



# **M6100, M5300, and M7100 Series Managed Switches**

User Manual

Version 11.0.0

April 2015  
202-11528-01

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, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice.

© NETGEAR, Inc. All rights reserved.

## Revision History

Publication Part Number	Publish Date	Comments
202-11528-01	April 2015	First publication



# Contents

## Chapter 1 Getting Started

Available Publications and Online Help .....	16
Register Your Product .....	16
Understanding the User Interfaces .....	16
Web Management Interface Overview .....	17
Software Requirements to Use the Web Interface .....	17
Use a Web Browser to Access the Switch and Log In .....	17
Web Interface Buttons and User-Defined Fields .....	18
Interface Naming Conventions .....	18
Online Help .....	19
Web Management Interface Device View .....	20
Using SNMP .....	21

## Chapter 2 Configure System Information

Initial Setup .....	24
Configure a Management VLAN .....	25
Configure the Initial Service Port Settings .....	27
View or Define System Information .....	28
View Backplane Information .....	31
View the Temperature Sensor Information .....	32
View the Fan Status .....	33
View the Device Status .....	34
View the System CPU Status .....	36
Configure the CPU Thresholds .....	37
View Switch Statistics .....	39
View USB Device Information .....	41
View Slot Information (M5300 only) .....	43
Configure a Loopback Interface .....	45
View the IPv6 Network Interface Neighbor Table .....	46
Configure the IPv4 Service Port .....	47
Configure the IPv6 Service Port .....	49
IPv4 Management VLAN Overview .....	51
Configure an IPv4 Management VLAN .....	51
Configure an IPv6 Management VLAN .....	53
Configure an IPv6 VLAN Interface .....	54
Time .....	56
Configure the Time Setting .....	56
Configure the SNTP Global Settings .....	57
View SNTP Global Status .....	60

Configure an SNTP Server.....	62
Configure Daylight Saving Time Settings .....	65
View the DayLight Saving Time Status .....	67
Configure DNS Settings .....	69
Configure Global DNS Settings.....	69
Add a Static Entry to the Local DNS Table.....	71
Configure the Switch Database Management Template Preference.....	72
Configure Green Ethernet Settings .....	74
Configure Green Ethernet Interface Settings.....	75
Configure Green Ethernet Local and Remote Devices .....	77
Configure Green Ethernet Remote Device Details.....	79
View the Green Ethernet Statistics Summary .....	80
Configure the Green Ethernet EEE LPI History.....	82
Licenses (M5300 only) .....	84
View License Keys for M5300 Series Switches .....	84
View License Features for M5300 Series Switches .....	85
Configure DHCP Server Settings .....	86
Configure DHCP Server .....	86
Configure the DHCP Pool .....	88
Configure DHCP Pool Options .....	91
View DHCP Server Statistics.....	92
View DHCP Bindings Information.....	93
View DHCP Conflicts .....	94
Configure the DHCP Relay.....	95
DHCP L2 Relay .....	97
Configure Global DHCP L2 Relay Settings .....	97
Configure a DHCP L2 Relay Interface .....	98
View DHCP L2 Relay Interface Statistics .....	99
Configure UDP Relay Global Settings .....	100
Configure UDP Relay Interface Settings .....	102
Enable or Disable DHCPv6 Server .....	104
Configure the DHCPv6 Pool .....	105
Configure the DHCPv6 Prefix Delegation.....	106
Configure DHCPv6 Interface Settings.....	107
View DHCPv6 Bindings Information .....	108
View DHCPv6 Server Statistics .....	110
Configure DHCPv6 Relay for an Interface .....	113
Configure Basic PoE .....	114
Configure PoE Settings.....	116
Configure PoE Ports .....	117
Configure SNMP .....	120
Configure the SNMP V1/V2 Community .....	120
Configure SNMP V1/V2 Trap Settings .....	122
Configure SNMP V1/V2 Trap Flags .....	123
View the Supported MIBs .....	125
Configure SNMP V3 Users.....	126
LLDP Overview .....	128
Configure LLDP Global Settings .....	128

Configure the LLDP Interface .....	129
View LLDP Statistics .....	130
View LLDP Local Device Information .....	132
View LLDP Remote Device Information .....	134
View LLDP Remote Device Inventory .....	135
Configure LLDP-MED Global Settings .....	136
Configure LLDP-MED Interface .....	137
View LLDP-MED Local Device Information .....	138
View LLDP-MED Remote Device Information .....	140
View LLDP-MED Remote Device Inventory .....	143
Configure ISDP .....	144
Configure ISDP Basic Global Settings .....	144
Configure ISDP Global Settings .....	145
Configure an ISDP Interface .....	147
View an ISDP Neighbor .....	147
View ISDP Statistics .....	149
Timer Schedule .....	150
Configure the Global Timer Settings .....	150
Configure the Timer Schedule .....	151

