable
5	1/0/5	Disable	0	Disable	Disable
6	1/0/6	Disable	0	Disable	Disable

The Operational State field displays the status of the voice VLAN for each interface.

8. Select the Administrative Mode **Disable** or **Enable** radio button.

The default value is Disable.

9. Use **Interface** to select the physical interface.

10. Use **Interface Mode** to select the voice VLAN mode for selected interface:

- **Disable.** The default value.
- **None.** Allow the IP phone to use its own configuration to send untagged voice traffic.
- **VLAN ID.** Configure the phone to send tagged voice traffic.
- **dot1p.** Configure voice VLAN 802.1p priority tagging for voice traffic. When this is selected, enter the dot1p value in the Value field.
- **Untagged.** Configure the phone to send untagged voice traffic.

**11.** Use **Value** to enter the VLAN ID or dot1p value.

This is enabled only when VLAN ID or dot1p is selected as interface mode.

**12.** Use **CoS Override Mode** to select the Cos override mode for selected interface.

The default is Disable.

## Configure GARP Switch Settings

---

**Note:** It can take up to 10 seconds for GARP configuration changes to take effect.

---

➤ **To configure GARP switch settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > VLAN > Advanced > GARP Switch Configuration**.



8. Select the GVRP Mode **Disable** or **Enable** radio button.

This sets the GARP VLAN Registration Protocol administrative mode for the switch. The factory default is Disable.

9. Select the GMRP Mode **Disable** or **Enable** radio button.

This sets the GARP Multicast Registration Protocol administrative mode for the switch. The factory default is Disable.

## Configure GARP Port Settings

---

**Note:** It can take up to 10 seconds for GARP configuration changes to take effect.

---

➤ **To configure GARP port settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.

7. Select **Switching > VLAN > Advanced > GARP Port Configuration**.

GARP Port Configuration						
1 2 LAGS All		Go To Interface		?		
	Interface	Port GVRP Mode	Port GMRP Mode	Join Timer (centisecs)	Leave Timer (centisecs)	Leave All Timer (centisecs)
<input type="checkbox"/>	1/0/1	Disable	Disable	20	60	1000
<input type="checkbox"/>	1/0/2	Disable	Disable	20	60	1000
<input type="checkbox"/>	1/0/3	Disable	Disable	20	60	1000
<input type="checkbox"/>	1/0/4	Disable	Disable	20	60	1000
<input type="checkbox"/>	1/0/5	Disable	Disable	20	60	1000
<input type="checkbox"/>	1/0/6	Disable	Disable	20	60	1000

8. Use the **Interface** check boxes to select the physical interface.

9. In the **Port GVRP Mode** field, select **Disable** or **Enable**.

This specifies the GARP VLAN Registration Protocol administrative mode for the port. If you select Disable, the protocol is not active and the join time, leave time, and leave all time have no effect. The factory default is Disable.

10. In the **Port GMRP Mode** field, select **Disable** or **Enable**.

This specifies the GARP Multicast Registration Protocol administrative mode for the port. If you select disable, the protocol is not active and the join time, leave time, and leave all time have no effect. The factory default is Disable.

11. In the **Join Time (centiseconds)** field, specify the time between the transmission of GARP PDUs registering (or reregistering) membership for a VLAN or multicast group in centiseconds.

Enter a number between 10 and 100 0.(1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). An instance of this timer exists for each GARP participant for each port.

12. In the **Leave Time (centiseconds)** field, specify the time to wait after receiving an unregister request for a VLAN or multicast group before deleting the associated entry, in centiseconds.

This allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service. Enter a number between 20 and 600 (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds). An instance of this timer exists for each GARP participant for each port.

13. In the **Leave All Time (centiseconds)** field, specify how frequently LeaveAll PDUs are generated.

A LeaveAll PDU indicates that all registrations are due to be deregistered soon. Participants need to rejoin in order to maintain registration. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5\*LeaveAllTime. The timer is specified in centiseconds. Enter a number between 200 and 6000 (2 to 60 seconds). The

factory default is 1000 centiseconds (10 seconds). An instance of this timer exists for each GARP participant for each port.

## Auto-VoIP Overview

The Auto-VoIP feature enables manual and auto assignment of VoIP phone traffic to a special VLAN (such as, voice VLAN), allowing the assignment of special QoS parameters to that traffic, giving it high priority services.

## Configure Protocol-Based Port Settings

➤ **To configure protocol-based port settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Auto-VoIP > Protocol-based > Port Settings**.

The screenshot shows the 'Protocol Based Port Settings' configuration page. It has two main sections: 'Protocol Based Global Settings' and 'Protocol Based Port Settings'. In the 'Protocol Based Global Settings' section, 'Prioritization Type' is set to 'Traffic Class' and 'Class Value' is set to '7'. In the 'Protocol Based Port Settings' section, there is a table with columns 'Interface', 'Auto VoIP Mode', and 'Operational Status'. The table lists interfaces 0/1 through 0/12, all of which have 'Auto VoIP Mode' set to 'Enable' and 'Operational Status' set to 'UP'. There are also 'LAGS' and 'All' buttons at the top and bottom of the table.

Interface	Auto VoIP Mode	Operational Status
0/1	Enable	UP
0/2	Enable	UP
0/3	Enable	UP
0/4	Enable	UP
0/5	Enable	UP
0/6	Enable	UP
0/7	Enable	UP
0/8	Enable	UP
0/9	Enable	UP
0/10	Enable	UP
0/11	Enable	UP
0/12	Enable	UP

8. Use **Prioritization Type** to specify the type of prioritization.

It can be Traffic Class or Remark.

9. Use **Class Value** to specify the CoS tag value to be reassigned for packets received on the voice VLAN when Remark CoS is enabled.

10. Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See *Save Configuration* on page 405.

## Configure OUI-Based Properties

- To display the OUI properties:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

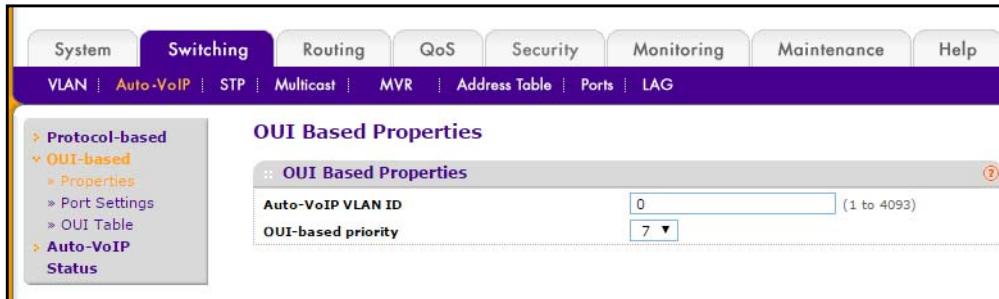
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Auto-VoIP > OUI-based > Properties**.



8. In the **Auto-VoIP VLAN ID** field, specify the VoIP VLAN ID on the switch.

The range is 1 to 4093. A VLAN ID value of 0 implies that there is no Auto-VoIP VLAN configured. VLAN ID default value is 2.

9. Use **OUI-based priority** to configure OUI-based priority on the switch.

The range is 0 to 7. The default value is 7.

10. Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See *Save Configuration* on page 405.

## Configure OUI-Based Port Settings

➤ **To display the OUI port settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **Switching > Auto-VoIP > OUI-based > Port Settings**.

Interface	Auto VoIP Mode	Operational Status
0/1	Enable	UP
0/2	Enable	UP
0/3	Enable	UP
0/4	Enable	UP
0/5	Enable	UP
0/6	Enable	UP
0/7	Enable	UP
0/8	Enable	UP
0/9	Enable	UP
0/10	Enable	UP
0/11	Enable	UP
0/12	Enable	UP

The screen displays the current operational status of the interface.

- Use the **Interface** check boxes to select the interface.
- In the **Auto VoIP Mode** menu, select **Enable** or **Disable**.

This sets the AutoVoIP mode on the selected interface. The default value is Enable.

- In the **Go To Interface** field, type the number of an interface.
- Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See *Save Configuration* on page 405.

## Configure the OUI Table

➤ **To configure the OUI table:**

- Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
- Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
- Launch a web browser.
- Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Auto-VoIP > OUI-based > OUI Table**.

:: OUI Table		
	Telephony OUI(s)	Description
<input type="checkbox"/>	00:01:E3	SIEMENS
<input type="checkbox"/>	00:03:6B	CISCO1
<input type="checkbox"/>	00:12:43	CISCO2
<input type="checkbox"/>	00:0F:E2	H3C
<input type="checkbox"/>	00:60:B9	NITSUKO
<input type="checkbox"/>	00:D0:1E	PINTEL
<input type="checkbox"/>	00:E0:75	VERILINK
<input type="checkbox"/>	00:E0:BB	3COM
<input type="checkbox"/>	00:04:0D	AVAYA1
<input type="checkbox"/>	00:1B:4F	AVAYA2

8. Use **Telephony OUI(s)** to select the VoIP OUI prefix to be added in the format AA:BB:CC.

Up to 128 OUIs can be configured.

9. Use **Description** to enter the description for the OUI.

The maximum length of description is 32 characters.

The following OUIs are present in the configuration by default:

- 00:01:E3 - SIEMENS
- 00:03:6B - CISCO1
- 00:12:43 - CISCO2
- 00:0F:E2 - H3C
- 00:60:B9 - NITSUKO
- 00:D0:1E - PINTEL
- 00:E0:75 - VERILINK
- 00:E0:BB - 3COM
- 00:04:0D - AVAYA1
- 00:1B:4F - AVAYA2

10. To add a new telephony OUI entry, click the **ADD** button.

11. To delete a created entry, click the **DELETE** button.

12. Click the **APPLY** button.

Your settings are saved.

## View the Auto-VoIP Status

➤ **To display the Auto-VoIP status:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

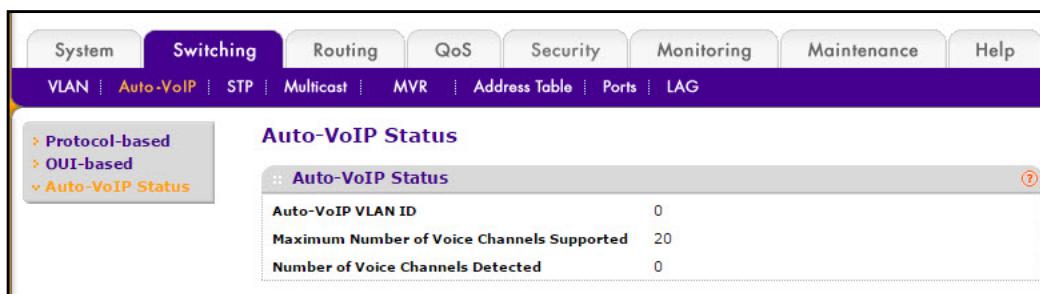
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Auto-VoIP > Auto-VoIP Status**.



8. To refresh the screen, click the **REFRESH** button.

## Spanning Tree Protocol Overview

The Spanning Tree Protocol (STP) provides a tree topology for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops. Spanning tree versions supported include Common STP, Multiple STP, and Rapid STP.

Classic STP provides a single path between end stations, avoiding and eliminating loops. For information about configuring Common STP, see *Configure CST Ports* on page 152.

Multiple Spanning Tree Protocol (MSTP) supports multiple instances of Spanning Tree to efficiently channel VLAN traffic over different interfaces. Each instance of the Spanning Tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree (RSTP), with slight

modifications in the working but not the end effect (chief among the effects is the rapid transitioning of the port to Forwarding). The difference between the RSTP and the traditional STP (IEEE 802.1D) is the ability to configure and recognize full-duplex connectivity and ports that are connected to end stations, resulting in rapid transitioning of the port to Forwarding state and the suppression of Topology Change Notification. These features are represented by the parameters *pointtopoint* and *edgeport*. MSTP is compatible with both RSTP and STP. It behaves appropriately to STP and RSTP bridges. A MSTP bridge can be configured to behave entirely as a RSTP bridge or an STP bridge.

---

**Note:** For two bridges to be in the same region, the force version should be 802.1s and their configuration name, digest key, and revision level should match. For additional information about regions and their effect on network topology, refer to the IEEE 802.1Q standard.

---

## Configure Spanning Tree Protocol

The Spanning Tree Configuration/Status screen contains fields for enabling STP on the switch.

➤ **To display the Spanning Tree Configuration/Status:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7.** Select **Switching > STP > Basic > STP Configuration**.

The screenshot shows the 'STP Configuration' page with two main sections:

- STP Configuration:**
  - Spanning Tree Admin Mode:** Radio buttons for Disable (selected) and Enable.
  - Force Protocol Version:** Radio buttons for IEEE 802.1d (selected), IEEE 802.1w, and IEEE 802.1s.
  - Configuration Name:** Text input field containing '2C-B0-5D-91-F6-F0'.
  - Configuration Revision Level:** Text input field containing '0' (with a note '(0 to 65535)').
  - Forward BPDU while STP Disabled:** Radio buttons for Disable (selected) and Enable.
  - BPDU Guard:** Radio buttons for Disable (selected) and Enable.
  - BPDU Filter:** Radio buttons for Disable (selected) and Enable.
  - Configuration Digest Key:** Text input field containing '0xac36177f50283cd4b83821d8ab26de62'.
  - Configuration Format Selector:** Text input field containing '0'.
- STP Status:**

MST ID	VID	FID
0	1	1
0	2	2
0	100	100

**8.** Select the **Spanning Tree Admin Mode Disable** or **Enable** radio button.

This specifies whether spanning tree operation is enabled on the switch.

**9.** Use **Force Protocol Version** to specify the Force Protocol Version parameter for the switch.

The options are IEEE 802.1d, IEEE 802.1w, and IEEE 802.1s.

**10.** In the **Configuration Name** field, specify an identifier used to identify the configuration currently being used.

It can be up to 32 alphanumeric characters.

**11.** In the **Configuration Revision Level** field, specify an identifier used to identify the configuration currently being used.

The values allowed are between 0 and 65535. The default value is 0.

**12.** Select the Forward BPDU while STP Disabled **Disable** or **Enable** radio button.

This specifies whether spanning tree BPDUs should be forwarded or not while spanning -tree is disabled on the switch.

**13.** Select the BPDU Guard **Disable** or **Enable** radio button.

This specifies whether the BPDU guard feature is enabled. The STP BPDU guard allows a network administrator to enforce the STP domain borders and keep the active topology consistent and predictable. The switches behind the edge ports with STP BPDU guard enabled are not able to influence the overall STP topology. At the reception of BPDUs, the BPDU guard operation disables the port that is configured with this option and transitions the port into a disabled state. This would lead to an administrative disabling of the port.

**14.** Select the BPDU Filter **Disable** or **Enable** radio button.

This specifies whether the BPDU Filter feature is enabled. STP BPDU filtering applies to all operational edge ports. The edge port in an operational state is supposed to be

connected to hosts that typically drop BPDU. If an operational edge port receives a BPDU, it immediately loses its operational status. In that case, if BPDU filtering is enabled on this port then the BPDU received on this port are dropped.

The following table describes the nonconfigurable information displayed on the screen.

**Table 42. STP Configuration**

Field	Description
Configuration Digest Key	Identifier used to identify the configuration currently being used.
MST ID	Table consisting of the MST instances (including the CST) and the corresponding VLAN IDs associated with each of them.
VID ID	Table consisting of the VLAN IDs and the corresponding FID associated with each of them.
FID ID	Table consisting of the FIDs and the corresponding VLAN IDs associated with each of them.

## Configure Advanced STP Settings

➤ **To configure advanced STP settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7.** Select **Switching > STP > Advanced > STP Configuration**.

The screenshot shows two stacked configuration pages for Spanning Tree. The top page, titled 'STP Configuration', contains fields for Spanning Tree Admin Mode (radio buttons for Disable or Enable), Force Protocol Version (radio buttons for IEEE 802.1d, IEEE 802.1w, or IEEE 802.1s), Configuration Name (text input field with value '00-04-06-02-04-07'), Configuration Revision Level (text input field with value '0' and a note '(0 to 65535)'), Forward BPDU while STP Disabled (radio buttons for Disable or Enable), BPDU Guard (radio buttons for Disable or Enable), BPDU Filter (radio buttons for Disable or Enable), Configuration Digest Key (text input field with value '0xac36177f50283cd4b83821d8ab26de62'), and Configuration Format Selector (text input field with value '0'). The bottom page, titled 'STP Status', displays MST ID 0, VID 1, and FID 1 in a table.

- 8.** Select the Spanning Tree Admin Mode **Disable** or **Enable** radio button.

This specifies whether spanning tree operation is enabled on the switch.

- 9.** Select a **Force Protocol Version** radio button.

This specifies the Force Protocol Version parameter for the switch. The options are IEEE 802.1d, IEEE 802.1w, and IEEE 802.1s.

- 10.** In the **Configuration Name** field, specify the identifier used to identify the configuration currently being used.

It can be up to 32 alphanumeric characters.

- 11.** In the **Configuration Revision Level** field, specify the identifier used to identify the configuration currently being used.

The values allowed are between 0 and 65535. The default value is 0.

- 12.** Select the Forward BPDU while STP Disabled **Disable** or **Enable** radio button.

This specifies whether spanning tree BPDUs should be forwarded while spanning-tree is disabled on the switch.

- 13.** Select the BPDU Guard **Disable** or **Enable** radio button.

This specifies whether the BPDU guard feature is enabled. The STP BPDU guard allows a network administrator to enforce the STP domain borders and keep the active topology consistent and predictable. The switches behind the edge ports with STP BPDU guard enabled are not able to influence the overall STP topology. At the reception of BPDUs, the BPDU guard operation disables the port that is configured with this option and transitions the port into a disabled state. This would lead to an administrative disable of the port.

- 14.** Select the BPDU Filter **Disable** or **Enable** radio button.

This specifies whether the BPDU Filter feature is enabled. STP BPDU filtering applies to all operational edge ports. An edge port in an operational state is supposed to be connected to hosts that typically drop BPDUs. If an operational edge port receives a

BPDU, it immediately loses its operational status. In that case, if BPDU filtering is enabled on this port, and the BPDUs received on this port are dropped.

The following table describes the nonconfigurable information displayed on the screen.

**Table 43. Advanced STP Configuration**

Field	Description
Configuration Digest Key	Identifier used to identify the configuration currently being used.
MST ID	Table consisting of the MST instances (including the CST) and the corresponding VLAN IDs associated with each of them.
VID ID	Table consisting of the VLAN IDs and the corresponding FID associated with each of them.
FID ID	Table consisting of the FIDs and the corresponding VLAN IDs associated with each of them.

## Configure Common Spanning Tree

You can configure Common Spanning Tree (CST) and Internal Spanning Tree on the switch.

➤ **To configure CST:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7.** Select **Switching > STP > Advanced > CST Configuration**.

The screenshot shows two stacked configuration pages for Spanning Tree settings:

- CST Configuration:**

Bridge Priority	32768	(0 to 61440)
Bridge Max Age (secs)	20	(6 to 40)
Bridge Hello Time (secs)	2	
Bridge Forward Delay (secs)	15	(4 to 30)
Spanning Tree Maximum Hops	20	(6 to 40)
Spanning Tree Tx Hold Count	6	(1 to 10)
- CST Status:**

Bridge Identifier	80:00:2C:B0:5D:91:F6:F0
Time Since Topology Change	1 day 0 hr 8 min 38 sec
Topology Change Count	1
Topology Change	False
Designated Root	80:00:00:07:03:05:05:06
Root Path Cost	40000
Root Port Identifier	80:01
Max Age (secs)	20
Forward Delay (secs)	15
Hold Time (secs)	6
CST Regional Root	80:00:2C:B0:5D:91:F6:F0
CST Path Cost	0
Port Triggered TC	

**8.** Specify values for CST in the appropriate fields:

- **Bridge Priority.** When switches or bridges are running STP, each is assigned a priority. After exchanging BPDU, the switch with the lowest priority value becomes the root bridge. Specify the bridge priority value for the Common and Internal Spanning Tree (CST). The valid range is 0–61440. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if the priority is attempted to be set to any value between 0 and 4095, it is set to 0. The default priority is 32768.
- **Bridge Max Age (secs).** Specifies the bridge maximum age time for the Common and Internal Spanning Tree (CST), which indicates the amount of time in seconds a bridge waits before implementing a topological change. The valid range is 6–40, and the value must be less than or equal to  $(2 * \text{Bridge Forward Delay}) - 1$  and greater than or equal to  $2 * (\text{Bridge Hello Time} + 1)$ . The default value is 20.
- **Bridge Hello Time (secs).** Specifies the bridge Hello time for the Common and Internal Spanning Tree (CST), which indicates the amount of time in seconds a root bridge waits between configuration messages. The value is fixed at 2 seconds. The value must be less than or equal to  $(\text{Bridge Max Age} / 2) - 1$ . The default Hello time value is 2.
- **Bridge Forward Delay (secs).** Specifies the bridge forward delay time, which indicates the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. The value must be greater or equal to  $(\text{Bridge Max Age} / 2) + 1$ . The time range is from 4 seconds to 30 seconds. The default value is 15.

- **Spanning Tree Maximum Hops.** Specifies the maximum number of bridge hops the information for a particular CST instance can travel before being discarded. The valid range is 1–127.
- **Spanning Tree Tx Hold Count.** Configures the maximum number of BPDUs the bridge is allowed to send within the hello time window. The default value is 6.

The following table describes the nonconfigurable information displayed on the screen.

**Table 44. CST Status**

Field	Description
Bridge identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time since topology change	The time in seconds since the topology of the CST last changed.
Topology change count	Number of times topology has changed for the CST.
Topology change	The value of the topology change parameter for the switch indicating if a topology change is in progress on any port assigned to the CST. It takes a value if True or False.
Designated root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Path cost to the designated root for the CST.
Root Port Identifier	Port to access the designated root for the CST.
Max Age(secs)	Path cost to the designated root for the CST.
Forward Delay(secs)	Derived value of the root port bridge forward delay parameter.
Hold Time(secs)	Minimum time between transmission of configuration BPDUs.
CST Regional Root	Priority and base MAC address of the CST regional root.
CST Path Cost	Path cost to the CST tree regional root.

## Configure CST Ports

You can configure the Common Spanning Tree (CST) and Internal Spanning Tree on a specific port on the switch.

➤ **To configure CST ports:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

- Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **Switching > STP > Advanced > CST Port Configuration**.

Interface	Port Priority	Admin Edge Port	Port Path Cost	Auto Calculated Port Path Cost	Hello Timer	External Port Path Cost	Auto Calculated External Port Path Cost	BPDUs Filter	BPDU Forwarding	BPDU Guard Effect	Auto Edge	Root Guard	Loop Guard	TCP Guard	Port Mode	Port Forwarding State
1/0/1	128	Enable	20000	Enabled	2	20000	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Forwarding
1/0/2	128	Enable	0	Enabled	2	0	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/3	128	Enable	0	Enabled	2	0	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/4	128	Enable	0	Enabled	2	0	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/5	128	Enable	0	Enabled	2	0	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/6	128	Enable	0	Enabled	2	0	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled
1/0/7	128	Enable	0	Enabled	2	0	Enabled	Disable	Disable	Disabled	Disable	Disable	Disable	Disable	Enable	Disabled

- Select an **Interface** check box to select one of the physical or port channel interfaces associated with VLANs associated with the CST.
- Use **Port Priority** to specify the priority for a particular port within the CST.

The port priority is set in multiples of 16. For example if the priority is any value between 0 and 15, it is set to 0. If you try to set it to any value between 16 and  $(2^{*}16-1)$  it is set to 16 and so on.

- Use **Admin Edge Port** to specify if the specified port is an edge port within the CIST.

It takes a value of TRUE or FALSE, where the default value is FALSE.

- Use **Port Path Cost** to set the path cost to a new value for the specified port in the common and internal spanning tree.

It takes a value in the range of 1 to 200000000.

- Use **External Port Path Cost** to set the external path cost to a new value for the specified port in the spanning tree.

It takes a value in the range of 1 to 200000000.

- For **BPDU Filter**, select **Enable** or **Disable**.

This configures the BPDU filter, which filters the BPDU traffic on this port when STP is enabled on this port.

- Select the BPDU Flood **Disable** or **Enable** radio button.

This setting configures the BPDU flood, which floods the BPDU traffic arriving on this port when STP is disabled on this port.

**15. In the **Auto Edge** field select **Disable** or **Enable**.**

This configures the auto edge mode of a port, which allows the port to become an edge port if it does not see BPDUs for some duration.

**16. In the **Root Guard** field, select **Disable** or **Enable**.**

This configures the root guard mode, which sets a port to discard any superior information received by the port and thus protects the root of the device against changing. The port gets put into the discarding state and does not forward any packets.

**17. Use **Loop Guard** to configure the loop guard on the port to protect Layer 2 forwarding loops. If loop guard is enabled, the port moves into the STP loop inconsistent blocking state instead of the listening/learning/forwarding state.**

**18. Use **TCN Guard** to configure the TCN guard for a port restricting the port from propagating any topology change information received through that port.**

The possible values are Enable or Disable.

**19. Use **Port Mode** to enable or disable Spanning Tree Protocol administrative mode associated with the port or port channel.**

The possible values are Enable or Disable.

The following table describes the nonconfigurable information displayed on the screen.

**Table 45. CST Port Configuration**

Field	Description
Auto Calculated Port Path Cost	Displays whether the path cost is automatically calculated (Enabled) or not (Disabled). Path cost is calculated based on the link speed of the port if the configured value for port path cost is zero.
Hello Timer	Displays the value of the parameter for the CST.
Auto Calculated External Port Path Cost	Displays whether the external path cost is automatically calculated (Enabled) or not (Disabled). External Path cost is calculated based on the link speed of the port if the configured value for external port path cost is zero.
BPDU Guard Effect	The BPDU guard effect disables the edge ports that receive BPDU packets. The possible values are Enable or Disable.
Port Forwarding State	The forwarding state of this port.

## View Spanning Tree CST Port Status

➤ **To view the Spanning Tree CST port status:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.

2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > STP > Advanced > CST Port Status**.

CST Port Status																
CST Port Status																
1 2 LAGS All																
Interface	Port ID	Port Forwarding State	Port Role	Designated Root	Designated Cost	Designated Bridge	Designated Port	Topology Change Acknowledge	Edge Port	Point-to-Point MAC	CST Regional Root	CST Path Cost	Port Up Time Since Counters Last Cleared	Loop Inconsistent State	Transitions Into Loop Inconsistent State	Transitions Out Of Loop Inconsistent State
1/0/1	80:01	Forwarding	Root	80:00:00:07:03:05:05:06	20000	80:00:C0:3F:0E:90:29:F0	00:08	False	Disabled	True	80:00:C0:3F:0E:90:29:F0	0	1 day 0 hr 9 min 11 sec	False	0	0
1/0/2	80:02	Disabled	Disabled	80:00:2C:B0:5D:91:F6:F0	0	80:00:2C:B0:5D:91:F6:F0	00:00	False	Disabled	False	80:00:2C:B0:5D:91:F6:F0	0	3 day 3 hr 25 min 30 sec	False	0	0
1/0/3	80:03	Disabled	Disabled	80:00:2C:B0:5D:91:F6:F0	0	80:00:2C:B0:5D:91:F6:F0	00:00	False	Disabled	False	80:00:2C:B0:5D:91:F6:F0	0	3 day 3 hr 25 min 30 sec	False	0	0
1/0/4	80:04	Disabled	Disabled	80:00:2C:B0:5D:91:F6:F0	0	80:00:2C:B0:5D:91:F6:F0	00:00	False	Disabled	False	80:00:2C:B0:5D:91:F6:F0	0	3 day 3 hr 25 min 30 sec	False	0	0
1/0/5	80:05	Disabled	Disabled	80:00:2C:B0:5D:91:F6:F0	0	80:00:2C:B0:5D:91:F6:F0	00:00	False	Disabled	False	80:00:2C:B0:5D:91:F6:F0	0	3 day 3 hr 25 min 30 sec	False	0	0
1/0/6	80:06	Disabled	Disabled	80:00:2C:B0:5D:91:F6:F0	0	80:00:2C:B0:5D:91:F6:F0	00:00	False	Disabled	False	80:00:2C:B0:5D:91:F6:F0	0	3 day 3 hr 25 min 30 sec	False	0	0

The following table describes the CST Port Status information displayed on the screen.

**Table 46. CST port status**

Field	Description
Interface	Identify the physical or port channel interfaces associated with VLANs associated with the CST.
Port ID	The port identifier for the specified port within the CST. It is made up from the port priority and the interface number of the port.
Port Forwarding State	The forwarding state of this port.
Port Role	Each MST bridge port that is enabled is assigned a Port Role for each spanning tree. The port role is one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port.
Designated Root	Root bridge for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Cost	Path cost offered to the LAN by the designated port.

**Table 46. CST port status (continued)**

Field	Description
Designated Bridge	Bridge identifier of the bridge with the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port	Port Identifier on the designated bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.
Topology Change Acknowledge	Identifies whether the next BPDU to be transmitted for this port would have the topology change acknowledgement flag set. It is either True or False.
Edge port	Indicates whether the port is enabled as an edge port. It takes the value "Enabled" or "Disabled".
Point-to-point MAC	Derived value of the point-to-point status.
CST Regional Root	Bridge Identifier of the CST regional root. It is made up using the bridge priority and the base MAC address of the bridge.
CST Path Cost	Path cost to the CST rRegional root.
Port Up Time Since Counters Last Cleared	Time since the counters were last cleared, displayed in days, hours, minutes, and seconds.
Loop Inconsistent State	This parameter identifies whether the port is in loop inconsistent state or not.
Transitions Into Loop Inconsistent State	The number of times this interface has transitioned into loop inconsistent state.
Transitions Out Of Loop Inconsistent State	The number of times this interface has transitioned out of loop inconsistent state.

## Configure an MST Instance

➤ **To configure Multiple Spanning Tree (MST) on the switch:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **Switching > STP > Advanced > MST Configuration**.

MST Configuration										
:: MST Configuration										
	MST ID	Priority	Bridge Identifier	Vlan Id	Time Since Topology Change	Topology Change Count	Topology Change	Designated Root	Root Path Cost	Root Port Identifier
<input type="checkbox"/>	0	32768	80:00:2C:B0:5D:91:F6:F0	1-2	1 day 0 hr 10 min 10 sec	1	False	80:00:00:07:03:05:05:06	40000	80:01
<input checked="" type="checkbox"/>	1	0	80:01:2C:B0:5D:91:F6:F0	100	0 day 0 hr 0 min 2 sec	1	True	80:01:2C:B0:5D:91:F6:F0	0	00:00

- To add an MST instance, configure the MST values and click the **ADD** button:

- MST ID.** Specify the ID of the MST to create. Valid values for this are between 1 and 4094.
- Priority.** Specifiy the bridge priority value for the MST. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDU, the switch with the lowest priority value becomes the root bridge. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example, if the priority is attempted to be set to any value between 0 and 4095, it is set to 0. The default priority is 32768.The valid range is 0–61440.
- VLAN ID.** This is a combo box of each VLAN on the switch. These can be selected or unselected for reconfiguring the association of VLANs to MST instances.

- To delete an MST instance, select the check box next to the instance and click the **DELETE** button.

- To modify an MST instance, select the check box next to the instance to configure, update the values, and click the **APPLY** button.

You can select multiple check boxes to apply the same setting to all selected ports.

- Click **CANCEL** to cancel the configuration on the screen and reset the data on the screen to the previous values of the switch.

For each configured instance, the information described in the following table displays on the screen.

**Table 47. MST Configuration**

Field	Description
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	The time, in seconds since the topology of the selected MST instance last changed.
Topology Change Count	Number of times topology has changed for the selected MST instance.

**Table 47. MST Configuration (continued)**

Field	Description
Topology Change	The value of the topology change parameter for the switch, indicating if a topology change is in progress on any port assigned to the selected MST instance. It takes a value if True or False.
Designated Root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge
Root Path Cost	Path cost to the designated root for this MST instance.
Root PortIdentifier	Port to access the designated root for this MST instance.

## View MST Port Status

➤ **To view the Spanning Tree MST port status:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

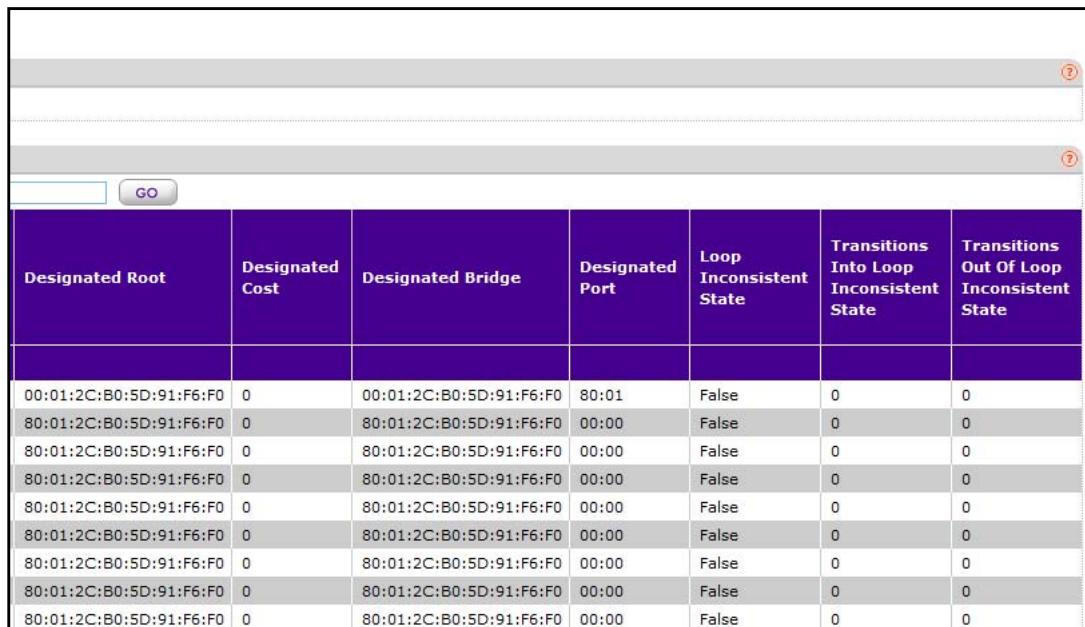
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7.** Select **Switching > STP > Advanced > MST Port Status**.



The screenshot shows a table titled "MST Port Status" with the following columns: Designated Root, Designated Cost, Designated Bridge, Designated Port, Loop Inconsistent State, Transitions Into Loop Inconsistent State, and Transitions Out Of Loop Inconsistent State. The table contains 9 rows of data, each corresponding to a port. The data is as follows:

Designated Root	Designated Cost	Designated Bridge	Designated Port	Loop Inconsistent State	Transitions Into Loop Inconsistent State	Transitions Out Of Loop Inconsistent State
00:01:2C:B0:5D:91:F6:F0	0	00:01:2C:B0:5D:91:F6:F0	80:01	False	0	0
80:01:2C:B0:5D:91:F6:F0	0	80:01:2C:B0:5D:91:F6:F0	00:00	False	0	0
80:01:2C:B0:5D:91:F6:F0	0	80:01:2C:B0:5D:91:F6:F0	00:00	False	0	0
80:01:2C:B0:5D:91:F6:F0	0	80:01:2C:B0:5D:91:F6:F0	00:00	False	0	0
80:01:2C:B0:5D:91:F6:F0	0	80:01:2C:B0:5D:91:F6:F0	00:00	False	0	0
80:01:2C:B0:5D:91:F6:F0	0	80:01:2C:B0:5D:91:F6:F0	00:00	False	0	0
80:01:2C:B0:5D:91:F6:F0	0	80:01:2C:B0:5D:91:F6:F0	00:00	False	0	0
80:01:2C:B0:5D:91:F6:F0	0	80:01:2C:B0:5D:91:F6:F0	00:00	False	0	0

---

**Note:** If no MST instances were configured on the switch, the screen displays a *No MSTs Available* message and does not display the fields shown in the field description table that follows.

---

- 8.** Use **MST ID** to select one MST instance from existing MST instances.
- 9.** Use **Interface** to select one of the physical or port channel interfaces associated with VLANs associated with the selected MST instance.
- 10.** Use **Port Priority** to specify the priority for a particular port within the selected MST instance.

The port priority is set in multiples of 16. For example if the priority is any value between 0 and 15, it is set to 0. If you try to set it to any value between 16 and  $(2 \times 16 - 1)$ , it is set to 16, and so on.

- 11.** Use **Port Path Cost** to set the path cost to a new value for the specified port in the selected MST instance.

It takes a value in the range of 1 to 200000000.

The following table describes the read-only MST port configuration information displayed on the Spanning Tree MST Configuration screen.

**Table 48. MST Port Status**

<b>Field</b>	<b>Description</b>
Auto Calculated Port Path Cost	Displays whether the path cost is automatically calculated (Enabled) or not (Disabled). Path cost is calculated based on the link speed of the port if the configured value for Port path cost is zero.
Port ID	The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.
Port Uptime Since Last Clear Counters	Time since the counters were last cleared, displayed in Days, Hours, Minutes, and Seconds.
Port Mode	Spanning Tree Protocol Administrative Mode associated with the port or port channel. The possible values are Enable or Disable.
Port Forwarding State	The Forwarding State of this port.
Port Role	Each MST bridge port that is enabled is assigned a Port Role for each spanning tree. The port role is one of the following values: root port, designated port, alternate port, backup port, master port or disabled Port.
Designated Root	Root bridge for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Cost	Path cost offered to the LAN by the designated port.
Designated Bridge	Bridge identifier of the bridge with the designated port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port	Port Identifier on the designated bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.

## View Spanning Tree Statistics

You can view information about the number and type of bridge protocol data units (BPDUs) transmitted and received on each port.

➤ **To view Spanning Tree statistics:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

- Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **Switching > STP > Advanced > STP Statistics**.

Interface	STP BPDUs Received	STP BPDUs Transmitted	RSTP BPDUs Received	RSTP BPDUs Transmitted	MSTP BPDUs Received	MSTP BPDUs Transmitted
1/0/1	0	0	0	7	43128	0
1/0/2	0	0	0	0	0	0
1/0/3	0	0	0	0	0	0
1/0/4	0	0	0	0	0	0
1/0/5	0	0	0	0	0	0
1/0/6	0	0	0	0	0	0
1/0/7	0	0	0	0	0	0
1/0/8	0	0	0	0	0	0
1/0/9	0	0	0	0	0	0
1/0/10	0	0	0	0	0	0
1/0/11	0	0	0	0	0	0

The following table describes the information available on the STP Statistics screen.

**Table 49. STP statistics**

Field	Description
Interface	Selects one of the physical or port channel interfaces of the switch.
STP BPDUs Received	Number of STP BPDUs received at the selected port.
STP BPDUs Transmitted	Number of STP BPDUs transmitted from the selected port.
RSTP BPDUs Received	Number of RSTP BPDUs received at the selected port.
RSTP BPDUs Transmitted	Number of RSTP BPDUs transmitted from the selected port.
MSTP BPDUs Received	Number of MSTP BPDUs received at the selected port.
MSTP BPDUs Transmitted	Number of MSTP BPDUs transmitted from the selected port.

## Configure Multicast

You can configure bridge multicast forwarding and manage MFBD and IGMP snooping.

### Configure Bridge Multicast Forwarding

When you create a VLAN, a default multicast forwarding option is assigned. You can use the Global Multicast Mode setting to set all VLANs currently configured on the switch to a selected forwarding mode. The global setting does not create a default setting for VLANs created subsequently—it simply ensures that all existing VLANs are configured with the specified mode. You can also configure how the switch forwards multicast packets on an individual or per-VLAN basis.

➤ **To configure bridge multicast forwarding:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Multicast > MFDB > Bridge Multicast Forwarding**.

:: Bridge Multicast Forwarding Table		
	VLAN ID	Forwarding Mode
<input checked="" type="checkbox"/>		<input type="button" value="▼"/>
<input type="checkbox"/>	1	Forward Unregistered
<input type="checkbox"/>	2	Forward Unregistered

8. Select a **VLAN ID** check box.
9. In the **Forwarding Mode** list, select the forwarding mode.

Possible values are as follows:

- **Forward Unregistered:** If a packet is received from a VLAN with a multicast destination address and no ports in the VLAN are registered to receive multicast packets for that address, then the packet is flooded to all ports in the VLAN. The responsibility for accepting or dropping the packets belongs to the hosts. If a multicast packet is received and there are ports registered to receive it, the packet is sent only to the registered ports.
- **Forward All:** All multicast packets received from a VLAN are flooded to all ports in the VLAN, regardless of port registrations to multicast addresses.
- **Filter Unregistered:** If a packet is received from a VLAN for a multicast destination address and no ports in the VLAN are registered to receive multicast packets for that address, then the packets are dropped.

The default value is Forward Unregistered.

**10.** Click the **REFRESH** button to update the screen to show the latest information.

**11.** Click the **APPLY** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

## View the MFDB Table

The Multicast Forwarding Database holds the port membership information for all active multicast address entries. The key for an entry consists of a VLAN ID and MAC address pair. Entries can contain data for more than one protocol.

➤ **To view the MFDB table:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Multicast > MFDB > MFDB Table**.

<b>MFDB Table</b>					
<b>:: MFDB Table</b>					
<input type="text" value="Search By MAC Address"/> <input type="button" value="GO"/>					
MAC Address	VLAN ID	Component	Type	Description	Forwarding Interfaces

8. Use **Search by MAC Address** to enter a MAC address whose MFDB table entry you want displayed.

Enter six two-digit hexadecimal numbers separated by colons, for example 00:01:23:43:45:67. Then click the **GO** button. If the address exists, that entry is displayed. An exact match is required.

The following table describes the nonconfigurable information displayed on the screen.

**Table 50. MFDB table**

Field	Description
MAC Address	The multicast MAC address for which you requested data.
VLAN ID	The VLAN ID to which the multicast MAC address is related.
Type	This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Component	This is the component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP snooping, GMRP, Static Filtering, and MLD snooping.
Description	The text description of this multicast table entry. Possible values are Management Configured, Network Configured, and Network Assisted.
Forwarding Interfaces	The resultant forwarding list is derived from combining all the forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

## View MFDB Statistics

➤ **To view MFDB statistics:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Multicast > MFDB > MFDB Statistics**.

MFDB Statistics	
:: MFDB Statistics	
Max MFDB Table Entries	1024
Most MFDB Entries Since Last Reset	0
Current Entries	0

## IGMP Snooping Overview

Internet Group Management Protocol (IGMP) snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch. Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

A traditional Ethernet network can be separated into different network segments to prevent placing too many devices onto the same shared media. Bridges and switches connect these segments. When a packet with a broadcast or multicast destination address is received, the switch forwards a copy into each of the remaining network segments in accordance with the IEEE MAC Bridge standard. Eventually, the packet is made accessible to all nodes connected to the network.

This approach works well for broadcast packets that are intended to be seen or processed by all connected nodes. In the case of multicast packets, however, this approach could lead to less efficient use of network bandwidth, particularly when the packet is intended for only a small number of nodes. Packets are flooded into network segments where no node has any interest in receiving the packet. While nodes rarely incur any processing overhead to filter packets addressed to unrequested group addresses, they are unable to transmit new packets onto the shared media for the period of time that the multicast packet is flooded. The problem of wasting bandwidth is even worse when the LAN segment is not shared, for example, in full-duplex links.

Allowing switches to snoop IGMP packets is a creative effort to solve this problem. The switch uses the information in the IGMP packets as they are being forwarded throughout the network to determine which segments should receive packets directed to the group address.

## Configure IGMP Snooping Interface Settings

You can configure IGMP snooping settings on specific interfaces.

➤ **To configure IGMP snooping interface settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Multicast > IGMP Snooping > Interface Configuration**.

Interface	Admin Mode	Group Membership Interval(secs)	Max Response Time(secs)	Present Expiration Time(secs)	Fast Leave Admin Mode
1/0/1	Disable	260	10	0	Disable
1/0/2	Disable	260	10	0	Disable
1/0/3	Disable	260	10	0	Disable
1/0/4	Disable	260	10	0	Disable
1/0/5	Disable	260	10	0	Disable
1/0/6	Disable	260	10	0	Disable
1/0/7	Disable	260	10	0	Disable
1/0/8	Disable	260	10	0	Disable

**Note:** Only a user with Read/Write access privileges can change the data on this screen.

8. Use the Interface check boxes to select the interface.
9. In the **Admin Mode** field, select **Enable** or **Disable**.

This specifies interface mode for the selected interface for IGMP snooping for the switch. The default is Disable.

10. In the **Group Membership Interval** field, specify the amount of time you want the switch to wait for a report for a particular group on a particular interface before it deletes that interface from the group.

Enter a value between 1 and 3600 seconds. The default is 260 seconds.

11. In the **Max Response Time** field, specify the amount of time the switch waits after sending a query on an interface because it did not receive a report for a particular group on that interface.

Enter a value greater than or equal to 1 and less than the group membership interval in seconds. The default is 10 seconds. The configured value must be less than the group membership interval.

12. In the **Present Expiration Time** field, specify the amount of time the switch waits to receive a query on an interface before removing it from the list of interfaces with multicast routers attached.

Enter a value between 0 and 3600 seconds. The default is 0 seconds. A value of zero indicates an infinite time-out, for example no expiration.

13. For **Fast Leave Admin** mode, select **Enable** or **Disable**.

This applies to the particular interface. The default is Disable.

14. Click the **APPLY** button.

Your settings are applied to the switch. Configuration changes take effect immediately.

## Configure IGMP Snooping Settings for VLANs

You can configure IGMP snooping settings for VLANs on the system.

➤ **To configure IGMP snooping settings for VLANs:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration**.

IGMP VLAN Configuration						
IGMP VLAN Configuration						
	VLAN ID	Admin Mode	Fast Leave Admin Mode	Group Membership Interval	Maximum Response Time	Multicast Router Expiry Time
<input type="checkbox"/>	200	Enable	Enable	260	10	0
<input checked="" type="checkbox"/>						

- To enable IGMP snooping on a VLAN, enter the VLAN ID in the appropriate field and configure the IGMP snooping values:
  - For **Admin Mode**, select **Enable** or **Disable** for IGMP snooping for the specified VLAN ID.
  - For **Fast Leave Admin Mode**, select **Enable** or **Disable** for the specified VLAN ID.
  - In the **Group Membership Interval** field, set the value for group membership interval of IGMP snooping for the specified VLAN ID.  
The valid range is (Maximum Response Time + 1) to 3600 seconds.
  - In the **Maximum Response Time** field, set the value for the maximum response time of IGMP snooping for the specified VLAN ID.  
The valid range is 1 to (Group Membership Interval – 1). Its value should be greater than group membership interval value.
  - In the **Multicast Router Expiry Time** field, set the value for multicast router expiry time of IGMP snooping for the specified VLAN ID.  
The valid range is 0 to 3600 seconds.
- To disable IGMP snooping on a VLAN and remove it from the list, select the check box next to the VLAN ID and click the **DELETE** button.
- To modify IGMP snooping settings for a VLAN, select the check box next to the VLAN ID, update the desired values, and click the **APPLY** button.

## Configure IGMP Snooping for a Multicast Router

You can configure the interface as the one the multicast router is attached to. All IGMP packets snooped by the switch are forwarded to the multicast router reachable from this interface. The configuration is not needed most of the time because the switch automatically detects the presence of the multicast router and forward IGMP packet accordingly. It is

needed only when you want to make sure that the multicast router always receives IGMP packets from the switch in a complex network.

➤ **To configure IGMP snooping for a multicast router:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Multicast > IGMP Snooping > Multicast Router Configuration**.

Interface	Multicast Router
1/0/1	Disable
1/0/2	Disable
1/0/3	Disable
1/0/4	Disable
1/0/5	Disable
1/0/6	Disable
1/0/7	Disable
1/0/8	Disable
1/0/9	Disable

8. Select one or more **Interface** check boxes.
9. In the **Multicast Router** list, select **Enable** or **Disable** for the selected interfaces.

## Configure IGMP Snooping for a Multicast Router VLAN

You can configure the interface to forward only the snooped IGMP packets that come from VLAN ID (<vlanId>) to the multicast router attached to this interface. The configuration is not needed most of the time because the switch automatically detects the presence of a multicast router and forwards IGMP packets accordingly. It is needed only when you want to make sure that the multicast router always receives IGMP packets from the switch in a complex network.

➤ **To configure IGMP snooping for a multicast router VLAN:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Multicast > IGMP Snooping > Multicast Router VLAN Configuration**.

Multicast Router VLAN Configuration		
:: Multicast Router VLAN Configuration		
Interface	1/0/1	
:: Multicast Router VLAN Configuration		
VLAN ID	Multicast Router	
<input type="checkbox"/>	<input type="text"/>	<input type="button"/>

8. Select one or more **Interface** check boxes.
9. In the **VLAN ID** list, select **Enabled** or **Disabled**.
10. In the **Multicast Router** list, select **Enabled** or **Disabled** for the VLAN ID.

## Configure IGMP Snooping Querier

IGMP snooping requires that one central switch or router periodically query all end devices on the network to announce their multicast memberships. This central device is the IGMP querier. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it stops forwarding multicasts to the port where the end device is located.

You can configure and display information about IGMP snooping queriers on the network and, separately, on VLANs.

➤ **To configure IGMP snooping querier:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Multicast > IGMP Snooping > Querier Configuration**.

8. Use **Querier Admin Mode** to select the administrative mode for IGMP snooping for the switch.

The default is Disable.

9. Use **Querier IP Address** to specify the snooping querier address to be used as the source address in periodic IGMP queries.

This address is used when no address is configured on the VLAN on which query is being sent.

10. Use **IGMP Version** to specify the IGMP protocol version used in periodic IGMP queries.

11. Use **Query Interval (secs)** to specify the time interval in seconds between periodic queries sent by the snooping querier.

The query interval must be a value in the range of 1 and 1800. The default value is 60.

12. Use **Querier Expiry Interval (secs)** to specify the time interval in seconds after which the last querier information is removed.

The querier expiry interval must be a value in the range of 60 and 300. The default value is 125.

**Table 51. IGMP Snooping Querier Configuration**

Field	Description
VLAN IDs Enabled For IGMP Snooping Querier	Displays VLAN IDs enabled for IGMP snooping querier.

## IGMP Snooping Querier VLAN Configuration

You can configure IGMP queriers for use with VLANs on the network.

➤ **To configure IGMP queriers for use with VLANs:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Multicast > IGMP Snooping > Querier VLAN Configuration**.

IGMP Snooping Querier VLAN Configuration								
:: IGMP Snooping Querier VLAN Configuration								
	VLAN ID	Querier Election Participate Mode	Querier VLAN Address	Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Max Response Time
<input type="checkbox"/>	<input type="text" value="100"/>	<input type="button" value="Enable"/>	<input type="text" value="192.168.10.2"/>	<input type="button" value="Disable"/>	<input type="text" value="2"/>			

8. To create a new VLAN ID for IGMP snooping, select New Entry from the VLAN ID field and complete the following fields.

You can also set pre-configurable snooping querier parameters.

- **VLAN ID.** Specifies the VLAN ID for which the IGMP snooping querier is to be enabled.
- **Querier Election Participate Mode.** Enable or disable querier participate mode.
  - **Disabled.** Upon seeing another querier of the same version in the VLAN, the snooping querier moves to the non-querier state.
  - **Enabled.** The snooping querier participates in querier election, in which the least IP address operates as the querier in that VLAN. The other querier moves to non-querier state.
- **Snooping Querier VLAN Address.** Specify the snooping querier IP address to be used as the source address in periodic IGMP queries sent on the specified VLAN.

**9.** Click the **APPLY** button.

The new settings are applied to the switch. Configuration changes take effect immediately

**10.** To disable snooping querier on a VLAN, select the VLAN ID and click the **DELETE** button.

**11.** Click the **REFRESH** button to update the screen with the latest information from the switch.

The following table describes the nonconfigurable information displayed on the screen.

**Table 52. IGMP Snooping Querier VLAN Configuration**

Field	Description
Operational State	Displays the operational state of the IGMP snooping querier on a VLAN. It can be in any of the following states: <ul style="list-style-type: none"> <li>• Querier: The snooping switch is the querier in the VLAN. The snooping switch sends out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch sees a better querier in the VLAN, it moves to non-querier mode.</li> <li>• Non-Querier: The snooping switch is in non-querier mode in the VLAN. If the querier expiry interval timer is expired, the snooping switch moves into querier mode.</li> <li>• Disabled: Snooping querier is not operational on the VLAN. The snooping querier moves to disabled mode when IGMP snooping is not operational on the VLAN or when the querier address is not configured or the network management address is also not configured.</li> </ul>
Operational Version	Displays the operational IGMP protocol version of the querier.
Last Querier Address	Displays the IP address of the last querier from which a query was snooped on the VLAN.
Last Querier Version	Displays the IGMP protocol version of the last querier from which a query was snooped on the VLAN.
Operational Max Response Time	Displays maximum response time to be used in the queries that are sent by the snooping querier.

## Configure MLD Snooping

You can configure the parameters for MLD snooping, which is used to build forwarding lists for multicast traffic. Note that only a user with Read/Write access privileges can change the data on this screen.

➤ **To configure MLD snooping:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Multicast > MLD Snooping > Configuration**.

VLAN ID	Status
1	Enabled

8. Use **MLD Snooping Admin Mode** to select the administrative mode for MLD snooping for the switch. The default is Disable.

The following table describes the nonconfigurable information displayed on the screen.

**Table 53. MLD Snooping Configuration**

Field	Definition
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.

**Table 53. MLD Snooping Configuration**

Field	Definition
Interfaces Enabled for MLD Snooping	A list of all the interfaces currently enabled for MLD snooping.
VLAN IDs Enabled For MLD Snooping	Displays VLAN IDs enabled for MLD snooping.

## Configure MLD Snooping for an Interface

➤ **To configure MLD snooping for an interface:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Multicast > MLD Snooping > Interface Configuration**.

Interface	Admin Mode	Group Membership Interval(secs)	Max Response Time(secs)	Present Expiration Time(secs)	Fast Leave Admin Mode
1/0/1	Disable	260	10	0	Disable
1/0/2	Disable	260	10	0	Disable
1/0/3	Disable	260	10	0	Disable
1/0/4	Disable	260	10	0	Disable
1/0/5	Disable	260	10	0	Disable
1/0/6	Disable	260	10	0	Disable
1/0/7	Disable	260	10	0	Disable
1/0/8	Disable	260	10	0	Disable
1/0/9	Disable	260	10	0	Disable
1/0/10	Disable	260	10	0	Disable
1/0/11	Disable	260	10	0	Disable

The **Interface** field displays all physical, VLAN, and LAG interfaces.

8. Select an interface.
9. In the **Admin Mode** list, select **Disable** or **Enable**.

This is the interface mode for the selected interface for MLD snooping for the switch. The default is Disable.

10. In the **Group Membership Interval (secs)** field, specify the amount of time you want the switch to wait for a report for a particular group on a particular interface before it deletes that interface from the group.

The valid range is from (2 to 3600) seconds. The configured value must be greater than Max Response Time. The default is 260 seconds.

11. In the **Max Response Time (secs)** field, specify the amount of time you want the switch to wait after sending a query on an interface because it did not receive a report for a particular group on that interface.

Enter a value greater or equal to 1 and less than the group membership interval in seconds. The default is 10 seconds. The configured value must be less than the group membership interval.

12. In the **Present Expiration Time** field, specify the amount of time you want the switch to wait to receive a query on an interface before removing it from the list of interfaces with multicast routers attached.

Enter a value between 0 and 3600 seconds. The default is 0 seconds. A value of zero indicates an infinite time-out, for example no expiration.

13. In the **Fast Leave Admin mode** list, select **Disable** or **Enable**.

This sets the Fast Leave mode for a particular interface from the menu. The default is Disable.

## Configure a MLD VLAN

➤ **To configure a MLD VLAN:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Multicast > MLD Snooping > MLD VLAN Configuration**.

MLD VLAN Configuration						
:: MLD VLAN Configuration						
	VLAN ID	Admin Mode	Fast Leave Admin Mode	Group Membership Interval	Maximum Response Time	Multicast Router Expiry Time
<input checked="" type="checkbox"/>	100	Enable	Enable	260	10	0

8. Select **VLAN ID** check boxes for VLAN IDs for which MLD snooping is enabled.
9. In the **Admin Mode** list, select **Enable** to enable MLD snooping for the specified VLAN ID.
10. Use **Fast Leave Admin Mode** to enable or disable the MLD snooping Fast Leave Mode for the specified VLAN ID.
11. In the **Group Membership Interval** field, set the value for group membership interval of MLD snooping for the specified VLAN ID.

The valid range is (Maximum Response Time + 1) to 3600.

12. In the **Maximum Response Time** field, set the value for maximum response time of MLD snooping for the specified VLAN ID.

The valid range is 1 to (Group Membership Interval – 1). Its value should be less than the group membership interval value.

13. In the **Multicast Router Expiry Time** field, set the value for the multicast router expiry time of MLD snooping for the specified VLAN ID.

The valid range is 0 to 3600.

## Configure a Multicast Router

➤ **To configure a multicast router:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The Login screen displays.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Multicast > MLD Snooping > Multicast Router Configuration**.

Interface	Multicast Router
1/0/1	Disable
1/0/2	Disable
1/0/3	Disable
1/0/4	Disable
1/0/5	Disable
1/0/6	Disable
1/0/7	Disable
1/0/8	Disable
1/0/9	Disable

8. Select the interface.

9. In the **Multicast Router** list, select **Enable** or **Disable** for the selected interface.

## Configure a Multicast Router VLAN

➤ **To configure a multicast router VLAN:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

- Select **Switching > Multicast > MLD Snooping > Multicast Router VLAN Configuration**.

Interface	VLAN ID	Multicast Router
1/0/1		Enable

- Select the interface.
- In the **VLAN ID** list, select the VLAN ID.
- In the **Multicast Router** list, select **Enable** or **Disable**.

This enables or disables the multicast router for the VLAN ID.

## Configure the MLD Snooping Querier

You can configure the parameters for the MLD snooping querier. Only a user with Read/Write access privileges can change the data on this screen.

➤ **To configure the MLD snooping querier:**

- Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
- Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
- Launch a web browser.
- Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

- Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Multicast > MLD Snooping > Querier Configuration**.

8. Select the Querier Admin Mode **Disable** or **Enable** radio button.

This specifies the administrative mode for MLD snooping for the switch. The default is Disable.

9. In the **Querier Address** field, specify the snooping querier address to be used as source address in periodic MLD queries.

This address is used when no address is configured on the VLAN on which query is being sent. The supported IPv6 formats are x:x:x:x:x:x:x and x::x.

10. In the **MLD Version** field, specify the MLD protocol version used in periodic MLD queries.

11. In the **Query Interval (secs)** field, specify the time interval in seconds between periodic queries sent by the snooping querier.

The query interval must be a value in the range of 1 and 1800. The default value is 60.

12. In the **Querier Expiry Interval (secs)** field, specify the time interval in seconds after which the last querier information is removed.

The querier expiry interval must be a value in the range of 60 and 300. The default value is 60.

The following table describes the nonconfigurable information displayed on the screen.

**Table 54. MLD Snooping Querier Configuration**

Field	Description
VLAN Ids Enabled For MLD Snooping Querier	Displays VLAN IDs enabled for MLD snooping querier.

## Configure an MLD Snooping Querier VLAN

➤ **To configure a MLD snooping querier VLAN:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.

2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Multicast > MLD Snooping > Querier VLAN Configuration**.

MLD Snooping Querier VLAN Configuration								
:: MLD Snooping Querier VLAN Configuration								
	VLAN ID	Querier Election Participate Mode	Querier VLAN Address	Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Max Response Time
<input type="checkbox"/>								

8. Use **VLAN ID** to specify the VLAN ID on which MLD snooping querier is administratively enabled and a VLAN exists in the VLAN database.
9. In the **Querier Election Participate Mode** list, select **Enable** or **Disable**.

This enables or disables the MLD snooping querier participate in election mode. When this mode is disabled, up on seeing other querier of the same version in the VLAN, the snooping querier move to non querier state. Only when this mode is enabled, does the snooping querier participate in querier election in which the lowest IP address wins the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.

10. In the **Querier VLAN Address** field, specify the snooping querier address to be used as the source address in periodic MLD queries sent on the specified VLAN.

The following table describes the nonconfigurable information displayed on the screen.

**Table 55. MLD Snooping Querier VLAN Configuration**

Field	Description
Operational State	Specifies the operational state of the MLD snooping querier on a VLAN. It can be in any of the following states: <ul style="list-style-type: none"> <li>• Querier: The snooping switch is the querier in the VLAN. The snooping switch sends out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch sees a better querier in the VLAN, it moves to non-querier mode.</li> <li>• Non-Querier: The snooping switch is in non-querier mode in the VLAN. If the querier expiry interval timer is expired, the snooping switch moves into querier mode.</li> <li>• Disabled: The snooping Querier is not operational on the VLAN. The snooping querier moves to disabled mode when MLD snooping is not operational on the VLAN or when the querier address is not configured or the network management address is also not configured.</li> </ul>
Operational Version	Displays the operational MLD protocol version of the querier.
Last Querier Address	Displays the IP address of the last querier from which a query was snooped on the VLAN.
Last Querier Version	Displays the MLD protocol version of the last querier from which a query was snooped on the VLAN.
Operational Max Response Time	Displays maximum response time to be used in the queries that are sent by the snooping querier.

## Configure MVR

➤ **To configure MVR:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

- Select **Switching > MVR > Basic > MVR Configuration**.

MVR Configuration	
:: MVR Configuration	
MVR Running	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
MVR Multicast Vlan	1 (1 to 4094)
MVR Max Multicast Groups	256
MVR Current Multicast Groups	0
MVR Global query response time	5 (1 to 100)
MVR Mode	<input checked="" type="radio"/> compatible <input type="radio"/> dynamic

- Select the MVR Running **Enable** or **Disable** radio button.

The factory default is **Disable**.

- In the **MVR multicast** field, specify the VLAN on which MVR multicast data is received.

All source ports belong to this VLAN. The value can be set in a range of 1 to 4093. The default value is 1.

The following table describes the nonconfigurable information displayed on the screen.

**Table 56. MVR Configuration**

Field	Definition
MVR Max Multicast Groups	Displays the maximum number of multicast groups that MVR supports.
MVR Current Multicast Groups	Displays current number of the MVR groups allocated.

- In the **MVR Global query response time** field, set the maximum time to wait for the IGMP reports membership on a receiver port.

This time applies only to receiver-port leave processing. When an IGMP query is sent from a receiver port, the switch waits for the default or configured MVR query time for an IGMP group membership report before removing the port from the multicast group membership. The value is equal to the tenths of a second. The range is from 1 to 100 tenths. The factory default is 5 tenths or one-half.

- Select MVR Mode **Compatible** or **Dynamic** radio button.

This specifies the MVR mode of operation. The factory default is **Compatible**.

## Configure Advanced MVR Settings

➤ **To configure advanced MVR settings:**

- Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.

2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > MVR > Advanced > MVR Configuration**.

MVR Configuration	
<b>MVR Running</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>MVR Multicast Vlan</b>	1 (1 to 4094)
<b>MVR Max Multicast Groups</b>	256
<b>MVR Current Multicast Groups</b>	0
<b>MVR Global query response time</b>	5 (1 to 100)
<b>MVR Mode</b>	<input checked="" type="radio"/> compatible <input type="radio"/> dynamic

8. Select the MVR Running **Disable** or **Enable** radio button.

The factory default is Disable.

9. In the **MVR Multicast VLAN** field, specify the VLAN on which MVR multicast data is received.

All source ports belong to this VLAN. The value can be set in a range of 1 to 4094. The default value is 1.

10. In the **MVR Global query response time** field, set the maximum time to wait for the IGMP reports membership on a receiver port.

This time applies only to receiver-port leave processing. When an IGMP query is sent from a receiver port, the switch waits for the default or configured MVR query time for an IGMP group membership report before removing the port from the multicast group membership. The value is equal to the tenths of second. The range is from 1 to 100 tenths. The factory default is 5 tenths or one-half.

11. Use the **MVR Mode** field to specify the MVR mode of operation.

The factory default is Compatible.

12. Click the **REFRESH** button to update the screen to show the latest MVR configuration.

- 13.** Click the **APPLY** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information displayed on the screen.

**Table 57. MVR Configuration**

Field	Definition
MVR Max Multicast Groups	Displays the maximum number of multicast groups that MVR supports.
MVR Current Multicast Groups	Displays current number of the MVR groups allocated.

## Configure MVR Groups

➤ **To configure MVR groups:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > MVR > Advanced > MVR Group Configuration**.

<b>MVR Group Configuration</b>				
:: MVR Group Configuration				
	<b>MVR Group IP</b>	Status	Members	Count
	169.254.100.100			

8. In the **MVR Group IP** list, specify the IP address for the new MVR group.
9. In the **Count** field, specify the number of contiguous MVR groups.

It is a service option helping user to create multiple MVR groups through the single click of the **ADD** button. If the field is empty, then clicking the button creates only one new group. The field is displayed as empty for each particular group. The range is from 1 to 256.

- 10.** To add a new MVR group, click the **ADD** button.
- 11.** To delete a selected MVR group, click the **DELETE** button.

The following table describes the nonconfigurable information displayed on the screen.

**Table 58. MVR Group Configuration**

Field	Definition
Status	Displays the status of the specific MVR group.
Members	Displays the list of ports that participate in the specific MVR group.

## Configure an MVR Interface

➤ **To configure an MVR interface:**

- 1.** Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
- 2.** Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
- 3.** Launch a web browser.
- 4.** Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

- 5.** Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- 6.** Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > MVR > Advanced > MVR Interface Configuration**.

MVR Interface Configuration					
:: MVR Interface Configuration					
1 All	Interface	Admin Mode	Type	Immediate Leave	Status
<input type="checkbox"/>	0/1	Disable	none	Disable	ACTIVE/InVLAN
<input type="checkbox"/>	0/2	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	0/3	Disable	none	Disable	ACTIVE/InVLAN
<input type="checkbox"/>	0/4	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	0/5	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	0/6	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	0/7	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	0/8	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	0/9	Disable	none	Disable	ACTIVE/InVLAN
<input type="checkbox"/>	0/10	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	0/11	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	0/12	Disable	none	Disable	INACTIVE/InVLAN

The Status field displays the status for each port.

8. Select **Interface** check boxes for the interface.
9. In the **Admin Mode** list, select **Enable** or **Disable**.  
This enables or disables MVR on a port. The factory default is **Disable**.
10. In the **Type** list, select **receiver** or **sourcet**.  
This sets the MVR port as a receiver or source port. The default port type is **none**.
11. In the **Immediate Leave** list, select **Enable** or **Disable**.  
This sets the Immediate Leave feature of MVR on a port. The factory default is **Disable**.
12. Click the **REFRESH** button to refresh the screen to show the latest MVR interface configuration.
13. Click the **APPLY** button.  
The updated configuration is sent to the switch. Configuration changes take effect immediately.

## Configure MVR Group Membership

- To configure MVR group membership:
  1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
  2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
  3. Launch a web browser.
  4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

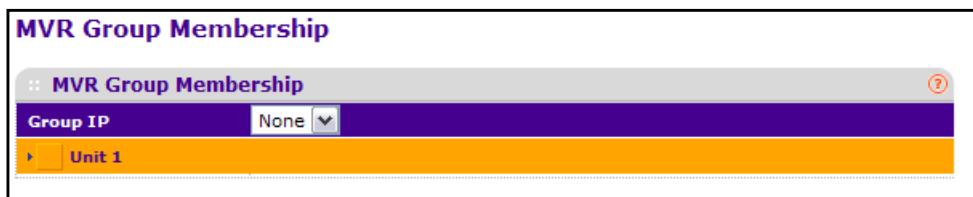
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > MVR > Advanced > MVR Group Membership**.



8. In the **Group IP** list, specify the IP multicast address of the MVR group.
9. Use the **Port List** to show the configured list of members of the selected MVR group.  
You can use this port list to add the ports you selected to this MVR group.
10. Click the **APPLY** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

## View MVR Statistics

➤ **To view MVR statistics:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7.** Select **Switching > MVR > Advanced > MVR Statistics**.

<b>Statistics</b>	
:: <b>Mvr Statistics</b>	
<b>IGMP Query Received</b>	0
<b>IGMP Report V1 Received</b>	0
<b>IGMP Report V2 Received</b>	0
<b>IGMP Leave Received</b>	0
<b>IGMP Query Transmitted</b>	0
<b>IGMP Report V1 Transmitted</b>	0
<b>IGMP Report V2 Transmitted</b>	0
<b>IGMP Leave Transmitted</b>	0
<b>IGMP Packet Receive Failures</b>	0
<b>IGMP Packet Transmit Failures</b>	0

**8.** Click the **REFRESH** button to refresh the screen to show the latest MVR statistics.

The following table describes the nonconfigurable information displayed on the screen.

**Table 59. MVR Statistics**

<b>Field</b>	<b>Definition</b>
IGMP Query Received	Displays the number of received IGMP queries.
IGMP Report V1 Received	Displays the number of received IGMP reports V1.
IGMP Report V2 Received	Displays the number of received IGMP reports V2.
IGMP Leave Received	Displays the number of received IGMP leaves.
IGMP Query Transmitted	Displays the number of transmitted IGMP queries.
IGMP Report V1 Transmitted	Displays the number of transmitted IGMP reports V1.
IGMP Report V2 Transmitted	Displays the number of transmitted IGMP reports V2.
IGMP Leave Transmitted	Displays the number of transmitted IGMP leaves.
IGMP Packet Receive Failures	Displays the number of IGMP packet receive failures.
IGMP Packet Transmit Failures	Displays the number of IGMP packet transmit failures.

## Manage MAC Addresses

You can view the MAC address table, convert dynamic MAC addresses to static addresses, and configure static addresses.

## View the MAC Address Table

This table contains information about unicast entries for which the switch has forwarding or filtering information. This information is used by the transparent bridging function in determining how to propagate a received frame.

➤ **To view the MAC Address Table:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7.** Select **Switching > Address Table > Advanced > Address Table**.

Address Table			
:: MAC Address Table			
Search By		VLAN ID	GO
Total MAC Addresses			43
VLAN ID	MAC Address	Port	status
1	00:06:02:05:06:05	0/12	Learned
1	00:07:03:05:05:05	5/1	Management
1	00:0F:FE:00:8E:76	0/12	Learned
1	00:16:9C:E1:D8:00	0/12	Learned
1	00:19:E7:D3:82:2D	0/12	Learned
1	00:1A:A0:1A:94:FA	0/12	Learned
1	00:E0:0C:BC:E5:60	0/12	Learned
1	52:54:40:22:46:5C	0/12	Learned
1	C8:0A:A9:32:F3:63	0/12	Learned
2	00:07:03:05:05:07	vlan 2	Management
3	00:07:03:05:05:07	vlan 3	Management
4	00:07:03:05:05:07	vlan 4	Management
5	00:07:03:05:05:07	vlan 5	Management
6	00:07:03:05:05:07	vlan 6	Management
7	00:07:03:05:05:07	vlan 7	Management
8	00:07:03:05:05:07	vlan 8	Management
9	00:07:03:05:05:07	vlan 9	Management
10	00:07:03:05:05:07	vlan 10	Management
11	00:07:03:05:05:07	vlan 11	Management
12	00:07:03:05:05:07	vlan 12	Management
13	00:07:03:05:05:07	vlan 13	Management
14	00:07:03:05:05:07	vlan 14	Management
15	00:07:03:05:05:07	vlan 15	Management
16	00:07:03:05:05:07	vlan 16	Management
17	00:07:03:05:05:07	vlan 17	Management
18	00:07:03:05:05:07	vlan 18	Management
19	00:07:03:05:05:07	vlan 19	Management
20	00:07:03:05:05:07	vlan 20	Management

**8.** Use **Search By** to search by MAC address, VLAN ID, or port.

- **Searched by MAC Address.** Select MAC address and enter the 6-byte hexadecimal MAC address in two-digit groups separated by colons, for example, 01:23:45:67:89:AB. Then click the **Go** button. If the address exists, that entry is displayed as the first entry followed by the remaining (greater) MAC addresses. An exact match is required.
- **Searched by VLAN ID.** Select VLAN ID, and enter the VLAN ID, for example 100. Then click the **Go** button. If the address exists, the entry is displayed as the first entry followed by the remaining (greater) mac addresses.
- **Searched by Port.** Select Port from the list and enter the port ID in Unit/Slot/Port format, for example 2/1/1. Then click the **Go** button. If the address exists, the entry is displayed as the first entry followed by the remaining (greater) MAC addresses.

The following table describes the nonconfigurable information displayed on the screen.

**Table 60. MAC Address Table**

Field	Description
Total MAC Address	Displaying the number of total MAC addresses learned or configured.
MAC Address	A unicast MAC address for which the switch has forwarding or filtering information. The format is a 6 byte MAC address that is separated by colons, for example, 01:23:45:67:89:AB.
VLAN ID	The VLAN ID associated with the MAC address.
Port	The port on which this address was learned.
Status	The status of this entry. The meanings of the values are as follows: <ul style="list-style-type: none"> <li>• <b>Static.</b> the value of the corresponding instance was added by the system or a user and cannot be relearned.</li> <li>• <b>Learned.</b> the value of the corresponding instance was learned, and is being used.</li> <li>• <b>Management.</b> the value of the corresponding instance is also the value of an existing instance of dot1dStaticAddress.</li> </ul>

## Configure Dynamic Addresses Aging Interval

You can set the address aging interval for the specified forwarding database.

➤ **To set the address aging interval:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Address Table> Advanced > Dynamic Addresses.**

Dynamic Address Table	
Address Aging Timeout (seconds)	300 (10 to 1000000)

8. Use **Address Aging Timeout (seconds)** to specify the time-out period in seconds for aging out dynamically learned forwarding information.

802.1D-1990 recommends a default of 300 seconds. The value can be specified as any number between 10 and 1000000 seconds. The factory default is 300.

## Configure a Static MAC Address

- To configure a MAC address:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Address Table> Advanced > Static MAC Address.**

Static MAC Address Configuration	
Port List	
Interface	1/0/1
Static MAC Address Table	
Static MAC Address	VLAN ID
D4:BE:D9:3A:90:53	200

8. Use **Interface** to select the physical interface or LAG.
9. Use the **Static MAC Address** to input the MAC address.
10. Select the **VLAN ID** associated with the MAC address.
11. To add a new static MAC address to the switch, click the **ADD** button.
12. To delete a static MAC address from the switch, click the **DELETE** button.

## Configure Port Settings

You can configure the physical interfaces on the switch.

➤ **To configure port settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Ports > Port Configuration**.

Port Configuration											
Port Configuration											
1	2	LAGS	All	Go To Port				GO			
		Port	Port Type	STP mode	Admin Mode	LACP Mode	Physical Mode	Physical Status	Link Status	Link Trap	Maximum Frame Size
											ifindex
		1/0/1	Normal	Enable	Enable	Enable	Auto	1000 Mbps	Link Up	Enable	1518
		1/0/2	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	1518
		1/0/3	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	1518
		1/0/4	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	1518
		1/0/5	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	1518
		1/0/6	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	1518
		1/0/7	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	1518
		1/0/8	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	1518
		1/0/9	Normal	Enable	Enable	Enable	Auto	Unknown	Link Down	Enable	1518

8. Use **Port** to select the interface.

**9.** Use **STP Mode** to select the Spanning Tree Protocol administrative mode for the port or LAG. The possible values are as follows:

- **Enable** -Select this to enable the Spanning Tree Protocol for this port.
- **Disable** -Select this to disable the Spanning Tree Protocol for this port.

**10.** Use the **Admin Mode** menu to select the port control administration state.

You must select Enable if you want the port to participate in the network. The factory default is enabled.

**11.** Use **LACP Mode** to select the Link Aggregation Control Protocol administration state.

The mode must be enabled in order for the port to participate in link aggregation. The factory default is enabled.

**12.** Use the **Physical Mode** list to select the port's speed and duplex mode.

If you select auto, the duplex mode and speed are set by the autonegotiation process. Note that the port's maximum capability (full duplex and speed) is advertised. Otherwise, your selection determines the port's duplex mode and transmission rate. The factory default is auto.

**13.** Use the **Link Trap object** to determine whether to send a trap when link status changes. The factory default is enabled.

**14.** Use **Maximum Frame Size** to specify the maximum Ethernet frame size the interface supports or is configured for, including Ethernet header, CRC, and payload (1518 to 9216).

The default maximum frame size is 1518.

**15.** Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See [Save Configuration](#) on page 405.

The following table describes the nonconfigurable information displayed on the screen.

**Table 61. Port Configuration**

Field	Description
Port Type	For normal ports this field is normal. Otherwise, the possible values are as follows: <ul style="list-style-type: none"> <li>• Mirrored. The port is a mirrored port on which all the traffic is copied to the probe port.</li> <li>• Probe. Use this port to monitor mirrored port.</li> <li>• Trunk Number. The port is a member of a link aggregation trunk. Look at the LAG screens for more information.</li> </ul>
Physical Status	Indicates the port speed and duplex mode.
Link Status	Indicates whether the link is up or down.
ifIndex	The ifIndex of the interface table entry associated with this port.

## Enter a Port Description

➤ To specify a port description:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

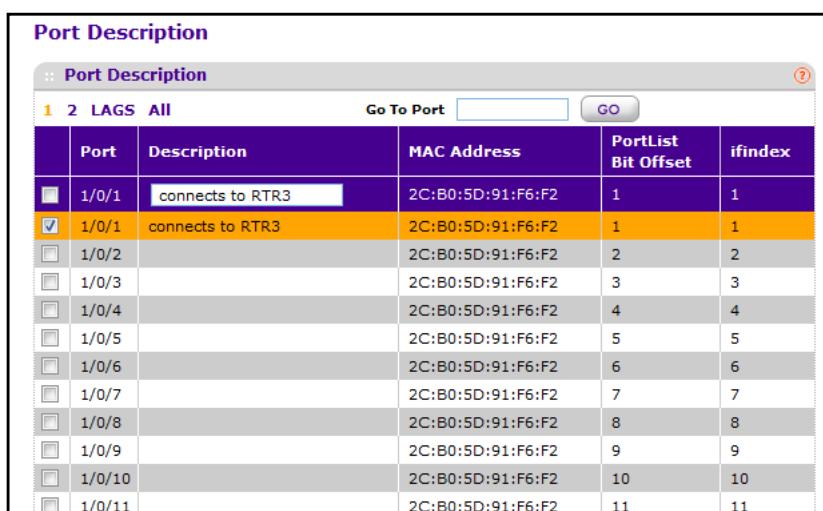
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Ports > Port Description**.



The screenshot shows a table titled "Port Description" with the following columns: Port, Description, MAC Address, PortList Bit Offset, and ifindex. The table lists 12 ports (1/0/1 to 1/0/11). The "Description" column for port 1/0/1 contains the value "connects to RTR3". Other ports have empty or default values in the description field.

	Port	Description	MAC Address	PortList Bit Offset	ifindex
<input type="checkbox"/>	1/0/1	connects to RTR3	2C:B0:5D:91:F6:F2	1	1
<input checked="" type="checkbox"/>	1/0/1	connects to RTR3	2C:B0:5D:91:F6:F2	1	1
<input type="checkbox"/>	1/0/2		2C:B0:5D:91:F6:F2	2	2
<input type="checkbox"/>	1/0/3		2C:B0:5D:91:F6:F2	3	3
<input type="checkbox"/>	1/0/4		2C:B0:5D:91:F6:F2	4	4
<input type="checkbox"/>	1/0/5		2C:B0:5D:91:F6:F2	5	5
<input type="checkbox"/>	1/0/6		2C:B0:5D:91:F6:F2	6	6
<input type="checkbox"/>	1/0/7		2C:B0:5D:91:F6:F2	7	7
<input type="checkbox"/>	1/0/8		2C:B0:5D:91:F6:F2	8	8
<input type="checkbox"/>	1/0/9		2C:B0:5D:91:F6:F2	9	9
<input type="checkbox"/>	1/0/10		2C:B0:5D:91:F6:F2	10	10
<input type="checkbox"/>	1/0/11		2C:B0:5D:91:F6:F2	11	11

8. Use **Port Description** to enter the description string to be attached to a port.

It can be up to 64 characters in length.

The following table describes the nonconfigurable information displayed on the screen.

**Table 62. Port Description**

Field	Description
Port	Selects the interface.
MAC Address	Displays the physical address of the specified interface.
PortList Bit Offset	Displays the bit offset value that corresponds to the port when the MIB object type PortList is used to manage in SNMP.
ifIndex	Displays the interface index associated with the port.

## Link Aggregation Group Overview

Link aggregation groups (LAGs), which are also known as port channels, allow you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. You assign the LAG VLAN membership after you create a LAG. The LAG by default becomes a member of the management VLAN.

A LAG interface can be either static or dynamic, but not both. All members of a LAG must participate in the same protocols. A static port channel interface does not require a partner system to be able to aggregate its member ports.

Static LAGs are supported. When a port is added to a LAG as a static member, it neither transmits nor receives LACPDUs.

## Configure LAG Settings

You can use LAGs to group one or more full-duplex Ethernet links to be aggregated together to form a link aggregation group, which is also known as a port channel. The switch treats the LAG as if it were a single link.

➤ **To configure LAG settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

**6.** Click the **Login** button.

The web management interface menu displays.

**7.** Select **Switching > LAG > LAG Configuration**.

LAG Configuration												
:: LAG Configuration												
	LAG Name	Description	LAG ID	Admin Mode	Hash Mode	STP Mode	Static Mode	Link Trap	Configured Ports	Active Ports	LAC Status	
	ch1		lag 1	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Disable	Disable			Down	
	ch2		lag 2	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Disable	Disable			Down	
	ch3		lag 3	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Disable	Disable			Down	

**8.** Use **LAG Name** to enter the name you want assigned to the LAG.

You can enter any string of up to 15 alphanumeric characters. A valid name must be specified for you to create the LAG.

**9.** Use the list to enable or disable **Admin Mode**.

When the LAG is disabled, no traffic flows and LACPDU is dropped, but the links that form the LAG are not released. The default is enable.

**10.** Use **Hash Mode** to select the load-balancing mode used on a port channel (LAG).

Traffic is balanced on a port channel (LAG) by selecting one of the links in the channel over which to transmit specific packets. The switch selects the link by creating a binary pattern from selected fields in a packet, and associating that pattern with a particular link:

- **Src MAC, VLAN, EType, incoming port**—Source MAC, VLAN, EtherType, and incoming port associated with the packet.
- **Dest MAC, VLAN, EType, incoming port**—Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
- **Src/Dest MAC, VLAN, EType, incoming port**—Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
- **Src IP and Src TCP/UDP Port**—Source IP and Source TCP/UDP fields of the packet.
- **Dest IP and Dest TCP/UDP Port**—Destination IP and Destination TCP/UDP Port fields of the packet.
- **Src/Dest IP and TCP/UDP Port**—Source/Destination IP and source/destination TCP/UDP Port fields of the packet.
- **Enhanced hashing mode**—Features MODULO-N operation based on the number of ports in the LAG, non-unicast traffic and unicast traffic hashing using a common hash algorithm, excellent load balancing performance, and packet attributes selection based on the packet type:
  - For L2 packets, source and destination MAC address are used for hash computation.
  - For L3 packets, source IP, destination IP address, TCP/UDP ports are used.

- 11.** Use **STP Mode** to enable or disable the Spanning Tree Protocol administrative mode associated with the LAG.

The possible values are as follows:

- **Disable**—Spanning tree is disabled for this LAG.
- **Enable**—Spanning tree is enabled for this LAG.

- 12.** Use **Static Mode** to select enable or disable.

When the LAG is enabled, it does not transmit or process received LACPDUs, for example, the member ports do not transmit LACPDUs and all the LACPDUs it can receive are dropped. The factory default is disabled.

- 13.** Use **Link Trap** to specify whether a trap is sent when link status changes.

The factory default is enabled, which causes the trap to be sent.

- 14.** Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See *Save Configuration* on page 405.

The following table describes the nonconfigurable information displayed on the screen.

**Table 63. LAG Configuration**

Field	Description
LAG Description	Enter the description string to be attached to a LAG. It can be up to 64 characters in length.
LAG ID	Identification of the LAG.
Configured Ports	Indicate the ports that are members of this port channel.
Active Ports	Indicates the ports that are actively participating in the port channel.
LAG State	Indicates whether the Link is up or down.

## Configure LAG Membership

You can select two or more full-duplex Ethernet links to be aggregated together to form a link aggregation group (LAG), which is also known as a port channel. The switch can treat the port channel as if it were a single link.

➤ **To configure LAG membership:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > LAG > LAG Membership**.

LAG Membership																											
LAG ID	Lag 1	LAG Name	ch1																								
LAG Description																											
Admin Mode	Enable	Link Trap	Disable																								
STP Mode	Enable	Static Mode	Disable																								
Hash Mode	Src/Dest MAC, VLAN, EType, incoming port																										
Port Selection Table																											
Unit 1																											
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24			
	✓	✓	✓																								
	25	26	27	28																							
Unit 2																											

8. Use **LAG ID** to select the identification of the LAG.
9. Use **LAG Name** to enter the name you want assigned to the LAG. You can enter any string of up to 15 alphanumeric characters. A valid name must be specified for you to create the LAG.
10. Use **LAG Description** to enter the description string to be attached to a LAG.

It can be up to 64 characters in length.

11. In the **Admin Mode** list, select **Enable** or **Disable**.

When the LAG is disabled, no traffic flows and LACPDU are dropped, but the links that form the LAG are not released. The factory default is enabled.

12. Use **Link Trap** to specify whether a trap is sent when link status changes.

The factory default is enable, which causes the trap to be sent.

13. Use **STP Mode** to enable or disable the Spanning Tree Protocol administrative mode associated with the LAG.

The possible values are as follows:

- **Disable**. Spanning tree is disabled for this LAG.
- **Enable**. Spanning tree is enabled for this LAG.

14. Use **Static Mode** to select Enable or Disable.

When the LAG is enabled, it does not transmit or process received LACPDUs, for example, the member ports do not transmit LACPDUs and all the LACPDUs it can receive are dropped. The factory default is Disable.

**15. Use Hash Mode** to select the load-balancing mode used on a port channel (LAG).

Traffic is balanced on a port channel (LAG) by selecting one of the links in the channel over which to transmit specific packets. The link is selected by creating a binary pattern from selected fields in a packet, and associating that pattern with a particular link:

- **Src MAC, VLAN ,EType , incoming port.** Source MAC, VLAN, EtherType, and incoming port associated with the packet.
- **Dest MAC, VLAN, EType, incoming port.** Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
- **Src/Dest MAC, VLAN, EType, incoming port.** Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
- **Src IP and Src TCP/UDP Port.** Source IP and Source TCP/UDP fields of the packet.
- **Dest IP and Dest TCP/UDP Port.** Destination IP and Destination TCP/UDP Port fields of the packet.
- **Src/Dest IP and TCP/UDP Port.** Source/Destination IP and source/destination TCP/UDP Port fields of the packet.
- **Enhanced Hashing mode.** Features MODULO-N operation based on the number of ports in the LAG, non-unicast traffic and unicast traffic hashing using a common hash algorithm, excellent load balancing performance, and packet attributes selection based on the packet type:
  - For L2 packets, source and destination MAC address are used for hash computation.
  - For L3 packets, source IP, destination IP address, TCP/UDP ports are used.

**16. Use the Port Selection Table** to select the ports as members of the LAG.

# Routing

---

# 4

This chapter covers the following topics:

- *Manage the Routing Table*
- *Configure IP Settings*
- *Configure Advanced IP Settings*
- *VLAN Overview*
- *ARP Overview*
- *Configure Router Discovery*

## Manage the Routing Table

The Routing Table collects routes from multiple sources: static routes and local routes. The Routing Table can use multiple routes to the same destination from multiple sources. The Routing Table lists all routes.

### Configure Basic Routes

➤ **To configure basic routes:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

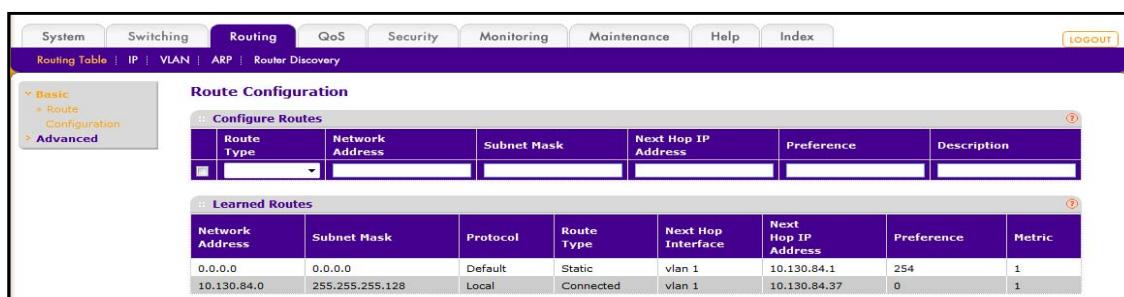
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Routing > Routing Table > Basic > Route Configuration**.



8. Use the **Route Type** field to specify the default or static reject.

If you are creating a default route, all that must be specified is the next hop IP address; otherwise, each field must be specified.

9. **Network Address** displays the IP route prefix for the destination.

10. **Subnet Mask** indicates the portion of the IP interface address that identifies the attached network.

This is also referred to as the subnet/network mask.

- 11. Next Hop IP Address** displays the outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.

The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

- 12. Preference** displays an integer value from 1 to 255.

You can specify the preference value (sometimes called administrative distance) of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, the user controls whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.

- 13. Use Description** to specify the description of this route.

The description must consist of alphanumeric, hyphen, or underscore characters. It can be up to 31 characters in length.

- 14.** To add a new static route entry to the switch, click the **ADD** button.

- 15.** To delete a static route entry from the switch, click the **DELETE** button.

Click the **REFRESH** button to refresh the screen to show the latest learned routes.

The following table describes the nonconfigurable information displayed on the screen.

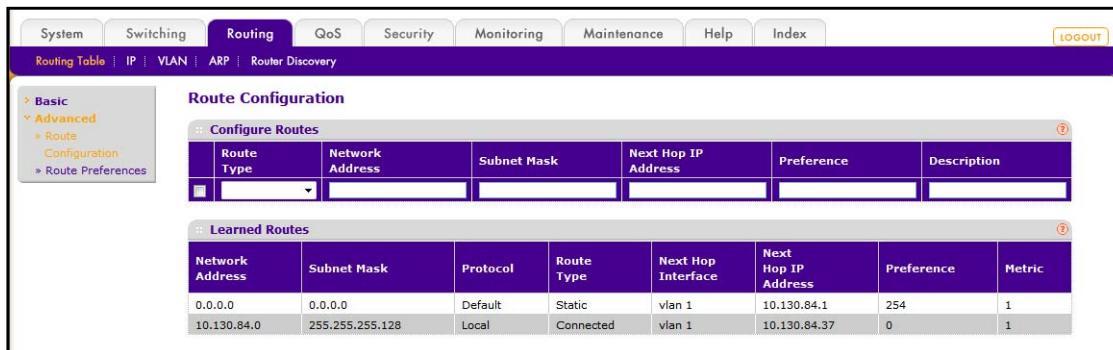
**Table 64. Route Configuration - Learned Routes**

Field	Description
Network Address	The IP route prefix for the destination.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
Protocol	This field tells which protocol created the specified route. The possibilities are as follows: <ul style="list-style-type: none"> <li>• Local</li> <li>• Static</li> </ul>
Route Type	This field can be Connected or Static or Dynamic based on the protocol.
Next Hop Interface	The outgoing router interface to use when forwarding traffic to the destination.
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network.
Metric	Administrative cost of the path to the destination. If no value is entered, default is 1. The range is 0 – 255.

## Configure Advanced Routes

➤ To configure advanced routes:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Routing > Routing Table > Advanced > Route Configuration**.



8. In the **Route Type** field, select **default** or **static reject**.

If you are creating a default route, all that must be specified is the next hop IP address; otherwise, each field must be specified. The fields that you must specify depend on your selections in this screen.

- **Network Address** displays the IP route prefix for the destination.
  - **Subnet Mask** indicates the portion of the IP interface address that identifies the attached network.
- This is also referred to as the subnet/network mask.
- **Next Hop IP Address** displays the outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

- **Preference** displays an integer value from (1 to 255). You can specify the preference value (sometimes called administrative distance) of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, the user controls whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.
- 9.** In the **Description** field, specify the description of this route.  
The description must consist of alpha-numeric, hyphen, or underscore characters. It can be up to 31 characters in length.
- 10.** To add a new static route entry to the switch, click the **ADD** button.
- 11.** To delete a static route entry from the switch, click the **DELETE** button.
- Click the **REFRESH** button to refresh the screen to show the latest learned routes.

The following table describes the nonconfigurable information displayed on the screen.

**Table 65. Route Configuration, Learned Routes Table**

Field	Description
Network Address	The IP route prefix for the destination.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
Protocol	This field tells which protocol created the specified route. The possibilities are as follows: <ul style="list-style-type: none"> <li>• Local</li> <li>• Static</li> </ul>
Route Type	This field can be either default or static. If creating a default route, all that must be specified is the next hop IP address, otherwise each field must be specified.
Next Hop Interface	The outgoing router interface to use when forwarding traffic to the destination.
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

**Table 65. Route Configuration, Learned Routes Table**

Field	Description
Preference	The preference is an integer value from 0 to 255. You can specify the preference value (sometimes called administrative distance) of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, the user controls whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.
Metric	Administrative cost of the path to the destination. If no value is entered, default is 1. The range is 0 –255.

## Configure Route Preferences

Use this panel to configure the default preference for each protocol, such as 60 for static routes, 120 for RIP. These values are arbitrary values in the range of 1 to 255 and are independent of route metrics. Most routing protocols use a route metric to determine the shortest path known to the protocol, independent of any other protocol.

The best route to a destination is chosen by selecting the route with the lowest preference value. When there are multiple routes to a destination, the preference values are used to determine the preferred route. If there is still a tie, the route with the best route metric is chosen. To avoid problems with mismatched metrics (for example, RIP and OSPF metrics are not directly comparable), you must configure different preference values for each of the protocols.

➤ **To configure route preferences:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Routing > Routing Table > Advanced > Route Preferences**.

Route Preferences	
Local	0
Static	1

(1 to 255)

8. Use **Static** to specify the static route preference value in the router.

The default value is 1. The range is 1 to 255.

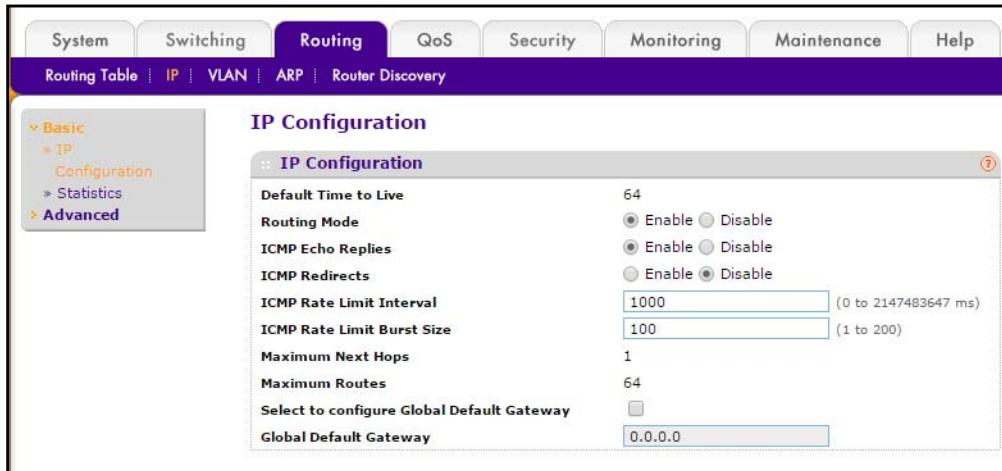
## Configure IP Settings

You can configure routing parameters for the switch, as opposed to an interface.

➤ **To change the IP configuration:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.

**7.** Select **Routing > IP > Basic > IP Configuration**.



The screen displays the default time to live, the maximum next hops, and the maximum routes.

**8.** Select the Routing Mode **Enable** or **Disable** radio button.

You must enable routing for the switch before you can route through any of the interfaces. The default value is disable.

**9.** Select the ICMP Echo Replies **Enable** or **Disable** radio button.

If ICMP echo replies are enabled, then only the router can send ECHO replies. By default ICMP echo replies are sent for echo requests.

**10.** Select the ICMP Redirects **Enable** or **Disable** radio button.

If it is enabled globally and on the interface level, then only the router can send ICMP redirects.

**11.** Use **ICMP Rate Limit Interval** to control the ICMP error packets by specifying the number of ICMP error packets that are allowed per burst interval.

By default, the rate limit is 100 packets/sec for example, burst interval is 1000 msec. To disable ICMP rate limiting, set this field to 0. The valid rate interval must be in the range 0 to 2147483647.

**12.** Use **ICMP Rate Limit Burst Size** to control the ICMP error packets by specifying the number of ICMP error packets that are allowed per burst interval.

By default, burst size is 100 packets. When the burst interval is 0, then configuring this field is not a valid operation. The valid burst size must be in the range 1 to 200.

**13.** Use **Select to configure Global Default Gateway** to edit the Global Default Gateway field.

**14.** Use **Global Default Gateway** to set the global default gateway to the manually configured value.

A default gateway configured with this command is more preferred than a default gateway learned from a DHCP server. Only one default gateway can be configured. If you invoke this command multiple times, each command replaces the previous value.

**15.** Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See *Save Configuration* on page 405.

## View IP Statistics

The statistics reported on this screen are as specified in RFC 1213.

➤ **To view IP statistics:**

- 1.** Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
- 2.** Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
- 3.** Launch a web browser.
- 4.** Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

- 5.** Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- 6.** Click the **Login** button.

The web management interface menu displays.

**7. click Routing > IP > Basic > Statistics.**

IP Statistics	
IP Statistics	
IplnReceives	9835
IplnHdrErrors	0
IplnAddrErrors	0
IpfwdDatagrams	0
IplnUnknownProtos	0
IplnDiscards	0
IplnDelivers	9017
IplnRequests	7956
IplnDiscards	0
IplnNoRoutes	0
IprasmTimeout	60
IprasmReqds	0
IprasmOKs	0
IprasmFails	0
IprfragOKs	0
IprfragFails	0
IprfragCreates	0
IproutingDiscards	0
IcmpInMsgs	1
IcmpInErrors	0
IcmpInDestUnreachs	0
IcmpInTimeExcds	0
IcmpInParmProbs	0
IcmpInSrcQuenches	0
IcmpInRedirects	0
IcmpInEchos	0
IcmpInEchoRps	1
IcmpInTimestamps	0
IcmpInTimestampRps	0
IcmpInAddrMasks	0
IcmpInAddrMaskRps	0
IcmpOutMsgs	1
IcmpOutErrors	0
IcmpOutDestUnreachs	0
IcmpOutTimeExcds	0
IcmpOutParmProbs	0
IcmpOutSrcQuenches	0
IcmpOutRedirects	0
IcmpOutEchos	1
IcmpOutEchoRps	0
IcmpOutTimestamps	0
IcmpOutTimestampRps	0
IcmpOutAddrMasks	0
IcmpOutAddrMaskRps	0

The following table describes the nonconfigurable information displayed on the screen.

**Table 66. IP statistics**

Field	Description
IplnReceives	The total number of input datagrams received from interfaces, including those received in error.
IplnHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on
IplnAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (such as 0.0.0.0) and addresses of unsupported classes (such as Class E). For entities that are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

**Table 66. IP statistics (continued)**

<b>Field</b>	<b>Description</b>
IpForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities that do not act as IP gateways, this counter includes only those packets that were source-routed through this entity, and the source-route option processing was successful.
IpInUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
IpInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but that were discarded (such as for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
IpInDelivers	The total number of input datagrams successfully delivered to IP user protocols (including ICMP).
IpOutRequests	The total number of IP datagrams that local IP user protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in ipForwDatagrams.
IpOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but that were discarded (such as, for lack of buffer space). This counter includes datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
IpOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams that meet this 'no-route' criterion. This includes any datagrams that a host cannot route because all of its default gateways are down.
IpReasmTimeout	The maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.
IpReasmReqds	The number of IP fragments received that needed to be reassembled at this entity.
IpReasmOKs	The number of IP datagrams successfully re-assembled.
IpReasmFails	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, and so on). This is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.
IpFragOKs	The number of IP datagrams that were successfully fragmented at this entity.
IpFragFails	The number of IP datagrams that were discarded because they needed to be fragmented at this entity but could not be, such as because their Don't Fragment flag was set.

**Table 66. IP statistics (continued)**

<b>Field</b>	<b>Description</b>
IpFragCreates	The number of IP datagram fragments that were generated as a result of fragmentation at this entity.
IpRoutingDiscards	The number of routing entries that were discarded even though they are valid. One possible reason for discarding such an entry could be to free up buffer space for other routing entries.
IcmpInMsgs	The total number of ICMP messages that the entity received. This counter includes all those counted by icmpInErrors.
IcmpInErrors	The number of ICMP messages that the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so on).
IcmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
IcmpInTimeExcds	The number of ICMP Time Exceeded messages received.
IcmpInParmProbs	The number of ICMP Parameter Problem messages received.
IcmpInSrcQuenches	The number of ICMP Source Quench messages received.
IcmpInRedirects	The number of ICMP Redirect messages received.
IcmpInEchos	The number of ICMP Echo (request) messages received.
IcmpInEchoReps	The number of ICMP Echo Reply messages received.
IcmpInTimestamps	The number of ICMP Timestamp (request) messages received.
IcmpInTimestampReps	The number of ICMP Timestamp Reply messages received.
IcmpInAddrMasks	The number of ICMP Address Mask Request messages received.
IcmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
IcmpOutMsgs	The total number of ICMP messages that this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.
IcmpOutErrors	The number of ICMP messages that this entity did not send due to problems discovered within ICMP, such as a lack of buffers. This value does not include errors discovered outside the ICMP layer, such as the inability of IP to route the resultant datagram. In some implementations there can be no types of error that contribute to this counter's value.
IcmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
IcmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
IcmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
IcmpOutSrcQuenches	The number of ICMP Source Quench messages sent.
IcmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this value is always zero, because hosts do not send redirects.
IcmpOutEchos	The number of ICMP Echo (request) messages sent.

**Table 66. IP statistics (continued)**

Field	Description
IcmpOutEchoReps	The number of ICMP Echo Reply messages sent.
IcmpOutTimestamps	The number of ICMP Timestamp (request) messages.
IcmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.
IcmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.

## Configure Advanced IP Settings

You can configure routing parameters for the switch as opposed to an interface.

➤ **To configure advanced IP settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

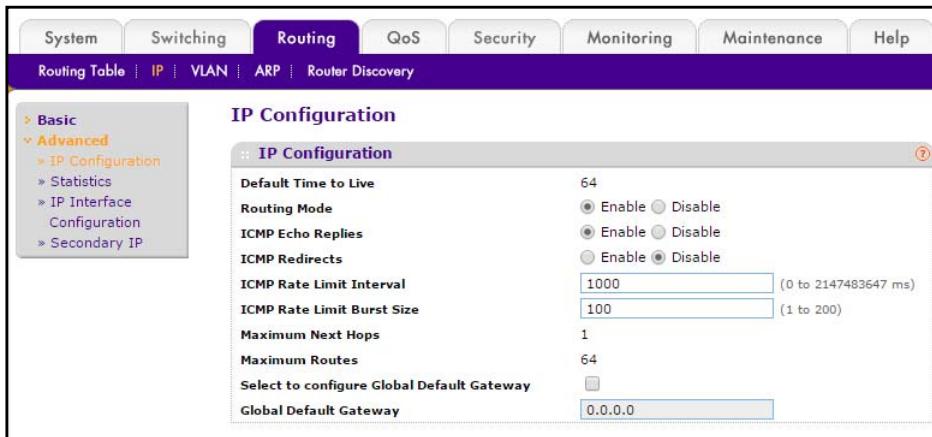
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Routing > IP > Advanced > IP Configuration**.



8. Select the Routing Mode **Enable** or **Disable** radio button.

You must enable routing for the switch before you can route through any of the interfaces. The default value is disabled.

9. Select the ICMP Echo Replies **Enable** or **Disable** radio button.

If ICMP echo replies are enabled, then only the router can send ECHO replies. By default ICMP echo replies are sent for echo requests.

10. Select the ICMP Redirects **Enable** or **Disable** radio button.

If this is enabled globally and on the interface level, then only the router can send ICMP redirects.

11. Use **ICMP Rate Limit Interval** to control the ICMP error packets by specifying the number of ICMP error packets that are allowed per burst interval.

By default, the rate limit is 100 packets/sec, for example, burst interval is 1000 msec. To disable ICMP rate limiting set this field to 0. The valid rate interval is in the range 0 to 2147483647.

12. Use **ICMP Rate Limit Burst Size** to control the ICMP error packets by specifying the number of ICMP error packets that are allowed per burst interval.

By default, the burst size is 100 packets. When the burst interval is 0, then configuring this field is not a valid operation. The valid burst size is in the range 1 to 200.

13. Use **Select to configure Global Default Gateway** to edit the Global Default Gateway field.

14. Use **Global Default Gateway** to set the global default gateway to the manually configured value.

A default gateway configured with this command is more preferred than a default gateway learned from a DHCP server. Only one default gateway can be configured. If you invoke this command multiple times, each command replaces the previous value.

The following table describes the nonconfigurable information displayed on the screen.

**Table 67. IP Configuration**

Field	Description
Default Time to Live	The default value inserted into the Time-To-Live field of the IP header of datagrams originated by the switch, if a TTL value is not supplied by the transport layer protocol.
Maximum Next Hops	The maximum number of hops supported by the switch. This is a compile-time constant.
Maximum Routes	The maximum number of routes (routing table size) supported by the switch. This is a compile-time constant.

## View IP Statistics

The statistics reported on this screen are as specified in RFC 1213.

➤ **To view the IP statistics:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Routing > IP > Advanced > IP Statistics**.

IP Statistics	
:: IP Statistics	
IplnReceives	21251
IplnHdrErrors	0
IplnAddrErrors	0
IpForwDatagrams	0
IplnUnknownProtos	0
IplnDiscards	0
IplnDelivers	21251
IpoOutRequests	28977
IpoOutDiscards	0
IpoOutNoRoutes	0
IprreasnTimeout	0
IprreasnReqds	0
IprreasnOKs	0
IprreasnFails	0
IpfragOKs	0
IpfragFails	0
IpfragCreates	0
IproutingDiscards	0
IcmpInMsgs	3
IcmpInErrors	0
IcmpInDestUnreachs	1
IcmpInTimeExcds	0
IcmpInParmProbs	0
IcmpInSrcQuenches	0
IcmpInRedirects	0

The following table describes the nonconfigurable information displayed on the screen.

**Table 68. IP statistics**

Field	Description
IplnReceives	The total number of input datagrams received from interfaces, including those received in error.
IplnHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.
IplnAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (such as 0.0.0.0) and addresses of unsupported classes (such as Class E). For entities that are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
IpForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities that do not act as IP gateways, this counter includes only those packets that were source-routed through this entity, and the source-route option processing was successful.
IplnUnknownProtos	The number of locally addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

**Table 68. IP statistics (continued)**

<b>Field</b>	<b>Description</b>
IplnDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but that were discarded (such as for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting reassembly.
IplnDelivers	The total number of input datagrams successfully delivered to IP user protocols (including ICMP).
IpOutRequests	The total number of IP datagrams that local IP user protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in ipForwDatagrams.
IpOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but that were discarded (such as for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
IpOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams that meet this 'no-route' criterion. Note that this includes any datagrams that a host cannot route because all of its default gateways are down.
IpReasmTimeout	The maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.
IpReasmReqds	The number of IP fragments received that needed to be reassembled at this entity.
IpReasmOKs	The number of IP datagrams successfully re-assembled.
IpReasmFails	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, and so on). This is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.
IpFragOKs	The number of IP datagrams that were successfully fragmented at this entity.
IpFragFails	The number of IP datagrams that were discarded because they needed to be fragmented at this entity but could not be, such as because their Don't Fragment flag was set.
IpFragCreates	The number of IP datagram fragments that were generated as a result of fragmentation at this entity.
IpRoutingDiscards	The number of routing entries that were discarded even though they are valid. One possible reason for discarding such an entry could be to free up buffer space for other routing entries.
IcmpInMsgs	The total number of ICMP messages that the entity received. Note that this counter includes all those counted by icmpInErrors.

**Table 68. IP statistics (continued)**

<b>Field</b>	<b>Description</b>
IcmpInErrors	The number of ICMP messages that the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so on).
IcmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
IcmpInTimeExclds	The number of ICMP Time Exceeded messages received.
IcmpInParmProbs	The number of ICMP Parameter Problem messages received.
IcmpInSrcQuenches	The number of ICMP Source Quench messages received.
IcmpInRedirects	The number of ICMP Redirect messages received.
IcmpInEchos	The number of ICMP Echo (request) messages received.
IcmpInEchoReps	The number of ICMP Echo Reply messages received.
IcmpInTimestamps	The number of ICMP Timestamp (request) messages received.
IcmpInTimestampReps	The number of ICMP Timestamp Reply messages received.
IcmpInAddrMasks	The number of ICMP Address Mask Request messages received.
IcmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
IcmpOutMsgs	The total number of ICMP messages that this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.
IcmpOutErrors	The number of ICMP messages that this entity did not send due to problems discovered within ICMP, such as a lack of buffers. This value should not include errors discovered outside the ICMP layer, such as the inability of IP to route the resultant datagram. In some implementations there can be no types of error that contribute to this counter's value.
IcmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
IcmpOutTimeExclds	The number of ICMP Time Exceeded messages sent.
IcmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
IcmpOutSrcQuenches	The number of ICMP Source Quench messages sent.
IcmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this value is always zero, since hosts do not send redirects.
IcmpOutEchos	The number of ICMP Echo (request) messages sent.
IcmpOutEchoReps	The number of ICMP Echo Reply messages sent.
IcmpOutTimestamps	The number of ICMP Timestamp (request) messages.
IcmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.

**Table 68. IP statistics (continued)**

Field	Description
IcmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.
IcmpOutAddrMaskReps	The number of ICMP Address Mask Reply messages sent.

## Configure an IP Interface

You can update IP interface data for this switch.

➤ **To configure an IP Interface:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Routing > IP > Advanced > IP Interface Configuration**.

The screenshot shows a table titled "IP Interface Configuration" with the following columns: Port, Description, VLAN ID, IP Address Configuration Method, IP Address, Subnet Mask, Routing Mode, Administrative Mode, and Link Speed Data Rate. The table lists 12 ports (0/1 to 0/12) all set to "None" for IP Address Configuration Method, with IP Address, Subnet Mask, and Routing Mode all set to "0.0.0.0". Administrative Mode is set to "Enable" for all ports. The table is currently displaying the first 12 rows, indicated by a "1. VLAGS All" header.

**Note:** To view the rest of the settings in this screen, you must scroll to the right.

8. Use **Go To Interface** to enter the Interface in slot/port format and click the **Go** button.

The entry corresponding to the specified interface is selected.

9. Use **Port** to select the interface.
10. Use **Description** to enter the description for the interface.
11. Use **IP Address Configuration Method** to enter the method by which an IP address is configured on the interface.

There are three methods: None, Manual, and DHCP. By default the method is None. Method None should be used to reset the DHCP method.

---

**Note:** When the configuration method is changed from **DHCP** to **None**, there is a minor delay before the screen refreshes.

---

12. Use **IP Address** to enter the IP address for the interface.

13. Use **Subnet Mask** to enter the subnet mask for the interface.

This is also referred to as the subnet/network mask, and defines the portion of the interface's IP address that is used to identify the attached network.

14. Use **Routing Mode** to enable or disable routing for an interface. The default value is enable.

15. Use **Administrative Mode** to enable or disable the administrative mode of the interface. The default value is Enable. This mode is not supported for Logical VLAN interfaces.

16. Use **Forward Net Directed Broadcasts** to select how network directed broadcast packets should be handled.

If you select Enable, network directed broadcasts are forwarded. If you select Disable, they are dropped. The default value is Disable.

17. Use **Encapsulation Type** to select the link layer encapsulation type for packets transmitted from the specified interface.

The possible values are Ethernet and SNAP. The default is Ethernet.

18. Use **Proxy Arp** to disable or enable proxy ARP for the specified interface.

19. Use **Local Proxy Arp** to disable or enable Local Proxy ARP for the specified interface.

20. Use **Bandwidth** to specify the configured bandwidth on this interface.

This parameter communicates the speed of the interface to higher-level protocols. OSPF uses bandwidth to compute link cost. The valid range is (1 to 10000000.

21. Use **ICMP Destination Unreachables** to specify the mode of sending ICMP destination unreachables on this interface.

If this is disabled, then this interface does not send ICMP destination unreachables. By default, the destination unreachables mode is enabled.

22. Use **ICMP Redirects** to enable/disable ICMP Redirects mode.

The router sends an ICMP redirect on an interface only if redirects are enabled both globally and on the interface. By default ICMP Redirects mode is enabled.

**23.** Use **IP MTU** to specify the maximum size of IP packets sent on an interface.

The valid range is 68 bytes to the link MTU. The default value is 0. A value of 0 indicates that the IP MTU is unconfigured. When the IP MTU is unconfigured, the router uses the link MTU as the IP MTU. The IP MTU is the maximum frame size minus the length of the Layer 2 header.

To delete the IP address from the selected interface, click the **DELETE** button.

Click the **REFRESH** button to refresh the screen to show the latest IP information.

The following table describes the nonconfigurable information displayed on the screen.

**Table 69. IP Interface Configuration**

Field	Description
VLAN ID	Displays the VLAN ID for the interface.
Link State	The state of the specified interface is either Active or Inactive. An interface is considered active if it the link is up and it is in the forwarding state.
Routing Interface Status	Indicates whether the link status is up or down.

## Configure a Secondary IP Address

➤ **To configure a secondary IP address:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7.** Select **Routing > IP > Advanced > Secondary IP**.



The screen displays the VLAN ID and primary IP address for this interface.

- 8.** In the **Routing Interface** list, select the interface.
- 9.** In the **Secondary IP Address** field, add a secondary IP address to the selected interface.
- 10.** In the **Secondary IP Subnet Mask** field, enter the subnet mask for the interface.

This is also referred to as the subnet/network mask, and defines the portion of the interface's IP address that is used to identify the attached network. This value is read-only once configured.

- 11.** To add a secondary IP address for the selected interface, click the **ADD** button.
- 12.** To delete the secondary IP address from the selected interface, click the **DELETE** button.

## VLAN Overview

You can configure managed switch software with some ports supporting VLANs and some supporting routing. You can also configure the software to allow traffic on a VLAN to be treated as if the VLAN were a router port.

When a port is enabled for bridging (default) rather than routing, all normal bridge processing is performed for an inbound packet, which is then associated with a VLAN. Its MAC destination address (MAC DA) and VLAN ID are used to search the MAC address table. If routing is enabled for the VLAN, and the MAC DA of an inbound unicast packet is that of the internal bridge-router interface, the packet is routed. An inbound multicast packet is forwarded to all ports in the VLAN, plus the internal bridge-router interface, if it was received on a routed VLAN.

Since a port can be configured to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port, or for a subset. VLAN routing can be used to allow more than one physical port to reside on the same subnet. It could also be used when a VLAN spans multiple physical networks, or when additional segmentation or security is required. This section shows how to configure the NETGEAR switch to support VLAN routing. A port can be either a VLAN port or a router port, but not both. However, a VLAN port can be part of a VLAN that is itself a router port.

## Use the VLAN Static Routing Wizard

The VLAN Static Routing Wizard creates a VLAN, adds selected ports to the VLAN. The VLAN Wizard gives the user the option to add the selected ports as a link aggregation groups (LAGs). The wizard does the following:

- Creates a VLAN and generates a unique name for VLAN.
- Adds selected ports to the newly created VLAN and removes selected ports from the default VLAN.
- Creates a LAG, adds selected ports to a LAG, then adds LAG to the newly created VLAN.
- Enables tagging on selected ports if the port is in another VLAN. Disables tagging if a selected port does NOT exist in another VLAN.
- Excludes ports NOT selected from the VLAN.
- Enables routing on the VLAN using the IP address and subnet mask entered.

➤ **To use the VLAN Routing Wizard:**

- Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
- Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
- Launch a web browser.
- Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

- Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **Routing > VLAN > VLAN Static Routing Wizard**.



- Use **VLAN ID** to specify the VLAN identifier (VID) associated with this VLAN.

The range of the VLAN ID is 1 to 4093.

9. Use **Ports** to display selectable physical ports and LAGs (if any).

Selected ports are added to the routing VLAN. Each port has three modes:

- **T (Tagged)**. Select the ports on which all frames transmitted for this VLAN are tagged. The ports that are selected are included in the VLAN.
- **U (Untagged)**. Select the ports on which all frames transmitted for this VLAN are untagged. The ports that are selected are included in the VLAN.
- **BLANK (Autodetect)**. Select the ports that can be dynamically registered in this VLAN through GVRP. This selection has the effect of excluding a port from the selected VLAN.

10. Use the **LAG Enabled** option to add selected ports to VLAN as a LAG.

The default is No.

11. Use **IP Address** to define the IP address of the VLAN interface.

12. Use **Network Mask** to define the subnet mask of the VLAN interface.

## Configure VLAN Routing

You can configure VLAN Routing interfaces on the system.

➤ **To configure VLAN routing:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7.** Select **Routing > VLAN > VLAN Routing**.

<b>VLAN Routing Configuration</b>					
<b>:: VLAN Routing Configuration</b>					
	<b>VLAN ID</b>	<b>Port</b>	<b>MAC Address</b>	<b>IP Address</b>	<b>Subnet Mask</b>
<input type="checkbox"/>	<input type="button" value="▼"/>				
<input type="checkbox"/>	100	0/4/1	2C:B0:5D:91:F8:B7	192.168.22.100	255.255.255.0

The screen displays the port interface and MAC address assigned to the VLAN for routing.

- 8.** Use **IP Address** to enter the IP address to be configured for the VLAN routing interface.
- 9.** Use **Subnet Mask** to enter the subnet mask to be configured for the VLAN routing interface.
- 10.** To add the VLAN routing Interface specified in the VLAN ID field to the switch configuration, click the **ADD** button.
- 11.** To remove the VLAN routing interface specified in the VLAN ID field from the switch configuration, click the **DELETE** button.

## ARP Overview

The ARP protocol associates a Layer 2 MAC address with a layer 3 IPv4 address. managed switch software features both dynamic and manual ARP configuration. With manual ARP configuration, you can statically add entries into the ARP table.

ARP is a necessary part of the Internet Protocol (IP) and is used to translate an IP address to a media (MAC) address, defined by a local area network (LAN) such as Ethernet. A station needing to send an IP packet must learn the MAC address of the IP destination, or of the next hop router, if the destination is not on the same subnet. This is achieved by broadcasting an ARP request packet, to which the intended recipient responds by unicasting an ARP reply containing its MAC address. Once learned, the MAC address is used in the destination address field of the Layer 2 header prepended to the IP packet.

The ARP cache is a table maintained locally in each station on a network. ARP cache entries are learned by examining the source information in the ARP packet payload fields, regardless of whether it is an ARP request or response. Thus, when an ARP request is broadcast to all stations on a LAN segment or virtual LAN (VLAN), all recipients store the sender's IP and MAC address in their respective ARP cache. The ARP response, being unicast, is normally seen only by the requestor, who stores the sender information in its ARP cache. Newer information always replaces existing content in the ARP cache.

The number of supported ARP entries is platform dependent.

Devices can be moved in a network, which means that the IP address that was at one time associated with a certain MAC address is now found using a different MAC address, or might no longer be in use (for example, it was reconfigured, disconnected, or powered off). This leads to stale information in the ARP cache unless entries are updated in reaction to new

information seen on the network, periodically refreshed to determine if an address still exists, or removed from the cache if the entry has not been identified as a sender of an ARP packet during the course of an ageout interval, usually specified through configuration.

## Display ARP Cache Entries

➤ **To display the ARP cache entries:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

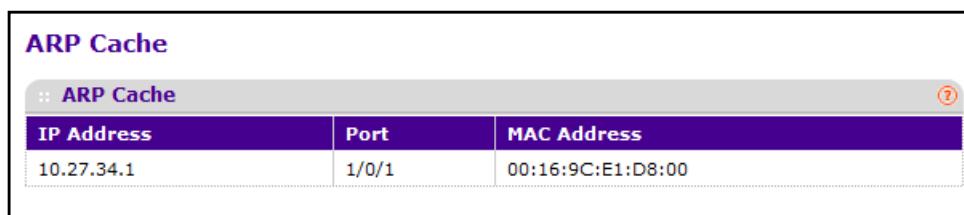
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Routing > ARP > Basic > ARP Cache**.



ARP Cache		
:: ARP Cache		
IP Address	Port	MAC Address
10.27.34.1	1/0/1	00:16:9C:E1:D8:00

8. Use **Port** to select the associated Unit/Slot/Port of the connection.

9. **IP Address** displays the IP address.

It must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.

10. **MAC Address** displays the unicast MAC address of the device.

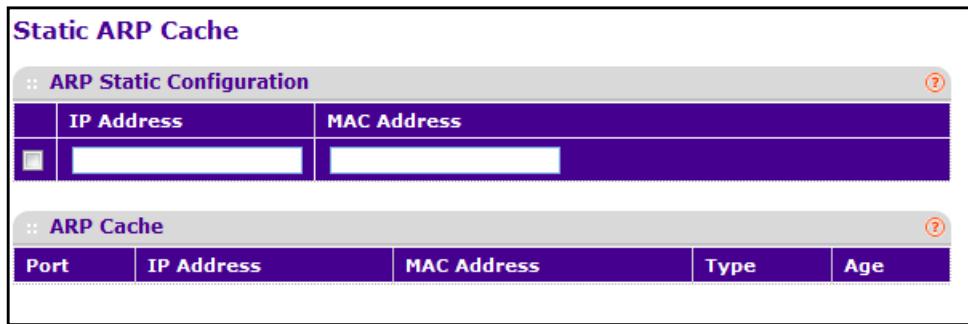
The address is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.

11. Click the **REFRESH** button to show the latest IP information.

## Configure the Static ARP Cache

➤ **To configure the static ARP cache:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Routing > ARP > Advanced > ARP Create**.



8. Add an entry to the Address Resolution Protocol table.
  - a. Use **IP Address** to enter the IP address. It must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.
  - b. Use **MAC Address** to specify the unicast MAC address of the device. Enter the address as six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.
9. To add a new static ARP entry to the switch, click the **ADD** button.
10. To delete an existing static ARP entry from the switch, click the **DELETE** button.
11. Click the **APPLY** button.

The MAC address mapping to the IP is updated. Configuration changes take effect immediately.

Click the **REFRESH** button to show the latest IP information.

The following table describes the nonconfigurable information displayed on the screen.

**Table 70. ARP Cache**

Field	Description
Port	The associated Unit/Slot/Port of the connection
IP Address	Displays the IP address. It must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.
MAC Address	The unicast MAC address of the device. The address is six two-digit hexadecimal numbers separated by colons, for example, 00:06:29:32:81:40.

## View or Configure the ARP Table

➤ **To view or configure the ARP table:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Routing > ARP > Advanced > ARP Table Configuration**.

Setting	Value	Description
Age Time(secs)	1200	(15 to 21600)
Response Time(secs)	10	(1 to 10)
Retries	10	(0 to 10)
Cache Size	509	(96 to 509)
Dynamic Renew	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	
Total Entry Count	2	
Peak Total Entries	2	
Active Static Entries	0	
Configured Static Entries	0	
Maximum Static Entries	16	
Remove From Table	None	

8. To configure the ARP Table, do the following:

- Use **Age Time** to enter the value for the switch to use for the ARP entry ageout time. You must enter a valid integer, which represents the number of seconds it takes for an ARP entry to age out. The range for this field is 15 to 21600 seconds. The default value for Age Time is 1200 seconds.
- Use **Response Time** to enter the value for the switch to use for the ARP response time-out. You must enter a valid integer, which represents the number of seconds the switch waits for a response to an ARP request. The range for this field is 1 to 10 seconds. The default value for Response Time is 10 seconds.
- Use **Retries** to enter an integer that specifies the maximum number of times an ARP request is retried. The range for this field is 0 to 10. The default value for Retries is 10.
- Use **Cache Size** to enter an integer that specifies the maximum number of entries for the ARP cache. The range for this field is 96 to 509. The default value for Cache Size is 509.
- Use **Dynamic Renew** to control whether the ARP component automatically attempts to renew ARP entries of type Dynamic when they age out. The default setting is Enable.
- Use **Remove from Table** to remove certain entries from the ARP Table. The choices listed specify the type of ARP entry to be deleted:
  - **All Dynamic Entries**
  - **All Dynamic and Gateway Entries**
  - **Specific Dynamic/Gateway Entry**. Selecting this allows the user to specify the required IP address.
  - **Specific Static Entry**. Selecting this allows the user to specify the required IP address.
  - **None**. Selected if the user does not want to delete any entry from the ARP Table.
- 9. Use **Remove IP Address** to enter the IP address against the entry that is to be removed from the ARP Table.

This appears only if the user selects **Specific Dynamic/Gateway Entry** or **Specific Static Entry** in the Remove from Table list.

The following table describes the nonconfigurable information displayed on the screen.

**Table 71. ARP Table Configuration**

Field	Description
Total Entry Count	Total number of entries in the ARP table.
Peak Total Entries	Highest value reached by Total Entry Count. This counter value is restarted whenever the ARP Table Cache Size value is changed.
Active Static Entries	Total number of active static entries in the ARP Table.
Configured Static Entries	Total number of configured static entries in the ARP Table.
Maximum Static Entries	Maximum number of static entries that can be defined.

## Configure Router Discovery

➤ **To configure router discovery:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7. Select Routing > Router Discovery.**

Router Discovery							
Router Discovery Configuration							
1 VLANs All		Go To Interface <input type="text"/> GO					
	Interface	Advertise Mode	Advertise Address	Maximum Advertise Interval	Minimum Advertise Interval	Advertise Lifetime	Preference Level
<input type="checkbox"/>	0/1	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/>	0/2	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/>	0/3	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/>	0/4	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/>	0/5	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/>	0/6	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/>	0/7	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/>	0/8	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/>	0/9	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/>	0/10	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/>	0/11	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/>	0/12	Disable	224.0.0.1	600	450	1800	0

**8. Select the **Interface** check box for the router interface.**

**9. Use **Advertise Mode** to select **Enable** or **Disable**.**

If you select **Enable**, router advertisements are transmitted from the selected interface.

**10. Use **Advertise Address** to select **Enable** or **Disable**.**

If you select **Enable**, router advertisements are transmitted from the selected interface.

**11. Use **Maximum Advertise Interval** to enter the maximum time (in seconds) allowed between router advertisements sent from the interface.**

**12. Use **Minimum Advertise Interval** to enter the minimum time (in seconds) allowed between router advertisements sent from the interface.**

The value must be in the range of 3 to 1800. The default value is 450.000000.

**13. Use **Advertise Lifetime** to enter the value (in seconds) to be used as the lifetime field in router advertisements sent from the interface.**

This is the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts.

**14. Use **Preference Level** to specify the preference level of the router as a default router relative to other routers on the same subnet.**

Higher numbered addresses are preferred. You must enter an integer.

**15. Click the **APPLY** button.**

The updated configuration is sent to the switch.

# Configure Quality of Service

5

This chapter covers the following topics:

- *QoS Overview*
- *Class of Service*
- *Differentiated Services*

## QoS Overview

You can configure Quality of Service (QoS) settings on the switch. In a typical switch, each physical port consists of one or more queues for transmitting packets on the attached network. Multiple queues per port are often provided to give preference to certain packets over others based on user-defined criteria. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in the other queues of the port. If a delay is necessary, packets get held in the queue until the scheduler authorizes the queue for transmission. As queues become full, packets cannot be held for transmission and get dropped by the switch.

QoS is a means of providing consistent, predictable data delivery by distinguishing between packets with strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given “special treatment” in a QoS-capable network. With this in mind, all elements of the network must be QoS-capable. The presence of at least one node that is not QoS-capable creates a deficiency in the network path and the performance of the entire packet flow is compromised.

## Class of Service

The Class of Service (CoS) queueing feature lets you directly configure certain aspects of switch queueing. This provides the desired QoS behavior for different types of network traffic when the complexities of DiffServ are not required. The priority of a packet arriving at an interface can be used to steer the packet to the appropriate outbound CoS queue through a mapping table. CoS queue characteristics that affect queue mapping, such as minimum guaranteed bandwidth or transmission rate shaping are user configurable at the queue (or port) level. Eight queues per port are supported.

You can set the Class of Service trust mode of an interface. Each port in the switch can be configured to trust one of the packet fields (802.1p or IP DSCP), or to not trust any packet's priority designation (untrusted mode). If the port is set to a trusted mode, it uses a mapping table appropriate for the trusted field being used. This mapping table indicates the CoS queue to which the packet should be forwarded on the appropriate egress ports. Of course, the trusted field must exist in the packet for the mapping table to be of any use, so there are default actions performed when this is not the case. These actions involve directing the packet to a specific CoS level configured for the ingress port as a whole, based on the existing port default priority as mapped to a traffic class by the current 802.1p mapping table.

Alternatively, when a port is configured as untrusted, it does not trust any incoming packet priority designation and uses the port default priority value instead. All packets arriving at the ingress of an untrusted port are directed to a specific CoS queue on the appropriate egress ports, in accordance with the configured default priority of the ingress port. This process is also used for cases where a trusted port mapping is unable to be honored, such as when a non-IP packet arrives at a port configured to trust the IP DSCP value.

## Configure CoS

➤ **To configure CoS:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **QoS > CoS > Basic > CoS Configuration**.



8. Use **Global** to specify all CoS configurable interfaces. The option Global represents the most recent global configuration settings.
9. Use **Interface** to specify CoS configuration settings based on the interface.
10. Use **Global Trust Mode** to specify whether to trust a particular packet marking at ingress. Global Trust Mode can be only one of the following:
  - untrusted
  - trust dot1p
  - trust ip-dscp
 The default value is trust dot1p.
11. Use **Interface Trust Mode** to specify whether to trust a particular packet marking at ingress. Interface Trust Mode can only be one of the following:
  - untrusted
  - trust dot1p
  - trust ip-dscp

The default value is untrusted.

**12.** Click the **APPLY** button.

The updated configuration is sent to the switch.

## Map 802.1p Priorities to Queues

➤ **To map 802.1p priorities to queues:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **QoS > CoS > Advanced > 802.1p to Queue Mapping**.

802.1p Priority	0	1	2	3	4	5	6	7
Queue	1	0	0	1	2	2	3	3

8. Use **Interface** to specify CoS configuration settings based on the interface or specify all CoS configurable interfaces.

9. Specify which internal traffic class to map the corresponding 802.1p value.

The queue number depends on the specific hardware.

The 802.1p Priority row contains traffic class selectors for each of the eight 802.1p priorities to be mapped. The priority goes from low (0) to high (3). For example, traffic with a priority of 0 is for most data traffic and is sent using best effort. Traffic with a higher priority, such as 3, might be time-sensitive traffic, such as voice or video.

The values in each list represent the traffic class. The traffic class is the hardware queue for a port. Higher traffic class values indicate a higher queue position. Before traffic in a lower queue is sent, it must wait for traffic in higher queues to be sent.

10. Click the **APPLY** button.

Your changes are applied to the system.

## Map IP DSCP Values to Queues

You can specify the internal traffic class to map to the corresponding DSCP value.

➤ **To map DSCP values to queues:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **QoS > CoS > Advanced > IP DSCP to Queue Mapping**.

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

The **IP DSCP** field displays an IP DSCP value from 0 to 63.

8. For each DSCP value, specify which internal traffic class to map to the corresponding IP DSCP value.

The queue number depends on the specific hardware.

9. Click the **APPLY** button.

Your settings are applied to the system.

## Configure CoS Settings for an Interface

You can apply an interface shaping rate to all interfaces or to a specific interface.

➤ **To configure CoS settings for an interface:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **QoS > CoS > Advanced > CoS Interface Configuration**.

The screenshot shows a table titled 'CoS Interface Configuration' with the following columns: 'LAGS All', 'Interface', 'Interface Trust Mode', and 'Interface Shaping Rate'. The table lists ten interfaces (1/0/1 to 1/0/10) all set to '802.1p' in 'Interface Trust Mode' and have a '0' value in 'Interface Shaping Rate'.

LAGS All	Interface	Interface Trust Mode	Interface Shaping Rate
	1/0/1	802.1p	0
	1/0/2	802.1p	0
	1/0/3	802.1p	0
	1/0/4	802.1p	0
	1/0/5	802.1p	0
	1/0/6	802.1p	0
	1/0/7	802.1p	0
	1/0/8	802.1p	0
	1/0/9	802.1p	0
	1/0/10	802.1p	0

- Use **Interface** to specify all CoS configurable interfaces.
- Use **Interface Trust Mode** to specify whether to trust a particular packet marking at ingress.

Interface Trust Mode can be only one of the following:

- untrusted
- trust dot1p
- trust ip-dscp

The default value is trust dot1p.

- Use **Interface Shaping Rate** to specify the maximum bandwidth allowed, typically used to shape the outbound transmission rate.

This value is controlled independently of any per-queue maximum bandwidth configuration. It is effectively a second-level shaping mechanism. The default value is 0. The valid range is 0 to 100 in increments of 1. The value 0 means that the maximum is unlimited.

- Click the **APPLY** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

## Configure an Interface Queue

You can define what a particular queue does by configuring switch egress queues. User-configurable parameters control the amount of bandwidth used by the queue, the queue depth during times of congestion, and the scheduling of packet transmission from the set of all queues on a port. Each port has its own CoS queue-related configuration.

The configuration process is simplified by allowing each CoS queue parameter to be configured globally or per port. A global configuration change is automatically applied to all ports in the system.

➤ **To configure an interface queue:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.

3. Launch a web browser.

4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **QoS > CoS >Advanced > Interface Queue Configuration**.

The screenshot shows a table titled 'Interface Queue Configuration' with the following columns: Interface, Queue ID, Minimum Bandwidth, Scheduler Type, and Queue Management Type. The table lists eight interfaces (1/0/1 to 1/0/7) with their respective settings. The 'Scheduler Type' column shows 'Weighted' for all ports, and the 'Queue Management Type' column shows 'TailDrop' for all ports.

Interface Queue Configuration					
:: Interface Queue Configuration					
<input checked="" type="checkbox"/>	LAGS	All	Go To Interface	<input type="text"/>	GO
	Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
<input checked="" type="checkbox"/>	1/0/1	0	0	Weighted	TailDrop
<input checked="" type="checkbox"/>	1/0/2	0	0	Weighted	TailDrop
<input checked="" type="checkbox"/>	1/0/3	0	0	Weighted	TailDrop
<input checked="" type="checkbox"/>	1/0/4	0	0	Weighted	TailDrop
<input checked="" type="checkbox"/>	1/0/5	0	0	Weighted	TailDrop
<input checked="" type="checkbox"/>	1/0/6	0	0	Weighted	TailDrop
<input checked="" type="checkbox"/>	1/0/7	0	0	Weighted	TailDrop

8. Select the check box next to the port or LAG to configure.

You can select multiple ports and LAGs to apply the same setting to the selected interfaces. Select the check box in the heading row to apply a trust mode or rate to all interfaces.

9. Configure any of the following settings:

- **Queue ID.** Use the list to select the queue to be configured (platform based).
- Use **Minimum Bandwidth** to specify the minimum guaranteed bandwidth allotted to this queue. Setting this value higher than its corresponding maximum bandwidth automatically increases the maximum to the same value. The default value is 0. The

valid range is 0 to 100 in increments of 1. The value 0 means no guaranteed minimum. The sum of individual Minimum Bandwidth values for all queues in the selected interface cannot exceed the defined maximum (100).

- Use **Scheduler Type** to specify the type of scheduling used for this queue. Options are Weighted and Strict. Defining on a per-queue basis allows the user to create the desired service characteristics for different types of traffic.
  - **Weighted.** Weighted round robin associates a weight to each queue. This is the default.
  - **Strict.** Services traffic with the highest priority on a queue first.

**Queue Management Type** displays the Queue depth management technique used for queues on this interface. This is used only if the device supports independent settings per-queue. Queue Management Type can only be tailDrop. All packets on a queue are safe until congestion occurs. At this point, any additional packets queued are dropped.

#### 10. Click the **APPLY** button.

Your changes are applied to the system.

## Differentiated Services

The QoS feature contains Differentiated Services (DiffServ) support that allows traffic to be classified into streams and given certain QoS treatment in accordance with defined per-hop behaviors.

Standard IP-based networks are designed to provide best effort data delivery service. “Best effort” service implies that the network delivers the data in a timely fashion, although this can depend on the environment. During times of congestion, packets might be delayed, sent sporadically, or dropped. For typical Internet applications, such as email and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. Conversely, any degradation of service has undesirable effects on applications with strict timing requirements, such as voice or multimedia.

### Defining DiffServ

To use DiffServ for QoS, you must first define the following categories and their criteria:

1. Class. Create classes and define class criteria.
2. Policy. Create policies, associate classes with policies, and define policy statements.
3. Service. Add a policy to an inbound interface.

Packets are classified and processed based on defined criteria. The classification criteria are defined by a class. The processing is defined by a policy's attributes. Policy attributes can be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs. A policy can contain multiples classes. When the policy is active, the actions taken depend on which class matches the packet.

Packet processing begins by testing the class match criteria for a packet. A policy is applied to a packet when a class match within that policy is found.

## DiffServ Wizard Overview

You can use the DiffServ Wizard to enable DiffServ on the switch by creating a traffic class, adding the traffic class to a policy, and then adding the policy to the ports selected on DiffServ Wizard screen. The DiffServ Wizard does the following:

- Creates a **DiffServ Class** and defines match criteria used as a filter to determine if incoming traffic meets the requirements to be a member of the class.
- Sets the **DiffServ Class** match criteria based on **Traffic Type** selection as below:
  - **VOIP**. Sets match criteria to UDP protocol.
  - **HTTP**. Sets match criteria to HTTP destination port.
  - **FTP**. Sets match criteria to FTP destination port.
  - **Telnet**. Sets match criteria to Telnet destination port.
  - **Every**. Sets match criteria all traffic.
- Creates a **Diffserv Policy** and adds it to the **DiffServ Class** created.
- If **Policing** is set to **YES**, then **DiffServ Policy** style is set to **Simple**. Traffic that conforms to the **Class Match** criteria is processed according to the **Outbound Priority** selection. **Outbound Priority** configures the handling of conforming traffic as below:
  - **High**. Sets policing action to markdscp ef.
  - **Med**. Sets policing action to markdscp af31.
  - **Low**. Sets policing action to send.
- If **Policing** is set to **NO**, then all traffic is marked as specified below:
  - **High**. Sets policy mark ipdscp ef.
  - **Med**. Sets policy mark ipdscp af31.
  - **Low**. Sets policy mark ipdscp be.
- Each port selected is added to the policy created.

## Use the DiffServ Wizard

➤ **To use the DiffServ Wizard:**

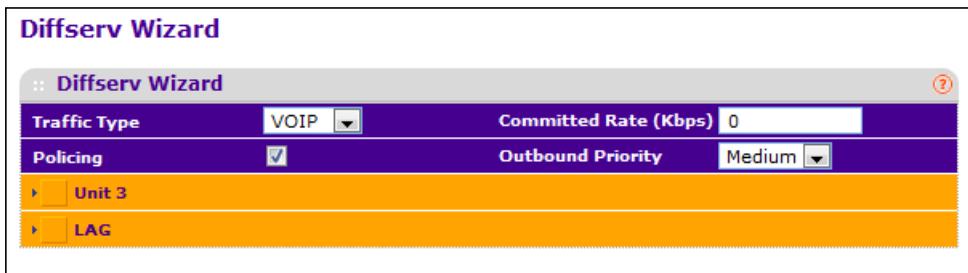
1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **QoS > DiffServ > DiffServ Wizard**.



8. Use **Traffic Type** to define the **DiffServ Class**.

The traffic type options are **VOIP**, **HTTP**, **FTP**, **Telnet**, and **Every**.

The ports that can be configured to support a **DiffServ policy** display. The **DiffServ policy** is added to the selected ports.

9. Use **Policing** to add policing to the **DiffServ Policy**.

The policing rate is applied.

10. Specify the Committed Rate:

- When **Policing** is enabled, the committed rate is applied to the policy and the policing action is set to conform.
- When **Policing** is disabled, the committed rate is not applied and the policy is set to markdscp.

11. Specify the Outbound Priority:

- When **Policing** is enabled, **Outbound Priority** defines the type of policing conform action where: **High** sets action to markdscp ef, **Med** sets action to markdscp af31, and **Low** sets action to send.
- When **Policing** is disabled, **Outbound Priority** defines the policy where: **High** sets policy to mark ipdscp ef, **Med** sets policy to mark ipdscp af31, **Low** set policy to mark ipdscp be.

## Configure DiffServ

Packets are filtered and processed based on defined criteria. The filtering criteria are defined by a class. The processing is defined by a policy's attributes. Policy attributes can be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs.

The configuration process begins with defining one or more match criteria for a class. Then one or more classes are added to a policy. Policies are then added to interfaces.

Packet processing begins by testing the match criteria for a packet. The all class type option defines that each match criteria within a class must evaluate to true for a packet to match that class. The any class type option specifies that at least one match criteria must evaluate to true for a packet to match that class. Classes are tested in the order in which they were added to the policy. A policy is applied to a packet when a class match within that policy is found.

➤ **To configure DiffServ:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

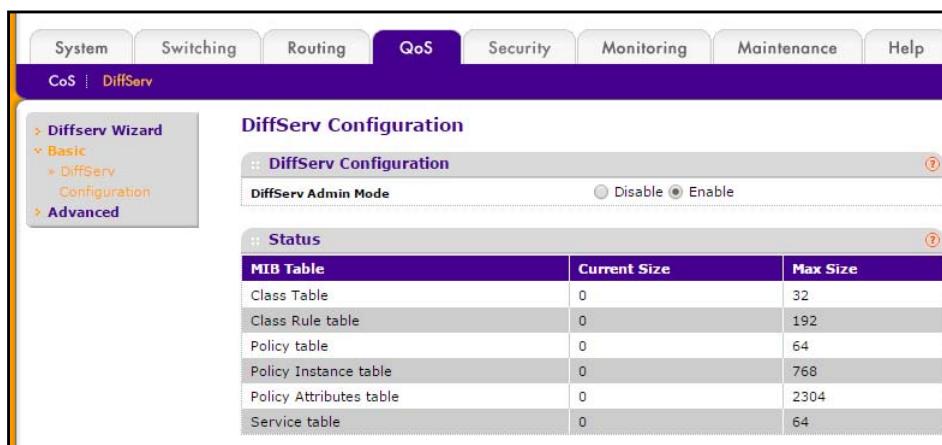
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **QoS > DiffServ > Basic > DiffServ Configuration**.



**Table 72. DiffServ Configuration**

Field	Description
DiffServ Admin Mode	The options mode for DiffServ. The default value is Enable. While disabled, the DiffServ configuration is retained when saved and can be changed, but it is not activated. When enabled, Diffserv services are activated.
Class table	Displays the number of configured DiffServ classes out of the total allowed on the switch.
Class Rule table	Displays the number of configured class rules out of the total allowed on the switch.
Policy table	Displays the number of configured policies out of the total allowed on the switch.
Policy Instance table	Displays the number of configured policy class instances out of the total allowed on the switch.
Policy Attributes table	Displays the number of configured policy attributes (attached to the policy class instances) out of the total allowed on the switch.
Service table	Displays the number of configured services (attached to the policies on specified interfaces) out of the total allowed on the switch.

## Configure the Global Diffserv Mode

Packets are filtered and processed based on defined criteria. The filtering criteria are defined by a class. The processing is defined by a policy's attributes. Policy attributes can be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs.

The configuration process begins with defining one or more match criteria for a class. Then one or more classes are added to a policy. Policies are then added to interfaces.

Packet processing begins by testing the match criteria for a packet. The all class type option defines that each match criteria within a class must evaluate to true for a packet to match that class. The any class type option specifies that at least one match criteria must evaluate to true for a packet to match that class. Classes are tested in the order in which they were added to the policy. A policy is applied to a packet when a class match within that policy is found.

➤ **To configure the global DiffServ mode:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

- Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **QoS > DiffServ > Advanced > Diffserv Configuration**.

The screenshot shows the 'DiffServ Configuration' screen. At the top, there is a section for 'DiffServ Admin Mode' with two radio buttons: 'Disable' (unselected) and 'Enable' (selected). Below this is a table titled 'Status' with the following data:

MIB Table	Current Size	Max Size
Class Table	0	32
Class Rule table	0	192
Policy table	0	64
Policy Instance table	0	768
Policy Attributes table	0	2304
Service table	0	36

- Select the DiffServ Admin Mode **Disable** or **Enable** radio button:

- Enable.** Differentiated services are active.
- Disable.** The DiffServ configuration is retained and can be changed, but it is not active.

- Click the **APPLY** button.

The changes are applied to the system.

The following table describes the information displayed in the Status table on the DiffServ Configuration screen:

**Table 73. Diffserv Configuration**

Field	Description
<b>Class table</b>	Displays the number of configured DiffServ classes out of the total allowed on the switch.
<b>Class Rule table</b>	Displays the number of configured class rules out of the total allowed on the switch.
<b>Policy table</b>	Displays the number of configured policies out of the total allowed on the switch.
<b>Policy Instance table</b>	Displays the number of configured policy class instances out of the total allowed on the switch.

**Table 73. Diffserv Configuration**

Field	Description
<b>Policy Attributes table</b>	Displays the number of configured policy attributes (attached to the policy class instances) out of the total allowed on the switch.
<b>Service table</b>	Displays the number of configured services (attached to the policies on specified interfaces) out of the total allowed on the switch.

## Configure a DiffServ Class

You can add a new DiffServ class name or rename or delete an existing class. The screen also allows you to define the criteria to associate with a DiffServ class. As packets are received, these DiffServ classes are used to prioritize packets. You can use multiple match criteria in a class. The logic is a Boolean logical AND for this criteria. After creating a class, you can click the class link to display the Class screen.

➤ **To configure a DiffServ class:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **QoS > DiffServ > Advanced > Class Configuration**.

Class Name		
:: Class Name		
	Class Name	Class Type
<input type="checkbox"/>		<input type="button" value="▼"/>
<input type="checkbox"/>	VoIP	All

8. To create a new class, enter a **class name**, select the **class type**, and click the **ADD** button. This field also lists all the existing DiffServ class names, from which one can be selected.

The switch supports only the **Class Type** value **All**, which means all the various match criteria defined for the class should be satisfied for a packet match. All signifies the logical AND of all the match criteria. You can select a class type only when you are creating a new class. After you create the class, this becomes a nonconfigurable field displaying the configured class type.

9. To rename an existing class, select the check box next to the configured class, update the name, and click the **APPLY** button.
10. To remove a class, select the check box beside the class name, then click the **DELETE** button.
11. Click the **REFRESH** button to refresh the screen with the most current data from the switch.

## Configure the Class Match Criteria

➤ **To configure the class match criteria:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7.** Select **QoS > DiffServ > Advanced > Class Configuration**.

The screenshot shows the 'Class Configuration' interface. At the top, there's a 'Class Information' section with 'Class Name' set to 'VoIP' and 'Class Type' set to 'All'. Below it is the 'DiffServ Class Configuration' section, which contains a list of match criteria. The 'Match Every' option is selected. Other options include Reference Class, Class of Service, VLAN, Secondary Class of Service, Secondary VLAN, Ethernet Type, Source MAC, Destination MAC, Protocol Type, Source IP, Source L4 Port, Destination IP, Destination L4 Port, IP DSCP, Precedence Value, and IP ToS. Each criterion has associated input fields for specifying values or masks. At the bottom of the configuration pane, there are tabs for 'Class Summary' and 'Match Criteria'.

**8.** Click the **class name** for an existing class.

The class configuration fields display.

**9. Class Name.** Displays the name for the configured DiffServ class.

**10. Class Type.** Displays the DiffServ class type.

Options: All

You can select a class type only when you are creating a new class. After you create the class, this becomes a nonconfigurable field displaying the class type that you selected.

**11.** Define the criteria to associate with a DiffServ class:

- **Match Every.** This adds to the specified class definition a match condition whereby all packets are considered to belong to the class.
- **Reference Class.** This lists the class(es) that can be assigned as reference class(es) to the current class.
- **Class of Service.** This lists all the values for the class of service match criterion in the range 0 to 7 from which one can be selected.
- **VLAN.** This is a value in the range of 0 – 4095.
- **Ethernet Type.** This lists the keywords for the Ethertype from which one can be selected.
- **Source MAC Address.** This is the source MAC address specified as six 2-digit hexadecimal numbers separated by colons.
- **Source MAC Mask.** This is a bit mask in the same format as MAC address indicating which parts of the source MAC address to use for matching against packet content.

- **Destination MAC Address.** This is the destination MAC address specified as six 2-digit hexadecimal numbers separated by colons.
- **Destination MAC Mask.** This is a bit mask in the same format as MAC address indicating which parts of the destination MAC address to use for matching against packet content.
- **Protocol Type.** This lists the keywords for the Layer 4 protocols from which one can be selected. The list includes 'other' as an option for the remaining values.
- **Source IP Address.** This is a valid source IP address in the dotted decimal format.
- **Source Mask.** This is a bit mask in IP dotted decimal format indicating which parts of the source IP address to use for matching against packet content.
- **Source L4 Port.** This lists the keywords for the known source Layer 4 ports from which one can be selected. The list includes 'other' as an option for the unnamed ports.
- **Destination IP Address.** This is a valid destination IP address in the dotted decimal format.
- **DestinationMask.** This is a bit mask in IP dotted decimal format indicating which parts of the destination IP address to use for matching against packet content.
- **Destination L4 Port.** This lists the keywords for the known destination Layer 4 ports from which one can be selected. The list includes 'other' as an option for the unnamed ports.
- **IP DSCP.** This lists the keywords for the known DSCP values from which one can be selected. The list includes 'other' as an option for the remaining values.
- **Precedence Value** -This lists the keywords for the IP Precedence value in the range 0 to 7.
- **IP ToS.** Configure the IP ToS field:
  - **ToS Bits.** This is the Type of Service octet value in the range 0x00 to 0xFF to compare against.
  - **ToS Mask.** This indicates which ToS bits are subject to comparison against the Service Type value.

**12.** Click the **APPLY** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

## Configure a DiffServ IPv6 Class

You can add a new IPv6 DiffServ class name or rename or delete an existing class. The screen also allows you to define the criteria to associate with a DiffServ class. As packets are received, these DiffServ classes are used to prioritize packets. You can use multiple match criteria in a class. The logic is a Boolean logical AND for this criteria. After creating a Class, you can click the class link to display the Class screen.

➤ **To configure a DiffServ class:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**.

IPv6 Class Configuration	
:: IPv6 Class Name	
Class Name	Class Type
<input checked="" type="checkbox"/>	<input type="button" value=""/>
<input type="checkbox"/> ipv6Class	All

8. To create a new class, enter a **class name**, select the **class type**, and click the **ADD** button.

This field also lists all the existing DiffServ class names, from which one can be selected.

The switch supports only the **Class Type** value **All**, which means all the various match criteria defined for the class should be satisfied for a packet match. All signifies the logical AND of all the match criteria. You can select the class type only when you are creating a new class. After you create the class, this field becomes a nonconfigurable field displaying the class type that you selected.

9. To rename an existing class, select the check box next to the configured class, update the name, and click the **APPLY** button.
10. To remove a class, click the check box beside the class name, then click the **DELETE** button.
11. Click the **REFRESH** button to refresh the screen with the most current data from the switch.

## Configure the DiffServ Class Match Criteria

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **QoS > DiffServ > Advanced > IPv6 Class Configuration**.

IPv6 Class Configuration		
:: IPv6 Class Name		
	Class Name	Class Type
<input type="checkbox"/>		<input type="button" value="?"/>
<input type="checkbox"/>	ipv6Class	All

- Click the **class name** for an existing class to go to the IPv6 DiffServ Class Configuration section of the screen.

The screenshot shows the 'IPv6 Class Configuration' interface. At the top, there's a header 'IPv6 Class Configuration'. Below it, the 'IPv6 Class Information' tab is active, showing a 'Class Name' field containing 'ipv6Class' and a 'Class Type' field set to 'All'. Below this, the 'IPv6 DiffServ Class Configuration' tab is active, displaying various match criteria fields. These include:

- Match Every:** Selected radio button. Fields: 'Any' dropdown, 'VoIP' dropdown.
- Reference Class:** Unselected radio button.
- Protocol Type:** Unselected radio button. Fields: 'ICMPv6' dropdown, 'Length' input field (0 to 255).
- Source Prefix/Length:** Unselected radio button. Fields: 'Source' dropdown, 'Length' input field (0 to 128).
- Source L4 Port:** Unselected radio button. Fields: 'Protocol' dropdown, 'Port' input field (0 to 65535).
- Destination Prefix/Length:** Unselected radio button. Fields: 'Protocol' dropdown, 'Port' input field (0 to 65535).
- Destination L4 Port:** Unselected radio button. Fields: 'Protocol' dropdown, 'Port' input field (0 to 65535).
- Flow Label:** Unselected radio button. Fields: 'Flow Label' input field (0 to 1048575).
- IP DSCP:** Unselected radio button. Fields: 'DSCP' dropdown, 'Length' input field (0 to 63).

At the bottom, there's a 'Class Summary' section with tabs for 'Match Criteria' (which is selected) and 'Values'.

- Specify the **Class Name**. Displays the name for the configured DiffServ class. The **Class Type** field displays the DiffServ class type. You can only select the class type when you are creating a new class. After you create a class, this becomes a nonconfigurable field displaying the class type you specified.
- Define the criteria to associate with a DiffServ class:
  - Match Every.** This adds to the specified class definition a match condition whereby all packets are considered to belong to the class.
  - Reference Class.** This lists the class(es) that can be assigned as reference class(es) to the current class.
  - Protocol Type.** This lists the keywords for the Layer 4 protocols from which one can be selected. The list includes other as an option for the remaining values.
  - Source Prefix Length.** This is a valid source IPv6 prefix to compare against an IPv6 packet. The prefix is always specified with the prefix length. The prefix can be entered in the range of ::0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF and the prefix length can be entered in the range of 0 to 128.
  - Source L4 Port.** This lists the keywords for the known source Layer 4 ports from which one can be selected. The list includes 'other' as an option for the unnamed ports.
  - Destination Prefix/Length.** This is a valid destination IPv6 prefix to compare against an IPv6 packet. The prefix is always specified with the prefix length. The prefix can be entered in the range of ::0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF and the prefix length can be entered in the range of 0 to 128.

- **Destination L4 Port.** This lists the keywords for the known destination Layer 4 ports from which one can be selected. The list includes other as an option for the unnamed ports.
- **Flow Label.** This is a 20-bit number that is unique to an IPv6 packet, used by end stations to signify Quality of Service handling in routers. Flow Label can be specified in the range of 0 to 1048575.
- **IP DSCP.** This lists the keywords for the known DSCP values from which one can be selected. The list includes other as an option for the remaining values.

**Match Criteria.** Displays the configured match criteria for the specified class.

**Values.** Displays the values of the configured match criteria.

**11.** Click the **APPLY** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

## Configure DiffServ Policy

You can associate a collection of classes with one or more policy statements. After creating a policy, you can click the policy link to display the Policy screen.

➤ **To configure a DiffServ policy:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **QoS > DiffServ > Advanced > Policy Configuration**.

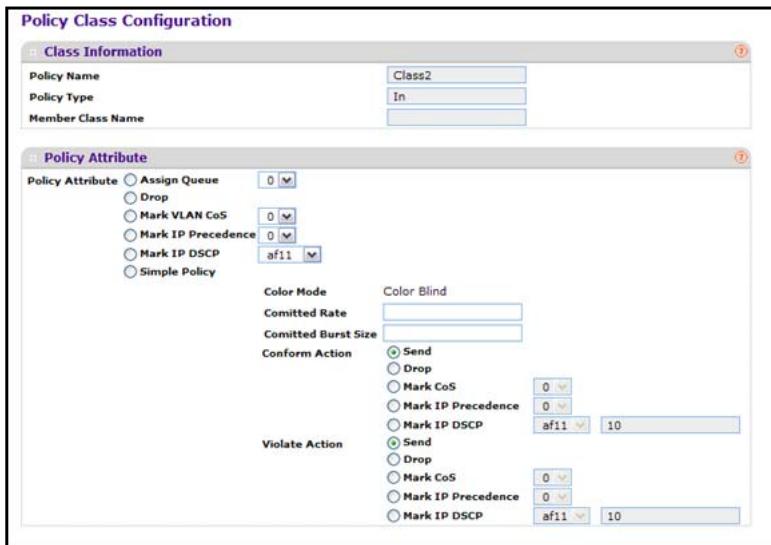
Policy Configuration			
:: Policy Configuration			
	Policy Name	Policy Type	Member Class
<input type="checkbox"/>	<input type="text" value="policy1"/>	<input type="button" value="In"/>	<input type="button" value="VoIP"/>

8. Use **Policy Name** to uniquely identify a policy using a case-sensitive alphanumeric string from 1 to 31 characters.
9. Select a **Member Class**.
10. The **Member Class** list includes all DiffServ classes currently defined as members of the specified policy. This list is automatically updated as a new class is added to or removed from the policy. You can select an item in this list only when an existing policy class instance is to be removed. After you remove the policy class instance this becomes a nonconfigurable field.
11. Use the **Policy Type** to select the type specific to inbound traffic direction.
12. To add a new policy to the switch, click the **ADD** button.
13. To delete the currently selected policy from the switch, click the **DELETE** button.

## Configure DiffServ Policy Attributes

➤ **To configure the DiffServ policy attributes:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **QoS > DiffServ > Advanced > Policy Class**.  
The Policy Class Configuration screen displays.
8. Click the name of the policy.



- Select the queue to which packets of this policy class are assigned.

This is an integer value in the range 0 to 7.

- Configure the policy attributes:

- Drop.** Select the **Drop** radio button. This flag indicates that the policy attribute is defined to drop every inbound packet.
- Mark VLAN CoS.** This is an integer value in the range from 0 to 7 for setting the VLAN priority.
- Mark IP Precedence.** This is an IP Precedence value in the range from 0 to 7.
- Mark IP DSCP.** This lists the keywords for the known DSCP values from which one can be selected. The list includes other as an option for the remaining values.
- Simple Policy.** Use this attribute to establish the traffic policing style for the specified class. This command uses single data rate and burst size resulting in two outcomes (conform and violate).

- If you select the **Simple Policy** attribute, you can configure the following fields:

- Color Mode.** This lists the color mode. The default is **Color Blind**.
  - Color Blind**
  - Color Aware**

**Color Aware** mode requires the existence of one or more color classes that are valid for use with this policy instance. A valid color class contains a single, nonexcluded match criterion for one of the following fields (provided the field does not conflict with the classifier of the policy instance itself):

- CoS**
- IP DSCP**
- IP Precedence**

- **Committed Rate.** This value is specified in the range 1 to 4294967295 kilobits per second (Kbps).
- **Committed Burst Size.** This value is specified in the range 1 to 128 KBytes. The committed burst size is used to determine the amount of conforming traffic allowed.
- **Conform Action.** This lists the actions to be taken on conforming packets according to the policing metrics, from which one can be selected. The default is send.
- **Violate Action.** This lists the actions to be taken on violating packets per the policing metrics, from which one can be selected. The default is send.
- For each of the Action Selectors one of the following actions can be taken:
  - **Drop.** These packets are immediately dropped.
  - **Mark IP DSCP.** These packets are marked by DiffServ with the specified DSCP value before being presented to the system forwarding element. This selection requires that the DSCP value field be set.
  - **Mark CoS.** These packets are marked by DiffServ with the specified CoS value before being presented to the system forwarding element. This selection requires that the Mark CoS value field be set.
  - **Send.** These packets are presented unmodified by DiffServ to the system forwarding element.
  - **Mark IP Precedence.** These packets are marked by DiffServ with the specified IP Precedence value before being presented to the system forwarding element. This selection requires that the Mark IP Precedence value field be set.

**12.** Click the **APPLY** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable information displayed on the screen.

**Table 74. Policy Class Configuration**

Field	Description
Policy Name	Displays name of the DiffServ policy.
Policy Type	Displays type of the policy as In.
Member Class Name	Displays name of each class instance within the policy.

## Configure DiffServ Policy Settings on an Interface

You can activate a policy on an interface.

➤ **To configure DiffServ policy settings on an interface:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.

3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
- The Login screen displays.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **QoS > DiffServ > Advanced > Service Interface Configuration**.

Service Interface Configuration				
:: Service Interface Configuration				
<b>1</b>	<b>2</b>	<b>LAGS</b>	<b>All</b>	
		Go To Interface <input type="text"/>		<b>GO</b>
	Interface	Policy In Name	Direction	Operational Status
	1/0/1			
	1/0/2			
	1/0/3			
	1/0/4			
	1/0/5			
	1/0/6			
	1/0/7			
	1/0/8			
	1/0/9			

8. Use **Interface** to select the interface for the DiffServer service.
9. In the **Policy Name** list, select a name.

This list includes all the policy names. This field is not shown for Read/Write users where inbound service policy attachment is not supported by the platform.

The following table describes the nonconfigurable information displayed on the screen.

**Table 75. Service Interface Configuration**

Field	Description
Direction	Shows that the traffic direction of this service interface is In.
Operational Status	Shows the operational status of this service interface, either Up or Down.

## View Service Statistics

You can view class-oriented statistical information for the policy, which is specified by the interface and direction. The Member Classes menu is populated on the basis of the specified

interface and direction and hence the attached policy (if any). Highlighting a member class name displays the statistical information for the policy class instance for the specified interface and direction.

➤ **To view service statistics:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

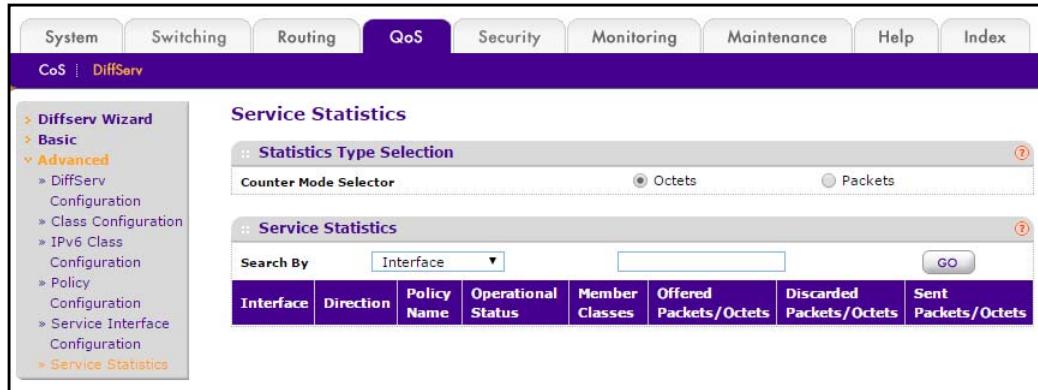
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **QoS > DiffServ > Advanced > Service Statistics**.



**Counter Mode Selector** specifies the format of the displayed counter values, which must be either Octets or Packets. The default is Octets.

The following table describes the information available on the Service Statistics screen.

**Table 76. Service Statistics**

<b>Field</b>	<b>Description</b>
Interface	List of all valid slot number and port number combinations in the system with a DiffServ policy currently attached in In direction.
Direction	List of the traffic direction of interface as In. Only shows the direction(s) for which a DiffServ policy is currently attached.
Policy Name	Name of the policy currently attached to the specified interface and direction.
Operational Status	Operational status of the policy currently attached to the specified interface and direction. The value is either Up or Down.
Member Classes	List of all DiffServ classes currently defined as members of the selected policy name. Choose one member class name at a time to display its statistics. If no class is associated with the chosen policy, then nothing displays in the list.
Offered Packets/Octets	A count of the total number of packets/octets offered to all class instances in this service policy before their defined DiffServ treatment is applied. This is the overall count per interface, per direction.
Discarded Packets/Octets	A count of the total number of packets/octets discarded for all class instances in this service policy for any reason due to DiffServ treatment. This is the overall count per interface, per direction.
Sent Packets/Octets	A count of the total number of packets/octets forwarded for all class instances in this service policy after their defined DiffServ treatments were applied. In this case, forwarding means the traffic stream was passed to the next functional element in the data path, such as the switching or routing function of an outbound link transmission element. This is the overall count per interface, per direction.

# Manage Device Security

# 6

This chapter covers the following topics:

- *Management Security Settings*
- *Configure RADIUS Settings*
- *TACACS*
- *Set Up a Login Authentication List*
- *Configure Management Access*
- *Manage Certificates*
- *Manage Telnet*
- *Download a Certificate*
- *Manage Telnet*
- *Port Authentication Overview*
- *Traffic Control*
- *Configure a Private Group*
- *Control DHCP Snooping Settings*
- *Configure an IP Source Guard Interface*
- *Configure Dynamic ARP Inspection*
- *Access Control List Overview*

## Management Security Settings

You can configure the login password, Remote Authorization Dial-In User Service (RADIUS) settings, Terminal Access Controller Access Control System (TACACS) settings, and authentication lists.

### Configure Users

By default, two user accounts exist:

- admin, with read/write privileges
- guest, with read only privileges

By default, both of these accounts do not have passwords. The names are not case-sensitive.

If you log in as the admin user, you are assigned read/write privileges and you can use the User Management screen to assign passwords and set security parameters for the default user accounts, and add and delete accounts (other than admin), up to a maximum of six. Only the admin user account is allowed read/write privileges.

➤ **To configure users:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7.** Select **Security > Management Security > Local User > User Management**.

<b>User Management</b>							
:: Manage Users							
	User Name	Edit Password	Password	Confirm Password	Access Mode	Lockout Status	Password Expiration Date
<input type="checkbox"/>		Disable <input type="button" value="▼"/>	*****	*****	<input type="button" value="▼"/>		
<input type="checkbox"/>	admin	Disable	*****	*****	READ_WRITE	FALSE	
<input type="checkbox"/>	guest	Disable	*****	*****	READ_ONLY	FALSE	

The screen displays the users and their lockout status.

**8.** If you are creating a new user, in the **User Name** field, type the name for a new user.

You can enter data in this field only when you are creating a new account. User names are up to eight characters in length and are not case-sensitive. Valid characters include all the alphanumeric characters as well as the hyphen ('-') and underscore ('\_') characters. The user name default is not valid. User names once created cannot be changed or modified.

**9.** To edit the password, do the following:

- a. In the **Edit Password** list, select **Enable**.
- b. In the **Password** field, type a password.

The password does not display as it is typed, only asterisks (\*) display. Passwords are up to eight alpha-numeric characters in length, and are case-sensitive.

- c. In the **Confirm Password** field, type the password again.

This field does not display the password as it is typed, but shows asterisks (\*).

**10.** In the **Access Mode** list, select a value.

The admin account requires read/write access, and all other accounts are assigned read-only access. The default value is Read Only.

**11.** To add a user, click the **ADD** button.

**12.** To delete the currently selected user account, click the **DELETE** button.

You cannot delete the admin user.

## Set the Password for a User

➤ **To set the password for a user:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.

4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Security > Management Security > Local User > User Password Configuration**.

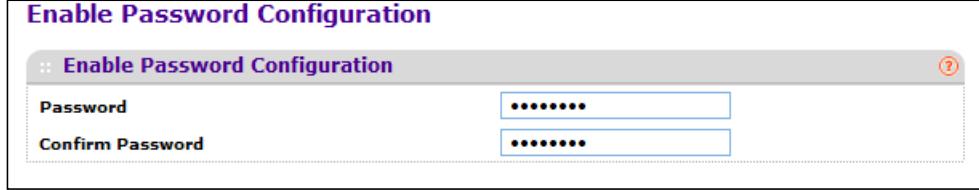
**Password Configuration**

:: Password Configuration	
<b>Password Minimum Length</b>	<input type="text" value="8"/> (0 to 64)
<b>Password Aging (days)</b>	<input type="text" value="0"/> (0 to 365)
<b>Password History</b>	<input type="text" value="0"/> (0 to 10)
<b>Lockout Attempts</b>	<input type="text" value="0"/> (0 to 5)

8. Use **Password Minimum Length** to specify the minimum character length of all new local user passwords.
9. Use **Password Aging (days)** to specify the maximum time for which the user passwords are valid, in days, from the time the password is set.  
Once a password expires, the user must enter a new password following the first login after password expiration. A value of 0 indicates that passwords never expire.
10. Use **Password History** to specify the number of previous passwords to store for prevention of password reuse.  
This ensures that each user does not reuse passwords often. A value of 0 indicates that no previous passwords are stored.
11. Use **Lockout Attempts** to specify the number of allowable failed local authentication attempts before the user's account is locked.  
A value of 0 indicates that user accounts is never locked.

## Enable Password Configuration

- **To enable password configuration:**
  1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
  2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
  3. Launch a web browser.

4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
  5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
  6. Click the **Login** button.  
The web management interface menu displays.
  7. Select **Security > Management Security > Enable Password**.
- 
8. Use **Password** to specify a password. Passwords are a maximum of 64 alphanumeric characters.
  9. Use **Confirm Password** to enter the password again to confirm that you entered it correctly.
  10. Click the **APPLY** button.  
Your settings are saved.

## Configure a Line Password

- **To configure a line password:**
1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
  2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
  3. Launch a web browser.
  4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
  5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
  6. Click the **Login** button.  
The web management interface menu displays.

**7. Select **Security > Management Security > Line Password.****

The screenshot shows a configuration interface titled "Line Password Configuration". It contains six input fields, each with a dotted password placeholder:

Field	Placeholder
Console Password	*****
Confirm Console Password	*****
Telnet Password	*****
Confirm Telnet Password	*****
SSH Password	*****
Confirm SSH Password	*****

**8. Use **Console Password** to enter the console password.**

Passwords are a maximum of 64 alphanumeric characters.

**9. Use **Confirm Console Password** to enter the password again to confirm that you entered it correctly.**

**10. Use **Telnet Password** to enter the Telnet password.**

Passwords are a maximum of 64 alphanumeric characters.

**11. Use **Confirm Telnet Password** to enter the password again to confirm that you entered it correctly.**

**12. Use **SSH Password** to enter the SSH password.**

Passwords are a maximum of 64 alphanumeric characters.

**13. Use **Confirm SSH Password** to enter the password again to confirm that you entered it correctly.**

**14. Click the **APPLY** button.**

Your settings are saved.

## Configure RADIUS Settings

RADIUS servers provide additional security for networks. The RADIUS server maintains a user database, which contains per-user authentication information. The switch passes information to the configured RADIUS server, which can authenticate a user name and password before authorizing use of the network. RADIUS servers provide a centralized authentication method for the following:

- Web access
- Access control port (802.1X)

You can add information about one or more RADIUS servers on the network.

➤ **To configure RADIUS:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.

2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Management Security > RADIUS > Radius Configuration**.

Radius Configuration	
:: Radius Configuration	
Current Server Address	192.168.10.100
Number of Configured Authentication Servers	1
Number of Configured Accounting Servers	0
Number of Named Authentication Server Groups	1
Number of Named Accounting Server Groups	0
Max Number of Retransmits	4 (1 to 15)
Timeout Duration (secs)	5 (1 to 30)
Accounting Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Radius Attribute 4 Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

The **Current Server IP Address** field is blank if no servers are configured (see *Configure a RADIUS Server* on page 268). The switch supports up to three configured RADIUS servers. If more than one RADIUS servers is configured, the current server is the server configured as the primary server. If no servers are configured as the primary server, the current server is the most recently added RADIUS server.

8. In the **Max Number of Retransmits** field, specify the value of the maximum number of times a request packet is retransmitted to the RADIUS server.

The valid range is 1 – 15. The default value is 4.

Give consideration to maximum delay time when configuring RADIUS maximum retransmits and RADIUS time-outs. If multiple RADIUS servers are configured, the maximum retransmit value on each is exhausted before the next server is attempted. A retransmit does not occur until the configured time-out value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals retransmit times time-out for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces are blocked until the RADIUS application returns a response.

9. In the **Timeout Duration** field, specify the time-out value, in seconds, for request retransmissions.

The valid range is 1 – 30. The default value is 5.

Give consideration to maximum delay time when configuring RADIUS maximum retransmits and RADIUS time-outs. If multiple RADIUS servers are configured, the maximum retransmit value on each is exhausted before the next server is attempted. A retransmit does not occur until the configured time-out value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the retransmit times time-out for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces are blocked until the RADIUS application returns a response.

**10.** Select the Accounting Mode **Disable** or **Enable** radio button.

This specifies whether the RADIUS accounting mode is enabled or disabled on the current server.

**11.** Select the RADIUS attribute 4 **Disable** or **Enable** radio button to enable or disable RADIUS attribute 4.

The default value is Disable. The **Radius Attribute 4 Value** is an optional field and can be seen only when Radius attribute 4 Mode is enabled. It takes an IP address value in the format (xx.xx.xx.xx).

The following table describes the nonconfigurable information displayed on the screen.

**Table 77. RADIUS Configuration**

Field	Description
Current Server Address	The address of the current server. This field is blank if no servers are configured.
Number of Configured Authentication Servers	Displays the number of configured authentication RADIUS servers. The value can range from 0 to 32.
Number of Configured Accounting Servers	Displays the number of RADIUS accounting servers configured. The value can range from 0 to 32.
Number of Named Authentication Server Groups	Displays the number of named RADIUS server authentication groups configured.
Number of Named Accounting Server Groups	Displays the number of Named RADIUS server accounting groups configured.

## Configure a RADIUS Server

You can view and configure various settings for the current RADIUS server configured on the system.

➤ **To configure a RADIUS server:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.

2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Management Security > RADIUS > Server Configuration**.

**Server Configuration**

Radius Server IP Address	Radius Server Name	Current	Port	Secret Configured	Secret	Primary Server	Message Authenticator	Server Type
192.168.10.100	radius1	True	1812	Yes	*****	Yes	Enable	Netgear

**Statistics**

Radius Server	Round Trip Time	Access Requests	Access Retransmissions	Access Accepts	Access Rejects	Access Challenges	Malformed Access Responses	Bad Authenticators	Pending Requests	Timeouts	Unknown Types	Packets Dropped
192.168.10.100	0.00	0	0	0	0	0	0	0	0	0	0	0

The **Current** field indicates whether a server is currently in use as the authentication server.

8. To add a RADIUS server, specify the following settings:
  - In the **Radius Server IP Address** field, specify the IP address of the RADIUS server.
  - In the **Radius Server Name** field, specify the name of the server.
  - Use **Port** to specify the UDP port used by this server.

The valid range is 0–65535.

- **Secret Configured.** The secret is applied only if this option is Yes.

If the option is No, anything entered in the Secret field has no effect and is not retained.

- Use **Secret** to specify the shared secret for this server.
- Use **Primary Server** to set the selected server as a primary or secondary server.
- Use **Message Authenticator** to enable or disable the message authenticator attribute for the selected server.

9. To add a new server to the switch, click the **ADD** button.

This button is only available to users with read/write permission.

**10.** To remove the selected server from the configuration, click the **DELETE** button.

This button is only available to users with Read/Write permission.

**11.** Click the **APPLY** button.

Your settings are saved.

**12.** To reset the authentication server and RADIUS statistics to their default values, click the **Clear Counters** button.

The following table describes the RADIUS server statistics available on the screen.

**Table 78. RADIUS Server configuration statistics**

Field	Description
Radius Server	Displays the address of the RADIUS server or the name of the RADIUS server for which the statistics are displayed.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to this server.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included in malformed access-responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that did not yet time out or receive a response.
Timeouts	The number of authentication time-outs on this server.
Unknown Types	The number of RADIUS packets of unknown type that were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

## Configure a RADIUS Accounting Server

You can view and configure various settings for one or more RADIUS accounting servers on the network.

➤ **To configure a RADIUS accounting server:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Management Security > RADIUS > Accounting Server Configuration**.

Accounting Server Configuration						
:: Accounting Server Configuration						
Accounting Server IP Address	Accounting Server Name	Port	Secret Configured	Secret	Accounting Mode	
<input type="text"/> 192.168.10.100	<input type="text"/> radius1	<input type="text"/> 1813	<input checked="" type="checkbox"/> Yes	<input type="text"/> *****	<input type="text"/>	<input type="text"/> Enable
:: Statistics						
Accounting Server	Round Trip Time	Accounting Requests	Accounting Retransmissions	Accounting Responses	Malformed Accounting Responses	Bad Authenticators
192.168.10.100	0.00	0	0	0	0	0
Pending Requests	Timeouts	Unknown Types	Packets Dropped			
0	0	0	0			

8. In the **Accounting Server IP Address** field, specify the IP address of the RADIUS accounting server to add.
9. In the **Accounting Server Name** field, enter the name of the accounting server to add.
10. In the **Port** field, specify the UDP port number the server uses to verify the RADIUS accounting server.

The valid range is 0–65535. If the user has read-only access, the value is displayed but cannot be changed.

11. From the **Secret Configured** menu, select **Yes** to add a RADIUS secret in the next field.

After you add the RADIUS accounting server, this field indicates whether the shared secret for this server was configured.

12. In the **Secret** field, type the shared secret to use with the specified accounting server.

**13.** From the **Accounting Mode** list, enable or disable the RADIUS accounting mode.

**14.** To delete a configured RADIUS accounting server, click the **DELETE** button.

To clear the accounting server statistics, click the **CLEAR COUNTERS** button.

The following table describes RADIUS accounting server statistics available on the screen.

**Table 79. RADIUS accounting server configuration**

Field	Description
Accounting Server Address	Displays the accounting server associated with the statistics.
Round Trip Time(secs)	Displays the time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Accounting Requests	Displays the number of RADIUS Accounting-Request packets sent not including retransmissions.
Accounting Retransmissions	Displays the number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
Accounting Responses	Displays the number of RADIUS packets received on the accounting port from this server.
Malformed Accounting Responses	Displays the number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	Displays the number of RADIUS Accounting-Response packets that contained invalid authenticators received from this accounting server.
Pending Requests	Displays the number of RADIUS Accounting-Request packets sent to this server that did not yet time out or receive a response.
Timeouts	Displays the number of accounting time-outs on this server.
Unknown Types	Displays the number of RADIUS packets of unknown type that were received from this server on the accounting port.
Packets Dropped	Displays the number of RADIUS packets that were received from this server on the accounting port and dropped for some other reason.

## TACACS

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 through user names and user-defined passwords.
- **Authorization:** Performed at login. When the authentication session is completed, an authorization session starts using the authenticated user name. The TACACS server checks the user privileges.

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

## Configure Global TACACS Settings

You can view or change the TACACS settings for communication between the switch and the TACACS server you configure through the inband management port.

➤ **To configure global TACACS settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Management Security > TACACS > TACACS Configuration**.

The screenshot shows a configuration interface titled "TACACS Configuration". Under the "TACACS Configuration" section, there are two input fields: "Key String" and "Connection Timeout". The "Key String" field has a placeholder "(0 to 128)" and contains the value "5". The "Connection Timeout" field has a placeholder "(1 to 30)" and contains the value "5". A help icon (a question mark) is located in the top right corner of the configuration section.

8. In the **Key String** field, specify the authentication and encryption key for TACACS communications between the switch and the TACACS server.

The valid range is 0–128 characters. The key must match the key configured on the TACACS server.

9. In the **Connection Timeout** field, specify the maximum number of seconds allowed to establish a TCP connection between the managed switch and the TACACS server.

10. Click the **APPLY** button.

Your settings are applied to the system.

## Configure TACACS Server Settings

You can configure up to five TACACS servers with which the switch can communicate.

➤ **To configure a TACACS server:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.

2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.

3. Launch a web browser.

4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Management Security > TACACS > TACACS Server Configuration**.

TACACS Server Configuration					
:: TACACS Server Configuration					
	TACACS Server	Priority(0 to 65535)	Port(0 to 65535)	Key String	Connection Timeout(1-30)
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	*****	<input type="text"/>
<input checked="" type="checkbox"/>	192.168.10.115	1	49	*****	5

8. Use **TACACS Server** to configure the TACACS server IP address.

9. Use **Priority** to specify the order in which the TACACS servers are to be used.

The range is 0 – 65535.

10. Use **Port** to specify the authentication port.

The range is 0 – 65535.

11. Use **Key String** to specify the authentication and encryption key for TACACS communications between the device and the TACACS server.

The valid range is 0 – 128 characters. The key must match the key used on the TACACS server.

12. Use **Connection Timeout** to specify the amount of time that passes before the connection between the device and the TACACS server time out.

The range is between 1 – 30.

- 13.** To add a new server to the switch, click the **ADD** button.

This button is available only to users with read/write permission.

- 14.** To delete the selected server from the configuration, click the **DELETE** button.

- 15.** Click the **APPLY** button.

Your settings are saved.

## Set Up a Login Authentication List

You can configure login lists. A login list specifies the authentication method(s) to be used to validate switch or port access for the users associated with the list. The preconfigured users, admin and guest, are assigned to a preconfigured list named defaultList, which you cannot delete. All newly created users are also assigned to the defaultList until you specifically assign them to a different list.

Two default lists are present: DefaultList and networkList.

➤ **To set up a login authentication list:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Management Security > Authentication List > Login Authentication List**.

Login Authentication List							
:: Login Authentication List							
	List Name	1	2	3	4	5	6
<input type="checkbox"/>		<input type="button" value="▼"/>					
<input checked="" type="checkbox"/>	defaultList	Local					
<input checked="" type="checkbox"/>	networkList	Local					

8. If you are creating a new login list, complete the **List Name** field.

The list name can be up to 15 alphanumeric characters long and is not case-sensitive.

9. For each of the lists, select the methods in the order they will appear in the authentication login list.

If you select a method that does not time out as the first method, such as 'local', no other method is tried, even if you specified more than one method. The options are as follows:

- **Enable**- The privileged EXEC password is used for authentication.
- **Line**- The line password is used for authentication.
- **Local**- The user's locally stored ID and password is used for authentication
- **None**- The user cannot be authenticated.
- **Radius**- The user's ID and password are authenticated using the RADIUS server instead of local server.
- **Tacacs**- The user's ID and password are authenticated using the TACACS server.

If the first method times out, the next method is selected.

10. To add a new login list to the switch, click the **ADD** button.

11. To remove the selected authentication login list from the configuration, click the **DELETE** button.

You can use this button only if you are logged in as admin (with Read/Write access).

12. Click the **APPLY** button.

Your settings are saved.

## Enable an Authentication List

You can configure enable lists. A enable list specifies the authentication method(s) you use to validate privileged EXEC access for the users associated with the list. The preconfigured users, admin and guest, are assigned to a preconfigured list named defaultList, which you cannot delete. All newly created users are also assigned to the defaultList until you specifically assign them to a different list

Two default lists are present: enableList and enableNetList.

➤ **To configure the enable authentication list:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Management Security > Authentication List > Enable Authentication List**.

:: Enable Authentication List						
	List Name	1	2	3	4	5
<input type="checkbox"/>		<input type="button" value=""/>				
<input type="checkbox"/>	enableList	Enable	None			
<input type="checkbox"/>	enableNetList	Enable	None			

8. If you are creating a new list, type the name in the **List Name** field.

The name can be up to 15 alphanumeric characters long and is not case-sensitive.

9. In the numbered lists (1, 2, 3, 4, 5) select the method to appear first in the selected authentication enable list.

The options are as follows:

- **Enable.** The privileged EXEC password is used for authentication.
- **Line.** The line password is used for authentication.
- **None.** The user cannot be authenticated.
- **RADIUS.** The user's name and password are authenticated using the RADIUS server instead of local server.
- **TACACS.** The user's name and password are authenticated using the TACACS server.
- **Deny.** Authentication always fails.

10. To add a new login list to the switch, click the **ADD** button.

11. To remove the selected authentication enable list from the configuration, click the **DELETE** button.

You can use this button only if you are logged in as admin (with Read/Write access).

12. Click the **APPLY** button.

Your settings are saved.

## Configure a Dot1x Authentication List

You can configure a dot1x list. A dot1x list specifies the authentication method(s) used to validate port access for the users associated with the list. Only one dot1x method can be supported. The default list is: dot1xList.

➤ **To configure a dot1x authentication list:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Security > Management Security > Authentication List > Dot1x Authentication List**.

Dot1x Authentication List		
:: Dot1x Authentication List		
	List Name	1
<input type="checkbox"/>	dot1xList	<input type="button" value=""/>

8. Select the check box for the dot1x list.
9. Select the method to appear first in the selected authentication login list.

The options are as follows:

- **IAS.** The user's ID and password in Internal Authentication Server Database are used for authentication.
- **Local.** The user's locally stored ID and password are used for authentication.
- **RADIUS.** The user's ID and password are authenticated using the RADIUS server instead of locally.
- **None.** The user is authenticated without a user name and password

## Configure an HTTP Authentication List

You can configure an HTTP list. An HTTP list specifies the authentication method(s) used to validate the switch or port access through HTTP.

➤ **To configure an HTTP authentication list:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Management Security > Authentication List > HTTP Authentication List**.

HTTP Authentication List					
:: HTTP Authentication List					
	List Name	1	2	3	4
<input checked="" type="checkbox"/>	httpList	Local			

8. Select the check box for a list name.
9. Use the numbered lists (1, 2, 3, 4) to select the method to appear in the selected authentication login list.

If you select a method in the first list that does not time out, such as local, no other method is tried, even if you specified more than one method. The options are as follows:

- **Local.** The user's locally stored ID and password are used for authentication.
- **Radius.** The user's ID and password are authenticated using the RADIUS server instead of locally.
- **TACACS.** The user's ID and password are authenticated using the TACACS server.

## HTTPS Authentication List

You can configure an HTTPS list. A login list specifies the authentication method(s) used to validate the switch or port access through HTTPS for the users associated with the list. The default list is: httpsList.

➤ **To configure an HTTPS authentication list:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Security > Management Security > Authentication List > HTTPS Authentication List**.

HTTPS Authentication List					
:: HTTPS Authentication List					
	List Name	1	2	3	4
<input checked="" type="checkbox"/>	httpsList	Local			

8. Select the check box for the HTTPS list.
9. In the numbered lists (1, 2, 3, 4) select the method to appear first in the selected authentication login list.

If you select a method that does not time out, such as local no other method is tried, even if you specified more than one method. The options are as follows:

- **Local**- The user's locally stored name and password are used for authentication.
- **None**- The user cannot be authenticated.
- **RADIUS**- The user's name and password are authenticated using the RADIUS server instead of local authentication.
- **TACACS**- The user authenticates without a user name and password.

## View Login Sessions

➤ **To view login sessions:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

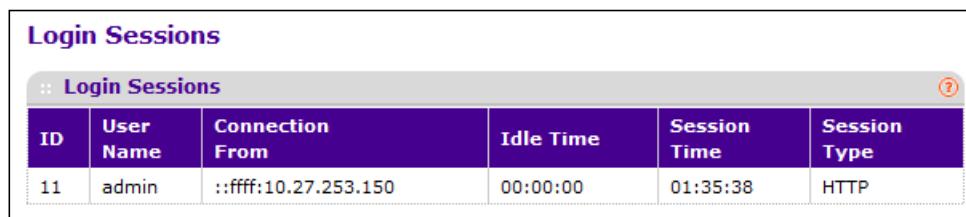
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Management Security > Login Sessions**.



The screenshot shows a table titled "Login Sessions" with a single row of data. The columns are labeled: ID, User Name, Connection From, Idle Time, Session Time, and Session Type. The data row is: 11, admin, ::ffff:10.27.253.150, 00:00:00, 01:35:38, HTTP.

Login Sessions					
:: Login Sessions					
ID	User Name	Connection From	Idle Time	Session Time	Session Type
11	admin	::ffff:10.27.253.150	00:00:00	01:35:38	HTTP

The following table describes the nonconfigurable information displayed on the screen.

**Table 80. Login Sessions**

Field	Description
ID	Identifies the ID of this row.
User Name	Shows the user's name whose session is open.
Connection From	Shows from which machine the user is connected.
Idle Time	Shows the idle session time.
Session Time	Shows the total session time.
Session Type	Shows the type of session: Telnet, serial or SSH

## Configure Management Access

You can configure HTTP and Secure HTTP access to the managed switch's management interface.

### Configure HTTP Server Settings

To access the switch over a web page, you must first configure it with IP information (IP address, subnet mask, and default gateway). You can configure the IP information using any of the following:

- BOOTP
- DHCP
- Terminal interface through the EIA-232 port

After you establish in-band connectivity, you can change the IP information using a web-based management.

➤ **To configure HTTP server settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Security > Access > HTTP > HTTP Configuration**.

HTTP Configuration	
:: HTTP Configuration	
<b>HTTP Access</b>	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
<b>Java Mode</b>	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
<b>HTTP Session Soft Timeout (Minutes)</b>	60 <small>(0 to 60)</small>
<b>HTTP Session Hard Timeout (Hours)</b>	24 <small>(0 to 168)</small>
<b>Maximum Number of HTTP Sessions</b>	16 <small>(0 to 16)</small>
<b>Authentication List</b>	HttpListName

The Authentication List field displays the authentication list that HTTP is using.

**8.** Select the HTTP Access **Disable** or **Enable** radio button.

This specifies whether the switch can be accessed from a web browser. If you choose to enable web mode, you can manage the switch from a web browser. The factory default is enabled.

**9.** Select the Java Mode **Disable** or **Enable** radio button.

This disables or enables the Java applet that displays a picture of the switch in the Device view tab of the System tab. If you run the applet, you can click the picture of the switch to select configuration screens instead of using the navigation tree on the left side of the screen. The factory default is Enable.

**10.** In the **HTTP Session Soft Timeout (Minutes)** field, set the inactivity time-out for HTTP sessions.

The value must be in the range of 1 to 60 minutes. The default value is 60 minutes. The currently configured value is shown when the screen displays.

**11.** In the **HTTP Session Hard Timeout (Hours)** field, set the hard time-out for HTTP sessions.

This time-out is unaffected by the activity level of the session. The value must be in the range of 1 to 168 hours. The default value is 24 hours. The currently configured value is shown when the screen is displayed.

**12.** In the **Maximum Number of HTTP Sessions** field, set the maximum allowable number of HTTP sessions.

The value must be in the range of 0 to 16. The default value is 16. The currently configured value is shown when the screen is displayed.

## Configure HTTPS Settings

Secure HTTP enables the transmission of HTTP over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. When you manage the switch by using a web interface, secure HTTP can help ensure that communication between the management system and the switch is protected from eavesdroppers and man-in-the-middle attacks.

You can configure the settings for HTTPS communication between the management station and the switch.

➤ **To configure HTTPS settings:**

- 1.** Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
- 2.** Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
- 3.** Launch a web browser.
- 4.** Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Access > HTTPS > HTTPS Configuration**.

The screenshot shows the 'HTTPS Configuration' screen with the following settings:

- HTTPS Admin Mode:** Disable (radio button selected)
- SSL Version 3:** Enable (radio button selected)
- TLS Version 1:** Enable (radio button selected)
- HTTPS Port:** 443 (1 to 65535)
- HTTPS Session Soft Timeout (Minutes):** 60 (1 to 60)
- HTTPS Session Hard Timeout (Hours):** 24 (1 to 168)
- Maximum Number of HTTPS Sessions:** 16 (0 to 16)
- Authentication List:** `HttpsListName`

8. Select the HTTPS Admin Mode **Disable** or **Enable** radio button.

This specifies the administrative mode of secure HTTP. The currently configured value is shown when the screen is displayed. The default value is Disable. You can download SSL certificates only when the HTTPS Admin mode is disabled.

9. Select the SSL Version 3 **Disable** or **Enable** radio button.

This disables or enables Secure Sockets Layer Version 3.0. The currently configured value is shown when the screen is displayed. The default value is Enable.

10. Select the TLS Version 1 **Disable** or **Enable** radio button.

This disables or enables Transport Layer Security Version 1.0. The currently configured value is shown when the screen is displayed. The default value is Enable.

11. Use **HTTPS Port** to set the HTTPS port number.

The value must be in the range of 1 to 65535. Port 443 is the default value. The currently configured value is shown when the screen is displayed.

12. Use **HTTPS Session Soft Timeout (Minutes)** to set the inactivity time-out for HTTPS sessions.

The value must be in the range of 1 to 60 minutes. The default value is 60 minutes. The currently configured value is shown when the screen is displayed.

13. Use **HTTPS Session Hard Timeout (Hours)** to set the hard time-out for HTTPS sessions.

This time-out is unaffected by the activity level of the session. The value must be in the range of 1 to 168 hours. The default value is 24 hours. The currently configured value is shown when the screen is displayed.

- 14.** Use **Maximum Number of HTTPS Sessions** to set the maximum allowable number of HTTPS sessions.

The value must be in the range of 0 to 16. The default value is 16. The currently configured value is shown when the screen is displayed.

## Manage Certificates

You can generate or delete certificates.

➤ **To manage certificates:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

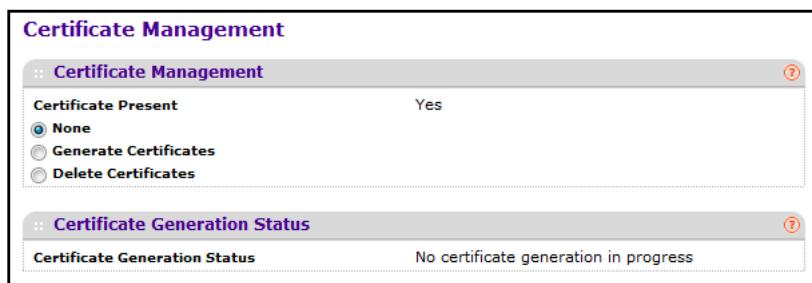
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Access > HTTPS > Certificate Management**.



The screen displays certificates that are present and the SSL certificate generation status.

8. Select a Certificate Present radio button:

- **None.** There is nothing to be done with respect to certificate management. This is the default selection.
- **Generate Certificates.** Begin generating the certificate files.

- **Delete Certificates.** Delete the corresponding certificate files, if present.

## Download a Certificate

You can transfer a certificate file to the switch.

For the web server on the switch to accept HTTPS connections from a management station, the web server needs a public key certificate. You can generate a certificate externally (for example, off-line) and download it to the switch.

Before you download a file to the switch, the following conditions must be true:

- The file to download from the TFTP server is on the server in the appropriate directory.
- The file is in the correct format.
- The switch has a path to the TFTP server.

➤ **To download a certificate:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

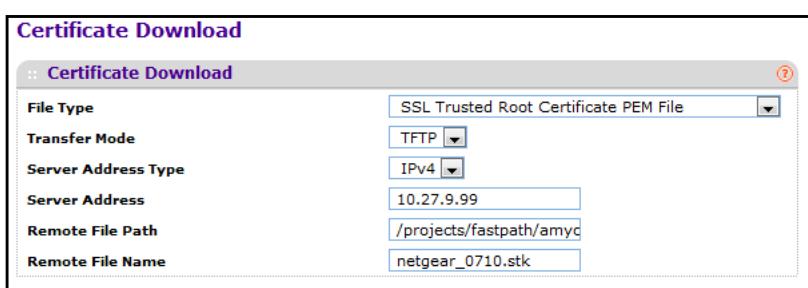
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Access > HTTPS > Certificate Download**



8. In the **File Type** list, specify the type of file:

- **SSL Trusted Root Certificate PEM File.** SSL Trusted Root Certificate file (PEM Encoded)

- **SSL Server Certificate PEM File.** SSL Server Certificate file (PEM Encoded)
  - **SSL DH Weak Encryption Parameter PEM File.** SSL Diffie-Hellman Weak Encryption Parameter file (PEM Encoded)
  - **SSL DH Strong Encryption Parameter PEM File.** SSL Diffie-Hellman Strong Encryption Parameter file (PEM Encoded)
- 9.** In the **Transfer Mode** menu, specify the protocol to use to transfer the file:
- **TFTP.** Trivial File Transfer Protocol
  - **SFTP.** Secure File Transfer Protocol
  - **SCP.** Secure Copy Protocol
- 10.** In the **Server Address Type** menu, specify either IPv4, IPv6, or DNS to indicate the format of the TFTP/SFTP/SCP Server Address field.
- The factory default is IPv4.
- 11.** In the **Server Address** field, type the IP address or DNS host name of the server in accordance with the format indicated by the server address type.
- The factory default is the IPv4 address 0.0.0.0.
- 12.** In the **Remote File Path** field, enter the path of the file to download.
- You can enter up to 96 characters. The factory default is blank.
- 13.** In the **Remote File Name** field, type the name of the file on the TFTP server to download.
- You can enter up to 32 characters. The factory default is blank.

## Configure SSH

- **To configure SSH:**
- 1.** Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
  - 2.** Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
  - 3.** Launch a web browser.
  - 4.** Enter the IP address of the switch in the web browser address field.
- The default IP address of the switch is 169.254.100.100.
- The Login screen displays.
- 5.** Enter the user name and password.
- The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
- 6.** Click the **Login** button.
- The web management interface menu displays.

**7.** Select **Security > Access > SSH > SSH Configuration**.

The screenshot shows the 'SSH Configuration' screen with the following settings:

- SSH Admin Mode:** Disable (radio button selected)
- SSH Version 1:** Enable (radio button selected)
- SSH Version 2:** Enable (radio button selected)
- SSH Session Timeout:** 5 minutes
- Maximum Number of SSH Sessions:** 5
- Current Number of SSH Sessions:** 0
- Keys Present:** No
- Login Authentication List:** networkList
- Enable Authentication List:** enableNetList

**8.** Select the **SSH Admin Mode** **Disable** or **Enable** radio button.

The currently configured value is displayed. The default value is Disable.

**9.** Select the **SSH Version 1** **Disable** or **Enable** radio button.

The currently configured value is shown when the screen is displayed. The default value is Enable.

**10.** Select the **SSH Version 2** **Disable** or **Enable** radio button.

The currently configured value is displayed. The default value is Enable.

**11.** In the **SSH Session Timeout** field, set the time-out value for incoming SSH sessions to the switch.

The acceptable range for this field is 1 – 5 minutes.

**12.** In the **Maximum Number of SSH Sessions** field, set the maximum number of inbound SSH sessions allowed on the switch.

The currently configured value is displayed. The acceptable range for this field is 0 – 5.

**13.** In the **Login Authentication List** menu, select an authentication list.

This list is used to authenticate users who try to login to the switch.

**14.** In the **Enable Authentication List** menu, select an authentication list.

This list is used to authenticate users who try to get “enable” level privilege.

**15.** To refresh the screen and to show the latest SSH sessions privileges, click the **REFRESH** button.

The following table describes the nonconfigurable information displayed on the screen.

**Table 81. SSH Configuration**

Field	Description
Current Number of SSH Sessions	Displays the number of SSH connections currently in use in the system.
Keys Present	Displays which keys, RSA, DSA or both, are present (if any).

## Manage Host Keys

You can generate or delete RSA and DSA keys.

➤ **To manage Host Keys:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

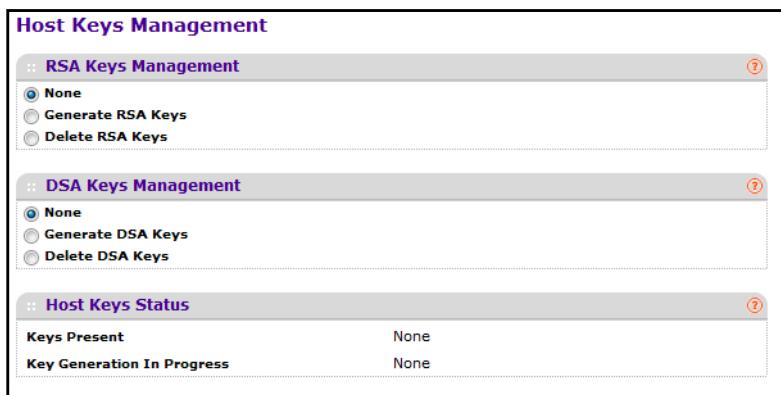
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Access > SSH > Host Keys Management**.



The **Keys Present** field displays which keys, RSA, DSA, or both, are present (if any).

The **Key Generation in Progress** field displays which key is being generated (if any), RSA, DSA, or None.

8. Select an RSA Keys Management radio button:
  - **None**. This is the default selection.
  - **Generate RSA Keys**. Select this option to begin generating the RSA host keys. To generate SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.

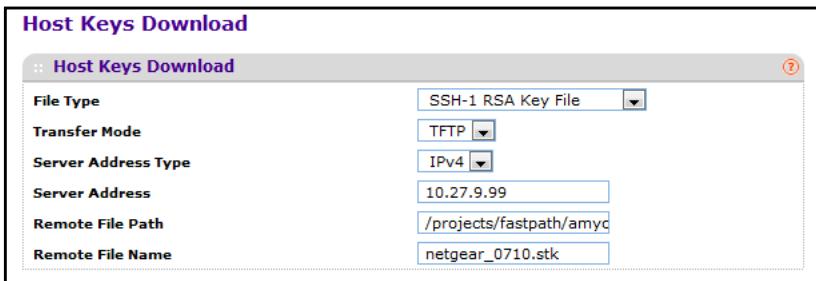
- **Delete RSA Keys.** Select this option to delete the corresponding RSA key file, if it is present.
9. Select a DSA Keys Management radio button:
- **None.** This is the default selection.
  - **Generate DSA Keys.** Select this option to begin generating the DSA host keys. To generate SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.
  - **Delete DSA Keys.** Select this option to delete the corresponding DSA key file, if it is present.
10. Click the **APPLY** button.
- The host key file starts downloading.
- Note:** To download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.
11. To refresh the screen and to show the latest SSH sessions, click the **REFRESH** button.

## Download Host Keys

You can transfer a file to or from the switch.

- **To download host keys:**
1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
  2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
  3. Launch a web browser.
  4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
  5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
  6. Click the **Login** button.  
The web management interface menu displays.

**7.** Select **Security > Access > SSH > Host Keys Download**.



- 8.** In the **File Type** menu, specify the type of file to transfer:
  - **SSH-1 RSA Key File.** SSH-1 Rivest-Shamir-Adleman (RSA) Key file
  - **SSH-2 RSA Key PEM File.** SSH-2 Rivest-Shamir-Adleman (RSA) Key file (PEM Encoded)
  - **SSH-2 DSA Key PEM File.** SSH-2 Digital Signature Algorithm (DSA) Key file (PEM Encoded)
- 9.** In the **Transfer Mode** menu, specify the protocol to use to transfer the file:
  - **TFTP.** Trivial File Transfer Protocol
  - **SFTP.** Secure File Transfer Protocol
  - **SCP.** Secure Copy Protocol
- 10.** In the **Server Address Type** field, specify either IPv4, IPv6, or DNS to indicate the format of the TFTP/SFTP/SCP Server Address field.  
The factory default is IPv4.
- 11.** Use **Server Address** to enter the IP address or DNS host name of the server in accordance with the format indicated by the server address type.  
The factory default is the IPv4 address 0.0.0.0.
- 12.** Use **Remote File Path** to enter the path of the file to download.  
You can enter up to 96 characters. The factory default is blank.
- 13.** Use **Remote File Name** to enter the name of the file on the TFTP server to download.  
You can enter up to 32 characters. The factory default is blank.
- 14.** Click the **APPLY** button.  
The host key file starts downloading.

**Note:** To download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.

## Manage Telnet

You can configure a Telnet authentication list and manage outbound and inbound Telnet.

### Configure a Telnet Authentication List

You can select the login and make the authentication list available. The login list specifies the authentication method(s) used to validate switch or port access for the users associated with the list. The enable list specifies the authentication method(s) used to validate privileged EXEC access for the users associated with the list. These lists can be created through the Authentication List link under Management Security.

➤ **To configure a Telnet authentication list:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Access > Telnet**.

The screenshot shows the Telnet configuration interface. It includes three main sections: 
 

- Authentication List:** Contains dropdown menus for "Login Authentication List" (set to "networkList") and "Enable Authentication List" (set to "enableNetList").
- Inbound Telnet:** Includes settings for "Telnet Server Admin Mode" (Enable selected), "Allow new telnet sessions" (Enable selected), "Session Timeout (Minutes)" (5), "Maximum Number of Sessions" (5), and "Current Number of Sessions" (0).
- Outbound Telnet:** Includes settings for "Allow new telnet sessions" (Enable selected), "Session Timeout (Minutes)" (5), "Maximum Number of Sessions" (5), and "Current Number of Sessions" (0).

8. In the **Login Authentication List** menu, specify which authentication list to use login through Telnet.  
The default value is networkList.
9. In the **Enable Authentication List** menu, specify which authentication list you are using when going into the privileged EXEC mode.  
The default value is enableNetList.

## Configure Inbound Telnet

You can regulate new Telnet sessions. If Allow New Telnet Sessions is enabled, new inbound Telnet sessions can be established until there are no more sessions available. If Allow New Telnet Sessions is disabled, no new inbound Telnet sessions are established. An established session remains active until the session is ended or an abnormal network error ends the session.

➤ **To configure inbound Telnet:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Security > Access > Telnet**.

The **Current Number of Sessions** field displays the number of current sessions.

8. In the Inbound Telnet section, select the Allow New Telnet Sessions **Disable** or **Enable** radio button.

The default value is Enable.

9. In the **Session Timeout** field, specify how many minutes of inactivity can occur on a Telnet session before the session is logged off.

You can enter any number from 1 to 160. The factory default is 5.

10. In the **Maximum Number of Sessions** field, specify how many simultaneous Telnet sessions are allowed.

The maximum is 5, which is also the factory default.

## Configure Outbound Telnet

You can regulate new outbound Telnet connections. If Allow New Telnet Sessions is enabled, new outbound Telnet sessions can be established until there are no more sessions available. If Allow New Telnet Sessions is disabled, no new outbound Telnet sessions are established. An established session remains active until the session is ended or an abnormal network error ends the session.

➤ **To configure outbound Telnet:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Access > Telnet**.

The screenshot shows the 'TELNET' configuration page with three main sections:

- Authentication List:** Contains dropdown menus for 'Login Authentication List' (set to 'networkList') and 'Enable Authentication List' (set to 'enableNetList').
- Inbound Telnet:** Contains settings for Telnet Server Admin Mode (Enable selected), Allow new telnet sessions (Enable selected), Session Timeout (Minutes) (5), Maximum Number of Sessions (5), and Current Number of Sessions (0).
- Outbound Telnet:** Contains settings for Allow new telnet sessions (Enable selected), Session Timeout (Minutes) (5), Maximum Number of Sessions (5), and Current Number of Sessions (0).

The **Current Number of Sessions** field displays the number of current sessions.

8. In the Outbound Telnet section, select the Allow New Telnet Sessions **Disable** or **Enable** radio button.

The default value is Enable.

9. In the **Maximum Number of Sessions** field, specify the maximum number of Outbound Telnet Sessions allowed.

The default value is 5. The valid range is 0 to 5.

10. In the **Session Timeout** field, specify the Outbound Telnet login inactivity time-out.

The default value is 5. The valid range is 1 to 160.

**Current Number of Sessions.** Displays the number of current sessions.

## Configure the Console Port

- **To configure the console port:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.

2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Access > Console Port**.

Console Port	
Serial Port Login Timeout (minutes)	5 (0 to 160)
Baud Rate (bps)	115200
Character Size (bits)	8
Flow Control	Disable
Stop Bits	1
Parity	None
Login Authentication List	defaultList
Enable Authentication List	enableList

8. In the **Serial Port Login Timeout (minutes)** field, enter a number between 0 and 160.

This specifies how many minutes of inactivity can occur on a serial port connection before the switch closes the connection. The factory default is 5. Entering 0 disables the time-out.

9. In the **Baud Rate (bps)** menu, select the default baud rate for the serial port connection.

You can choose from 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 baud. The factory default is 115200 baud.

10. In the **Login Authentication List** menu, specify which authentication list to use when you log in through Telnet.

The default value is defaultList.

11. In the **Enable Authentication List** menu, specify which authentication list to use when going into the privileged EXEC mode.

The default value is enableList.

The following table describes the nonconfigurable information displayed on the screen.

**Table 82. Console Port**

Field	Description
Character Size (bits)	The number of bits in a character. This is always 8.
Flow Control	Whether hardware flow control is enabled or disabled. It is always disabled.
Stop Bits	The number of stop bits per character. It is always 1.
Parity	The parity method used on the serial port. It is always None.

## Configure Denial of Service Settings

➤ **To configure denial of service:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Security > Access > Denial of Service Configuration**.

**Denial of Service Configuration**

<b>Denial of Service Configuration</b>	
<b>Denial of Service Min TCP Header Size</b>	<input type="text" value="20"/> (0 to 255)
<b>Denial of Service ICMPv4</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>Denial of Service Max ICMPv4 Packet Size</b>	<input type="text" value="512"/> (0 to 16376)
<b>Denial of Service ICMPv6</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>Denial of Service Max ICMPv6 Packet Size</b>	<input type="text" value="512"/> (0 to 16376)
<b>Denial of Service First Fragment</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>Denial of Service ICMP Fragment</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>Denial of Service SIP=DIP</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>Denial of Service SMAC=DMAC</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>Denial of Service TCP FIN&amp;URG&amp;PSH</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>Denial of Service TCP Flag&amp;Sequence</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>Denial of Service TCP Fragment</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>Denial of Service TCP Offset</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>Denial of Service TCP Port</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>Denial of Service TCP SYN</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>Denial of Service TCP SYN&amp;FIN</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
<b>Denial of Service UDP Port</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

8. In the **Denial of Service Min TCP Header Size** field, specify the Min TCP Hdr Size allowed.

If DoS TCP fragment is enabled, the switch drops these packets:

- First TCP fragments with a TCP payload: IP\_Payload\_Length - IP\_Header\_Size < Min\_TCP\_Header\_Size.
- Its range is 0 to 255. The default value is 20.

9. Use **Denial of Service ICMPv4** to enable ICMPv4 DoS prevention.

ICMPv4 DoS prevention causes the switch to drop ICMPv4 packets with a type set to ECHO\_REQ (ping) and a size greater than the configured ICMPv4 Pkt Size. The factory default is disabled.

10. Use **Denial of Service Max ICMPv4 Packet Size** to specify the Max ICMPv4 Pkt Size allowed.

If ICMPv4 DoS prevention is enabled, the switch drops IPv4 ICMP ping packets with a size greater than the configured Max ICMPv4 Pkt Size. Its range is 0 to 16376. The default value is 512.

11. Use **Denial of Service ICMPv6** to enable ICMPv6 DoS prevention.

ICMPv6 DoS prevention causes the switch to drop ICMPv6 packets with a type set to ECHO\_REQ (ping) and a size greater than the configured ICMPv6 Pkt Size. The factory default is disabled.

12. Use **Denial of Service Max ICMPv6 Packet Size** to specify the Max IPv6 ICMP Pkt Size allowed.

If ICMPv6 DoS prevention is enabled, the switch drops IPv6 ICMP ping packets with a size greater than this configured Max ICMPv6 Pkt Size. Its range is 0 to 16376. The default value is 512.

**13. Use Denial of Service First Fragment** to enable first fragment DoS prevention.

First fragment DoS prevention causes the switch to check DoS options on first fragment IP packets when switch are receiving fragmented IP packets. Otherwise, the switch ignores the first fragment IP packages. The factory default is disabled.

**14. Use Denial of Service ICMP Fragment** to enabling ICMP fragment DoS prevention.

ICMP fragment DoS prevention causes the switch to drop ICMP fragmented packets. The factory default is disabled.

**15. Use Denial of Service SIP=DIP** to enable SIP=DIP DoS prevention.

This causes the switch to drop packets with a source IP address equal to the destination IP address. The factory default is disabled.

**16. Use Denial of Service SMAC=DMAC** to enable SMAC=DMAC DoS prevention.

This causes the switch to drop packets with a source MAC address equal to the destination MAC address. The factory default is disabled.

**17. Use Denial of Service TCP FIN&URG&PSH** to enable TCP FIN & URG & PSH DoS prevention.

This causes the switch to drop packets with TCP flags FIN, URG, and PSH set and TCP Sequence Number=0. The factory default is disabled.

**18. Use Denial of Service TCP Flag &Sequence** to enable TCP flag DoS prevention.

This causes the switch to drop packets with TCP control flags set to 0 and TCP sequence number set to 0. The factory default is disabled.

**19. Use Denial of Service TCP Fragment** to enable TCP fragment DoS prevention.

This causes the switch to drop packets:

- First TCP fragments that has a TCP payload: IP\_Payload\_Length - IP\_Header\_Size < Min\_TCP\_Header\_Size.
- The factory default is disabled.

**20. Use Denial of Service TCP Offset** to enable TCP offset DoS prevention.

This causes the switch to drop packets with a TCP header Offset=1. The factory default is disabled.

**21. Use Denial of Service TCP Port** to enable TCP port DoS prevention.

This causes the switch to drop packets with TCP source port equal to TCP destination port. The factory default is disabled.

**22. Use Denial of Service TCP SYN** to enable TCP SYN DoS prevention.

This causes the switch to drop packets with TCP flags SYN set. The factory default is disabled.

**23. Use Denial of Service TCP SYN&FIN** to enable TCP SYN & FIN DoS prevention.

This causes the switch to drop packets with TCP flags SYN and FIN set. The factory default is disabled.

#### 24. Use **Denial of Service UDP Port** to enable UDP Port DoS prevention.

This causes the switch to drop packets with UDP source port equal to UDP destination port. The factory default is disabled.

## Port Authentication Overview

In port-based authentication, when 802.1X is enabled globally and on the port, successful authentication of any one supplicant attached to the port results in all users being able to use the port without restrictions. At any given time, only one supplicant is allowed to attempt authentication on a port in this mode. Ports in this mode are under bidirectional control. This is the default authentication mode.

The 802.1X network has three components:

- **Authenticators.** Specify the port that is authenticated before permitting system access.
- **Supplicants.** Specify the host connected to the authenticated port requesting access to the system services.
- **Authentication Server.** Specifies the external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the user is authorized to access system services.

## Configure Global 802.1X Settings

You can use 802.1X to enable or disable port access control on the system.

#### ➤ To configure global 802.1X settings:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7.** Select **Security > Port Authentication > Basic > 802.1X Configuration**.

The screenshot shows the '802.1X Configuration' page with the following settings:

- Administrative Mode:** Disable (radio button selected)
- VLAN Assignment Mode:** Disable (radio button selected)
- EAPOL Flood Mode:** Disable (radio button selected)
- Dynamic VLAN Creation Mode:** Disable (dropdown menu)
- Monitor Mode:** Disable (dropdown menu)
- Users:** admin (dropdown menu)
- Login:** defaultList (dropdown menu)
- Authentication List:** dot1xList (dropdown menu)

The Authentication List field displays the authentication list that is used by 802.1X.

**8.** Select the Administrative Mode **Disable** or **Enable** radio button.

This enables or disables 802.1X administrative mode on the switch.

- **Enable.** 802.1X is permitted on the switch.

---

**Note:** If 802.1X is enabled, authentication is performed by a RADIUS server. This means that the primary authentication method must be RADIUS. To set the method, select **Security > Management Security > Authentication List** and select RADIUS as method 1 for defaultList. For more information, see *Configure a RADIUS Server* on page 268.

---

- **Disable.** The switch does not check for 802.1X authentication before allowing traffic on any ports, even if the ports are configured to allow only authenticated users. Default value.

**9.** Select the VLAN Assignment Mode **Disable** or **Enable** radio button.

The default value is Disable.

**10.** Select the EAPOL Flood Mode **Disable** or **Enable** radio button.

The default value is Disable.

**11.** In the **Monitor Mode** field, select **Enable** or **Disable**.

The default value is Disable. The feature monitors the dot1x authentication process and helps in diagnosis of the authentication failure cases.

**12.** In the **Users** list, select the user name that uses the selected login list for 802.1x port security.

**13.** In the **Login** list, select the login list to apply to the specified user.

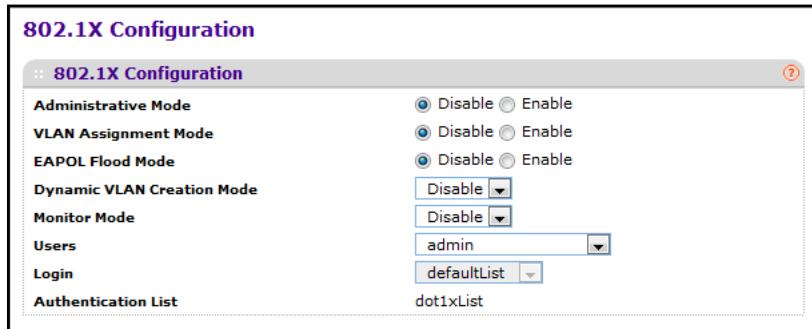
All configured login lists are listed in this menu.

## Configure 802.1X Settings

You can enable or disable port access control on the system.

➤ **To configure 801.1X settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Security > Port Authentication > Advanced > 802.1X Configuration**.



The Authentication List field displays the authentication list that is used by 802.1x.

8. Select the Administrative Mode **Disable** or **Enable** radio button.  
The default value is Disable.
9. Select the VLAN Assignment Mode **Disable** or **Enable** radio button.  
The default value is Disable.
10. Select the EAPOL Flood Mode **Disable** or **Enable** radio button.  
The default value is Disable.
11. In the **Monitor Mode** menu, select **Disable** or **Enable**.

The default value is Disable. The feature monitors the dot1x authentication process and helps in diagnosis of the authentication failure cases.

12. In the **Users** list, select the user name that uses the selected login list for 802.1x port security.
13. In the **Login** list, select the login list to apply to the specified user. All configured login lists are displayed.

## Configure 802.1X Settings for Port Authentication

You can enable and configure port access control on one or more ports.

➤ **To configure 802.1X settings for the port:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

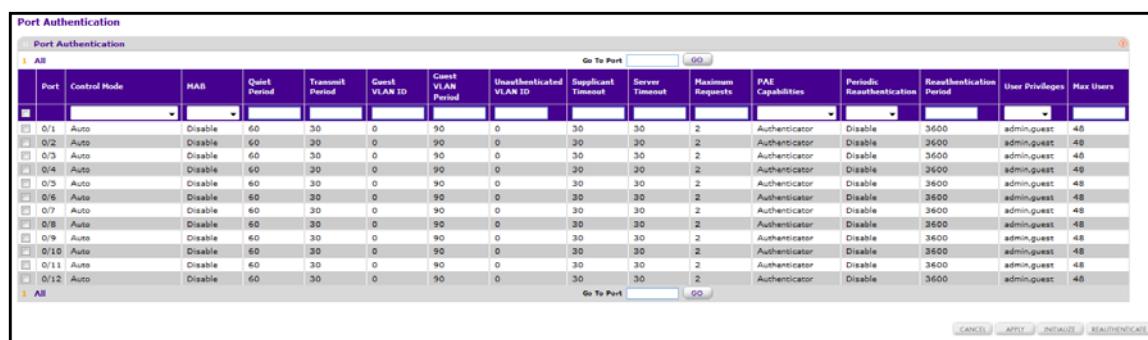
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Port Authentication > Advanced > Port Authentication**.



The screenshot shows a table titled "Port Authentication" with the following columns: Port, Control Mode, HAB, Quiet Period, Transmit Period, Guest VLAN ID, Guest VLAN Period, Unauthenticated VLAN ID, Supplicant Timeout, Server Timeout, Maximum Requests, PAE Capabilities, Periodic Reauthentication, Reauthentication Period, User Privileges, and Max Users. There are 12 rows, each corresponding to a port (0/1 to 0/12). Most ports have "Auto" as their Control Mode and "Disable" as their HAB. The "Guest VLAN ID" column contains values like 90, 0, 90, 0, etc. The "PAE Capabilities" column shows "Authenticator" for most ports and "Disable" for others. The "User Privileges" column shows "admin.guest" for most ports and "admin" for others. The "Max Users" column shows values like 48, 49, 48, 49, etc.

**Note:** Use the horizontal scroll bar at the bottom of the screen to view all the fields on the Port Authentication screen.

8. Select the check box next to the port to configure.

You can select multiple check boxes to apply the same settings to the selected ports, or select the check box in the heading row to apply the same settings to all ports.

9. For the selected port(s), specify the following settings:
  - **Control Mode.** This selector lists the options for control mode. The control mode is set only if the link status of the port is link up. The options are as follows:
    - **force unauthorized.** The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized.
    - **force authorized.** The authenticator PAE unconditionally sets the controlled port to authorized.
    - **auto.** The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server.
    - **mac based.** The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server on a per supplicant basis.
    - **N/A.** The control mode is not applicable.
  - Use **MAB** to enable or disable MAP. The default selection is Disable.
  - **Quiet Period.** This input field allows the user to configure the quiet period for the selected port. This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it does not attempt to acquire a supplicant. The quiet period is the period for which the authenticator does not attempt to acquire a supplicant after a failed authentication exchange with the supplicant. The quiet period must be a number in the range of 0 to 65535. A quiet period value of 0 means that the authenticator state machine never acquires a supplicant. The default value is 60. Changing the value does not change the configuration until the **APPLY** button is clicked.
  - **Transmit Period.** This input field allows the user to configure the transmit period for the selected port. The transmit period is the value, in seconds, of the timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The transmit period must be a number in the range of 1 to 65535. The default value is 30. Changing the value does not change the configuration until the **APPLY** button is clicked.
  - **GuestVLAN ID.** This field allows the user to configure the guest VLAN ID on the interface. The valid range is 0 to 4093. The default value is 0. Changing the value does not change the configuration until the **APPLY** button is clicked. Enter 0 to clear the guest VLAN ID on the interface.
  - **Guest VLAN Period.** This input field allows the user to enter the guest VLAN period for the selected port. The guest VLAN period is the value, in seconds, of the timer used by the GuestVlan authentication. The guest VLAN time-out must be a value in the range of 1 to 300. The default value is 90. Changing the value does not change the configuration until the **APPLY** button is clicked.
  - **Unauthenticated VLAN ID.** This input field allows the user to enter the unauthenticated VLAN ID for the selected port. The valid range is 0-4093. The default

value is 0. Changing the value does not change the configuration until the Submit button is clicked. Enter 0 to clear the unauthenticated VLAN ID on the interface.

- **Supplicant Timeout.** This input field allows the user to enter the supplicant time-out for the selected port. The supplicant time-out is the value, in seconds, of the timer used by the authenticator state machine on this port to time-out the supplicant. The supplicant time-out must be a value in the range of 1 to 65535. The default value is 30. Changing the value does not change the configuration until the **APPLY** button is clicked.
- **Server Timeout.** This input field allows the user to enter the server time-out for the selected port. The server time-out is the value, in seconds, of the timer used by the authenticator on this port to time-out the authentication server. The server time-out must be a value in the range of 1 to 65535. The default value is 30. Changing the value does not change the configuration until the **APPLY** button is clicked.
- **Maximum Requests.** This input field allows the user to enter the maximum requests for the selected port. The maximum requests value is the maximum number of times the authenticator state machine on this port retransmits an EAPOL EAP Request/Identity before timing out the supplicant. The maximum requests value must be in the range of 1 to 10. The default value is 2. Changing the value does not change the configuration until the **APPLY** button is clicked.
- **PAE Capabilities.** This field selects the port access entity (PAE) functionality of the selected port. Possible values are Authenticator or Supplicant.
- **Periodic Reauthentication.** This select field allows the user to enable or disable reauthentication of the supplicant for the specified port. The selectable values are 'enable or disable'. If the value is 'enable' reauthentication occurs. Otherwise, reauthentication is not allowed. The default value is Disable. Changing the selection does not change the configuration until the **APPLY** button is clicked.
- **Reauthentication Period.** This input field allows the user to enter the reauthentication period for the selected port. The reauthentication period is the value, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The reauthentication period must be a value in the range of 1 to 65535. The default value is 3600. Changing the value does not change the configuration until the **APPLY** button is clicked.
- **User Privileges.** This select field allows the user to add the specified user to the list of users with access to the specified port or all ports.
- **Max Users.** This field allows the user to enter the maximum number of supplicants on the specified interface.

**10.** Click the **INITIALIZE** button to begin the initialization sequence on the selected port.

This button is clickable only if the control mode is auto. Otherwise, it is grayed out. When this button is clicked, the action is immediate. Clicking the **APPLY** button is not required for the action to occur.

**11.** Click the **REAUTHENTICATE** button to begin the reauthentication sequence on the selected port.

This button is only clickable if the control mode is auto. Otherwise, it is grayed out. When this button is clicked, the action is immediate. Clicking the **APPLY** button is not required for the action to occur.

## View the Port Summary

You can view information about the port access control settings on a specific port.

➤ **To view the port summary:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Port Authentication > Advanced > Port Summary**.

Port Summary																		
:: Port Summary																		
1 2 All																		
Port	Control Mode	Operating Control Mode	Reauthentication Enabled	Control Direction	Protocol Version	PAE Capabilities	Authenticator	Backend State	VLAN Assigned	VLAN Assigned Reason	Key Transmission Enabled	Session Timeout	Session Termination Action	Port Status	Port Method			
1/0/1	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A	Port Based			
1/0/2	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A	Port Based			
1/0/3	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A	Port Based			
1/0/4	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A	Port Based			
1/0/5	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A	Port Based			

The following table describes the fields on the Port Summary screen.

**Table 83. Port summary**

Field	Description
Port	Specifies the port whose settings are displayed in the current table row.
Control Mode	This field indicates the configured control mode for the port. Possible values are as follows: <ul style="list-style-type: none"> <li>• Force Unauthorized: The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized.</li> <li>• Force Authorized: The authenticator PAE unconditionally sets the controlled port to authorized.</li> <li>• Auto: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server.</li> <li>• MAC Based: The authenticator PAE sets the controlled port mode to reflect the outcome of authentication exchanges between a supplicant, an authenticator, and an authentication server on a per supplicant basis.</li> </ul>
Operating Control Mode	This field indicates the control mode under which the port is actually operating. Possible values are as follows: <ul style="list-style-type: none"> <li>• ForceUnauthorized</li> <li>• ForceAuthorized</li> <li>• Auto</li> <li>• MAC Based</li> <li>• N/A: If the port is in detached state, it cannot participate in port access control.</li> </ul>
Reauthentication Enabled	This field shows whether reauthentication of the supplicant for the specified port is allowed. The possible values are 'true' and 'false'. If the value is 'true' reauthentication occurs. Otherwise, reauthentication is not allowed.
Control Direction	This displays the control direction for the specified port. The control direction dictates the degree to which protocol exchanges take place between supplicant and authenticator. This affects whether the unauthorized controlled port exerts control over communication in both directions (disabling both incoming and outgoing frames) or just in the incoming direction (disabling only the reception of incoming frames). This field is not configurable on some platforms.
Protocol Version	This field displays the protocol version associated with the selected port. The only possible value is 1, corresponding to the first version of the 802.1x specification. This field is not configurable.
PAE Capabilities	This field displays the port access entity (PAE) functionality of the selected port. Possible values are Authenticator or Supplicant. This field is not configurable.

**Table 83. Port summary**

Field	Description
Authenticator PAE State	<p>This field displays the current state of the authenticator PAE state machine. Possible values are as follows:</p> <ul style="list-style-type: none"> <li>• Initialize</li> <li>• Disconnected</li> <li>• Connecting</li> <li>• Authenticating</li> <li>• Authenticated</li> <li>• Aborting</li> <li>• Held</li> <li>• ForceAuthorized</li> <li>• ForceUnauthorized.</li> </ul>
Backend State	<p>This field displays the current state of the backend authentication state machine. Possible values are as follows:</p> <ul style="list-style-type: none"> <li>• Request</li> <li>• Response</li> <li>• Success</li> <li>• Fail</li> <li>• Timeout</li> <li>• Initialize</li> <li>• Idle</li> </ul>
Vlan Assigned	<p>This field displays the VLAN ID assigned to the selected interface by the authenticator. This field is displayed only when the port control mode of the selected interface is not MAC-based. This field is not configurable.</p>
Vlan Assigned Reason	<p>This field displays reason for the VLAN ID assigned by the authenticator to the selected interface. This field is displayed only when the port control mode of the selected interface is not MAC-based. This field is not configurable. Possible values are as follows:</p> <ul style="list-style-type: none"> <li>• Radius</li> <li>• Unauth</li> <li>• Default</li> <li>• Not Assigned</li> </ul>
Key Transmission Enabled	<p>This field displays if key transmission is enabled on the selected port. This is not a configurable field. The possible values are 'true' and 'false'. If the value is 'false' key transmission does not occur. Otherwise, key transmission is supported on the selected port.</p>
Session Timeout	<p>This field displays session timeout set by the Radius server for the selected port. This field is displayed only when the port control mode of the selected port is not MAC-based.</p>

**Table 83. Port summary**

Field	Description
Session Termination Action	This field displays termination action set by the RADIUS server for the selected port. This field is displayed only when the port control mode of the selected port is not MAC-based. Possible values are as follows: <ul style="list-style-type: none"> <li>• Default</li> <li>• Reauthenticate</li> </ul> If the termination action is default then at the end of the session, the client details are initialized. Otherwise, re-authentication is attempted.
Port Status	This field shows the authorization status of the specified port. The possible values are Authorized, Unauthorized, and N/A. If the port is in detached state, the value is N/A because the port cannot participate in port access control.

## View the Client Summary

➤ **To view the client summary:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

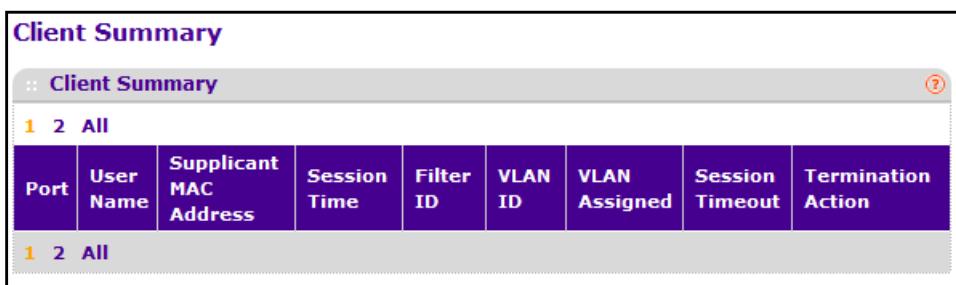
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Port Authentication > Advanced > Client Summary**.



The following table describes the nonconfigurable information displayed on the screen.

**Table 84. Client summary**

Field	Description
Port	The port to be displayed.
User Name	This field displays the user name representing the identity of the supplicant device.
Supplicant Mac Address	This field displays supplicant's device MAC address.
Session Time	This field displays the time since the supplicant was logged, in seconds.
Filter ID	This field displays policy filter ID assigned by the authenticator to the supplicant device.
Vlan ID	This field displays VLAN ID assigned by the authenticator to the supplicant device.
Vlan Assigned	This field displays reason for the VLAN ID assigned by the authenticator to the supplicant device.
Session Timeout	This field displays session timeout set by the RADIUS server to the supplicant device.
Termination Action	This field displays termination action set by the RADIUS server to the supplicant device.

## Traffic Control

You can configure MAC filters, storm control, port security, and protected port settings. To display the screen, select **Security > Traffic Control**.

### Configure MAC Filter Settings

You can create MAC filters that limit the traffic allowed into and out of specified ports on the system.

➤ **To configure MAC filter settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Traffic Control > MAC Filter > MAC Filter Configuration**.

8. In the **MAC Filter** list, select **Create Filter**.

This is the list of MAC address and VLAN ID pairings for all configured filters. To change the port mask(s) for an existing filter, select the entry to change. To add a new filter, select **Create Filter** from the top of the list.

9. From the **VLAN ID** list, select the VLAN to use with the MAC address to fully identify packets you want filtered.

You can change this field only when the Create Filter option is selected from the MAC Filter menu.

10. In the **MAC Address** list, specify the MAC address of the filter in the format 00:01:1A:B2:53:4D.

You can change this field when you select the Create Filter option. You cannot define filters for the following MAC addresses:

- 00:00:00:00:00
- 01:80:C2:00:00:00 to 01:80:C2:00:00:0F
- 01:80:C2:00:00:20 to 01:80:C2:00:00:21
- FF:FF:FF:FF:FF:FF

11. Use **Source Port Members** to list the ports you want included in the inbound filter.

If a packet with the MAC address and VLAN ID you selected is received on a port that is not in the list, it is dropped.

- 12.** Use **Destination Port Members** to list the ports to be included in the outbound filter.

Packets with the MAC address and VLAN ID you selected is transmitted only out of ports that are in the list. Destination ports can be included only in the multicast filter.

- 13.** To delete a configured MAC filter, select it from the menu, and then click the **DELETE** button.

- 14.** Click the **APPLY** button.

Your settings are applied to the system.

## View the MAC Filter Summary

You can view the MAC filters that are configured on the system.

➤ **To view the MAC filter summary:**

- 1.** Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
- 2.** Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
- 3.** Launch a web browser.
- 4.** Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

- 5.** Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- 6.** Click the **Login** button.

The web management interface menu displays.

- 7.** Select **Security > Traffic Control > MAC Filter > MAC Filter Summary**.

<b>MAC Filter Summary</b>			
:: MAC Filter Summary			
MAC Address	VLAN ID	Source Port Members	Destination Port Members
D3:02:F1:93:B3:01	1	1/0/9	1/0/16 - 1/0/17

The following table describes the information displayed on the screen:

**Table 85. MAC Filter Summary User Manual**

Field	Description
MAC Address	The MAC address of the filter in the format 00:01:1A:B2:53:4D.
VLAN ID	The VLAN ID associated with the filter.

**Table 85. MAC Filter Summary User Manual (continued)**

Field	Description
Source Port Members	A list of ports to be used for filtering inbound packets.
Destination Port Members	A list of ports to be used for filtering outbound packets.

## Configure the Global Port Security Mode

Use the port security feature to lock one or more ports on the system. When a port is locked, only packets with an allowable source MAC addresses can be forwarded. All other packets are discarded.

➤ **To configure the global port security mode:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Traffic Control > Port Security > Port Administration**.

The screenshot shows the 'Port Security Configuration' page. The 'Port Security Settings' section contains a 'Port Security Mode' field with two radio buttons: 'Disable' (selected) and 'Enable'. The 'Port Security Violations' section has columns for 'Port', 'Last Violation MAC', and 'VLAN ID'.

8. In the **Port Security Mode** field, select the appropriate radio button to enable or disable port security on the switch.

The Port Security Violations table shows information about violations that occurred on ports that are enabled for port security. The following table describes the fields in the Port Security violations table.

**Table 86. Port Security Configuration**

Field	Description
Port	Displays the physical interface.
Last Violation MAC	Displays the source MAC address of the last packet that was discarded at a locked port.
VLAN ID	Displays the VLAN ID corresponding to the last violation MAC address.

## Configure Port Security Settings

A MAC address can be defined as allowable by one of two methods: dynamically or statically. Both methods are used concurrently when a port is locked.

Dynamic locking implements a first arrival mechanism for port security. You specify how many addresses can be learned on the locked port. If the limit has not been reached, then a packet with an unknown source MAC address is learned and forwarded normally. When the limit is reached, no more addresses are learned on the port. Any packets with source MAC addresses that were not already learned are discarded. You can effectively disable dynamic locking by setting the number of allowable dynamic entries to zero.

Static locking allows you to specify a list of MAC addresses that are allowed on a port. The behavior of packets is the same as for dynamic locking: only packets with an allowable source MAC address can be forwarded.

➤ **To configure port security settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7.** Select **Security > Traffic Control > Port Security > Interface Configuration**.

Port Security Interface Configuration					
:: Interface Configuration					
	1	2	LAGS	All	Go To Port
	Port	Security Mode	Max Allowed Dynamically Learned MAC	Max Allowed Statically Locked MAC	Violation Trap
<input type="checkbox"/>		<input type="button" value="▼"/>			<input type="button" value="▼"/>
<input type="checkbox"/>	1/0/1	Disable	600	48	Disable
<input type="checkbox"/>	1/0/2	Disable	600	48	Disable
<input type="checkbox"/>	1/0/3	Disable	600	48	Disable
<input type="checkbox"/>	1/0/4	Disable	600	48	Disable
<input type="checkbox"/>	1/0/5	Disable	600	48	Disable

**8.** **Port.** Selects the interface to be configured.

**9.** Select the check box next to the port or LAG to configure.

Select multiple check boxes to apply the same setting to all selected interfaces. Select the check box in the heading row to apply the same settings to all interfaces.

**10.** Specify the following settings:

- **Security Mode.** Enables or disables the port security feature for the selected interface.
- **Max Allowed Dynamically Learned MAC.** Sets the maximum number of dynamically learned MAC addresses on the selected interface.
- **Max Allowed Statically Locked MAC.** Sets the maximum number of statically locked MAC addresses on the selected interface.
- **Violation Traps.** Enables or disables the sending of new violation traps designating when a packet with a disallowed MAC address is received on a locked port.

## Convert a Dynamic MAC Address to a Static Address

You can convert a dynamically learned MAC address to a statically locked address.

➤ **To convert learned MAC addresses:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Traffic Control > Port Security > Dynamic MAC Address**.

8. To convert a dynamically learned MAC address to a statically locked address, select the **Convert Dynamic Address to Static** check box.

The dynamic MAC address entries are converted to static MAC address entries in a numerically ascending order until the static limit is reached.

9. In the **Port List** menu, select the physical interface.

The Dynamic MAC Address Table shows the MAC addresses and their associated VLANs learned on the selected port.

10. Click the **REFRESH** button to refresh the screen and to show the latest MAC address(es) learned on a specific port.

## Configure Static MAC Addresses

➤ **To configure static MAC addresses:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Traffic Control > Port Security > Static MAC Address**.

Static MAC Address Configuration	
:: Port List	
Interface	1/0/1
:: Static MAC Address Table	
Static MAC Address	VLAN ID
<input type="checkbox"/>	

8. In the **Interface** list, select the physical interface.
9. To add MAC addresses, enter them in the **Static MAC Address** field.
10. In the **VLAN ID** menu, select the VLAN ID corresponding to the MAC address being added.
11. To add a new static MAC address to the switch, click the **ADD** button.
12. To delete a existing static MAC address from the switch, click the **DELETE** button.
13. Click the **APPLY** button.

Your settings are saved.

## Configure a Private Group

➤ **To configure a private group:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Traffic Control > Private Group > Private Group Configuration**.

Private Group Configuration			
	Group Name	Group ID	Group Mode
<input type="checkbox"/>	pgroup1	1	community

8. In the **Group Name** field, enter the private group name.

The name can be up to 24 bytes of non-blank characters.

9. In the optional **Group ID** field, specify the private group identifier.

The range of group ID is 1 to 192.

10. In the **Group Mode** menu, select **isolated** or **community**.

When in isolated mode, the member port in the group cannot forward its egress traffic to any other members in the same group. By default, the mode is community mode. Each member port can forward traffic to other members in the same group, but not to members in other groups.

11. To create a new private group in the switch, click the **ADD** button.

12. To delete a selected private group from the switch, click the **DELETE** button.

## Configure Private Group Membership

➤ **To configure private group membership:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Traffic Control > Private Group > Private Group Membership**.

8. In the **Group ID** menu, select the group.
9. In the **Port List** menu, select the ports for this private group.

The port list displays when at least one group is configured.

**Table 87. Private Group Membership**

Field	Description
Group Name	This field identifies the name for the private group you selected. It can be up to 24 non-blank characters long.
Group Mode	<p>This field identifies the mode of the private group you selected. The modes are as follows:</p> <ul style="list-style-type: none"> <li>• community</li> <li>• isolated</li> </ul> <p>The group mode can be either isolated or community. When in isolated mode, the member port in the group cannot forward its egress traffic to any other members in the same group. By default, the mode is community mode. In community mode, each member port can forward traffic to other members in the same group, but not to members in other groups.</p>

## Configure Protected Ports

If a port is configured as protected, it does not forward traffic to any other protected port on the switch, but it forwards traffic to unprotected ports. You can configure the ports as protected or unprotected. You need read-write access privileges to modify the configuration.

➤ **To configure protected ports:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

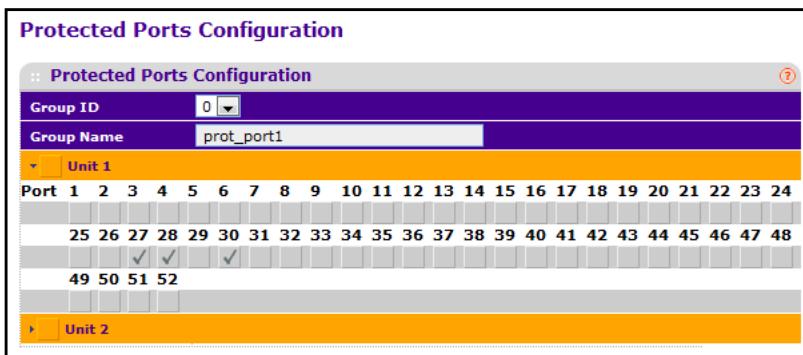
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Traffic Control > Protected Ports**.



8. In the **Group ID** list, select a group of protected ports that can be combined into a logical group.

Traffic can flow between protected ports belonging to different groups, but not within the same group. The selection box lists all the possible protected port group IDs supported for the current platform. The valid range of the group ID is 0 to 2.

9. Use the optional **Group Name** field to associate a name with the protected ports group (used for identification purposes).

It can be up to 32 alphanumeric characters long, including blanks. The default is blank. This field is optional.

10. Click the orange bar to display the available ports.

11. Select the check box below each port to configure it as a protected port.

The selection list consists of physical ports, protected as well as unprotected. The protected ports are tick-marked to differentiate between them. No traffic forwarding is possible between two protected ports. If left unconfigured, the default state is unprotected.

12. Click the **REFRESH** button to refresh the screen with the most current data from the switch.

13. Click the **APPLY** button.

The changes are applied to the system. Configuration changes take effect immediately.

## Private VLAN Overview

A private VLAN contains switch ports that cannot communicate with each other, but can access another network. These ports are called private ports. Each private VLAN contains one or more private ports and a single uplink port or uplink aggregation group. Note that all traffic between private ports is blocked at all layers, not just Layer 2 traffic, but also traffic such as FTP, HTTP, and Telnet.

## Configure a Private VLAN Type

➤ **To configure a private VLAN type:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.

3. Launch a web browser.

4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Traffic Control > Private VLAN > Private VLAN Type Configuration**.

Private VLAN Type Configuration		
:: Private VLAN Type Configuration		
	VLAN ID	Private VLAN Type
<input checked="" type="checkbox"/>	1	Unconfigured
<input type="checkbox"/>	2	Unconfigured

The VLAN ID field displays the VLAN for which private VLAN type is being set. The factory default is Unconfigured.

8. Use **Private VLAN Type** to specify the type of private VLAN. The factory default is Unconfigured.

9. Click the **APPLY** button.

The changes are applied to the system. Configuration changes take effect immediately.

## Configure the Private VLAN Association

➤ **To configure the private VLAN association:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Security > Traffic Control > Private VLAN> Private VLAN Association Configuration**.

Private VLAN Association Configuration				
:: Private VLAN Association				
	Primary VLAN	Secondary VLAN(s)	Isolated VLAN	Community VLAN(s)
<input type="checkbox"/>	<input type="button" value="▼"/>			

8. Use **Primary VLAN** to select the primary VLAN ID of the domain.  
This is used to associate secondary VLANs to the domain.
9. Use **Secondary VLAN(s)** to display all the statically created VLANs (excluding the primary and default VLANs).  
This field is used to associate VLANs to the selected primary VLAN.
10. To delete the IP subnet-based VLAN from the switch, click the **DELETE** button.
11. Click the **APPLY** button.

Your changes are applied to the system. Configuration changes take effect immediately.

The following table describes the nonconfigurable information displayed on the screen.

**Table 88. Private VLAN Association Configuration**

Field	Description
Isolated VLAN	Displays the isolated VLAN associated with the selected primary VLAN.
Community VLAN(s)	Displays the list of community VLAN(s) associated with the selected primary VLAN.

## Configure the Private VLAN Port Mode

➤ **To configure the private VLAN port mode:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Traffic Control > Private VLAN> Private VLAN Port Mode Configuration.**

Interface	Port Vlan Mode
0/1	General
0/2	General
0/3	General
0/4	General
0/5	General
0/6	General
0/7	General
0/8	General
0/9	General
0/10	General
0/11	General
0/12	General

8. Use the **Interface** check boxes to select the physical or LAG interface.  
 9. Use **Switch Port Mode** to select the switch port mode. The factory default is 'General'.
  - **General:** Sets port in General mode.
  - **Host:** Sets port in Host mode. Used for private VLAN configuration.
  - **Promiscuous:** Sets port in Promiscuous mode. Used for private VLAN configuration.
 10. Click the **APPLY** button.

The changes are applied to the system. Configuration changes take effect immediately.

## Configure Private VLAN Host Interface

➤ **To configure a private VLAN host interface:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Traffic Control > Private VLAN > Private VLAN Host Interface Configuration**.

Interface	Host Primary VLAN (2 to 4093)	Host Secondary VLAN (2 to 4093)	Operational VLAN(s)
0/1	0	0	
0/2	0	0	
0/3	0	0	
0/4	0	0	
0/5	0	0	
0/6	0	0	
0/7	0	0	
0/8	0	0	
0/9	0	0	
0/10	0	0	
0/11	0	0	
0/12	0	0	

The **Interface** field displays the selected physical or LAG interface.

The **Operational VLANs** fields display the operational VLANs.

8. Use **Host Primary VLAN** to set the primary VLAN ID for Host Association mode.  
The range of the VLAN ID is 2–4093.
9. Use **Host Secondary VLAN** to set the secondary VLAN ID for Host Association mode.  
The range of the VLAN ID is 2–4093.
10. To delete the IP subnet-based VLAN from the switch, click the **DELETE** button.
11. Click the **APPLY** button.

The changes are applied to the system. Configuration changes take effect immediately.

## Configure Private VLAN Promiscuous Interface Settings

➤ **To configure private VLAN promiscuous interface settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Traffic Control > Private VLAN > Private VLAN Promiscuous Interface Configuration**.

Private VLAN Promiscuous Interface Configuration			
:: Private VLAN Promiscuous Interface Configuration			
<b>1 LAGS All</b>	<b>Go To Interface</b> <input type="text"/> <b>GO</b>		<b>(?)</b>
Interface	Promiscuous Primary VLAN (2 to 4093)	Promiscuous Secondary VLAN(s) Range[2-4093]	Operational VLAN(s)
0/1	0		
0/2	0		
0/3	0		
0/4	0		
0/5	0		
0/6	0		
0/7	0		
0/8	0		
0/9	0		
0/10	0		
0/11	0		
0/12	0		

8. Select the physical or LAG interface.
9. Use **Promiscuous Primary VLAN** to set the primary VLAN ID for Promiscuous Association mode. The range of the VLAN ID is 2-4093.
10. Use **Promiscuous Secondary VLAN ID(s)** to set the secondary VLAN ID List for Promiscuous Association mode.

You can enter individual VLAN IDs, ranges of VLAN IDs, or a combination of both. To specify a individual VLAN ID, type a number, such as 10. To specify a VLAN ID range, type numbers separated by a hyphen, such as 10-13. To specify a combination, use commas to separate each entry, for example: 10,15,40-43,1000-1005,2000. The range of the VLAN ID is 2-4093.

**Note:** The VLAN ID List given in this field replaces the configured Secondary VLAN list in the association.

11. To delete the IP subnet-based VLAN from the switch, click the **DELETE** button.
12. Click the **APPLY** button.

The changes are applied to the system. Configuration changes take effect immediately.

## Storm Control Overview

A broadcast storm is the result of an excessive number of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses can overload network resources and/or cause the network to time out.

The switch measures the incoming broadcast/multicast/unknown unicast packet rate per port and discards packets when the rate exceeds the defined value. Storm control is enabled per interface, by defining the packet type and the rate at which the packets are transmitted.

## Configure Storm Control Global Settings

➤ **To configure storm control global settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

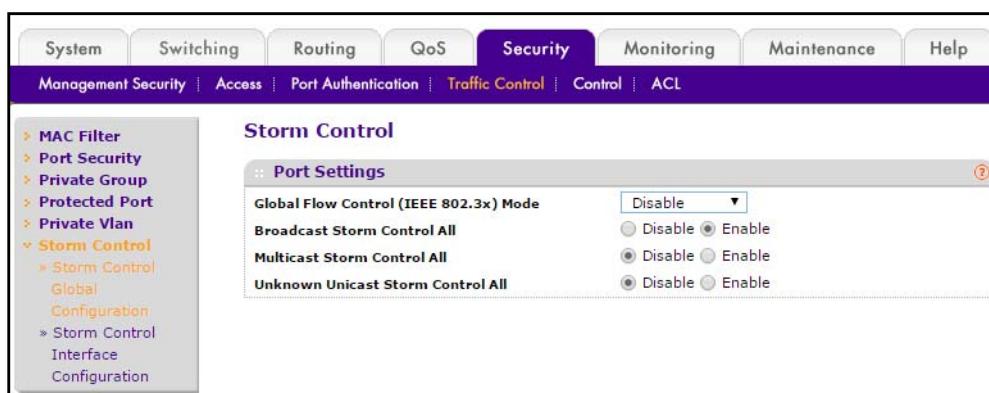
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Traffic Control > Storm Control > Storm Control Global Configuration**.



The following four controls provide an easy way to enable or disable each type of packets to be rate-limited on every port in a global fashion. The effective storm control state of each port can be viewed by going to the port configuration screen.

- **Global Flow Control (IEEE 802.3x) Mode.** Select **Disable** or **Enable**. The factory default is Disable.

- Select the Broadcast Storm Control All **Disable** or **Enable** radio button.

This enables or disables the Broadcast Storm Recovery mode on all ports. When you specify Enable for Broadcast Storm Recovery and the broadcast traffic on any Ethernet port exceeds the configured threshold, the switch blocks (discards) the broadcast traffic. The factory default is Enable.

- Select the Multicast Storm Control All **Disable** or **Enable** radio button.

This enables or disables the Multicast Storm Recovery mode on all ports. When you specify Enable for Multicast Storm Recovery and the multicast traffic on any Ethernet port exceeds the configured threshold, the switch blocks (discards) the multicast traffic. The factory default is Disable.

- Select the Unknown Unicast Storm Control All **Disable** or **Enable** radio button.

This enables or disables the Unicast Storm Recovery mode on all ports. When you specify Enable for Unicast Storm Recovery and the unicast traffic on any Ethernet port exceeds the configured threshold, the switch blocks (discards) the unicast traffic. The factory default is Disable.

## View Storm Control Settings for an Interface

➤ **To view storm control settings for an interface:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7. Select **Security >Traffic Control > Storm Control > Storm Control Interface Configuration.****

Port Configuration												
Port Configuration												
All												
Broadcast Storm			Multicast Storm			Unicast Storm						
Port	Flow Control	Recovery Mode	Recovery Level Type	Recovery Level	Control Action	Recovery Mode	Recovery Level Type	Recovery Level	Recovery Mode	Recovery Level Type	Recovery Level	Recovery Level
0/1	Disable	Enable	Percent	5	RateLimit	Disable	Percent	5	Disable	Percent	5	
0/2	Disable	Enable	Percent	5	RateLimit	Disable	Percent	5	Disable	Percent	5	
0/3	Disable	Enable	Percent	5	RateLimit	Disable	Percent	5	Disable	Percent	5	

The following table describes the nonconfigurable information displayed on the screen.

**Table 89. Storm control interface configuration**

Field	Description
Flow Control	Enable or disable IEEE 802.3x flow control by selecting the corresponding line on the menu. Flow control helps to prevent data loss when the port cannot keep up with the number of frames being switched. When enabled, the switch can send a PAUSE frame to stop traffic on a port if the amount of memory used by packets on the port exceeds a preconfigured threshold and responds to pause requests from partner devices. The paused port does not forward packets for the period of time specified in the PAUSE frame. When the PAUSE frame time elapses or the utilization returns to a specified low threshold, the switch enables the port to again transmit frames. The factory default is disabled. For LAG interfaces Flow Control mode is displayed blank, as flow control is not applicable.
Broadcast Storm Recovery Mode	Enable or disable this option by selecting the corresponding line on the entry field. When you specify Enable for broadcast storm recovery and the broadcast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the broadcast traffic. The factory default is enable.
Broadcast Storm Recovery Level Type	The broadcast storm recovery level as a percentage of link speed or as packets per second.
Broadcast Storm Recovery Level	The threshold at which storm control activates. The factory default is 5 percent of port speed for pps type.
Multicast Storm Recovery Mode	Enable or disable this option by selecting the corresponding line on the entry field. When you specify Enable for multicast storm recovery and the multicast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the multicast traffic. The factory default is disabled.
Multicast Storm Recovery Level Type	The multicast storm recovery level as a percentage of link speed or as packets per second.
Multicast Storm Recovery Level	The threshold at which storm control activates. The factory default is 5 percent of port speed for pps type.
Unicast Storm Recovery Mode	Enable or disable this option by selecting the corresponding line on the entry field. When you specify Enable for unicast storm recovery and the unicast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the unicast traffic. The factory default is disabled.

**Table 89. Storm control interface configuration**

Field	Description
Unicast Storm Recovery Level Type	Specify the unicast storm recovery level as a percentage of link speed or as packets per second.
Unicast Storm Recovery Level	Specify the threshold at which storm control activates. The factory default is 5 percent of port speed for pps type.

## Control DHCP Snooping Settings

You can configure the DHCP snooping settings.

### Configure Global DHCP Snooping Settings

➤ **To configure global DHCP snooping settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Control > DHCP Snooping > Global Configuration**.

VLAN ID	DHCP Snooping Mode
1	Disable

8. Use **DHCP Snooping Mode** to enable or disable the DHCP snooping feature.

The factory default is disabled.

9. Use **MAC Address Validation** to enable or disable the validation of sender MAC address for DHCP snooping.

The factory default is enabled.

10. For DHCP snooping VLAN configuration, use **VLAN ID** to enter the VLAN for which the DHCP snooping mode is to be enabled.

11. Use **DHCP Snooping Mode** to enable or disable the DHCP snooping feature for the entered VLAN.

The factory default is disabled.

12. Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See *Save Configuration* on page 405.

## Configure the DHCP Snooping Interface

➤ **To configure the DHCP snooping interface:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Control > DHCP Snooping > Interface Configuration**.

DHCP Snooping Interface Configuration					
:: DHCP Snooping Interface Configuration					
1	2	LAGS	All	Go To Interface	GO
		Interface	Trust Mode	Logging Invalid Packets	Rate Limit(pps)
					Burst Interval(secs)
		1/0/1	Disable	Disable	N/A
		1/0/2	Disable	Disable	N/A
		1/0/3	Disable	Disable	N/A
		1/0/4	Disable	Disable	N/A
		1/0/5	Disable	Disable	N/A

8. Select the interface for which data is to be configured.

9. In the **Trust Mode** menu, select **Enable** or **Disable**.

If trust mode is enabled, the DHCP snooping application considers the port as trusted. The factory default is disabled.

10. In the **Logging Invalid Packets** menu select **Enable** or **Disable**.

If this feature is enabled, DHCP snooping application logs invalid packets on this interface. The factory default is disabled.

11. In the **Rate Limit (pps)** field, specify rate limit value for DHCP snooping purpose.

If the incoming rate of DHCP packets exceeds this value for consecutive burst interval seconds, the port is shut down. If this value is N/A then burst interval has no meaning, hence it is disabled. The default value is N/A. It can be set to -1, which means N/A. The range of Rate Limit is 0 to 300.

12. In the **Burst Interval (secs)** field, specify the burst interval value for rate limiting purpose on this interface.

If the rate limit is N/A, the burst interval has no meaning and it is N/A. The default value is N/A. It can be set to value -1, which means N/A. The range of Burst Interval is 1 to 15).

## Configure DHCP Snooping Static Binding

### ➤ To configure DHCP snooping static binding:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Control > DHCP Snooping > Binding Configuration**.

:: Static Binding Configuration				
	Interface	MAC Address	VLAN ID	IP Address
<input checked="" type="checkbox"/>	<input type="button" value="▼"/>	<input type="text"/>	<input type="button" value="▼"/>	<input type="text"/>

:: Dynamic Binding Configuration				
Interface	MAC Address	VLAN ID	IP Address	Lease Time
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

8. Select the interface to add a binding into the DHCP snooping database.
9. Use **MAC Address** to specify the MAC address for the binding entry to be added.  
This is the key to the binding database.
10. Use **VLAN ID** to select the VLAN from the list for the binding rule.  
The range of the VLAN ID is 1 to 4093.
11. Use **IP Address** to specify valid IP address for the binding rule.
12. To add DHCP snooping binding entry into the database, click the **ADD** button.
13. To delete selected static entries from the database, click the **DELETE** button.

## Configure DHCP Snooping Dynamic Binding

➤ **To configure DHCP snooping dynamic binding:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.

The web management interface menu displays.

**7. Select **Security > Control > DHCP Snooping > Binding Configuration.****

:: Static Binding Configuration				
	Interface	MAC Address	VLAN ID	IP Address
<input type="checkbox"/>	<input type="button" value="▼"/>	<input type="text"/>	<input type="button" value="▼"/>	<input type="text"/>

:: Dynamic Binding Configuration				
Interface	MAC Address	VLAN ID	IP Address	Lease Time
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

**8.** The **Interface** field displays the interface to which a binding entry is associated in the DHCP snooping database.

**9.** Use **MAC Address** to display the MAC address for the binding in the binding database.

**10.** Use **VLAN ID** to display the VLAN for the binding entry in the binding database.

The range of the VLAN ID is 1 to 4093.

**11.** Specify the **IP Address**.

This is the IP address for the binding entry in the binding database.

**12.** **Lease Time.** Displays the remaining lease time for the dynamic entries.

**13.** Click **CLEAR** to delete all DHCP snooping binding entries.

## Configure Persistent DHCP Snooping

➤ **To configure persistent DHCP snooping:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

- Select **Security > Control > DHCP Snooping > Persistent Configuration.**

**DHCP Snooping Persistent Configuration**

Store  Local  Remote

Remote IP Address: 0.0.0.0

Remote File Name: (1 to 32 alphanumeric characters)

Write Delay: 300 (15 to 86400) seconds

- Use **Store** to select the local store or remote store.

Selecting Local disables the remote fields like Remote File Name and Remote IP address.

- Use **Remote IP Address** to configure the remote IP address on which the snooping database is stored when Remote is selected.
- Use **Remote File Name** to configure the remote file name to store the database when remote is selected.
- Use **Write Delay** to configure the maximum write time to write the database into local or remote.

The range of Write Delay is 15 to 86400.

## View DHCP Snooping Statistics

➤ **To view DHCP snooping statistics:**

- Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
- Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
- Launch a web browser.
- Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

- Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

7. click **Security > Control > DHCP Snooping > Statistics.**

DHCP Snooping Statistics			
:: DHCP Snooping Statistics			
1	2	LAGS	All
Interface	MAC Verify Failures	Client Ifc Mismatch	DHCP Server Msgs Received
1/0/1	0	0	0
1/0/2	0	0	0
1/0/3	0	0	0
1/0/4	0	0	0
1/0/5	0	0	0
1/0/6	0	0	0
1/0/7	0	0	0
1/0/8	0	0	0

Click **CLEAR** to clear all interfaces statistics.

Click the **REFRESH** button to refresh the data on the screen with the latest statistics.

The following table describes the nonconfigurable information displayed on the screen.

**Table 90. DHCP Snooping Statistics**

Field	Description
Interface	The untrusted and snooping enabled interface for which statistics are to be displayed.
MAC Verify Failures	Number of packets that were dropped by DHCP snooping as there is no matching DHCP snooping binding entry found.
Client Ifc Mismatch	The number of DHCP messages that are dropped based on source MAC address and client HW address verification.
DHCP Server Msgs Received	The number of server messages that are dropped on an untrusted port.

## Configure an IP Source Guard Interface

➤ **To configure an IP source guard interface:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Control > IP Source Guard > Interface Configuration**.

IP Source Guard Interface Configuration			
IP Source Guard Interface Configuration			
1	2	LAGS	All
Interface	IPSG Mode	IPSG Port Security	
1/0/1	Disable	Disable	
1/0/2	Disable	Disable	
1/0/3	Disable	Disable	
1/0/4	Disable	Disable	
1/0/5	Disable	Disable	
1/0/6	Disable	Disable	

8. Select an **Interface** to enable IPSG.

9. In the **IPSG Mode** menu, select **Enable** or **Disable**.

This enables or disables validation of the sender IP address on this interface. If IPSG is enabled, packets are not forwarded if the sender IP address is not in the DHCP snooping binding database. The factory default is Disable.

10. Use **IPSG Port Security** to enable or disables the IPSG port security on the selected interface.

If IPSG port security is enabled then the packets are not forwarded if the sender MAC address is not in the FDB table and it is not in DHCP snooping binding database. To enforce filtering based on MAC address, other required configurations are as follows:

- Enable port-security globally.
- Enable port-security on the interface level.

IPSG port security can't be enabled if IPSG is Disabled. The factory default is disabled.

## Configure IP Source Guard Binding

- **To configure IP source guard binding:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.

4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Security > Control > IP Source Guard > Binding Configuration**. To con

IP Source Guard Binding Configuration				
:: Static Binding Configuration				
<b>Interface</b>	<b>MAC Address</b>	<b>VLAN ID</b>	<b>IP Address</b>	<b>Filter Type</b>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
:: Dynamic Binding Configuration				
<b>Interface</b>	<b>MAC Address</b>	<b>VLAN ID</b>	<b>IP Address</b>	<b>Filter Type</b>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

8. To configure static binding, specify the following:
  - a. **Interface**. Selects the interface to add a binding into the IPSG database.
  - b. Use **MAC Address** to specify the MAC address for the binding.
  - c. Use **VLAN ID** to select the VLAN from the list for the binding rule.
  - d. Use **IP Address** to specify valid IP address for the binding rule.
  - e. To add IPSG static binding entry into the database, click the **ADD** button.
  - f. To delete selected static entries from the database, click the **DELETE** button.
9. Click the **CLEAR** button to clear all the dynamic binding entries

The following table describes the nonconfigurable information displayed on the screen.

**Table 91. Dynamic Binding Configuration**

Field	Description
Interface	Displays the interface to add a binding into the IPSG database.
MAC Address	Displays the MAC address for the binding entry.
VLAN ID	Displays the VLAN from the list for the binding entry.
IP Address	Displays valid IP address for the binding entry.
Filter Type	Filter type used on the interface. One is source IP address filter type, the other is source IP address and MAC address filter type.

## Configure Dynamic ARP Inspection

➤ **To configure dynamic ARP inspection:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

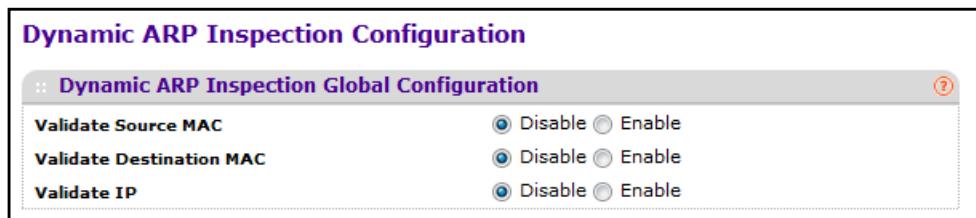
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Control > Dynamic ARP Inspection > DAI Configuration**.



8. Select the Validate Source MAC **Disable** or **Enable** radio button.

This specifies the DAI Source MAC Validation Mode. If you select Enable, Sender MAC validation for the ARP packets is enabled. The factory default is Disable.

9. Select the Validate Destination MAC **Disable** or **Enable** radio button.

This specifies the DAI Destination MAC Validation mode for the switch. If you select Enable, Destination MAC validation for the ARP response packets is enabled. The factory default is Disable.

10. Select the Validate IP **Disable** or **Enable** radio button.

This specifies the DAI IP Validation mode for the switch by selecting Enable or Disable radio button. If you select Enable, IP address validation for the ARP packets is enabled. The factory default is Disable.

## Configure Dynamic ARC Inspection

➤ **To configure dynamic ARC inspection:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration**.

Dynamic ARP Inspection Configuration					
:: VLAN Configuration					
	VLAN ID	Dynamic ARP Inspection	Logging Invalid Packets	ARP ACL Name	Static Flag
<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
<input type="checkbox"/>	1	Disable	Enable		Disable
<input type="checkbox"/>	2	Disable	Enable		Disable
<input type="checkbox"/>	100	Disable	Enable		Disable

8. Use the **VLAN ID** check boxes to select the DAI-capable VLANs.
9. Use **Dynamic ARP Inspection** to indicate whether the dynamic ARP inspection is enabled on this VLAN.  
If set to Enable, dynamic ARP inspection is enabled.
10. Use **Logging Invalid Packets** to indicate whether the dynamic ARP inspection logging is enabled on this VLAN.  
If set to Enable, invalid ARP packets information is logged.
11. Use **ARP ACL Name** to specify a name for the ARP access list.  
A VLAN can be configured to use this ARP ACL containing rules as the filter for ARP packet validation. The name can contain up to 31 alphanumeric characters.

- 12.** Use **Static Flag** to determine whether the ARP packet needs validation using the DHCP snooping database in case ARP ACL rules don't match.

If the flag is enabled, then the ARP packet is validated by the ARP ACL rules only. If the flag is disabled, then the ARP packet needs further validation using the DHCP snooping entries. The factory default is Disable.

## Configure a Dynamic ARC Inspection Interface

- To configure a dynamic ARC inspection interface:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > Control> Dynamic ARP Inspection > DAI Interface Configuration**.

Dynamic ARP Inspection Interface Configuration				
:: DAI Interface Configuration				
1	2	LAGS	All	Go To Interface <input type="text"/>
<input type="checkbox"/>		<input type="checkbox"/>		<input type="button" value="GO"/>
<input type="checkbox"/>	1/0/1	Disable	15	1
<input type="checkbox"/>	1/0/2	Disable	15	1
<input type="checkbox"/>	1/0/3	Disable	15	1
<input type="checkbox"/>	1/0/4	Disable	15	1
<input type="checkbox"/>	1/0/5	Disable	15	1
<input type="checkbox"/>	1/0/6	Disable	15	1

8. Use **Interface** to selects the physical interface.
9. Use **Trust Mode** to indicate whether the interface is trusted for dynamic ARP Inspection purposes.

When set to Disable, ARP packets coming to this interface are subjected to ARP inspection. If enabled, ARP packets coming to this interface are forwarded without

checking. The factory default is Disable.

**10. Use Rate Limit (pps)** to specify rate limit value for dynamic ARP Inspection purpose.

If the rate of incoming ARP packets exceeds this value for consecutive burst interval seconds, ARP packets are dropped. If this value is N/A there is no limit. The value can set to –1, which means N/A. The range of Rate Limit is 0–300. The factory default is 15 pps (packets per second).

**11. Use Burst Interval (secs)** to specify the burst interval value for rate limiting purpose on this interface.

If the rate limit is None, burst interval has no meaning, and displays as N/A. The factory default is 1 second.

## Configure a DAI ACL

➤ **To configure a dynamic ARP inspection ACL:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

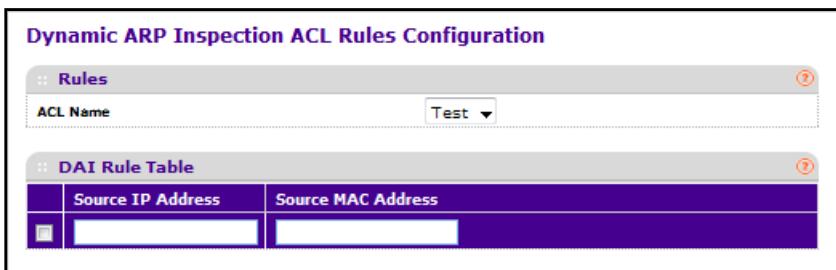
7. Select **Security > Control > Dynamic ARP Inspection > DAI ACL Configuration**.

:: DAI ACL Configuration	
<input type="checkbox"/>	Name
<input type="checkbox"/>	dai1

8. Use **Name** to create new ARP ACL for DAI.
9. To add a new DAI ACL, click the **ADD** button.
10. To remove the currently selected DAI ACL from the switch configuration, click the **DELETE** button.

## Configure a Dynamic ARP Inspection ACL Rule

- To configure a dynamic ARP Inspection ACL rule:
  1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
  2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
  3. Launch a web browser.
  4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
  5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
  6. Click the **Login** button.  
The web management interface menu displays.
  7. Select **Security > Control > Dynamic ARP Inspection > DAI ACL Rule Configuration**.



The **Source IP Address** field and the source MAC address field indicate the sender IP address match value and the sender MAC address match value for the DAI ARP ACL.

8. Use **ACL Name** to select the DAI ARP ACL.
9. To add a new rule to the selected ACL, click the **ADD** button.
10. To remove the currently selected rule from the selected ACL, click the **DELETE** button.

## View DAI Statistics

- To view DAI statistics:
  1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
  2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
  3. Launch a web browser.

- Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

- Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **Security > Control > Dynamic ARP Inspection > DAI Statistics**.

VLAN	DHCP Drops	DHCP Permits	ACL Drops	ACL Permits	Bad Source MAC	Bad Dest MAC	Invalid IP	Forwarded	Dropped
1	0	0	0	0	0	0	0	0	0

Click the **REFRESH** button to refresh the data on the screen with the latest DAI statistics.

To clear the DAI statistics, click the **CLEAR** button.

The following table describes the nonconfigurable information displayed on the screen.

**Table 92. Dynamic ARP inspection statistics**

Field	Description
VLAN	The enabled VLAN ID for which statistics are to be displayed.
DHCP Drops	Number of ARP packets that were dropped by DAI because there is no matching DHCP snooping binding entry found.
DHCP Permits	Number of ARP packets that were forwarded by DAI because there is a matching DHCP snooping binding entry found.
ACL Drops	Number of ARP packets that were dropped by DAI because there is no matching ARP ACL rule found for this VLAN and the static flag is set on this VLAN.
ACL Permits	Number of ARP packets that were permitted by DAI because there is a matching ARP ACL rule found for this VLAN.

**Table 92. Dynamic ARP inspection statistics**

Field	Description
Bad Source MAC	Number of ARP packets that were dropped by DAI because the sender MAC address in ARP packet didn't match the source MAC in Ethernet header.
Bad Dest MAC	Number of ARP packets that were dropped by DAI because the target MAC address in ARP reply packet didn't match the destination MAC in Ethernet header.
Invalid IP	Number of ARP packets that were dropped by DAI because the sender IP address in the ARP packet or target IP address in ARP reply packet is invalid. Invalid addresses include 0.0.0.0, 255.255.255.255, IP multicast addresses, class E addresses (240.0.0.0/4), loopback addresses (127.0.0.0/8).
Forwarded	Number of valid ARP packets forwarded by DAI.
Dropped	Number of invalid ARP packets dropped by DAI.

## Access Control List Overview

Access control lists (ACLs) ensure that only authorized users can access specific resources while blocking off any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and above all provide security for the network. The managed switch software supports IPv4, IPv6, and MAC ACLs.

You first create an IPv4-based or IPv6-based or MAC based ACL ID. Then, you create a rule and assign it to a unique ACL ID. Next, you define the rules, which can identify protocols, source, and destination IP and MAC addresses, and other packet-matching criteria. Finally, use the ID number to assign the ACL to a port or to a LAG.

### Use the ACL Wizard

The ACL Wizard helps you to create a simple ACL and apply it to the selected ports easily and quickly. First you must select an ACL type to create an ACL. Then add ACL rule to this ACL, and apply this ACL on the selected ports. The ACL Wizard allows you to create the ACL but doesn't allow you to modify it. If you want to modify it, go to the ACL configuration screen.

➤ **To use the ACL Wizard:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > ACL > ACL Wizard**.

8. Use **ACL Type** to specify the ACL type you are using to create the ACL.

You can select one type from 10 optional types:

- **ACL Based on Destination MAC.** To create an ACL based on the destination MAC address, destination MAC mask, and VLAN.
- **ACL Based on Source MAC.** To create an ACL based on the source MAC address, source MAC mask, and VLAN.
- **ACL Based on Destination IPv4.** To create an ACL based on the destination IPv4 address and IPv4 address mask.
- **ACL Based on Source IPv4.** To create an ACL based on the source IPv4 address and IPv4 address mask.
- **ACL Based on Destination IPv6.** To create an ACL based on the destination IPv6 prefix and IPv6 prefix length.
- **ACL Based on Source IPv6.** To create an ACL based on the source IPv6 prefix and IPv6 prefix length.
- **ACL Based on Destination IPv4 L4 Port.** To create an ACL based on the destination IPv4 Layer4 port number.
- **ACL Based on Source IPv4 L4 Port.** To create an ACL based on the source IPv4 Layer 4 port number.

- **ACL Based on Destination IPv6 L4 Port.** To create an ACL based on the destination IPv6 Layer 4 port number.
  - **ACL Based on Source IPv6 L4 Port.** To create an ACL based on the source IPv6 Layer 4 port number.
- 9.** Use **Rule ID** to enter a whole number in the range of 1 to 511.  
 This number is used to identify the rule.
- 10.** Use **Action** to specify what action should be taken if a packet matches the rule's criteria.  
 The choices are permit or deny.
- 11.** Select **True** or **False** from the **Match Every** menu.  
**True** indicates that all packets match the selected ACL and rule and is either permitted or denied. In this case, since all packets match the rule, the option of configuring other match criteria is not offered. To configure specific match criteria for the rule, remove the rule and re-create it, or reconfigure **Match Every** to **False** for the other match criteria to be visible.
- 12.** Use **Destination MAC** to specify the destination MAC address to compare against an Ethernet frame.  
 The valid format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC address of 01:80:C2:xx:xx:xx.
- 13.** Use **Destination MAC Mask** to specify the destination MAC address mask specifying which bits in the destination MAC to compare against an Ethernet frame.  
 The valid format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC mask of 00:00:00:ff:ff:ff.
- 14.** To add a new rule to the ACL, click the **ADD** button.
- 15.** To remove the currently selected rule from the ACL, click the **DELETE** button.
- 16.** Click the **APPLY** button.  
 Updated configuration is sent to the switch. Configuration changes take effect immediately.

## Create a MAC ACL

A MAC ACL consists of a set of rules that are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit/Deny) is taken and the additional rules are not checked for a match.

There are multiple steps involved in defining a MAC ACL and applying it to the switch:

1. Create the ACL name (see the following procedure in this topic).
2. Create rules for the ACL (see [Configure MAC Rules](#) ).
3. Assign the ACL by its name to a port (see [Configure ACL MAC Binding](#) ).
4. Optionally, view the configurations (see [View or Delete MAC Bindings](#) ).

➤ **To create a MAC ACL:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > ACL > Basic > MAC ACL**.

Name	Rules	Direction
macACL	0	

The MAC ACL screen displays the number of ACLs currently configured in the switch and the maximum number of ACLs that can be configured. The current size is equal to the number of configured IPv4 and IPv6 ACLs plus the number of configured MAC ACLs.

8. To add a MAC ACL, specify a name for the MAC ACL in the **Name** field, and click the **ADD** button.

The name string can include alphabetic, numeric, hyphen, underscore, or space characters only. The name must start with an alphabetic character.

Each configured ACL displays the following information:

- **Rules.** Displays the number of rules currently configured for the MAC ACL.
- **Direction.** Displays the direction of packet traffic affected by the MAC ACL, which can be Inbound or blank.

9. To delete a MAC ACL, select the check box next to the Name field, then click the **DELETE** button.

10. To change the name of a MAC ACL, select the check box next to the Name field, update the name, then click the **APPLY** button.
11. To add a new MAC ACL to the switch configuration, click the **ADD** button.

## Configure MAC Rules

You can define rules for MAC-based ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. A default 'deny all' rule is the last rule of every list.

➤ **To configure MAC rules:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Security > ACL > Basic > MAC Rules.**

Rule Table	ID	Action	Assign Queue Id	Mirror Interface	Redirect Interface	Match Every	Cnt	Destination MAC Mask	Destination MAC Key	EtherType Key	EtherType User Value	Source MAC	Source MAC Mask	VLAN	Logging	Rate Limit Conform Disc Rate	Rate Limit Burst Size	Time Range	Rule Status

8. Use **ID** to enter a whole number in the range of 1 to 511.  
This number is used to identify the rule.
9. In the **Action** menu, select **permit** or **deny** to specify what action is taken if a packet matches the rule's criteria.
10. Use **Assign Queue ID** to specify the hardware egress queue identifier used to handle all packets matching this ACL rule.  
The valid range of queue IDs is 0 to 7.
11. **Mirror Interface** to specify the specific egress interface where the matching traffic stream is copied in addition to being forwarded normally by the device.

This field cannot be set if a redirect interface is already configured for the ACL rule. This field is visible for a Permit action.

- 12.** Use **Redirect Interface** to specify the specific egress interface where the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device.

This field cannot be set if a mirror interface is already configured for the ACL rule.

- 13.** Use **Match Every** to specify an indication to match every Layer 2 MAC packet.

The valid values are as follows:

- **True.** Every packet must match the selected ACL rule.
- **False.** It is not mandatory for every packet to match the selected ACL rule.

- 14.** Use **CoS** to specify the 802.1p user priority to compare against an Ethernet frame.

The valid range of values is 0 to 7.

- 15.** Use **Destination MAC** to specify the destination MAC address to compare against an Ethernet frame.

The valid format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a Destination MAC address of 01:80:C2:xx:xx:xx.

- 16.** Use **Destination MAC Mask** to specify the destination MAC address mask specifying which bits in the destination MAC to compare against an Ethernet frame.

The valid format is xx:xx:xx:xx:xx:xx. The BPDU keyword can be specified using a destination MAC mask of 00:00:00:ff:ff:ff.

- 17.** Use **EtherType Key** to specify the EtherType value to compare against an Ethernet frame.

The valid values are the following:

- Appletalk
- ARP
- IBM SNA
- IPv4
- IPv6
- IPX
- MPLS multicast
- MPLS unicast
- NetBIOS
- Novell
- PPPoE
- Reverse ARP
- User Value

- 18.** Use **EtherType User Value** to specify the user-defined customized EtherType value to be used when the user has selected *User Value* as the EtherType key, to compare against an Ethernet frame.

The valid range of values is 0x0600 to 0xFFFF.

19. Use **Source MAC** to specify the source MAC address to compare against an Ethernet frame. The valid format is xx:xx:xx:xx:xx:xx.
20. Use **Source MAC Mask** to specify the source MAC address mask specifying which bits in the source MAC to compare against an Ethernet frame.

The valid format is xx:xx:xx:xx:xx:xx.

21. Use **VLAN** to specify the VLAN ID to compare against an Ethernet frame. The valid range of values is 1 to 4095. Either VLAN Range or VLAN can be configured.
22. **Logging.** When set to 'Enable', logging is enabled for this ACL rule (subject to resource availability in the device).

If the Access List Trap flag is also enabled, this causes periodic traps to be generated indicating the number of times this rule was 'hit' during the current report interval. A fixed 5 minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval. This field is supported only for a Deny action.

23. **Rate Limit Conform Data Rate.** Value of Rate Limit Conform Data Rate specifies the conforming data rate of MAC ACL rule.

The valid values are 1 to 4294967295 in Kbps.

24. **Rate Limit Burst Size.** Value of Rate Limit Burst Size specifies burst size of MAC ACL rule.

The valid values are 1 to 128 in Kbytes.

25. **Time Range.** Name of time range associated with the MAC ACL rule.

26. Use **Rule Status.** Displays if the ACL rule is active or inactive.

Blank means that no timer schedules are assigned to the rule.

27. To delete a rule, select the check box associated with the rule and click the **DELETE** button.

28. To change a rule, select the check box associated with the rule change the desired fields.

29. Click the **APPLY** button.

Configuration changes take effect immediately.

## Configure ACL MAC Binding

When an ACL is bound to an interface, all the rules that were defined are applied to the selected interface. You can assign MAC ACL lists to ACL priorities and interfaces.

➤ **To configure ACL MAC binding:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > ACL > Basic > MAC Binding Configuration**.

Interface	Direction	ACL Type	ACL ID	Sequence Number
1/0/5	Inbound	MAC ACL	macACL	1
1/0/9	Inbound	MAC ACL	macACL	1

8. Select an existing MAC ACL from the ACL ID menu.

You can select one and bind it to the interfaces you want. The packet filtering direction for ACL is Inbound, which means the MAC ACL rules are applied to traffic entering the port.

9. Specify an optional sequence number to indicate the order of this access list relative to other access lists already assigned to this interface and direction.

A low number indicates high precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If you do not specify the sequence number, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. The valid range is 1–4294967295.

10. Click the appropriate orange bar to expose the available ports or LAGs.

The Port Selection Table provides a list of all available valid interfaces for ACL binding. All nonrouting physical interfaces, VLAN interface, and interfaces participating in LAGs are listed.

- To add the selected ACL to a port or LAG, click the box directly below the port or LAG number so that an X appears in the box.
- To remove the selected ACL from a port or LAG, click the box directly below the port or LAG number to clear the selection. An X in the box indicates that the ACL is applied to the interface.

- 11.** Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See [Save Configuration](#) on page 405.

The following table describes the information displayed in the **Interface Binding Status**.

**Table 93. Interface Binding Status**

324 Field	Description
Interface	The interface of the ACL assigned.
Direction	The selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.
ACL ID	The ACL number (in the case of IP ACL) or ACL name (in the case of MAC ACL) identifying the ACL assigned to the selected interface and direction.
Sequence Number	The sequence number signifying the order of the specified ACL relative to other ACLs assigned to the selected interface and direction.

## View or Delete MAC Bindings

➤ **To view or delete MAC bindings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7. Select Security > ACL > Basic > Binding Table.**

<b>MAC Binding Table</b>					
:: MAC Binding Table					
	Interface	Direction	ACL Type	ACL ID	Sequence Number
<input type="checkbox"/>	1/0/5	In Bound	MAC ACL	macACL	1
<input type="checkbox"/>	1/0/9	In Bound	MAC ACL	macACL	1

To delete a MAC ACL-to-interface binding, select the check box next to the interface and click the **DELETE** button.

The following table describes the information displayed in the **MAC Binding Table**.

**Table 94. MAC Binding Table**

324 Field	Description
Interface	The interface of the ACL assigned.
Direction	The selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.
ACL ID	The ACL name identifying the ACL assigned to the selected interface and direction.
Sequence Number	The sequence number signifying the order of the specified ACL relative to the other ACLs assigned to the selected interface and direction.

## Configure an IP ACL

An IP ACL consists of a set of rules that are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit/Deny) is taken and the additional rules are not checked for a match.

➤ **To configure an IP ACL:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **Security > ACL > Advanced > IP ACL**.

IP ACL ID	Rules	Type
10	0	Basic IP ACL

The screen displays the current size of the ACL table and the maximum size of the ACL table. The current size is equal to the number of configured IPv4 and IPv6 ACLs plus the number of configured MAC ACLs. The maximum size is 100.

The **Current Number of ACL** displays the current number of all ACLs configured on the switch.

The **Maximum ACL** displays the maximum number of IP ACLs that can be configured on the switch, depending on the hardware.

- In the **IP ACL** field, specify the ACL ID or IP ACL name.

The ID is an integer in the following range:

- 1–99: Creates an IP basic ACL, which allows you to permit or deny traffic from a source IP address.
- 100–199: Creates an IP extended ACL, which allows you to permit or deny specific types of Layer 3 or Layer 4 traffic from a source IP address to a destination IP address. This type of ACL provides more granularity and filtering capabilities than the standard IP ACL.
- IP ACL Name: Create a named IP ACL, instead of configuring the IP extended ACL. IP ACL Name string must use alphanumeric characters only and must start with an alphabetic character.

Each configured ACL displays the following information:

- Rules.** Displays the number of rules currently configured for the IP ACL.
- Type.** Identifies the ACL as a basic IP ACL, extended IP ACL, or named IP ACL.

- To delete an IP ACL, select the check box next to the IP ACL ID field, then click the **DELETE** button.

- To add a new IP ACL, click the **ADD** button.

## Configure Rules for an IP ACL

You can configure the rules for the IP access control lists (ACLs) that you created.

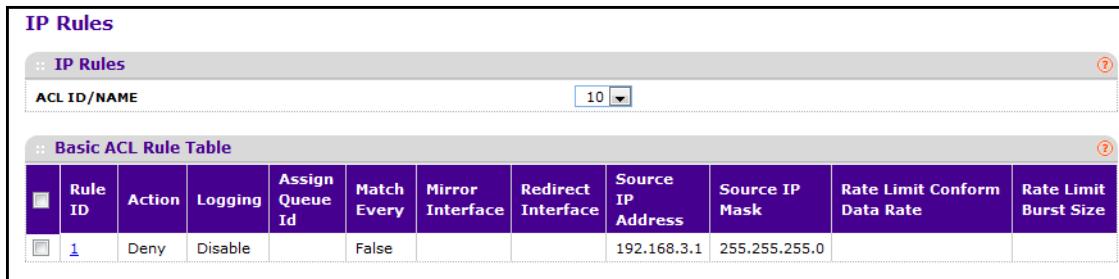
---

**Note:** There is an implicit deny all rule at the end of an ACL list. This means that if an ACL is applied to a packet and if none of the explicit rules match, then the final implicit “deny all” rule applies and the packet is dropped.

---

➤ **To configure rules for an IP ACL:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Security > ACL > Advanced > IP Rules.**



The screenshot shows the 'IP Rules' configuration page. At the top, there's a header bar with tabs for 'IP Rules' and 'Basic ACL Rule Table'. Below the header is a search bar labeled 'ACL ID/NAME' with a dropdown set to '10'. The main area is titled 'Basic ACL Rule Table' and contains a table with one row. The table columns are: Rule ID (containing '1'), Action (containing 'Deny'), Logging (containing 'Disable'), Assign Queue Id (empty), Match Every (containing 'False'), Mirror Interface (empty), Redirect Interface (empty), Source IP Address (containing '192.168.3.1'), Source IP Mask (containing '255.255.255.0'), Rate Limit Conform Data Rate (empty), and Rate Limit Burst Size (empty). There are also 'Help' and 'Edit' icons in the top right corner of the table.

What is shown on this screen varies depending on the current step in the rule configuration process

8. To add an IP ACL rule, select the ACL ID to add the rule to, complete the fields described in the following list, and click the **ADD** button. (Displays only for ACL IDs from 1 to 99.)
  - **Rule ID.** Enter a whole number in the range of 1 to 511.  
This number is used to identify the rule. An IP ACL can add up to 511 rules.
  - **Action.** Specify the action to be taken if a packet matches the rule's criteria. The choices are permit or deny.

- **Logging.** When set to Enable, logging is enabled for this ACL rule (subject to resource availability in the device). If the Access List Trap flag is also enabled, this causes periodic traps to be generated indicating the number of times this rule was 'hit' during the current report interval. A fixed 5-minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval. This field is visible for a Deny action.
  - **Assign Queue ID.** Specifies the hardware egress queue identifier used to handle all packets matching this IP ACL rule. The valid range of queue IDs is 0 to 7. This field is visible when Permit is chosen as Action.
  - **Match Every.** Select **True** or **False**. True signifies that all packets match the selected IP ACL and rule and is either permitted or denied. In this case, since all packets match the rule, the option of configuring other match criteria is not offered. To configure specific match criteria for the rule, remove the rule and recreate it, or reconfigure Match Every to False for the other match criteria to be visible.
  - **Redirect Interface.** Specifies the specific egress interface where the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device. This field cannot be set if a mirror interface is already configured for the ACL rule. This field is enabled for a Permit action.
  - **Source IP Address.** Enter an IP address using dotted-decimal notation to be compared to a packet's source IP address as a match criteria for the selected IP ACL rule.
  - **Source IP Mask.** Specify the IP Mask in dotted-decimal notation to be used with the Source IP address value.
  - **Rate Limit Conform Data Rate.** The value of Rate Limit Conform Data Rate specifies the conforming data rate of IP ACL rule. The valid values are 1 to 4294967295 in Kbps.
  - **Rate Limit Burst Size.** The value of Rate Limit Burst Size specifies the burst size of the IP ACL rule. The valid values are 1 to 128 in Kbytes.
  - **Time Range.** Name of the time range associated with the IP ACL rule.
  - **Rule Status.** Displays if the ACL rule is active or inactive. Blank means that no timer schedules are assigned to the rule.
- 9.** To delete an IP ACL rule, select the check box associated with the rule, and then click the **DELETE** button.
- 10.** To update an IP ACL rule, select the check box associated with the rule, update the desired fields.
- You cannot modify the rule ID of an existing IP rule.
- 11.** Click the **APPLY** button.
- The updated configuration is sent to the switch. Configuration changes take effect immediately.

**Note:** To modify an existing IP extended ACL rule, click the **Rule ID**. The number is a hyperlink to the Extended ACL Rule Configuration screen.

## Configure IP Extended Rules

You can configure the rules for the IP access control lists that you created. There is an implicit deny all rule at the end of an ACL list. This means that if an ACL is applied to a packet and if none of the explicit rules match, then the final implicit deny all rule applies and the packet is dropped.

➤ **To configure IP extended rules:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > ACL > Advanced > IP Extended Rules**.

Rule ID	Action	Logging	Assign Queue ID	Mirror Interface	Redirect Interface	Match Every	Protocol Type	TCP Flag	Source IP Address	Source IP Mask	Source L4 Port	Destination IP Address	Destination IP Mask	Destination L4 Port	Service Type	Rate Limit Conform Data Rate	Rate Limit Burst Size	Time Range	Rule Status
1	Permit	Disable	0/1			False	4 (IP)									1	1		

What is shown on this screen varies depending on the current step in the rule configuration process.

8. Use **ACL ID/Name** to select the IP ACL.
9. Configure the new rule:
  - **Rule ID.** Enter a whole number in the range of 1 to 51.

This number identifies the rule. An IP ACL can use up to 511 rules.

- **Action.** Specify the action to take if a packet matches the rule's criteria. The choices are permit or deny.
- **Logging.** When set to Enable, logging is enabled for this ACL rule (subject to resource availability in the device). If the Access List Trap flag is also enabled, this causes periodic traps to be generated indicating the number of times this rule was hit during the current report interval. A fixed 5-minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval. This field is visible for a Deny action.
- **Assign Queue ID.** Specifies the hardware egress queue identifier used to handle all packets matching this IP ACL rule. The valid range of queue IDs is 0 to 7.
- **Mirror Interface.** Specifies the specific egress interface where the matching traffic stream is copied in addition to being forwarded normally by the device. This field cannot be set if a redirect interface is already configured for the ACL rule. This field is visible for a Permit action.
- **Redirect Interface.** Specifies the specific egress interface where the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device. This field cannot be set if a mirror Interface is already configured for the ACL rule. This field is enabled for a Permit action.
- **Match Every.** Select **True** or **False**. True signifies that all packets match the selected IP ACL and rule and is either permitted or denied. In this case, since all packets match the rule, the option of configuring other match criteria is not offered. To configure specific match criteria for the rule, remove the rule and recreate it, or reconfigure Match Every to False for the other match criteria to be visible.
- **Protocol Type.** Specify that a packet's IP protocol is a match condition for the selected IP ACL rule. The possible values are ICMP, IGMP, IP, TCP, and UDP.
- **TCP Flag.** Specify that a packet's TCP flag is a match condition for the selected IP ACL rule. The TCP flag values are URG, ACK, PSH, RST, SYN, FIN. Each TCP flag has these possible values w and can be set separately:
  - **Ignore.** A packet matches this ACL rule whether or not the TCP flag in this packet is set.
  - **Set (+).** A packet matches this ACL rule if the TCP flag in this packet is set.
  - **Clear (-).** A packet matches this ACL rule if the TCP flag in this packet is not set.
- **Source IP Address.** Enter an IP address using dotted-decimal notation to be compared to a packet's source IP address as a match criteria for the selected IP ACL rule.
- **Source IP Mask.** Specify the IP Mask in dotted-decimal notation to be used with the Source IP address value.
- **Source L4 Port.** Specify a packet's source Layer 4 port as a match condition for the selected extended IP ACL rule. This is an optional configuration. The possible values are DOMAIN, ECHO, FTP, FTPDATA, WWW-HTTP, SMTP, SNMP, TELNET, and TFTP. Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

- **Destination IP Address.** Enter an IP address using dotted-decimal notation to be compared to a packet's destination IP address as a match criteria for the selected extended IP ACL rule.
  - **Destination IP Mask.** Specify the IP mask in dotted-decimal notation to be used with the destination IP address value.
  - **Destination L4 Port.** Specify the destination Layer 4 port match conditions for the selected extended IP ACL rule. The possible values are DOMAIN, ECHO, FTP, FTPDATA, WWW-HTTP, SMTP, SNMP, TELNET and TFTP. Each of these values translates into its equivalent port number, which is used as both the start and end of the port range. This is an optional configuration.
  - **Service Type.** Select a service type match condition for the extended IP ACL rule. The possible values are IP DSCP, IP precedence, and IP TOS, which are alternative ways of specifying a match criterion for the same Service Type field in the IP header; however, each uses a different user notation. After you make a selection, you can specify the appropriate:
    - **IP DSCP.** Specify the **IP DiffServ Code Point (DSCP)** field. The DSCP is the high-order six bits of the service type octet in the IP header. This is an optional configuration. To specify the IP DSCP, select a keyword, or select **Other** and enter an integer from 0 to 63. (When you select **Other**, a field displays where you can enter the numeric value of the DSCP.)
    - **IP Precedence.** The IP Precedence field in a packet is defined as the high-order three bits of the service type octet in the IP header. This is an optional configuration. Enter an integer from 0 to 7.
    - **IP TOS.** The IP TOS field in a packet is defined as all eight bits of the service type octet in the IP header. The TOS Bits value is a hexadecimal number from 00 to FF. The TOS Mask value is a hexadecimal number from 00 to FF. The TOS mask denotes the bit positions in the TOS Bits value that are used for comparison against the IP TOS field in a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a TOS Bits value of 0xA0 and a TOS Mask of 0xFF. This is an optional configuration.
  - **Rate Limit Conform Data Rate.** The value of Rate Limit Conform Data Rate specifies the conforming data rate of IP ACL rule. The valid values are 1 to 4294967295 in Kbps.
  - **Rate Limit Burst Size.** Value of Rate Limit Burst Size specifies the burst size of the IP ACL rule. The valid values are 1 to 128 in Kbytes.
  - **Time Range.** Name of time range associated with the IP Extended ACL rule.
  - **Rule Status.** Displays if the ACL rule is active or inactive. Blank means that no timer schedules are assigned to the rule.
- 10.** To delete an IP ACL rule, select the check box associated with the rule, and then click the **DELETE** button.
- 11.** To modify an existing IP extended ACL rule, click the **Rule ID**. The number is a hyperlink to the Extended ACL Rule Configuration screen.

## Configure an IPv6 ACL

An IPv6 ACL consists of a set of rules that are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit/Deny) is taken and the additional rules are not checked for a match. You can specify or create rules for the IP ACL.

➤ **To configure an Pv6 ACL:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > ACL > Advanced > IPv6 ACL**.

The screenshot shows the 'IPv6 ACL' configuration page. The top section, 'IPv6 Configuration', displays the 'Current Number of ACL' as 4 and the 'Maximum ACL' as 100. The bottom section, 'IPv6 ACL Table', lists two entries:

	IPv6 ACL	Rules	Type
<input type="checkbox"/>			IPv6 ACL
<input type="checkbox"/>	ipv6ACL	1	IPv6 ACL

8. **IPv6 ACL** is the IPv6 ACL ID or IPv6 ACL name, which is dependent on the IPv6 ACL type. The IPv6 ACL Name string includes alphanumeric characters only.  
The name must start with an alphabetic character.
9. To add a new IPv6 ACL, click the **ADD** button.
10. To remove the currently selected IPv6 ACL from the switch configuration, click the **DELETE** button.

The following table describes the nonconfigurable information displayed on the screen.

**Table 95. IPv6 ACL Configuration**

Field	Description
Current Number of ACL	The current number of IP ACLs configured on the switch.
Maximum ACL	The maximum number of IP ACLs that can be configured on the switch, depending on the hardware.
Rules	The number of rules associated with the IP ACL.
Type	The type is IPv6 ACL.

## Configure IPv6 Rules

You can configure the rules for the IPv6 access control lists (ACLs) that you created. By default, no specific value is in effect for any of the IPv6 ACL rules.

➤ **To configure IPv6 rules:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > ACL > Advanced > IPv6 Rules**.

8. Use **Rule ID** to enter a whole number in the range of 1 to 511 to identify the rule.

An IP ACL can use up to 511 rules.

9. Use **Action** to specify the action to take if a packet matches the rule's criteria.

The choices are permit or deny.

10. Use **Logging** to enable logging for this ACL rule (subject to resource availability in the device).

If the Access List Trap flag is also enabled, this causes periodic traps to be generated indicating the number of times this rule was 'hit' during the current report interval. A fixed 5 minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval. This field is visible for a Deny action.

11. Use **Assign Queue ID** to specify the hardware egress queue identifier used to handle all packets matching this IPv6 ACL rule.

The valid range of queue IDs is 0 to 7. This field is visible for a Permit action.

12. Use **Mirror Interface** to specify the specific egress interface where the matching traffic stream is copied in addition to being forwarded normally by the device.

This field cannot be set if a redirect interface is already configured for the ACL rule. This field is visible for a Permit action.

13. Use **Redirect Interface** to specify the specific egress interface where the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device.

This field cannot be set if a mirror interface is already configured for the ACL rule. This field is visible for a Permit action.

14. Use **Match Every** to select **True** or **False**.

**True** signifies that all packets match the selected IPv6 ACL and rule and is either permitted or denied. In this case, since all packets match the rule, the option of configuring other match criteria is not offered. To configure specific match criteria for the rule, remove the rule and re-create it, or reconfigure 'Match Every' to 'False' for the other match criteria to be visible.

15. **Protocol.** There are two ways to configure IPv6 protocol:

- a. Specify an integer ranging from 1 to 255 after selecting protocol keyword *other*. This number represents the IP protocol.
- b. Select the name of a protocol from the existing list of Internet Protocol (IPv6), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMPv6).

16. Use **Source Prefix / Prefix Length** to specify IPv6 prefix combined with IPv6 prefix length of the network or host from which the packet is being sent.

Prefix length can be in the range 0 to 128.

17. Use **Source L4 Port** to specify a packet's source Layer 4 port as a match condition for the selected IPv6 ACL rule.

Source port information is optional. Source port information can be specified in two ways:

- Select the keyword **other** from the menu and specify the number of the port in the range from 0 to 65535.

- Select one of the keywords from the list: DOMAIN, ECHO, FTP, FTPDATA, WWW-HTTP, SMTP, SNMP, TELNET, and TFTP. Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.
- 18.** Use **Destination Prefix / Prefix Length** to enter prefix combined with prefix length to be compared to a packet's destination IP address as a match criteria for the selected IPv6 ACL rule.
- The prefix length can be in the range 0 to 128.
- 19.** Use **Destination L4 Port** to specify a packet's destination Layer 4 port as a match condition for the selected IPv6 ACL rule.
- Destination port information is optional. Destination port information can be specified in two ways:
- Select the keyword **other** and specify the number of the port in the range from 0 to 65535.
  - Select one of the keywords from the list: DOMAIN, ECHO, FTP, FTPDATA, WWW-HTTP, SMTP, SNMP, TELNET, and TFTP. Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.
- 20.** **Flow Label.** Flow label is 20-bit number that is unique to an IPv6 packet, used by end stations to signify quality-of-service handling in routers.
- Flow label can be specified within the range 0 to 1048575.
- 21.** Use **IPv6 DSCP Service** to specify the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order six bits of the service type octet in the IPv6 header.
- This is an optional configuration. Enter an integer from 0 to 63. The IPv6 DSCP is selected by possibly selecting one of the DSCP keyword from a field. If a value is to be selected by specifying its numeric value, then select the 'Other' option in the field and a text box displays where you can enter the numeric value of the DSCP.
- 22.** **Rate Limit Conform Data Rate.** Value of Rate Limit Conform Data Rate specifies the conforming data rate of IPv6 ACL rule.
- The valid values are 1 to 4294967295 in Kbps.
- 23.** **Rate Limit Burst Size.** Value of Rate Limit Burst Size specifies the burst size of the IPv6 ACL rule.
- The valid values are 1 to 128 in Kbytes.
- 24.** **Time Range.** Name of time range associated with the IPv6 ACL rule.
- 25.** **Rule Status.** Displays if the ACL rule is active or inactive.
- Blank means that no timer schedules are assigned to the rule.
- 26.** To add an IPv6 rule, click the **ADD** button.
- 27.** To delete a rule, select it and click the **DELETE** button.

## Configure ACL Interface Bindings

When an ACL is bound to an interface, all the rules that were defined are applied to the selected interface. You can assign ACL lists to ACL priorities and interfaces.

➤ **To configure ACL interface bindings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.

3. Launch a web browser.

4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > ACL > Advanced > IP Binding Configuration**.

**IP Binding Configuration**

:: Binding Configuration			
ACL ID	10	Direction	Inbound
Sequence Number	0	(1 to 4294967295)	
Port Selection Table			
<input checked="" type="checkbox"/> Unit 1 <input checked="" type="checkbox"/> Unit 2 <input checked="" type="checkbox"/> LAG			

:: Interface Binding Status				
Interface	Direction	ACL Type	ACL ID/Name	Sequence Number
1/0/8	Inbound	IP ACL	101	1

8. Select an existing IP ACL from the ACL ID menu.

The packet filtering direction for ACL is Inbound, which means that the IP ACL rules are applied to traffic entering the port.

9. Specify an optional sequence number to indicate the order of this access list relative to other access lists already assigned to this interface and direction.

A low number indicates high precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the

user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. The valid range is 1–4294967295.

10. Click the appropriate orange bar to expose the available ports or LAGs. The Port Selection Table specifies list of all available valid interfaces for ACL mapping. All non-routing physical interfaces and interfaces participating in LAGs are listed.
  - To add the selected ACL to a port or LAG, click the box directly below the port or LAG number so that an X appears in the box.
  - To remove the selected ACL from a port or LAG, click the box directly below the port or LAG number to clear the selection. An X in the box indicates that the ACL is applied to the interface.
11. Click the **APPLY** button.

Your settings are saved.

The following table describes the nonconfigurable information displayed on the screen.

**Table 96. IP Binding Configuration**

Field	Description
Interface	The selected interface.
Direction	The selected packet filtering direction for ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.
ACL ID/Name	The ACL number (in the case of an IP ACL) or ACL name (in the case of named IP ACL and IPv6 ACL) identifying the ACL assigned to the selected interface and direction.
Sequence Number	The sequence number signifying the order of specified ACL relative to other ACLs assigned to the selected interface and direction.

## View or Delete IP ACL Bindings

➤ **To view or delete the IP ACL bindings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **Security > ACL > Advanced > Binding Table**.

IP ACL Binding Table					
:: IP ACL Binding Table					
	Interface	Direction	ACL Type	ACL ID/Name	Sequence Number
<input checked="" type="checkbox"/>	1/0/8	In Bound	IP ACL	101	1

- To delete an IP ACL-to-interface binding, select the check box next to the interface and click the **DELETE** button.

The following table describes the information displayed in the **IP ACL Binding Table**.

**Table 97. IP ACL Binding Table**

Field	Description
Interface	The selected interface.
Direction	The selected packet filtering direction for the ACL.
ACL Type	The type of ACL assigned to the selected interface and direction.
ACL ID/Name	The ACL number (in the case of an IP ACL) or ACL name (in the case of a named IP ACL and IPv6 ACL) identifying the ACL assigned to the selected interface and direction.
Sequence Number	The sequence number signifying the order of specified ACL relative to other ACLs assigned to the selected interface and direction.

## View or Delete VLAN ACL Bindings

You can view or delete the VLAN ACL bindings.

➤ **To view or delete VLAN ACL bindings in the VLAN Binding Table:**

- Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
- Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
- Launch a web browser.
- Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
- The Login screen displays.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **Security > ACL > Advanced > VLAN Binding Table**.

<b>ACL Vlan Binding Table</b>					
:: VLAN Binding Configuration					
	VLAN ID	Direction	Sequence Number	ACL Type	ACL ID
<input type="checkbox"/>			0	<input type="button" value="▼"/>	<input type="button" value="▼"/>

- To delete a VLAN ACL-to-interface binding, select the check box next to the interface and click the **DELETE** button.

- Use **ACL Type** to specify the type of ACL.

The valid ACL types include IP ACL, MAC ACL, and IPv6 ACL.

- Use **ACL ID** to display all the ACLs configured, depending on the ACL type selected.

The following table describes the information displayed in the **ACL VLAN Binding Table**.

**Table 98. ACL VLAN Binding Table**

Field	Description
Direction	The packet filtering direction for the ACL.
VLAN ID	The VLAN ID for ACL mapping.
Sequence Number	An optional sequence number can be specified to indicate the order of this access list relative to other access lists already assigned to this VLAN and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this VLAN and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user (for example the value is 0), a sequence number that is one greater than the highest sequence number currently in use for this VLAN and direction is used. The valid range is 1 to 4294967295.

# Monitoring the System

7

This chapter covers the following topics:

- *View Port Statistics*
- *View EAP Statistics*
- *Logs Overview*
- *Port Mirroring Overview*
- *sFlow Overview*

## View Port Statistics

You can view a summary of per-port traffic statistics on the switch.

➤ **To view port statistics:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Monitoring > Ports > Port Statistics**.

The screenshot shows a table titled "Port Statistics" with a header row labeled "Status". Below the header, there are two tabs: "LAGS All" (selected) and "All". The table has 13 rows, each representing a port or LAG. The columns are: Interface, Total Packets received without Errors, Packets received with Errors, Broadcast Packets received, Packets transmitted without Errors, Transmit Packet Errors, Collision Frames, and Time since counters last cleared. The data for the first few ports is as follows:

Interface	Total Packets received without Errors	Packets received with Errors	Broadcast Packets received	Packets transmitted without Errors	Transmit Packet Errors	Collision Frames	Time since counters last cleared
0/1	789757	0	299442	1677536	0	0	31 day 9 hr 51 min 9 sec
0/2	0	0	0	0	0	0	31 day 9 hr 51 min 9 sec
0/3	109676	0	36	420083	0	0	31 day 9 hr 51 min 9 sec
0/4	0	0	0	0	0	0	31 day 9 hr 51 min 9 sec
0/5	0	0	0	0	0	0	31 day 9 hr 51 min 9 sec
0/6	0	0	0	0	0	0	31 day 9 hr 51 min 9 sec
0/7	0	0	0	0	0	0	31 day 9 hr 51 min 9 sec
0/8	0	0	0	0	0	0	31 day 9 hr 51 min 9 sec
0/9	0	0	0	0	0	0	31 day 9 hr 51 min 9 sec
0/10	0	0	0	0	0	0	31 day 9 hr 51 min 9 sec
0/11	0	0	0	0	0	0	31 day 9 hr 51 min 9 sec
0/12	0	0	0	0	0	0	31 day 9 hr 51 min 9 sec

8. Use the buttons at the bottom of the screen to perform the following actions:

- To clear all the counters for all ports on the switch, select the check box in the row heading and click the **CLEAR** button.
- To clear the counters for a specific port, select the check box associated with the port and click **CLEAR**.

- To refresh the screen and display the current statistics, click the **REFRESH** button.

The following table describes the port statistics fields.

**Table 99. Port statistics**

Field	Description
Interface	The interface of the interface table entry associated with this port on an adapter.
Total Packets Received Without Errors	The total number of packets received that were without errors.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Transmitted Without Errors	The number of frames that were transmitted by this port to its segment.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Collision Frames	The best estimate of the total number of collisions on this Ethernet segment.
Time Since Counters Last Cleared	The elapsed time in days, hours, minutes, and seconds since the statistics for this port were last cleared.

## View Detailed Port Statistics

➤ **To view detailed port statistics:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7. Select Monitoring > Ports> Port Detailed Statistics.**

The screenshot shows the 'Port Detailed Statistics' interface. At the top, there are dropdown menus for 'Interface' (set to 0/1) and 'CST' (set to CST). Below these are various configuration parameters:

Interface	0/1
MST ID	CST
ifIndex	1
Port Type	Normal
Port Channel ID	Disable
Port Role	
STP Mode	Enable
STP State	
Admin Mode	Enable
Flow Control Mode	Disable
LACP Mode	Enable
Physical Mode	Auto
Physical Status	1000 Mbps
Link Status	Link Up
Link Trap	Enable
Packets RX and TX 64 Octets	1612226
Packets RX and TX 65-127 Octets	440500
Packets RX and TX 128-255 Octets	93632
Packets RX and TX 256-511 Octets	180132
Packets RX and TX 512-1023 Octets	89944
Packets RX and TX 1024-1518 Octets	51297
Packets RX and TX 1519-2047 Octets	0
Packets RX and TX 2048-4095 Octets	0
Packets RX and TX 4096-9216 Octets	0

You can use the buttons at the bottom of the screen to perform the following actions:

- To clear all counters, click the **CLEAR** button.  
This resets all statistics for this port to the default values.
- To refresh the data on the screen and display the most current statistics, click the **REFRESH** button.

The following table describes the detailed port information displayed on the screen. To view information about a different port, select the port number from the **Interface** menu.

**Table 100. Port Detailed Statistics screen fields**

Field	Description
MST ID	Display the MST instances associated with the interface.
ifIndex	The ifIndex of the interface table entry associated with this port on an adapter.
Port Type	For normal ports this field is normal. Otherwise, the possible values are as follows: <ul style="list-style-type: none"> <li>Mirrored. This port is a participating in port mirroring as a mirrored port. Look at the Port Mirroring screens for more information.</li> <li>Probe. This port is a participating in port mirroring as the probe port. Look at the Port Mirroring screens for more information.</li> <li>Trunk Member. The port is a member of a link aggregation trunk. Look at the Port Channel screens for more information.</li> </ul>

**Table 100. Port Detailed Statistics screen fields (continued)**

Field	Description
Port Channel ID	If the port is a member of a port channel, the port channel's interface ID and name are shown. Otherwise Disable is shown.
Port Role	Each MST bridge port that is enabled is assigned a port role for each spanning tree. The port role is one of the following values: Root, Designated, Alternate, Backup, Master, or Disabled.
STP Mode	The Spanning Tree Protocol administrative mode associated with the port or port channel. The possible values are as follows: <ul style="list-style-type: none"> <li>• Enable. Spanning tree is enabled for this port.</li> <li>• Disable. Spanning tree is disabled for this port.</li> </ul>
STP State	The port's current Spanning Tree state. This state controls what action a port takes on receipt of a frame. If the bridge detects a malfunctioning port, it places that port into the broken state. The five states are defined in IEEE 802.1D: <ul style="list-style-type: none"> <li>• Disabled</li> <li>• Blocking</li> <li>• Listening</li> <li>• Learning</li> <li>• Forwarding</li> <li>• Broken</li> </ul>
Admin Mode	The port control administration state. The port must be enabled in order for it to be allowed into the network. The factory default is enabled.
Flow Control Mode	Indicates whether flow control is enabled or disabled for the port. This field is not valid for LAG interfaces.
LACP Mode	Indicates the Link Aggregation Control Protocol administration state. The mode must be enabled in order for the port to participate in link aggregation.
Physical Mode	Indicates the port speed and duplex mode. In autonegotiation mode the duplex mode and speed are set from the autonegotiation process.
Physical Status	Indicates the port speed and duplex mode.
Link Status	Indicates whether the link is up or down.
Link Trap	Indicates whether or not the port sends a trap when link status changes.
Packets RX and TX 64 Octets	The total number of packets (including bad packets) received or transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
Packets RX and TX 65-127 Octets	The total number of packets (including bad packets) received or transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 128-255 Octets	The total number of packets (including bad packets) received or transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

**Table 100. Port Detailed Statistics screen fields (continued)**

<b>Field</b>	<b>Description</b>
Packets RX and TX 256-511 Octets	The total number of packets (including bad packets) received or transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 512-1023 Octets	The total number of packets (including bad packets) received or transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1024-1518 Octets	The total number of packets (including bad packets) received or transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1519-2047 Octets	The total number of packets (including bad packets) received or transmitted that were between 1519 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 2048-4095 Octets	The total number of packets (including bad packets) received or transmitted that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 4096-9216 Octets	The total number of packets (including bad packets) received or transmitted that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).
Octets Received	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This svalue can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets Received 64 Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
Packets Received 65-127 Octets	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 128-255 Octets	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 256-511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 512-1023 Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 1024-1518 Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

**Table 100. Port Detailed Statistics screen fields (continued)**

Field	Description
Packets Received > 1518 Octets	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Total Packets Received Without Errors	The total number of packets received that were without errors.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Total Packets Received with MAC Errors	The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Jabbers Received	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad frame check sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). Note that this definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
Fragments Received	The total number of packets received that were less than 64 octets in length with ERROR CRC (excluding framing bits but including FCS octets).
Undersize Received	The total number of packets received that were less than 64 octets in length with GOOD CRC (excluding framing bits but including FCS octets).
Alignment Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad frame check sequence (FCS) with a nonintegral number of octets.
Rx FCS Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets
Overruns	The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.
Total Received Packets Not Forwarded	A count of valid frames received which were discarded (for example filtered) by the forwarding process.
802.3x Pause Frames Received	A count of MAC control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
Unacceptable Frame Type	The number of frames discarded from this port due to being an unacceptable frame type.

**Table 100. Port Detailed Statistics screen fields (continued)**

<b>Field</b>	<b>Description</b>
Total Packets Transmitted (Octets)	The total number of octets of data (including those in bad packets) transmitted on the network (excluding framing bits but including FCS octets). This value can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets Transmitted 64 Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
Packets Transmitted 65-127 Octets	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 128-255 Octets	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 256-511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 512-1023 Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 1024-1518 Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted > 1518 Octets	The total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. This counter has a max increment rate of 815 counts per sec at 10 Mb/s.
Maximum Frame Size	The maximum Ethernet frame size the interface supports or is configured to be, including Ethernet header, CRC, and payload of 1518 to 9216. The default maximum frame size is 1518.
Total Packets Transmitted Successfully	The number of frames that were transmitted by this port to its segment.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the broadcast address, including those that were discarded or not sent.
Total Transmit Errors	The sum of single, multiple, and excessive collisions.

**Table 100. Port Detailed Statistics screen fields (continued)**

<b>Field</b>	<b>Description</b>
Total Transmit Packets Discarded	The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.
Single Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Excessive Collision Frames	A count of frames for which transmission on a particular interface fails due to excessive collisions.
STP BPDUs Received	Number of STP BPDUs received at the selected port.
STP BPDUs Transmitted	Number of STP BPDUs transmitted from the selected port.
RSTP BPDUs Received	Number of RSTP BPDUs received at the selected port.
RSTP BPDUs Transmitted	Number of RSTP BPDUs transmitted from the selected port.
MSTP BPDUs Received	Number of MSTP BPDUs received at the selected port.
MSTP BPDUs Transmitted	Number of MSTP BPDUs transmitted from the selected port.
802.3x Pause Frames Transmitted	A count of MAC control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
GVRP PDUs Received	The count of GVRP PDUs received in the GARP layer.
GVRP PDUs Transmitted	The count of GVRP PDUs transmitted from the GARP layer.
GVRP Failed Registrations	The number of times attempted GVRP registrations could not be completed.
GMRP PDUs Received	The count of GMRP PDUs received from the GARP layer.
GMRP PDUs Transmitted	The count of GMRP PDUs transmitted from the GARP layer.
GMRP Failed Registrations	The number of times attempted GMRP registrations could not be completed.
EAPOL Frames Received	The number of valid EAPOL frames of any type that were received by this authenticator.
EAPOL Frames Transmitted	The number of EAPOL frames of any type that were transmitted by this authenticator.
Time Since Counters Last Cleared	The elapsed time in days, hours, minutes, and seconds since the statistics for this port were last cleared.

## View EAP Statistics

You can view information about EAP packets received on a specific port.

➤ **To view EAP statistics:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Monitoring > Ports > EAP Statistics**.

EAP Statistics														
:: EAP Statistics														
1 2 All														
	Ports	PAE Capabilities	EAPOL										EAP	
			Frames Received	Frames Transmitted	Start Frames Received	Logoff Frames Received	Last Frame Version	Last Frame Source	Invalid Frames Received	Length Error Frames Received	Response/ID Frames Received	Response Frames Received	Request/ID Frames Transmitted	Request Frames Transmitted
<input type="checkbox"/>	1/0/1	Authenticator	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	0
<input type="checkbox"/>	1/0/2	Authenticator	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	0
<input type="checkbox"/>	1/0/3	Authenticator	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	0
<input type="checkbox"/>	1/0/4	Authenticator	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	0
<input type="checkbox"/>	1/0/5	Authenticator	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	0
<input type="checkbox"/>	1/0/6	Authenticator	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	0
<input type="checkbox"/>	1/0/7	Authenticator	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	0
<input type="checkbox"/>	1/0/8	Authenticator	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	0

8. Use the buttons at the bottom of the screen to perform the following actions:

- To clear all the EAP counters for all ports on the switch, select the check box in the row heading and click the **CLEAR** button.
- To clear the counters for a specific port, select the check box associated with the port and click the **CLEAR** button.
- To refresh the data on the screen and display the most current statistics, click the **REFRESH** button.

The following table describes EAP statistics.

**Table 101. EAP statistics**

Field	Description
Port	Selects the port to be displayed. When the selection is changed, a screen refresh occurs causing all fields to be updated for the newly selected port. All physical interfaces are valid.
PAE Capabilities	This displays the PAE capabilities of the selected port.
EAPOL Frames Received	This displays the number of valid EAPOL frames of any type that were received by this authenticator.
EAPOL Frames Transmitted	This displays the number of EAPOL frames of any type that were transmitted by this authenticator.
EAPOL Start Frames Received	This displays the number of EAPOL start frames that were received by this authenticator.
EAPOL Logoff Frames Received	This displays the number of EAPOL logoff frames that were received by this authenticator.
EAPOL Last Frame Version	This displays the protocol version number carried in the most recently received EAPOL frame.
EAPOL Last Frame Source	This displays the source MAC address carried in the most recently received EAPOL frame.
EAPOL Invalid Frames Transmitted	This displays the number of EAPOL frames that were received by this authenticator in which the frame type is not recognized.
EAPOL Length Error Frames Received	This displays the number of EAPOL frames that were received by this authenticator in which the frame type is not recognized.
EAP Response/ID Frames Received	This displays the number of EAP response/identity frames that were received by this authenticator.
EAP Response Frames Received	This displays the number of valid EAP response frames (other than resp/ID frames) that were received by this authenticator.
EAP Request/ID Frames Transmitted	This displays the number of EAP request/identity frames that were transmitted by this authenticator.
EAP Request Frames Transmitted	This displays the number of EAP request frames (other than request/identity frames) that were transmitted by this authenticator.

## Perform a Cable Test

➤ **To perform a cable test:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.

4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Monitoring > Ports > Cable Test**.

Cable Test				
Cable Test				
1	2	All	Go To Port	GO
<input type="checkbox"/>	Port	Cable Status	Cable Length	Failure Location
<input type="checkbox"/>	1/0/1	Normal	1m - 1m	
<input type="checkbox"/>	1/0/2	Cable status test failed		
<input type="checkbox"/>	1/0/3	No Cable		
<input type="checkbox"/>	1/0/4	No Cable		
<input type="checkbox"/>	1/0/5	No Cable		
<input type="checkbox"/>	1/0/6	No Cable		
<input type="checkbox"/>	1/0/7	No Cable		
<input type="checkbox"/>	1/0/8	No Cable		
<input type="checkbox"/>	1/0/9	No Cable		
<input type="checkbox"/>	1/0/10	No Cable		
<input type="checkbox"/>	1/0/11	No Cable		
<input type="checkbox"/>	1/0/12	Cable status test failed		
<input type="checkbox"/>	1/0/13	No Cable		

8. Select the check box for the port to which the cable to be tested is connected.
  9. Click the **APPLY** button.
- A cable test is performed on the selected port. The cable test might take up to two seconds to complete. If the port has an active link, the cable status is always Normal. The command returns a cable length estimate if this feature is supported by the PHY for the current link speed. If the link is down and a cable is attached to a 10/100 Ethernet adapter, then the cable status can be Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded.

The following table describes the nonconfigurable information displayed on the Cable Test screen.

**Table 102. Cable test**

Field	Description
Cable Status	This displays the cable status: <ul style="list-style-type: none"> <li>• <b>Normal.</b> The cable is working correctly.</li> <li>• <b>Open.</b> The cable is disconnected or there is a faulty connector.</li> <li>• <b>Short.</b> There is an electrical short in the cable.</li> <li>• <b>Cable Test Failed.</b> The cable status could not be determined. The cable might in fact be working.</li> </ul>
Cable Length	The estimated length of the cable in meters. The length is displayed as a range between the shortest estimated length and the longest estimated length. Unknown is displayed if the cable length could not be determined. The cable length is displayed only if the cable status is Normal.
Failure Location	The estimated distance in meters from the end of the cable to the failure location. The failure location is only displayed if the cable status is Open or Short.

## Logs Overview

The switch generates messages in response to events, faults, or errors occurring on the platform as well as changes in configuration or other occurrences. These messages are stored locally and can be forwarded to one or more centralized points of collection for monitoring purposes or long term archival storage. Local and remote configuration of the logging capability includes filtering of messages logged or forwarded based on severity and generating component.

## View or Configure Buffered Logs

This log stores messages in memory based upon the settings for message component and severity. On stackable systems, this log exists only on the top of stack platform. Other platforms in the stack forward their messages to the top of stack log.

➤ **To view or configure buffered logs:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

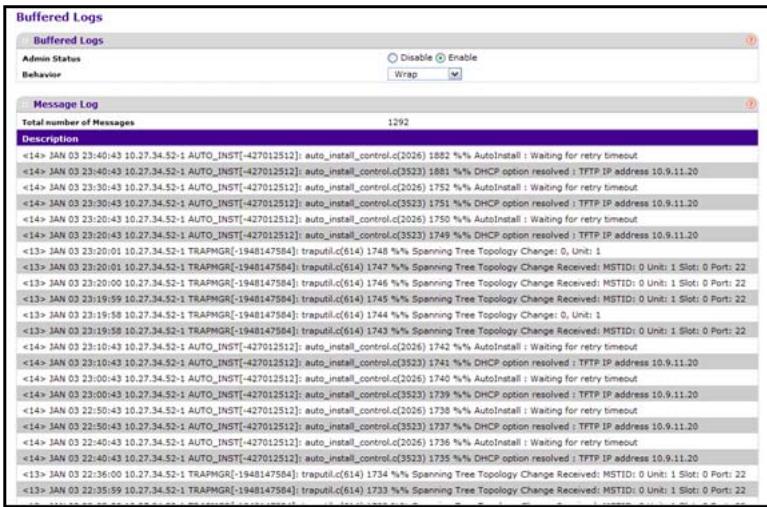
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Monitoring > Logs > Buffered Logs**.



A log that is disabled does not log messages.

8. To enable or disable a log, select the **Disable** or **Enable** radio button.

**Behavior** Indicates the behavior of the log when it is full. It can either wrap around or stop when the log space is filled.

9. To refresh the screen to show the latest messages in the log, click the **REFRESH** button.

10. To clear the buffered log in the memory, click the **CLEAR** button.

## Message Format in Logs

This topic applies to the format of all logged messages that are displayed for the message log, persistent log, or console log.

Messages logged to a collector or relay through syslog use an identical format of either type:

### If system is not stacked

```
<15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12
transitioned to root state on message age timer expiry.
```

This example indicates a message with severity 7 (15 mod 8) (debug) on a system that is not stacked and generated by component MSTP running in thread ID 2110 on Aug 24 05:34:05 by line 318 of file mspt\_api.c. This is the 237th message logged.

### If the system is stacked

- <15>Aug 24 05:34:05 0.0.0.0-1 MSTP[2110]: mspt\_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry.

This example indicates a message with severity 7 (15 mod 8) (debug) on a system that is stacked and generated by component MSTP running in thread ID 2110 on Aug 24 05:34:05 by line 318 of file mstp\_api.c. This is the 237th message logged with system IP 0.0.0.0 and task-id 1.

- <15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt\_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry.

This example indicates a user-level message (1) with severity 7 (debug) on a system that is not stacked and generated by component MSTP running in thread ID 2110 on Aug 24 05:34:05 by line 318 of file mstp\_api.c. This is the 237th message logged. Messages logged to a collector or relay through syslog use an identical format to the previous message.

- **Total number of Messages:** For the message log, only the latest 200 entries are displayed on the screen.

## Enable the Command Log

➤ **To enable the command log:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Monitoring > Logs > Command Log Configuration**.



8. Select the Admin Mode **Enable** radio button.

CLI command logging is enabled.

## Configure the Console Log

This allows logging to any serial device attached to the host.

➤ **To configure the console log:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Monitoring > Logs > Console Log Configuration**.



A log that is disabled does not log messages.

8. To enable the log, select the Admin Status **Enable** radio button.
9. In the Severity Filter list, select a severity level.

A log records messages equal to or above a configured severity threshold. These severity levels are available:

- **Emergency (0)**. The system is unusable
- **Alert (1)**. Action must be taken immediately
- **Critical (2)**. Critical conditions
- **Error (3)**. Error conditions
- **Warning (4)**. Warning conditions

- **Notice (5)**. Normal but significant conditions
- **Informational (6)**. Informational messages
- **Debug (7)**. Debug-level messages

## Configure the Syslog

➤ **To configure the syslog:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Monitoring > Logs > Sys Log Configuration**.

The screenshot shows the 'Syslog Configuration' page with two main sections: 'Syslog Configuration' and 'Host Configuration'.

**Syslog Configuration:**

Admin Status	
<input checked="" type="radio"/> Disable	<input type="radio"/> Enable
Local UDP Port	
514 (1 to 65535)	
Messages Received	205
Messages Relayed	0
Messages Ignored	0

**Host Configuration:**

	IP Address Type	Host Address	Status	Port	Severity Filter
<input type="checkbox"/>	<input type="button" value="▼"/>	<input type="text"/>	<input type="button" value=""/>	<input type="button" value=""/>	<input type="button" value="▼"/>

8. To enable the log, select the Admin Status **Enable** radio button.

When the syslog configuration is enabled, messages are sent to configured collector/relays using the values configured for each collector/relay.

Setting the Admin Status to **Disable** stops logging to all syslog hosts. No messages are sent to any collector or relay.

9. In the **Local UDP Port** field, type the local port number on the local host from which syslog messages are sent.

The default port is 514.

10. In the **IP Address Type** list, select one of the following:
  - IPv4
  - IPv6
  - DNS
11. In the **Host Address** field, type the address of the host configured for syslog.
12. In the **Port** field, type the port number on the host to which syslog messages are sent.  
The default port is 514.

13. In the **Severity Filter** list, select a severity level.

A log records messages equal to or above a configured severity threshold. These severity levels are available:

- **Emergency (0)**. The system is unusable
- **Alert (1)**. Action must be taken immediately
- **Critical (2)**. Critical conditions
- **Error (3)**. Error conditions
- **Warning (4)**. Warning conditions
- **Notice (5)**. Normal but significant conditions
- **Informational (6)**. Informational messages
- **Debug (7)**. Debug-level messages

## View Trap Logs

---

**Note:** You can save the trap logs as a file by using **System Utilities > Upload File from Switch**.

---

- **To view trap logs:**
1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
  2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
  3. Launch a web browser.
  4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
  5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **Monitoring > Logs > Trap Logs**.

Trap Logs		
Trap Logs		
Log	System Up Time	Trap
0	2 days 23:19:51	Spanning Tree Topology Change: 0, Unit: 1
1	2 days 23:19:51	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
2	2 days 23:19:50	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
3	2 days 23:19:49	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
4	2 days 23:19:48	Spanning Tree Topology Change: 0, Unit: 1
5	2 days 23:19:48	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
6	2 days 22:35:50	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
7	2 days 22:35:49	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
8	2 days 22:35:48	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
9	2 days 22:35:47	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
10	2 days 22:35:47	Spanning Tree Topology Change: 0, Unit: 1
11	2 days 22:35:47	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
12	2 days 19:15:17	Spanning Tree Topology Change: 0, Unit: 1
13	2 days 19:15:17	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
14	2 days 19:15:16	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
15	2 days 19:15:15	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
16	2 days 19:15:14	Spanning Tree Topology Change: 0, Unit: 1
17	2 days 19:15:14	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
18	2 days 19:10:49	Spanning Tree Topology Change: 0, Unit: 1
19	2 days 19:10:49	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
20	2 days 19:10:48	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22
21	2 days 19:10:47	Spanning Tree Topology Change Received: MSTID: 0 Unit: 1 Slot: 0 Port: 22

The screen also displays information about the traps that were sent.

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

This resets all statistics for the trap logs to the default values.

The following table describes the fields in the Trap Logs screen.

**Table 103. Trap Logs**

Field	Description
Number of Traps Since Last Reset	The number of traps that occurred since the switch last rebooted.
Trap Log Capacity	The maximum number of traps stored in the log. If the number of traps exceeds the capacity, the entries overwrite the oldest entries.
Number of Traps since log last viewed	The number of traps that occurred since the traps were last displayed. Displaying the traps by any method (terminal interface display, web display, upload file from switch, and so on) causes this counter to be cleared to 0.
Log	The sequence number of this trap.

**Table 103. Trap Logs (continued)**

Field	Description
System Up Time	The time at which this trap occurred, expressed in days, hours, minutes and seconds, since the last reboot of the switch.
Trap	Information identifying the trap.

## Event Logs

You can view the event log, which contains error messages from the system. The event log is not cleared on a system reset.

➤ **To view event logs:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Monitoring > Logs> Event Logs**.

Event Logs						
:: Event Logs						
Entry	Type	Filename	Line	TaskID	Code	Time
1	EVENT>	bootos.c	220	0	AAAAAAA	0 0 0 31
2	EVENT>	unitmgr.c	5806	0	0000000	0 0 3 27
3	EVENT>	bootos.c	220	0	AAAAAAA	0 0 0 31
4	EVENT>	bootos.c	220	0	AAAAAAA	0 0 0 31
5	EVENT>	unitmgr.c	5806	0	0000000	0 0 31 42
6	EVENT>	bootos.c	220	0	AAAAAAA	0 0 0 31
7	EVENT>	unitmgr.c	5806	0	0000000	0 0 13 34
8	EVENT>	bootos.c	220	0	AAAAAAA	0 0 0 31
9	EVENT>	unitmgr.c	5806	0	0000000	0 0 2 4
10	EVENT>	bootos.c	220	0	AAAAAAA	0 0 0 31
11	EVENT>	unitmgr.c	5806	0	0000000	0 0 2 39
12	EVENT>	bootos.c	220	0	AAAAAAA	0 0 0 31
13	EVENT>	unitmgr.c	5806	0	0000000	0 0 5 36
14	EVENT>	bootos.c	220	0	AAAAAAA	0 0 0 31
15	EVENT>	unitmgr.c	5806	0	0000000	0 0 6 0
16	EVENT>	bootos.c	220	0	AAAAAAA	0 0 0 31
17	EVENT>	unitmgr.c	5806	0	0000000	0 0 2 47
18	EVENT>	bootos.c	220	0	AAAAAAA	0 0 0 31
19	EVENT>	unitmgr.c	5806	0	0000000	0 1 48 17
20	EVENT>	bootos.c	220	0	AAAAAAA	0 0 0 31
21	EVENT>	unitmgr.c	5806	0	0000000	0 0 12 10
22	EVENT>	bootos.c	220	0	AAAAAAA	0 0 0 31
23	EVENT>	unitmgr.c	5806	0	0000000	0 0 0 45
24	EVENT>	bootos.c	220	0	AAAAAAA	0 0 0 31
25	EVENT>	unitmgr.c	5806	0	0000000	0 0 1 48
26	EVENT>	bootos.c	220	0	AAAAAAA	0 0 0 31
27	EVENT>	unitmgr.c	5806	0	0000000	0 0 3 40
28	EVENT	-	220	0	*****	0 0 0 24

You can use the buttons at the bottom of the screen to perform the following actions:

- To clear the messages out of the event log, click the **CLEAR** button.
- To refresh the screen and display the current statistics, click the **REFRESH** button.

**Table 104. Event Logs**

Field	Description
Entry	The sequence number of the event.
Type	The type of the event.
File Name	The file in which the event originated.
Line	The line number of the event.
Task Id	The task ID of the event.
Code	The event code.
Time	The time this event occurred.

## Configure Persistent Logs

A persistent log is a log that is stored in persistent storage. Persistent storage survives across platform reboots. The first log type is the system startup log. The system startup log stores the first N messages received after system reboot. The second log type is the system

operation log. The system operation log stores the last N messages received during system operation.

➤ **To configure persistent logs:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

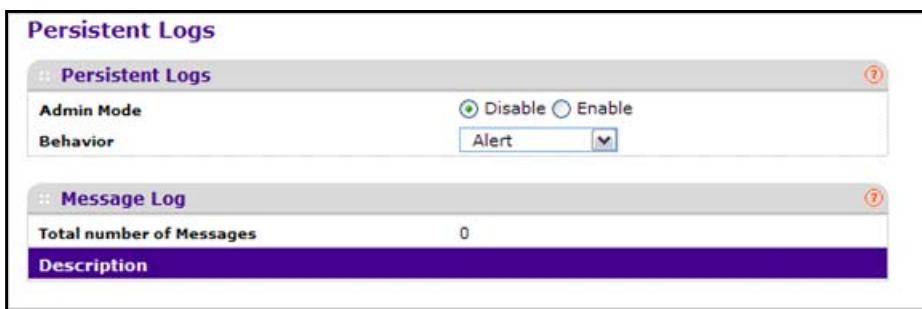
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Monitoring > Logs > Persistent Logs**.



8. To enable or disable logging, select the Admin Mode **Enable** or **Disable** radio button.

A log that is disabled does not log messages.

9. In the **Behavior** menu, select a log severity level.

A log records messages equal to or above a configured severity threshold. These severity levels are available:

severity levels are available:

- **Emergency (0)**. The system is unusable
- **Alert (1)**. Action must be taken immediately
- **Critical (2)**. Critical conditions
- **Error (3)**. Error conditions
- **Warning (4)**. Warning conditions

- **Notice (5)**. Normal but significant conditions
- **Informational (6)**. Informational messages
- **Debug (7)**. Debug-level messages

**10.** To refresh the screen, click the **REFRESH** button.

### Persistent Log Message Format

The total number of messages is the number of persistent log messages displayed on the switch.

<15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt\_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry

This example indicates a user-level message (1) with severity 7 (debug) on a system that is not stacked and generated by component MSTP running in thread ID 2110 on Aug 24 05:34:05 by line 318 of file mspt\_api.c. This is the 237th message logged. Messages logged to a collector or relay through a syslog use a format identical to this message.

## Port Mirroring Overview

Port mirroring selects the network traffic for analysis by a network analyzer. This is done for specific ports of the switch. As such, many switch ports are configured as source ports and one switch port is configured as a destination port. You can configure how traffic is mirrored on a source port. Packets that are received on the source port, which are transmitted on a port, or are both received and transmitted can be mirrored to the destination port.

The packet that is copied to the destination port is in the same format as the original packet on the wire. This means that if the mirror is copying a received packet, the copied packet is VLAN tagged or untagged as it was received on the source port. If the mirror is copying a transmitted packet, the copied packet is VLAN tagged or untagged as it is being transmitted on the source port.

## Configure Port Mirroring

### ➤ To configure port mirroring:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **Monitoring > Mirroring > Multiple Port Mirroring**.



You can select items in this screen using the following methods:

- Select a Unit ID (1, 2, 3, and so on) to display the physical ports of the selected unit.
  - Select **LAG** to display a list of LAGs only.
  - Select **CPU** to display a list of CPUs only.
  - Select **VLANs** to display a list of available VLANs.
  - Select **All** to display a list of all physical ports, LAG, CPU, and VLANs.
  - Select a specific interface by entering its number in the **Go To Interface** field.
- Select the Admin Mode **True** (enabled) or **False** (disabled) radio button for the selected session.

When a session is enabled (True), any traffic entering or leaving the source ports of the session is copied (mirrored) onto the corresponding destination port or a remote switched port analyzer (RSPAN) VLAN. By default, Admin Mode is disabled (False). When disabled, port mirroring is not active on the selected port, but the mirroring information is retained.

- In the **Destination Port** field, specify the destination interface to which port traffic is to be copied.

You can configure only one destination port on the system. It acts as a probe port and receives all the traffic from configured mirrored port(s). The default value is blank.

- Select the check box next to an **interface** to specify the configured port(s) as mirrored port(s).

Traffic of the configured port(s) is sent to the probe port.

- 11.** In the **Direction** menu, specify the direction of the traffic to be mirrored from the configured mirrored port(s).

If the value is not configured, it is shown as None. The default value is None. The following values are available:

- **None**—The value is not configured.
- **Tx and Rx**—Monitors transmitted and received packets.
- **Tx**—Monitors transmitted packets only.
- **Rx**—Monitors received packets only.

**Note:** For VLANs only, the **Tx and Rx** and **None** options are applicable.

- **Tx and Rx**—Specify VLAN as the source VLAN.
- **None**—Remove the specified source VLAN.
- If the VLAN is configured as the source VLAN, its direction is displayed as a blank field.

- 12.** To apply the settings to the system, click the **APPLY** button.

If the port is configured as a source port, the **Mirroring Port** field value is **Mirrored**.

- 13.** To delete a mirrored port, select the check box next to the mirrored port, and then click the **DELETE** button.

- 14.** Click the **APPLY** button.

Your settings are applied to the switch.

## Configure an RSPAN VLAN

You can configure the VLAN to use the remote switched port analyzer (RSPAN) VLAN. RSPAN allows you to mirror traffic from multiple source ports (or from all ports that are members of a VLAN) from different network devices and send the mirrored traffic to a destination port (a probe port connected to a network analyzer) on a remote device. The mirrored traffic is tagged with the RSPAN VLAN ID and transmitted over trunk ports in the RSPAN VLAN.

➤ **To configure an RSPAN VLAN:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Monitoring > Mirroring > RSPAN VLAN**.

VLAN ID	Admin Mode
1	Disable

The **VLAN ID** column lists all VLANs on the device.

8. Select the VLAN to use as the RSPAN VLAN.
  9. In the **Admin Mode** list, select to **Enable** or **Disable** RSPAN support on the corresponding VLAN.
- The default value is Disable.

10. Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See *Save Configuration* on page 405.

## Configure an RSPAN Source Switch

➤ **To configure the RSPAN source switch:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

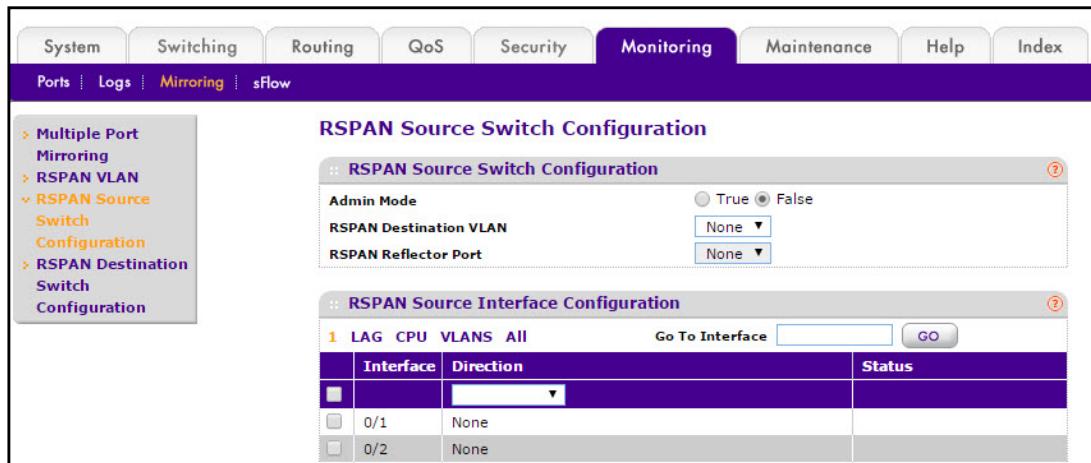
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Monitoring > Mirroring > RSPAN Source Switch Configuration**.



8. Select the Admin Mode **True** (enable) or **False** (disable) radio button for the selected session.

When a particular session is enabled, any traffic entering or leaving the source ports of the session is copied (mirrored) onto the corresponding destination port or a remote switched port analyzer (RSPAN) VLAN. By default, Admin Mode is False (disabled).

9. In the **RSPAN Destination VLAN** list, select a VLAN ID.
10. In the **RSPAN Reflector Port** list, select a reflector port interface.
11. Click the **APPLY** button.

Your changes take effect immediately.

## Configure an RSPAN Source Interface

➤ **To configure an RSPAN source interface:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

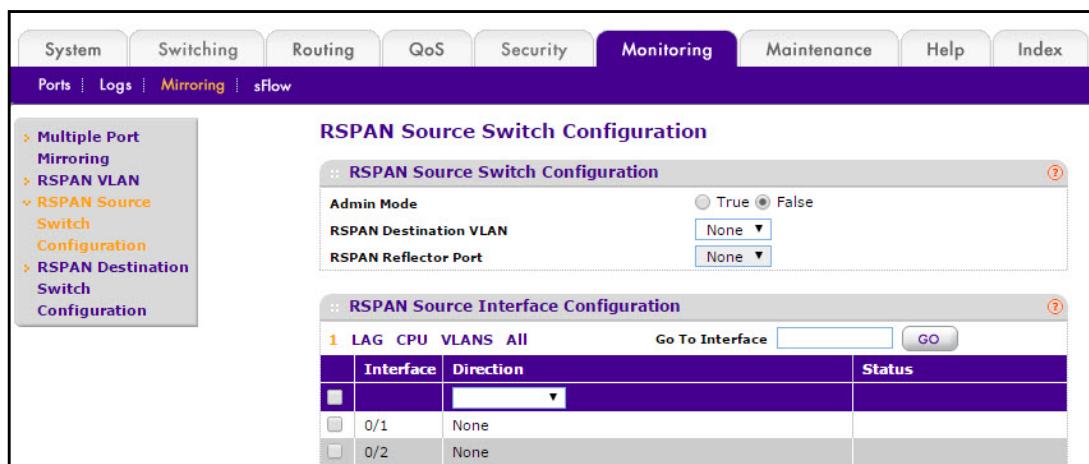
**5.** Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

**6.** Click the **Login** button.

The web management interface menu displays.

**7.** Select **Monitoring > Mirroring > RSPAN Source Switch Configuration**.



**8.** Select items in this screen using one of the following methods:

- Select a Unit ID (1, 2, 3, and so on) to display the physical ports of the selected unit.
- Select **LAG** to display a list of LAGs only.
- Select **CPU** to display a list of CPUs only.
- Select **VLANs** to display a list of available VLANs.
- Select **All** to display a list of all physical ports, LAG, CPU, and VLANs.
- Select a specific interface by entering its number in the **Go To Interface** field.

**9.** In the **Interface** list, select an interface to specify the configured port(s) as mirrored port(s).

Traffic of the configured port(s) is sent to the probe port.

**10.** In the **Direction** list, select a value to specify the direction of the traffic to be mirrored from the configured mirrored port(s).

If the value is not configured, **None** is displayed. The default value is **None**.

- **None**—The value is not configured.
- **Tx and Rx**—Monitor transmitted and received packets.
- **Tx**—Monitor transmitted packets only.
- **Rx**—Monitor received packets only.

**Note:** For VLANs only, the **Tx and Rx** and **None** options are applicable.

- **Tx and Rx**—Specify VLAN as the source VLAN.
- **None**—Remove the specified source VLAN.

If the VLAN is configured as the source VLAN, its direction is displayed as a blank field.

## Configure the RSPAN Destination Switch

➤ **To configure the RSPAN destination switch:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

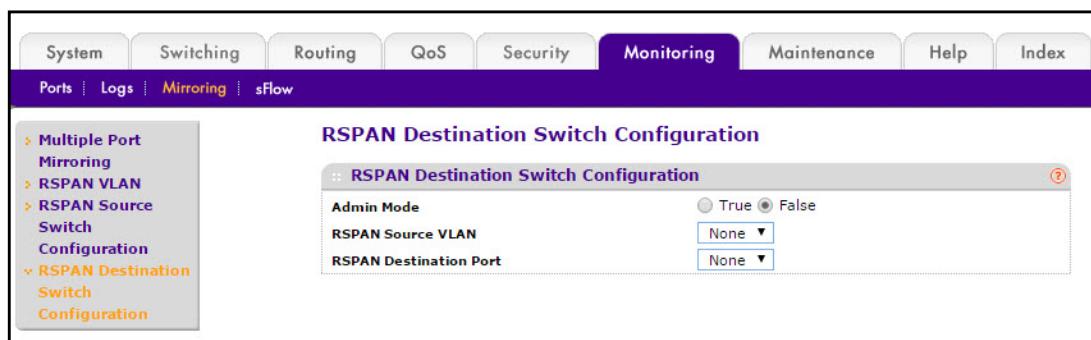
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Monitoring > Mirroring > RSPAN Destination Switch Configuration**.



8. Select the Admin Mode **True** (enabled) or **False** (disabled) for the selected session.

When a particular session is enabled, any traffic entering or leaving the source ports of the session is copied (mirrored) onto the corresponding destination port or a remote switched port analyzer (RSPAN) VLAN. By default, the Admin Mode is disabled.

9. Select the **RSPAN Source VLAN** from the list of available VLAN IDs.
10. Select the **RSPAN Destination Port** from the list of destination interfaces.
11. Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See [Save Configuration](#) on page 405.

## sFlow Overview

You can configure sFlow agent information, sFlow agents, sFlow receivers, and sFlow interfaces.

### Configure sFlow Agent Information

➤ **To configure sFlow agent information:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Monitoring > sFlow > Basic > sFlow Agent Information**.



The screen displays the agent version and agent address.

- **Agent Version.** Uniquely identifies the version and implementation of this MIB. The version string must use the following structure: MIB Version;Organization;Software Revision where:
    - MIB Version: '1.3', the version of this MIB.
    - Organization: NETGEAR Inc.
    - Revision: 1.0
  - **Agent Address.** The IP address associated with this agent.
8. In the **Source Interface** list, select the management interface to be used for sFlow Agent. Possible values are as follows:
- **None**
  - **Routing interface**
  - **Routing VLAN**
  - **Routing loopback interface**
  - **Tunnel interface**
  - **Service port**
- By default, VLAN 1 is used as source interface.
9. Click the **APPLY** button.

The settings are sent to the switch. Configuration changes take effect immediately. These changes are not retained across a power cycle unless you save the configuration. See *Save Configuration* on page 405.

To refresh the screen, click the **REFRESH** button to show the latest sFlow agent information.

## Configure an sFlow Agent

- **To configure an sFlow agent:**
1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
  2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
  3. Launch a web browser.
  4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
  5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
  6. Click the **Login** button.  
The web management interface menu displays.

**7.** Select **Monitoring > sFlow > Advanced > sFlow Agent**.



The screen displays the agent version and agent address.

- **Agent Version.** Uniquely identifies the version and implementation of this MIB. The version string must use the following structure: MIB Version;Organization;Software Revision where:
  - MIB Version: '1.3', the version of this MIB
  - Organization: NETGEAR Inc.
  - Revision: 1.0
- **Agent Address.** The IP address associated with this agent.

**8.** In the **Source Interface** list, select the management interface to be used for sFlow Agent.

Possible values are as follows:

- **None**
- **Routing interface**
- **Routing VLAN**
- **Routing loopback interface**
- **Tunnel interface**
- **Service port**

By default, VLAN 1 is used as source interface.

**9.** Click the **APPLY** button.

Your changes take effect immediately.

Click the **REFRESH** button to refresh the screen to show the latest sFlow agent information.

## Configure the sFlow Receiver

➤ **To configure the sFlow receiver:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.

3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
- The Login screen displays.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Monitoring > sFlow > Advanced > sFlow Receiver Configuration**.

sFlow Receiver Configuration								
	Receiver Index	Receiver Owner	Receiver Timeout	No Timeout	Maximum Datagram Size	Receiver Address	Receiver Port	Datagram Version
1	0		0	False	1400	0.0.0.0	6343	5
2	0		0	False	1400	0.0.0.0	6343	5
3	0		0	False	1400	0.0.0.0	6343	5
4	0		0	False	1400	0.0.0.0	6343	5
5	0		0	False	1400	0.0.0.0	6343	5
6	0		0	False	1400	0.0.0.0	6343	5
7	0		0	False	1400	0.0.0.0	6343	5
8	0		0	False	1400	0.0.0.0	6343	5

8. **Receiver Owner.** The entity making use of this sFlowRcvrTable entry.  
The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string. The entry must be claimed before any changes can be made to other sampler objects.
9. **Receiver Timeout.** The time (in seconds) remaining before the sampler is released and stops sampling.  
A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. The valid range is 0 to 2147483647. A value of zero sets the selected receiver configuration to its default values.
10. Use **No Timeout** to select True or False from the menu to set the no time-out sampling for the receiver.  
Sampling is not stopped until 'No Timeout' selected entry is True. The default value is False.
11. **Maximum Datagram Size.** The maximum number of data bytes that can be sent in a single sample datagram.  
Set this value to avoid fragmentation of the sFlow datagrams. The default value is 1400. The allowed range is 200 to 9116.

12. **Receiver Address.** The IP address of the sFlow collector. If set to 0.0.0.0 no sFlow datagrams are sent.
13. **Receiver Port.** The destination port for sFlow datagrams. The allowed range is (1 to 65535).
14. Click the **APPLY** button.

Your settings are saved.

## Configure sFlow Interface Settings

The sFlow agent collects statistical packet-based sampling of switched flows and sends them to the configured receivers. A data source configured to collect flow samples is called a sampler. sFlow agent also collects time-based sampling of network interface statistics and sends them to the configured sFlow receivers. A data source configured to collect counter samples is called a poller.

➤ **To configure sFlow interface settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Monitoring > sFlow > Advanced > sFlow Interface Configuration**.

sFlow Interface Configuration						
:: sFlow Interface Configuration						
1 All		Poller		Sampler		
Interface	Receiver Index	Poller Interval	Receiver Index	Sampling Rate	Maximum Header Size	
0/1	0	0	0	0	128	
0/2	0	0	0	0	128	
0/3	0	0	0	0	128	
0/4	0	0	0	0	128	
0/5	0	0	0	0	128	
0/6	0	0	0	0	128	
0/7	0	0	0	0	128	
0/8	0	0	0	0	128	
0/9	0	0	0	0	128	
0/10	0	0	0	0	128	
0/11	0	0	0	0	128	
0/12	0	0	0	0	128	

The **Interface** field displays the interface for this flow poller and sampler. This agent supports physical ports only.

8. In the **Poller Receiver Index** field, specify the allowed range for the sFlow receiver associated with this counter poller.

The allowed range is 1 to 8.

9. In the **Poller Interval** field, specify the maximum number of seconds between successive samples of the counters associated with this data source.

A sampling interval of 0 disables counter sampling. The allowed range is 0 to 86400 secs.

10. In the **Sampler Receiver Index** field, specify the sFlow receiver for this flow sampler.

If set to 0, the sampler configuration is set to the default and the sampler is deleted. Only active receivers can be set. If a receiver expires, then all samplers associated with the receiver also expire. The allowed range is 1 to 8.

11. In the **Sampling Rate** field, specify the statistical sampling rate for packet sampling from this source.

A sampling rate of 1 counts all packets. A sampling rate of 0 disables sampling. The allowed range is 1024 to 65536.

12. In the **Maximum Header Size** field, specify the maximum number of bytes that should be copied from a sampled packet.

The allowed range is 20 to 256.

# Maintenance

---

# 8

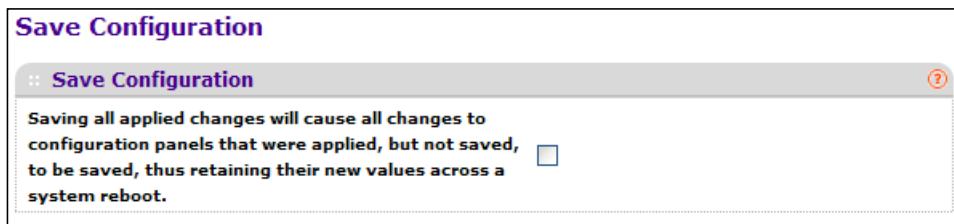
This chapter covers the following topics:

- *Save Configuration*
- *Configure Auto Install*
- *Reboot a Switch*
- *Upload Files*
- *Download Files*
- *File Management Overview*
- *Use the Ping IPv4 Utility*
- *Use the Ping IPv6 Utility*
- *Run Traceroute IPv4*
- *Configure Traceroute IPv6 Settings*

## Save Configuration

➤ **To save the configuration:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Maintenance > Save Config > Save Configuration.**



8. Select the check box.
9. Click the **APPLY** button.

Your configuration changes are saved across a system reboot. All changes submitted since the previous save or system reboot are retained by the switch.

## Configure Auto Install

➤ **To configure Auto Install:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

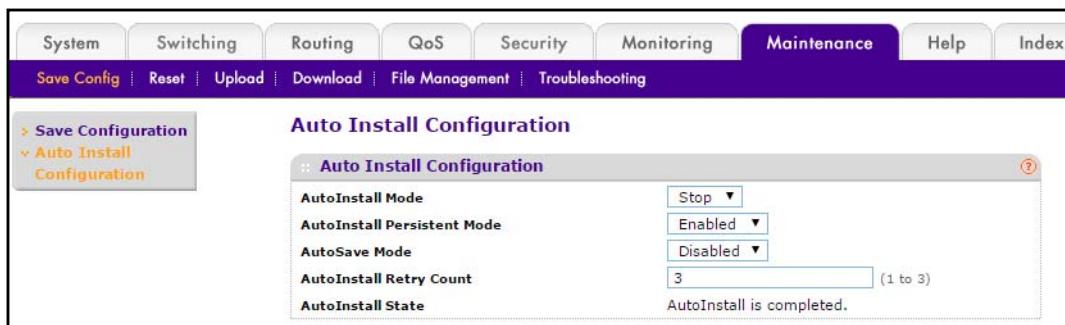
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Maintenance > Save Config > Auto Install Configuration**.



8. Use **Auto Install** to select the start/stop auto install mode on the switch.
  9. Use **AutoInstall Persistent Mode** to enable/disable AutoInstall persistent mode.
  10. In the **AutoSave Mode** to select Enabled or Disabled and click the **APPLY** button.
- Configuration changes you made are saved across a system reboot. All changes submitted since the previous save or system reboot are retained by the switch.
11. Use **AutoInstall Retry Count** to specify the number of times the unicast TFTP tries will be made for the DHCP-specified file before falling back for broadcast TFTP tries.

The Autoinstall State field displays the current status of the AutoInstall process.

## Reboot a Switch

### ➤ To reboot a switch:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

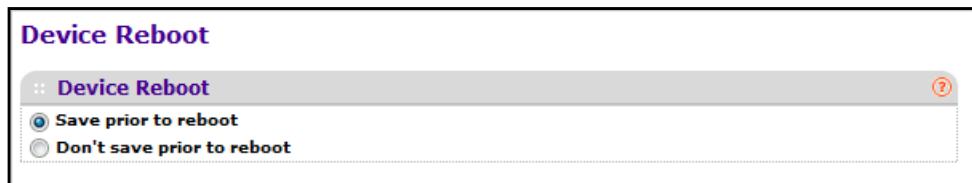
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Maintenance > Reset > Device Reboot**.



8. Select a Device Reboot radio button:

- **Save prior to reboot** saves the current configuration before the switch reboots.
- **Don't save prior to reboot** reboots without saving.

9. Click the **APPLY** button.

If the Save option is selected, the current configuration is saved.

The switch reboots.

## Reset the Switch to Factory Default Settings

You can reset the system configuration to the factory default values.

---

**Note:** If you reset the switch to the default configuration, the IP address is reset to 169.254.100.100, and the DHCP client is enabled.

---

➤ **To reset the switch to the factory default settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.  
The Login screen displays.
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Maintenance > Reset > Factory Default**.

**Factory Default**

:: Factory Default

Check this box and click **APPLY** below to return all configuration settings to default values

8. Select the check box and click the **APPLY** button.

All configuration parameters are reset to their factory default values. All changes you made are lost, even if you issued a save. You are shown a confirmation screen after you click the button.

## Reset All User Passwords to Factory Defaults

You can reset all user passwords to their factory defaults.

➤ **To reset the passwords:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Maintenance > Reset > Password Reset**.

**Password Reset**

:: Password Reset

Check this box and click **APPLY** below to reset all user passwords.

8. Select the check box.
9. Click the **APPLY** button.

All user passwords reset to their factory default values. All changes you made are lost, even if you saved the configuration.

## Upload Files

You can upload files from the switch.

### Upload a File from the Switch to the TFTP Server

➤ **To upload a file from the switch to the TFTP server:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.  
The default IP address of the switch is 169.254.100.100.
5. Enter the user name and password.  
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Maintenance > Upload > File Upload**.

File Upload	
File Type	Archive
Image Name	image1
Transfer Mode	TFTP
Server Address Type	IPv4
Server Address	0.0.0.0
Remote File Path	
Remote File Name	

8. Use **File Type** to specify what type of file to upload:
  - **Archive**. Specify archive (STK) code to retrieve from the operational flash.
  - **Image Name**. Select one of the images from the list:

- **image1.** Select image1 to upload image1.
- **image2.** Select image2 to upload image2
- **CLI Banner.** CLI Banner when you want retrieve the CLI banner file.
- **Text Configuration.** Specify configuration in text mode to retrieve the stored configuration.
- **Script File.** The Script file to retrieve the stored configuration.
- **Error Log.** The Error log to retrieve the system error (persistent) log, sometimes referred to as the event log.
- **Buffered Log.** The Buffered Log to retrieve the system buffered (in-memory) log.
- **Trap Log.** Trap ILg to retrieve the system trap records.
- **Tech Support.** Tech Support to retrieve the switch information needed for trouble-shooting.

The factory default is Archive.

- 9.** Use **Transfer Mode** to specify what protocol to use to transfer the file:
  - **TFTP.** Trivial File Transfer Protocol
  - **SFTP.** Secure File Transfer Protocol
  - **SCP.** Secure Copy Protocol
- 10.** Use **Server Address Type** to specify either IPv4, IPv6, or DNS to indicate the format of the Server Address field.  
The factory default is IPv4.
- 11.** Use **Server Address** to enter the IP address of the server in accordance with the format indicated by the server address type.  
The factory default is the IPv4 address 0.0.0.0.
- 12.** Use **Remote File Path** to enter the path where you want to upload the file.  
The file path can include alphabetic, numeric, forward slash, dot, or underscore characters only. You can enter up to 160 characters. The factory default is blank.
- 13.** Use **Remote File Name** to enter the name of the file to download from the server.  
You can enter up to 32 characters. The factory default is blank.
- 14.** Use **Local File Name** to specify the local script file name to upload.  
This field is visible only when File Type is Script File.
- 15.** Use **User Name** to enter the user name for remote login to the SFTP/SCP server where the file is sent.  
This field is visible only when the SFTP or SCP transfer mode is selected.
- 16.** Use **Password** to enter the password for remote login to the SFTP/SCP server where the file is sent.  
This field is visible only when the SFTP or SCP transfer mode is selected.

- 17.** The last row of the table is used to display information about the progress of the file transfer.

## Upload an HTTP File

➤ **To upload an HTTP file:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

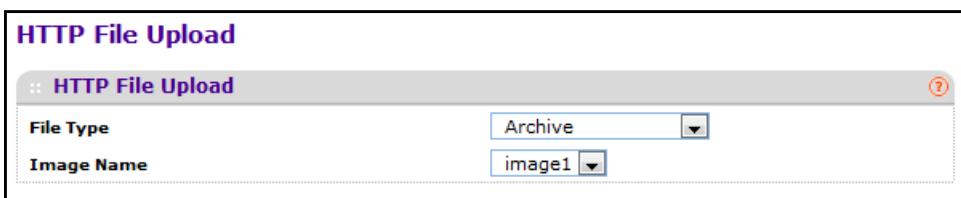
5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Maintenance > Upload > HTTP File Upload**.



8. In the **File Type** menu, specify what type of file to upload:
  - **Archive.** Specify archive (STK) code to retrieve from the operational flash:
  - **Image Name.** Select one of the images from the list:
    - **Image1.** Specify the code image1 to retrieve.
    - **Image2.** Specify the code image2 to retrieve.
  - **CLI Banner.** Specify CLI Banner when you want retrieve the CLI banner file.
  - **Text Configuration.** Specify configuration in text mode to retrieve the stored configuration.
  - **Script File.** Specify script file to retrieve the stored configuration.
  - **Error Log.** Specify error log to retrieve the system error (persistent) log, sometimes referred to as the event log.
  - **Trap Log.** Specify trap log to retrieve the system trap records.
  - **Buffered Log.** Specify buffered log to retrieve the system buffered (in-memory) log.

- **Tech Support.** Specify Tech Support to retrieve the switch information needed for troubleshooting.

The factory default is Archive.

9. Use **Local File Name** to specify the local script file name to upload when the file type is Script File.

## Upload a USB File

### ➤ To upload a file to USB

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Maintenance > Upload > USB File Upload**.

Upload File To USB	
:: Upload File To USB	
<b>File Type</b>	Archive
<b>Image Name</b>	image1
<b>USB File</b>	[Empty Input Field]

8. In the **File Type** list, specify what type of file to upload:
    - **Archive.** Specify archive (STK) code when to retrieve from the operational flash:
    - **Text Configuration.** Specify configuration in text mode to retrieve the stored configuration.
- The factory default is **Archive**.
9. In the **Image Name** list, select one of the images:
    - **Image1.** Specify the code image1 to retrieve.
    - **Image2.** Specify the code image2 to retrieve.

10. In the **USB File** name field, specify the file name and path for the file.

You can enter up to 32 characters. The factory default is blank.

11. Click the **APPLY** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

## Download Files

The switch supports system file downloads from a remote system to the switch by using either TFTP or HTTP.

### Download Files

➤ **To download a file:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Maintenance > Download > File Download**.

File Download	
:: File Download	
<b>File Type</b>	Archive
<b>Image Name</b>	image1
<b>Transfer Mode</b>	TFTP
<b>Server Address Type</b>	IPv4
<b>Server Address</b>	0.0.0.0
<b>Remote File Path</b>	
<b>Remote File Name</b>	

8. Use **File Type** to specify what type of file to transfer.

- **Archive.** Specify archive (STK) code to upgrade the operational flash:
  - **Image1.** Specify the code image1 to download.
  - **Image2.** Specify the code image2 to download.
- **CLI Banner.** Specify CLI Banner when you want a banner to be displayed before the login prompt.
- **Text Configuration.** Specify configuration in text mode to update the switch's configuration.  
If the file has errors, the update is stopped.
- Use **Config Script** to specify the script configuration file.
- Use **SSH-1 RSA Key File** to specify the SSH-1 Rivest-Shamir-Adleman (RSA) Key File.
- Use **SSH-2 RSA Key PEM File** to specify the SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded).
- Use **SSH-2 DSA Key PEM File** to specify the SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded).
- Use **SSL Trusted Root Certificate PEM File** to specify the SSL Trusted Root Certificate File (PEM Encoded).
- Use **SSL Server Certificate PEM File** to specify the SSL Server Certificate File (PEM Encoded).
- Use **SSL DH Weak Encryption Parameter PEM File** to specify the SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded).
- Use **SSL DH Strong Encryption Parameter PEM File** to specify the SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).

The factory default is Image1.

**Note:** To download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.

**Note:** To download SSL PEM files SSL must be administratively disabled and there can be no active SSH sessions.

9. Use **Image Name** to select one of the images from the list:
  - **Image1.** Specify the code image1 to retrieve.
  - **Image2.** Specify the code image2 to retrieve.
10. Use **Transfer Mode** to specify what protocol to use to transfer the file:
  - **TFTP.** Trivial File Transfer Protocol
  - **SFTP.** Secure File Transfer Protocol
  - **SCP.** Secure Copy Protocol
11. Use **Server Address Type** to specify either IPv4, IPv6, or DNS to indicate the format of the TFTP/SFTP/SCP Server Address field.

The factory default is IPv4.

12. Use **Server Address** to enter the IP address of the server in accordance with the format indicated by the server address type.

The factory default is the IPv4 address 0.0.0.0.

13. Use **Remote File Path** to enter the path of the file to download.

The file path cannot include the following symbols: '\:\*?"<>|'. Up to 32 characters can be entered. The factory default is blank.

14. Use **Remote File Name** to enter the name of the file to download from the server.

You can enter up to 32 characters. The factory default is blank.

15. Use **User Name** to enter the user name for remote login to SFTP/SCP server where the file resides.

This field is visible only when the SFTP or SCP transfer mode is selected.

16. Use **Password** to enter the password for remote login to SFTP/SCP server where the file resides.

This field is visible only when the SFTP or SCP transfer mode is selected.

17. The last row of the table is used to display information about the progress of the file transfer.

The screen refreshes automatically until the file transfer completes.

## Download HTTP Files

### ➤ To download a file to the switch by using HTTP:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7.** Select **Maintenance > Download > HTTP File Download**.

**Note:** To download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.

**Note:** To download SSL PEM files, SSL must be administratively disabled and there can be no active SSH sessions.

**8.** Use **File Type** to specify what type of file to transfer:

- **Archive.** Specify archive (STK) code to upgrade the operational flash:
  - **Image1.** Specify the code image1 to download.
  - **Image2.** Specify the code image2 to download.
- **CLI Banner.** Specify CLI Banner when you want a banner to be displayed before the login prompt.
- **Text Configuration.** Specify configuration in text mode to update the switch's configuration. If the file has errors, the update is stopped.
- Use **Config Script** to specify the script configuration file.
- Use **SSH-1 RSA Key File** to specify the SSH-1 Rivest-Shamir-Adleman (RSA) Key File.
- Use **SSH-2 RSA Key PEM File** to specify the SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded)
- Use **SSH-2 DSA Key PEM File** to specify the SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded).
- Use **SSL Trusted Root Certificate PEM File** to specify the SSL Trusted Root Certificate File (PEM Encoded).
- Use **SSL Server Certificate PEM File** to specify the SSL Server Certificate File (PEM Encoded).
- Use **SSL DH Weak Encryption Parameter PEM File** to specify the SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded).
- Use **SSL DH Strong Encryption Parameter PEM File** to specify the SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).

The factory default is Archive.

**9.** Use **Image Name** to select one of the images from the list:

- **Image1.** Specify the code image1 to retrieve.

- **Image2.** Specify the code image2 to retrieve.

**10.** If you are downloading an image (Archive), select the image on the switch to overwrite.

This field is visible only when Archive is selected as the File Type.

---

**Note:** NETGEAR recommends that you not overwrite the active image. The system displays a warning that you are trying to overwrite the active image.

---

**11.** Click **BROWSE** to open a file upload window to locate the file to download.

**12.** Use **Select File** to browse and select the name and the path for the file to download.

You can enter up to 80 characters. The factory default is blank.

**13.** Click the **APPLY** button.

The download starts.

The **Download Status** field displays the status during transfer file to the switch.

---

**Note:** After a file transfer is started, wait until the screen refreshes. When the screen refreshes, the *Select File* option is blanked out. This indicates that the file transfer is done.

---

## Download a File to a USB Device

➤ **To download a file to a USB device:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.

3. Launch a web browser.

4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

**7.** Select **Maintenance > Download > USB File Upload**.

The screenshot shows a configuration interface titled "Download File From USB". It has three main input fields: "File Type" set to "Archive", "Image Name" set to "image1", and "USB File" which is currently empty. There is also a small question mark icon in the top right corner of the form area.

- 8.** Use **File Type** to specify what type of file to upload:
  - **Archive**. Specify archive (STK) code to retrieve from the operational flash:
  - **Text Configuration** to specify configuration in text mode to retrieve the stored configuration. The factory default is **Archive**.
- 9.** Use **Image Name** to select one of the images from the list:
  - **Image1**. Specify the code image1 to retrieve.
  - **Image2**. Specify the code image2 to retrieve.
- 10.** Use **USB File** to give a name along with path for the file to upload.  
You can enter up to 32 characters. The factory default is blank.
- 11.** Click the **APPLY** button.  
Configuration changes take effect immediately.

## File Management Overview

The system maintains two versions of the managed switch software in permanent storage. One image is the active image, and the second image is the backup image. The active image is loaded during subsequent switch restarts. This feature reduces switch down time when upgrading or downgrading the managed switch software.

### Copy a File

➤ **To copy a file:**

- 1.** Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
- 2.** Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
- 3.** Launch a web browser.
- 4.** Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

- 5.** Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Maintenance > File Management > Copy**.



8. Use **Source Image** to select the image1 or image2 as source image when copy occurs.
9. Use **Destination Image** to select the image1 or image2 as destination image when copy occurs.

## Configure Dual Image Settings

The Dual Image feature allows the switch to retain two images in permanent storage. The user designates one of these images as the active image to be loaded during subsequent switch restarts. This feature reduces switch down time when upgrading or downgrading the image.

➤ **To configure dual image settings:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Maintenance > File Management > Dual Image Configuration**.

<b>Dual Image Configuration</b>						
:: Dual Image Configuration						
	Unit	Image Name	Active Image	Next Active Image	Image Description	Version
<input type="checkbox"/>	1	image1	False	False		9.0.2.18
<input checked="" type="checkbox"/>	1	image2	True	True		10.15.17.33

8. Use **Unit** to select the unit.
9. Use **Next Active Image** to make the selected image the next active image for subsequent reboots.
10. Use **Image Description** to specify the description for the image that you selected.
11. Click **DELETE** to delete the selected image from permanent storage on the switch.
12. Click the **APPLY** button.

The updated configuration is sent to the switch. Configuration changes take effect immediately.

---

**Note:** After activating an image, you must perform a system reset of the switch in order to run the new code.

---

The following table describes the nonconfigurable information displayed on the screen.

**Table 105. Dual Image Configuration**

Field	Description
Image Name	This displays the image name for the selected unit.
Active Image	Displays the current active image of the selected unit.
Version	Displays the version of the image1 code file.

## Use the Ping IPv4 Utility

Use this screen to tell the switch to send a Ping request to a specified IP address. You can use this to check whether the switch can communicate with a particular IP station. When you click the **APPLY** button, the switch sends specified number of ping requests and the results are displayed.

If a reply to the ping is not received, the following message displays:

- Tx = Count, Rx = 0 Min/Max/Avg RTT = 0/0/0 msec

If a reply to the ping is received, the following messages display:

- Received response for Seq Num 0 Rtt xyz usec
- Received response for Seq Num 1 Rtt abc usec
- Received response for Seq Num 2 Rtt def usec
- Tx = Count, Rx = Count Min/Max/Avg RTT = xyz/abc/def msec.

➤ **To configure the settings and ping a host on the network:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Maintenance > Troubleshooting > Ping IPv4**.

Ping Details	
IP Address/Host Name	(Max 255 characters/x.x.x.x)
Count	1 (1 to 15)
Interval(secs)	3 (1 to 60)
Datagram Size	0 (0 to 65507)
<b>Ping</b>	

8. Use **IP Address/Host Name** to enter the IP address or host name of the station you want the switch to ping.

The initial value is blank. The IP address or host name that you enter is not retained across a power cycle.

9. Optionally, configure the following settings:

- **Count.** Enter the number of echo requests to send. The count you enter is not retained across a power cycle.

- **Interval (secs).** Enter the interval between ping packets in seconds. The interval you enter is not retained across a power cycle.
- **Datagram Size.** Enter the Size of ping packet. The size you enter is not retained across a power cycle.

PING displays the result after the switch sends a Ping request to the specified address.

**10.** Click the **APPLY** button.

The switch sends the number of pings specified in the **Count** field, and the results are displayed below the configurable data in the **Ping** area.

## Use the Ping IPv6 Utility

This screen is used to send a ping request to a specified host name or IPv6 address. You can use this to check whether the switch can communicate with a particular IPv6 station. When you click the **APPLY** button, the switch sends three pings and the results are displayed on the screen. The output is Send count=3, Receive count=n from (IPv6 Address). Average round trip time = n ms.

➤ **To configure the settings and ping a host name or IPv6 address on the network:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Maintenance > Troubleshooting > Ping IPv6**.

The screenshot shows the 'Ping IPv6' configuration interface. It includes a dropdown menu for 'Ping' set to 'Global', a field for 'IPv6 Address/Host Name' with a placeholder '(>xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/ Max 255 characters)', a 'Datagram Size' input set to '64' (with a note '(48 to 2048)'), and a large 'Result' text area below.

8. Use **Ping** to select either global IPv6 address, host name, or link local address to ping.
9. Use **IPv6 Address/Hostname** to enter the IPv6 address or host name of the station you want the switch to ping. T  
he initial value is blank. The IPv6 address or host name you enter is not retained across a power cycle.
10. Use **Datagram Size** to enter the datagram size.  
The valid range is 48 to 2048.  
Results display after the switch sends a ping IPv6 request to the specified IPv6 address.

## Run Traceroute IPv4

Use this screen to tell the switch to send a traceroute request to a specified IP address or host name. You can use this to discover the paths packets take to a remote destination. When you click the **APPLY** button, the switch sends a traceroute and the results are displayed on the screen.

If a reply to the traceroute is received, the following messages display:

```
1 x.y.z.w 9869 usec 9775 usec 10584 usec
2 0.0.0.0 0 usec * 0 usec * 0 usec *
3 0.0.0.0 0 usec * 0 usec * 0 usec *
Hop Count = w Last TTL = z Test attempt = x Test Success = y.
```

- **To configure the traceroute settings and send probe packets to discover the route to a host on the network:**
  1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
  2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
  3. Launch a web browser.
  4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

- Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

- Click the **Login** button.

The web management interface menu displays.

- Select **Maintenance > Troubleshooting > Traceroute IPv4**.

TraceRoute IPv4	
IP Address/Hostname	(Max 255 Characters/x.x.x.x)
Probes Per Hop	3 (1 to 10)
Max TTL	30 (1 to 255)
Init TTL	1 (1 to 255)
MaxFail	5 (0 to 255)
Interval	3 (1 to 60)
Port	33434 (1 to 65535)
Size	0 (0 to 65507)

Results	

- Use **IP Address/Hostname** to enter the IP address or host name of the station you want the switch to discover path.

The initial value is blank. The IP address or host name that you enter is not retained across a power cycle.

- Optionally, configure the following settings:

- Probes Per Hop.** Enter the number of probes per hop. The initial value is the default. The probes per hop you enter is not retained across a power cycle.
- MaxTTL.** Enter the maximum TTL for the destination. The initial value is default value. The MaxTTL you enter is not retained across a power cycle.
- InitTTL.** Enter the initial TTL to be used. The initial value is default value. The InitTTL you enter is not retained across a power cycle.
- MaxFail.** Enter the maximum number of failures allowed in the session. The initial value is default value. The value you enter is not retained across a power cycle.
- Interval (secs).** Enter the Time between probes in seconds. The initial value is default value. The interval you enter is not retained across a power cycle.

- **Port.** Enter the UDP Dest port in probe packets. The initial value is default value. The port you enter is not retained across a power cycle.
- **Size.** Enter the size of probe packets. The initial value is default value. The size you enter is not retained across a power cycle.

**10.** Click the **APPLY** button.

The traceroute initiates. The results display in the TraceRoute area.

## Configure Traceroute IPv6 Settings

You can tell the switch to send a traceroute request to a specified IP address or host name. You can use this to discover the paths packets take to a remote destination. Once you click the **APPLY** button, the switch sends a traceroute and the results are displayed on the screen.

If a reply to the traceroute is received, the following messages display:

```
1 a:b:c:d:e:f:g 9869 usec 9775 usec 10584 usec
2 0:0:0:0:0:0:0 0 usec * 0 usec * 0 usec *
Hop Count = w Last TTL = z Test attempt = x Test Success = y.
```

➤ **To configure the traceroute IPv6 settings**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address field.

The default IP address of the switch is 169.254.100.100.

The Login screen displays.

5. Enter the user name and password.

The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Maintenance > Troubleshooting > Traceroute IPv6**.

**Traceroute IPv6**

**Traceroute IPv6** (?)

**IPv6 Address/Host Name**

**Port**  (1 to 65535)

**Results** (?)

8. Use **IPv6 Address/Hostname** to enter the IPv6 address or host name of the station you want the switch to discover path.

The initial value is blank. The IPv6 address or host name you enter is not retained across a power cycle.

9. Use **Port** to enter the UDP Dest port in probe packets.

The initial value is the default value. The port you enter is not retained across a power cycle.

# Default Settings



This appendix describes the default settings for many of the NETGEAR M4100 Managed Switch software features.

## Factory Default Settings

The following table describes the factory default settings for the switch.

**Table 106. Factory default settings**

Feature	Default
IP address	169.254.100.100
Subnet mask	255.255.0.0
Default gateway	0.0.0.0
Protocol	DHCP
Management VLAN ID	1
Minimum password length	Eight characters
IPv6 management mode	Enabled
SNTP client	Enabled
SNTP server	Not configured
Global logging	Enabled
CLI command logging	Disabled
Console logging	Enabled (Severity level: debug and above)
RAM logging	Enabled (Severity level: debug and above)
Persistent (FLASH) logging	Disabled
DNS	Enabled (No servers configured)
SNMP	Enabled (SNMPv1/SNMPv2, SNMP v3)
SNMP Traps	Enabled

**Table 106. Factory default settings (continued)**

<b>Feature</b>	<b>Default</b>
Auto Install	Enabled
Auto Save	Disabled
sFlow	Enabled
ISDP	Enabled (Versions 1 and 2)
RMON	Enabled
TACACS	Not configured
RADIUS	Not configured
SSH/SSL	Disabled
Telnet	Enabled
Denial of Service Protection	Disabled
Dot1x Authentication (IEEE 802.1X)	Disabled
MAC-Based Port Security	All ports are unlocked
Access Control Lists (ACL)	None configured
IP Source Guard (IPSG)	Disabled
DHCP Snooping	Disabled
Dynamic ARP Inspection	Disabled
Protected Ports	None
Private Groups	None
Flow Control Support (IEEE 802.3x)	Enabled
Head of Line Blocking Prevention	Disabled
Maximum Frame Size	1518 bytes
Auto-MDI/MDIX Support	Enabled
Auto Negotiation	Enabled
Advertised Port Speed	Maximum Capacity
Broadcast Storm Control	Enabled
Port Mirroring	Disabled
LLDP	Enabled
LLDP-MED	Disabled

**Table 106. Factory default settings (continued)**

<b>Feature</b>	<b>Default</b>
MAC Table Address Aging	300 seconds (Dynamic Addresses)
DHCP Layer 2 Relay	Disabled
Default VLAN ID	1
Default VLAN Name	Default
GVRP	Disabled
GARP Timers	Leave: 60 centiseconds Leave All: 1000 centiseconds Join: 20 centiseconds
Voice VLAN	Disabled
Guest VLAN	Disabled
RADIUS-assigned VLANs	Disabled
Double VLANs	Disabled
Spanning Tree Protocol (STP)	Enabled
STP Operation Mode	IEEE 802.1s Multiple Spanning Tree
Optional STP Features	Disabled
STP Bridge Priority	32768
Multiple Spanning Tree	Enabled
Link Aggregation	No link aggregation groups (LAGs) configured
LACP System Priority	1
Routing Mode	Disabled
IP Helper and UDP Relay	Enabled
Tunnel and Loopback Interfaces	None
DiffServ	Enabled
Auto VoIP	Enabled
Auto VoIP Traffic Class	6
Bridge Multicast Filtering	Disabled
MLD Snooping	Disabled
IGMP Snooping	Disabled
IGMP Snooping Querier	Disabled
GMRP	Disabled

## B Configuration Examples

---

B

This appendix contains information about how to configure the following features:

- *Virtual Local Area Networks*
- *Access Control Lists*
- *Differentiated Services (DiffServ)*
- *802.1X*
- *MSTP*

## Virtual Local Area Networks

A local area network (LAN) can generally be defined as a broadcast domain. Hubs, bridges, or switches in the same physical segment or segments connect all end node devices. End nodes can communicate with each other without the need for a router. Routers connect LANs together, routing the traffic to the appropriate port.

A virtual LAN (VLAN) is a local area network with a definition that maps workstations on some basis other than geographic location (for example, by department, type of user, or primary application). To enable traffic to flow between VLANs, traffic must go through a router, just as if the VLANs were on two separate LANs.

A VLAN is a group of computers, servers, and other network resources that behave as if they were connected to a single network segment—even though they might not be. For example, all marketing personnel might be spread throughout a building. Yet if they are all assigned to a single VLAN, they can share resources and bandwidth as if they were connected to the same segment. The resources of other departments can be invisible to the marketing VLAN members, accessible to all, or accessible only to specified individuals, depending on how the IT manager has set up the VLANs.

VLANs offer a number of advantages:

- It is easy to do network segmentation. Users that communicate most frequently with each other can be grouped into common VLANs, regardless of physical location. Each group's traffic is contained largely within the VLAN, reducing extraneous traffic and improving the efficiency of the whole network.
- They are easy to manage. The addition of nodes, as well as moves and other changes, can be dealt with quickly and conveniently from a management interface rather than from the wiring closet.
- They provide increased performance. VLANs free up bandwidth by limiting node-to-node and broadcast traffic throughout the network.
- They ensure enhanced network security. VLANs create virtual boundaries that can be crossed only through a router. So standard, router-based security measures can be used to restrict access to each VLAN.

Packets received by the switch are treated in the following way:

- When an untagged packet enters a port, it is automatically tagged with the port's default VLAN ID tag number. Each port has a default VLAN ID setting that is user configurable (the default setting is 1). The default VLAN ID setting for each port can be changed in the Port PVID Configuration screen. See [Configure Port PVID](#) on page 128.
- When a tagged packet enters a port, the tag for that packet is unaffected by the default VLAN ID setting. The packet proceeds to the VLAN specified by its VLAN ID tag number.
- If the port through which the packet entered is not a member of the VLAN specified by the VLAN ID tag, the packet is dropped.
- If the port is a member of the VLAN specified by the packet's VLAN ID, the packet can be sent to other ports with the same VLAN ID.

- Packets leaving the switch are either tagged or untagged, depending on the setting for that port's VLAN membership properties. A U for a given port means that packets leaving the switch from that port are untagged. Inversely, a T for a given port means that packets leaving the switch from that port are tagged with the VLAN ID that is associated with the port.

The example given in this section comprises numerous steps to illustrate a wide range of configurations to help provide an understanding of tagged VLANs.

## VLAN Example Configuration

This example demonstrates several scenarios of VLAN use and describes how the switch handles tagged and untagged traffic.

In this example, you create two new VLANs, change the port membership for default VLAN 1, and assign port members to the two new VLANs:

1. In the Basic VLAN Configuration screen, create the following VLANs:
  - A VLAN with VLAN ID 10.
  - A VLAN with VLAN ID 20.S
 See [Configure a Basic VLAN](#) on page 118.
2. In the VLAN Membership screen specify the VLAN membership as follows:
  - For the default VLAN with VLAN ID 1, specify the following members: port 7 (U) and port 8 (U).
  - For the VLAN with VLAN ID 10, specify the following members: port 1 (U), port 2 (U), and port 3 (T).
  - For the VLAN with VLAN ID 20, specify the following members: port 4 (U), port 5 (T), and port 6 (U).
 See [Configure VLAN Membership](#) on page 125.
3. In the Port PVID Configuration screen, specify the PVID for ports g1 and g4 so that packets entering these ports are tagged with the port VLAN ID:
  - Port g1: PVID 10
  - Port g4: PVID 20
 See [Configure Port PVID](#) on page 128.
4. With the VLAN configuration that you set up, the following situations produce results as described:
  - If an untagged packet enters port 1, the switch tags it with VLAN ID 10. The packet has access to port 2 and port 3. The outgoing packet is stripped of its tag to leave port 2 as an untagged packet. For port 3, the outgoing packet leaves as a tagged packet with VLAN ID 10.
  - If a tagged packet with VLAN ID 10 enters port 3, the packet has access to port 1 and port 2. If the packet leaves port 1 or port 2, it is stripped of its tag to leave the switch as an untagged packet.

- If an untagged packet enters port 4, the switch tags it with VLAN ID 20. The packet has access to port 5 and port 6. The outgoing packet is stripped of its tag to become an untagged packet as it leaves port 6. For port 5, the outgoing packet leaves as a tagged packet with VLAN ID 20.

## Access Control Lists

Access control lists (ACLs) ensure that only authorized users can access specific resources while blocking off any unwarranted attempts to reach network resources.

ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and provide security for the network. ACLs are normally used in firewall routers that are positioned between the internal network and an external network, such as the Internet. They can also be used on a router positioned between two parts of the network to control the traffic entering or exiting a specific part of the internal network. The added packet processing required by the ACL feature does not affect switch performance. That is, ACL processing occurs at wire speed.

Access lists are a sequential collection of permit and deny conditions. This collection of conditions, known as the filtering criteria, is applied to each packet that is processed by the switch or the router. The forwarding or dropping of a packet is based on whether or not the packet matches the specified criteria.

Traffic filtering requires the following two basic steps:

1. Create an access list definition.

The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. Additionally, you can assign traffic that matches the criteria to a particular queue or redirect the traffic to a particular port. A default *deny all* rule is the last rule of every list.

2. APPLY the access list to an interface in the inbound direction.

The managed switch allows ACLs to be bound to physical ports and LAGs. The switch software supports MAC ACLs and IP ACLs.

## MAC ACL Sample Configuration

The following example shows how to create a MAC-based ACL that permits Ethernet traffic from the Sales department on specified ports and denies all other traffic on those ports.

1. From the MAC ACL screen, create an ACL with the name Sales\_ACL for the Sales department of your network.

See [Create a MAC ACL](#) on page 347.

By default, this ACL is bound on the inbound direction, which means the switch examines traffic as it enters the port.

2. From the MAC Rules screen, create a rule for the Sales\_ACL with the following settings:

- ID: 1

- Action: Permit
- Assign Queue ID: 0
- Match Every: False
- CoS: 0
- Destination MAC: 01:02:1A:BC:DE:EF
- Destination MAC Mask: 00:00:00:00:FF:FF
- EtherType User Value:
- Source MAC: 02:02:1A:BC:DE:EF
- Source MAC Mask: 00:00:00:00:FF:FF
- VLAN ID: 2

For more information about MAC ACL rules, see [Configure MAC Rules](#) on page 349.

3. From the MAC Binding Configuration screen, assign the Sales\_ACL to the interface gigabit ports 6, 7, and 8, and then click the **APPLY** button.

See [Configure ACL MAC Binding](#) on page 351.

You can assign an optional sequence number to indicate the order of this access list relative to other access lists if any are already assigned to this interface and direction.

4. The MAC Binding Table displays the interface and MAC ACL binding information.

See [View or Delete MAC Bindings](#) on page 353.

The ACL named Sales\_ACL looks for Ethernet frames with destination and source MAC addresses and MAC masks defined in the rule. Also, the frame must be tagged with VLAN ID 2, which is the Sales department VLAN. The CoS value of the frame must be 0, which is the default value for Ethernet frames. Frames that match this criteria are permitted on interfaces 6, 7, and 8 and are assigned to the hardware egress queue 0, which is the default queue. All other traffic is explicitly denied on these interfaces. To allow additional traffic to enter these ports, you must add a new *permit* rule with the desired match criteria and bind the rule to interfaces 6, 7, and 8.

## Standard IP ACL Example Configuration

The following example shows how to create an IP-based ACL that prevents any IP traffic from the Finance department from being allowed on the ports that are associated with other departments. Traffic from the Finance department is identified by each packet's network IP address.

1. From the IP ACL screen, create a new IP ACL with an IP ACL ID of 1.

See [Configure an IP ACL](#) on page 354).

2. From the IP Rules screen, create a rule for IP ACL 1 with the following settings:

- Rule ID: 1
- Action: Deny
- Assign Queue ID: 0 (optional: 0 is the default value)

- Match Every: False
- Source IP address: 192.168.187.0
- Source IP Mask: 255.255.255.0

For additional information about IP ACL rules, see [Configure Rules for an IP ACL](#) on page 355.

3. Click the **ADD** button.
4. From the IP Rules screen, create a second rule for IP ACL 1 with the following settings:
  - Rule ID: 2
  - Action: Permit
  - Match Every: True
5. Click the **ADD** button.
6. From the IP Binding Configuration screen, assign ACL ID 1 to the interface gigabit ports 2, 3, and 4, and assign a sequence number of 1.

See [Configure ACL Interface Bindings](#) on page 365.

By default, this IP ACL is bound on the inbound direction, so it examines traffic as it enters the switch.

7. Click the **APPLY** button.
8. Use the IP Binding Table screen to view the interfaces and IP ACL binding information.

See [View or Delete IP ACL Bindings](#) on page 366.

The IP ACL in this example matches all packets with the source IP address and subnet mask of the Finance department's network and deny it on the Ethernet interfaces 2, 3, and 4 of the switch. The second rule permits all non-Finance traffic on the ports. The second rule is required because there is an explicit *deny all* rule as the lowest-priority rule.

## Differentiated Services (DiffServ)

Standard IP-based networks are designed to provide *best effort* data delivery service. *Best effort* service implies that the network deliver the data in a timely fashion, although the environment can affect performance. During times of congestion, packets might be delayed, sent sporadically, or dropped. For typical Internet applications, such as email and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. However, any degradation of service has undesirable effects on applications with strict timing requirements, such as voice or multimedia.

Quality of Service (QoS) can provide consistent, predictable data delivery by distinguishing between packets with strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given special treatment in a QoS-capable network. With this in mind, all elements of the network must be QoS-capable. If one node is unable to meet the necessary timing requirements, this creates a deficiency in the network path and the performance of the entire packet flow is compromised.

There are two basic types of QoS:

- **Integrated Services:** Network resources are apportioned based on request and are reserved (resource reservation) according to network management policy (RSVP, for example).
- **Differentiated Services:** Network resources are apportioned based on traffic classification and priority, giving preferential treatment to data with strict timing requirements.

The managed switch support DiffServ.

The DiffServ feature contains a number of conceptual QoS building blocks you can use to construct a differentiated service network. Use these same blocks in different ways to build other types of QoS architectures.

There are 3 key QoS building blocks needed to configure DiffServ:

- Class
- Policy
- Service (for example, the assignment of a policy to a directional interface)

## Class

You can classify incoming packets at Layers 2, 3 and 4 by inspecting the following information for a packet:

- Source/destination MAC address
- EtherType
- Class of Service (802.1p priority) value (first/only VLAN tag)
- VLAN ID range (first/only VLAN tag)
- Secondary 802.1p priority value (second/inner VLAN tag)
- Secondary VLAN ID range (second/inner VLAN tag)
- IP service type octet (also known as: ToS bits, precedence value, DSCP value)
- Layer 4 protocol (TCP, UDP, and so on)
- Layer 4 source/destination ports
- Source/destination IP address

From a DiffServ point of view, there are two types of classes:

- DiffServ traffic classes
- DiffServ service levels/forwarding classes

## DiffServ Traffic Classes

With DiffServ, you define which traffic classes to track on an ingress interface. You can define simple BA classifiers (DSCP) and a wide variety of multifield (MF) classifiers:

- Layer 2; Layers 3, 4 (IP only)

- Protocol-based
- Address-based

You can combine these classifiers with logical AND or OR operations to build complex MF classifiers (by specifying a class type of *all* or *any*, respectively). That is, within a single class, multiple match criteria are grouped together as an AND expression or a sequential OR expression, depending on the defined class type. Only classes of the same type can be nested; class nesting does not allow for the negation (for example, *exclude* option) of the referenced class.

To configure DiffServ, you must define service levels, namely the forwarding classes/PHBs identified by a given DSCP value, on the egress interface. These service levels are defined by configuring BA classes for each.

## Creating Policies

Use DiffServ policies to associate a collection of classes that you configure with one or more QoS policy statements. The result of this association is referred to as a policy.

From a DiffServ perspective, there are two types of policies:

- **Traffic Conditioning Policy:** A policy applied to a DiffServ traffic class
- **Service Provisioning Policy:** A policy applied to a DiffServ service level

You must manually configure the various statements and rules used in the traffic conditioning and service provisioning policies to achieve the desired Traffic Conditioning Specification (TCS) and the Service Level Specification (SLS) operation, respectively.

## Traffic Conditioning Policy

Traffic conditioning pertains to actions performed on incoming traffic. There are several distinct QoS actions associated with traffic conditioning:

- **Dropping.** Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot co-exist on the same interface.
- **Marking IP DSCP or IP Precedence.** Marking/re-marking the DiffServ code point in a packet with the DSCP value representing the service level associated with a particular DiffServ traffic class. Alternatively, the IP Precedence value of the packet can be marked/re-marked.
- **Marking CoS (802.1p).** Sets the 3-bit priority field in the first/only 802.1p header to a specified value when packets are transmitted for the traffic class. An 802.1p header is inserted if it does not already exist. This is useful for assigning a Layer 2 priority level based on a DiffServ forwarding class (for example, DSCP or IP Precedence value) definition to convey some QoS characteristics to downstream switches that do not routinely look at the DSCP value in the IP header.
- **Policing.** A method of constraining incoming traffic associated with a particular class so that it conforms to the terms of the TCS. Special treatment can be applied to out-of-profile

packets that are either in excess of the conformance specification or are nonconformant. The DiffServ feature supports the following types of traffic policing treatments (actions):

- drop. The packet is dropped.
- mark cos. The 802.1p user priority bits are (re)marked and forwarded.
- mark dscp. The packet DSCP is (re)marked and forwarded.
- mark prec. The packet IP precedence is (re)marked and forwarded.
- send: The packet is forwarded without DiffServ modification.

**Color Mode Awareness.** Policing in the DiffServ feature uses either *color blind* or *color aware* mode. Color blind mode ignores the coloration (marking) of the incoming packet. Color aware mode takes into consideration the current packet marking when determining the policing outcome. An auxiliary traffic class is used in conjunction with the policing definition to specify a value for one of the 802.1p, Secondary 802.1p, IP DSCP, or IP Precedence fields designating the incoming color value to be used as the conforming color. The color of exceeding traffic can be optionally specified as well.

- **Counting.** Updating octet and packet statistics to keep track of data handling along traffic paths within DiffServ. In this DiffServ feature, counters are not explicitly configured by the user, but are designed into the system based on the DiffServ policy being created. See the Statistics section of this document for more details.
- **Assigning QoS Queue.** Directs traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.
- **Redirecting.** Forces classified traffic stream to a specified egress port (physical or LAG). This can occur in addition to any marking or policing action. It can also be specified along with a QoS queue assignment.

## DiffServ Example Configuration

➤ **To create a DiffServ class/policy and attach it to a switch interface:**

1. From the QoS Class Configuration screen, create a new class with the following settings:
  - Class Name: Class1
  - Class Type: All
 For more information, see [Configure a DiffServ Class](#) on page 247.
2. Click the Class1 hyperlink to view the DiffServ Class Configuration screen for this class.
3. Configure the following settings for Class1:
  - Protocol Type: UDP
  - Source IP Address: 192.12.1.0
  - Source Mask: 255.255.255.0
  - Source L4 Port: Other, and enter 4567 as the source port value
  - Destination IP Address: 192.12.2.0

- Destination Mask: 255.255.255.0
- Destination L4 Port: Other, and enter 4568 as the destination port value

For more information, see [Configure a DiffServ Class](#) on page 247.

4. Click the **APPLY** button.
5. From the Policy Configuration screen, create a new policy with the following settings:
  - Policy Selector: Policy1
  - Member Class: Class1

For more information, see [Configure DiffServ Policy](#) on page 254 .

6. Click the **ADD** button.

The new policy is added.

7. Click the Policy1 hyperlink to view the Policy Class Configuration screen for this policy.
8. Configure the policy attributes as follows:
  - Assign Queue: 3
  - Policy Attribute: Simple Policy
  - Color Mode: Color Blind
  - Committed Rate: 1000000 Kbps
  - Committed Burst Size: 128 KB
  - Confirm Action: Send
  - Violate Action: Drop

For more information, see [Configure DiffServ Policy](#) on page 254.

9. From the Service Configuration screen, select the check box next to interfaces g7 and g8 to attach the policy to these interfaces
10. Click the **APPLY** button.

See [Configure DiffServ Policy Settings on an Interface](#) on page 257.

All UDP packet flows destined to the 192.12.2.0 network with an IP source address from the 192.12.1.0 network that includes a Layer 4 source port of 4567 and destination port of 4568 from this switch on ports 7 and 8 are assigned to hardware queue 3.

On this network, traffic from streaming applications uses UDP port 4567 as the source and 4568 as the destination. This real-time traffic is time sensitive, so it is assigned to a high-priority hardware queue. By default, data traffic uses hardware queue 0, which is designated as a best-effort queue.

Also the *confirmed action* on this flow is to send the packets with a committed rate of 1000000 Kbps and burst size of 128 KB. Packets that violate the committed rate and burst size are dropped.

## 802.1X

Local area networks (LANs) are often deployed in environments that permit unauthorized devices to be physically attached to the LAN infrastructure, or permit unauthorized users to attempt to access the LAN through equipment already attached. In such environments, it might be desirable to restrict access to the services offered by the LAN to those users and devices that are permitted to use those services.

Port-based network access control makes use of the physical characteristics of LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics and of preventing access to that port in cases in which the authentication and authorization process fails. In this context, a port is a single point of attachment to the LAN, such as ports of MAC bridges and associations between stations or access points in IEEE 802.11 wireless LANs.

The IEEE 802.11 standard describes an architectural framework within which authentication and consequent actions take place. It also establishes the requirements for a protocol between the authenticator (the system that passes an authentication request to the authentication server) and the supplicant (the system that requests authentication), as well as between the authenticator and the authentication server.

The managed switches support a guest VLAN, which allows unauthenticated users limited access to the network resources.

---

**Note:** You can use QoS features to provide rate limiting on the guest VLAN to limit the network resources the guest VLAN provides.

---

Another 802.1X feature is the ability to configure a port to enable or disable EAPoL packet forwarding support. You can disable or enable the forwarding of EAPoL when 802.1X is disabled on the device.

The ports of an 802.1X authenticator switch provide the means by which it can offer services to other systems reachable through the LAN. Port-based network access control allows the operation of a switch's ports to be controlled in order to ensure that access to its services is permitted only by systems that are authorized to do so.

Port access control provides a means of preventing unauthorized access by supplicants to the services offered by a system. Control over the access to a switch and the LAN to which it is connected can be desirable in order to restrict access to publicly accessible bridge ports or to restrict access to departmental LANs.

Access control is achieved by enforcing authentication of supplicants that are attached to an authenticator's controlled ports. The result of the authentication process determines whether the supplicant is authorized to access services on that controlled port.

A port access entity (PAE) is able to adopt one of two distinct roles within an access control interaction:

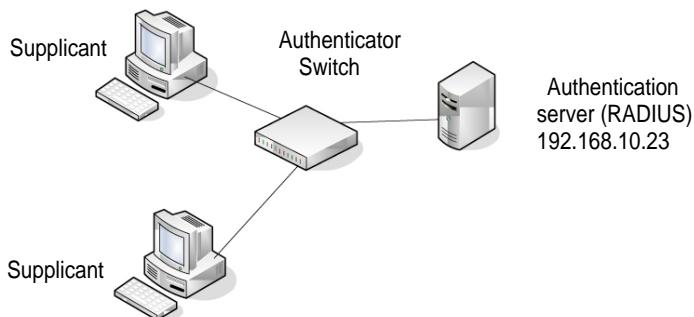
1. **Authenticator:** A port that enforces authentication before allowing access to services available through that port.
2. **Supplicant:** A port that attempts to access services offered by the authenticator.

Additionally, there exists a third role:

3. **Authentication server:** Performs the authentication function necessary to check the credentials of the supplicant on behalf of the authenticator.

All three roles are required in order to complete an authentication exchange.

The managed switches support the authenticator role only, in which the PAE is responsible for communicating with the supplicant. The authenticator PAE is also responsible for submitting the information received from the supplicant to the authentication server in order for the credentials to be checked, which determine the authorization state of the port. The Authenticator PAE controls the authorized/unauthorized state of the controlled port depending on the outcome of the RADIUS-based authentication process.



**Figure 1. 802.1X authenticator and supplicant roles**

## 802.1X Sample Configuration

This example shows how to configure the switch so that 802.1X-based authentication is required on the ports in a corporate conference room (1/0/5–1/0/8). These ports are available to visitors and must be authenticated before granting access to the network. The authentication is handled by an external RADIUS server. When the visitor is successfully authenticated, traffic is automatically assigned to the guest VLAN. This example assumes that a VLAN was configured with a VLAN ID of 150 and VLAN name of Guest.

1. From the Port Authentication screen, select ports 1/0/5, 1/0/6, 1/0/7 and 1/0/8.
2. From the Port Control menu, select Unauthorized.

The Port Control setting for all other ports where authentication is not needed should Authorized. When the Port Control setting is Authorized, the port is unconditionally put in a force-authorized state and does not require any authentication. When the Port Control setting is Auto, the authenticator PAE sets the controlled port mode

3. In the Guest VLAN field for ports 1/0/5–1/0/8, enter 150 to assign these ports to the guest VLAN.

You can configure additional settings to control access to the network through the ports. See [Port Security Interface Configuration](#) on page 287 for information about the settings.

4. Click the **APPLY** button.
5. From the 802.1X Configuration screen, set the Port Based Authentication State and Guest VLAN Mode to Enable, and then click the **APPLY** button.

Ssee [Port Security Configuration](#) on page 286.

This example uses the default values for the port authentication settings, but there are several additional settings that you can configure. For example, the EAPOL Flood Mode field allows you to enable the forwarding of EAPoL frames when 802.1X is disabled on the device.

6. From the RADIUS Server Configuration screen, configure a RADIUS server with the following settings:
  - Server Address: 192.168.10.23
  - Secret Configured: Yes
  - Secret: secret123
  - Active: Primary

For more information, see [RADIUS](#) on page 245.

7. Click the **ADD** button.
8. From the Authentication List screen, configure the default List to use RADIUS as the first authentication method.

Ssee [Set Up a Login Authentication List](#) on page 275.

This example enables 802.1X-based port security on managed switch and prompts the hosts connected on ports g5–g8 for an 802.1X-based authentication. The switch passes the authentication information to the configured RADIUS server.

## MSTP

Spanning Tree Protocol (STP) runs on bridged networks to help eliminate loops. If a bridge loop occurs, the network can become flooded with traffic. IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) supports multiple instances of Spanning Tree to efficiently channel VLAN traffic over different interfaces. Each instance of the Spanning Tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree, with slight modifications in the working but not the end effect (chief among the effects is the rapid transitioning of the port to the forwarding state).

The difference between the RSTP and the traditional STP (IEEE 802.1D) is the ability to configure and recognize full duplex connectivity and ports that are connected to end stations, resulting in rapid transitioning of the port to the rorwarding state and the suppression of topology change notification. These features are represented by the parameters *pointtopoint* and *edgeport*. MSTP is compatible to both RSTP and STP. It behaves appropriately to STP and RSTP bridges.

A MSTP bridge can be configured to behave entirely as a RSTP bridge or a STP bridge. So, an IEEE 802.1s bridge inherently also supports IEEE 802.1w and IEEE 802.1D.

The MSTP algorithm and protocol provide simple and full connectivity for frames assigned to any given VLAN throughout a bridged LAN comprising arbitrarily interconnected networking devices, each operating MSTP, STP, or RSTP. MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent Multiple Spanning Tree Instance (MSTI), within Multiple Spanning Tree (MST) Regions composed of LANs and or MSTP bridges. These regions and the other bridges and LANs are connected into a single Common Spanning Tree (CST). (IEEE DRAFT P802.1s/D13)

MSTP connects all bridges and LANs with a single Common and Internal Spanning Tree (CIST). The CIST supports the automatic determination of each MST region, choosing its maximum possible extent. The connectivity calculated for the CIST provides the CST for interconnecting these regions, and an Internal Spanning Tree (IST) within each region. MSTP ensures that frames with a given VLAN ID are assigned to one and only one of the MSTIs or the IST within the region, that the assignment is consistent among all the networking devices in the region and that the stable connectivity of each MSTI and IST at the boundary of the region matches that of the CST. The stable active topology of the bridged LAN with respect to frames consistently classified as belonging to any given VLAN thus simply and fully connects all LANs and networking devices throughout the network, though frames belonging to different VLANs can take different paths within any Region, per IEEE DRAFT P802.1s/D13.

All bridges, whether they use STP, RSTP, or MSTP, send information in configuration messages through bridge protocol data units (BPDUs) to assign port roles that determine each port's participation in a fully and simply connected active topology based on one or more spanning trees. The information communicated is known as the spanning tree priority vector. The BPDU structure for each of these different protocols is different. A MSTP bridge transmits the appropriate BPDU depending on the received type of BPDU from a particular port.

An MST region comprises one or more MSTP bridges with the same MST configuration identifier, using the same MSTIs, and without any bridges attached that cannot receive and transmit MSTP BPDUs. The MST configuration identifier has the following components:

- 1.** Configuration identifier format selector
- 2.** Configuration name
- 3.** Configuration revision level
- 4.** Configuration digest: 16-byte signature of type HMAC-MD5 created from the MST Configuration Table (a VLAN ID to MSTID mapping)

As there are multiple instances of Spanning Tree, there is an MSTP state maintained on a per-port, per-instance basis (or on a per-port, per-VLAN basis, as any VLAN can be in one and only one MSTI or CIST). For example, port A can be forwarding for instance 1 while discarding for instance 2. The port states changed since IEEE 802.1D specification.

To support multiple spanning trees, a MSTP bridge must be configured with an unambiguous assignment of VLAN IDs (VIDs) to spanning trees. This is achieved by ensure the following:

- 1.** The allocation of VIDs to FIDs is unambiguous.
- 2.** Each FID supported by the bridge is allocated to exactly one spanning tree instance.

The combination of VID to FID and then FID to MSTI allocation defines a mapping of VIDs to spanning tree instances, represented by the MST Configuration Table.

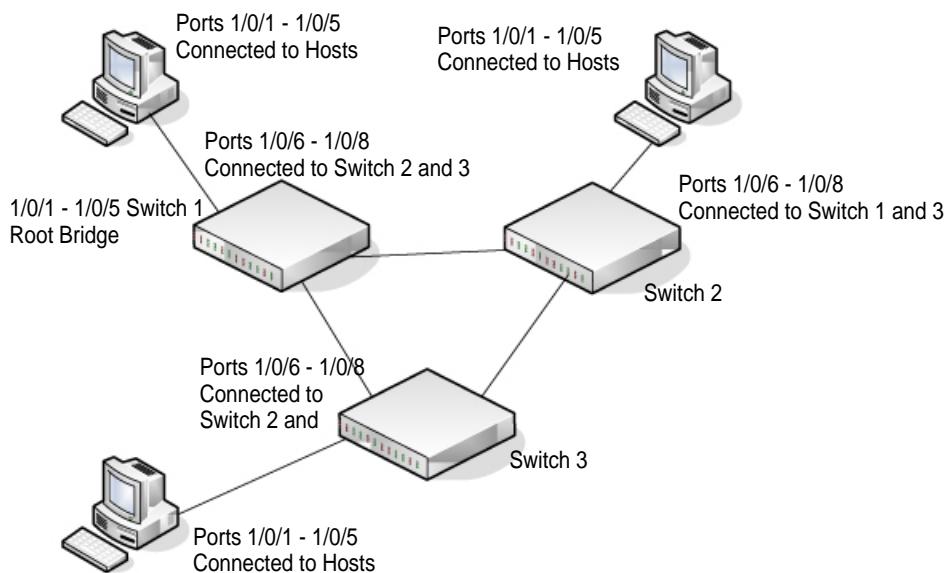
With this allocation we ensure that every VLAN is assigned to one and only one MSTI. The CIST is also an instance of spanning tree with a MSTID of 0.

An instance might occur that has no VIDs allocated to it, but every VLAN must be allocated to one of the other instances of spanning tree.

The portion of the active topology of the network that connects any two bridges in the same MST region traverses only MST bridges and LANs in that region, and never bridges of any kind outside the region, in other words, connectivity within the region is independent of external connectivity.

## MSTP Sample Configuration

This example shows how to create an MSTP instance from a switch. The example network has three different managed switches that serve different locations in the network. In this example, ports 1/0/1–1/0/5 are connected to host stations, so those links are not subject to network loops. Ports 1/0/6–1/0/8 are connected across switches 1, 2, and 3.



**Figure 2. MSTP configuration**

- **Perform the following procedures on each switch to configure MSTP:**
  1. Use the VLAN Configuration screen to create VLANs 300 and 500.  
See [VLAN Overview](#) on page 223.
  2. Use the VLAN Membership screen to include ports 1/0/1 - 1/0/8 as tagged (T) or untagged (U) members of VLAN 300 and VLAN 500.  
See [VLAN Overview](#) on page 223.

3. From the STP Configuration screen, enable the Spanning Tree State option.  
See *Spanning Tree Protocol Overview* on page 145.
4. Use the default values for the rest of the STP configuration settings.  
By default, the STP Operation Mode is MSTP and the configuration name is the switch MAC address.
5. From the CST Configuration screen, set the Bridge Priority value for each of the three switches to force Switch 1 to be the root bridge:
  - Switch 1: 4096
  - Switch 2: 12288
  - Switch 3: 20480

---

**Note:** Bridge priority values are multiples of 4096.

---

If you do not specify a root bridge and all switches use the same Bridge Priority value, the switch with the lowest MAC address is elected as the root bridge (see *Configure Common Spanning Tree* on page 150).

6. From the CST Port Configuration screen, select ports 1/0/1 - 1/0/8 and select Enable from the STP Status menu.  
See *Configure Common Spanning Tree* on page 150.
7. Click the **APPLY** button.
8. Select ports 1/0/1–1/0/5 (edge ports), and select Enable from the Fast Link menu.  
Since the edge ports are not at risk for network loops, ports with Fast Link enabled transition directly to the forwarding state.
9. Click the **APPLY** button.  
You can use the CST Port Status screen to view spanning tree information about each port.
10. From the MST Configuration screen, create an MST instances with the following settings:
  - MST ID: 1
  - Priority: Use the default (32768)
  - VLAN ID: 300For more information, see *Configure an MST Instance* on page 156.
11. Click the **ADD** button.
12. Create a second MST instance with the following settings:
  - MST ID: 2
  - Priority: 49152
  - VLAN ID: 500

**13.** Click the **ADD** button.

In this example, assume that Switch 1 has become the root bridge for MST instance 1, and Switch 2 has become the root bridge for MST instance 2. Switch 3 has hosts in the Sales department (ports 1/0/1, 1/0/2, and 1/0/3) and in the HR department (ports 1/0/4 and 1/0/5). Switches 1 and 2 also use hosts in the Sales and Human Resources departments. The hosts connected from Switch 2 use VLAN 500, MST instance 2 to communicate with the hosts on Switch 3 directly. Likewise, hosts of Switch 1 use VLAN 300, MST instance 1 to communicate with the hosts on Switch 3 directly.

The hosts use different instances of MSTP to effectively use the links across the switch. The same concept can be extended to other switches and more instances of MSTP.