## **Chapter 3 Chassis and Stacking**

M6100 Series Switch Chassis Overview .....	155
Configure Basic Chassis Settings .....	155
View the Chassis Protocol Information .....	158
View Chassis Backplane-Port Configuration .....	161
View the Chassis Backplane-Port Packet-Path .....	162
Configure the Chassis Power Settings .....	164
Configure the System Power .....	165
Configure the Power Auto-Rebalance .....	166
View Blade Power Consumption .....	167
View Power Redundancy .....	168
View the Power Modules .....	169
View EPS Power Modules and EPS Ports .....	170
View the Power Matrix .....	172
Rebalance the Chassis Power .....	173
Configure Chassis Firmware Synchronization .....	174
View NSF Summary Data .....	175
View NSF Checkpoint Statistics .....	177
M5300 Series Switch Stacking Overview .....	178
Firmware Synchronization and Upgrade .....	179
Stack Configuration Maintenance .....	180
Stack Master Election .....	180
Stack Factory Defaults Reset Behavior .....	180
Stack NSF .....	181
Stack Configuration .....	182
Select a New Stack Master .....	182
Specify the Stack Sample Mode .....	183
Configure a Stack Member .....	183

View the Stack Status .....	187
Configure the mode of the Stack Ports.....	188
Run Stack Port Diagnostics .....	190
Configure Stack Firmware Synchronization .....	192

## **Chapter 4 Configure Switching Information**

Configure VLANs .....	195
Configure Basic VLAN Settings.....	195
Configure an Advanced VLAN.....	197
Configure an Internal VLAN.....	198
Configure VLAN Trunking .....	199
Configure VLAN Membership .....	201
View VLAN Status .....	203
Configure Port PVID Settings .....	204
Configure a MAC-Based VLAN.....	206
Configure Protocol-Based VLAN Groups .....	207
Configure Protocol-Based VLAN Group Membership.....	209
Configure an IP Subnet-Based VLAN.....	210
Configure a Port DVLAN .....	211
Configure a Voice VLAN.....	212
Configure GARP Switch Settings .....	214
Configure GARP Port .....	215
Auto-VoIP .....	216
Configure Protocol-Based Port Settings.....	216
Configure Auto-VoIP OUI-Based Properties .....	217
OUI-Based Port Settings .....	218
Configure the OUI Table.....	219
View the Auto-VoIP Status .....	221
iSCSI Overview .....	222
Configure Global iSCSI Settings .....	222
View iSCSI Sessions .....	224
Control iSCSI Target Settings .....	225
View iSCSI Sessions .....	226
View iSCSI Session Details.....	227
Spanning Tree Protocol.....	228
Configure Basic STP Settings .....	229
Configure Advanced STP Settings .....	231
Configure CST Settings .....	234
Configure CST Port Settings.....	236
View CST Port Status .....	238
Configure MST Settings.....	240
View the Spanning Tree MST Port Status .....	242
View STP Statistics .....	244
Configure PVST VLAN Settings.....	245
Configure the PVST Interface Settings .....	247
View PVST Statistics.....	249
Multicast.....	250

View the MFDB Table .....	250
View the MFDB Statistics .....	252
IGMP Snooping .....	253
Configure IGMP Snooping .....	254
Configure IGMP Snooping for Interfaces .....	255
Configure IGMP Snooping for VLANs .....	257
Configure a Multicast Router .....	258
Configure a Multicast Router VLAN .....	259
IGMP Snooping Querier Overview .....	260
Configure IGMP Snooping Querier .....	260
Configure IGMP Snooping Querier for VLANs .....	262
Configure MLD Snooping .....	263
Configure a MLD Snooping Interface .....	265
Configure MLD VLAN Settings .....	266
Enable or Disable a Multicast Router on an Interface .....	267
Configure Multicast Router VLAN Settings .....	268
Configure MLD Snooping Querier .....	269
Configure MLD Snooping Querier VLAN Settings .....	271
Configure MVR .....	272
Configure Basic MVR Settings .....	272
Configure Advanced MVR Settings .....	274
Configure an MVR Group .....	275
Configure an MVR Interface .....	276
Configure MVR Group Membership .....	277
View MVR Statistics .....	278
MAC Address Table .....	280
Configure the MAC Address Table .....	280
Set the Dynamic Address Aging Interval .....	281
Configure a Static MAC Address .....	282
Port Settings .....	283
Configure Port Settings .....	283
Configure Port Descriptions .....	286
View Port Transceiver Information .....	287
Link Aggregation Groups .....	288
Configure LAG Settings .....	289
Configure LAG Membership .....	291
Configure the Virtual Port-Channel Global Settings .....	293
Configure the Keep-Alive Parameters .....	296
View the VPC Peer Link Settings .....	298
Configure the Peer Link Settings .....	299
Configure the Peer Detection Settings .....	300
Configure the Virtual Port Channel Interface .....	302
View Virtual Port Channel Interface Details .....	304
View Virtual Port Channel Interface Details .....	305
View Virtual Port Channel Keep-Alive Statistics .....	306
View Virtual Port Channel Peer Link Statistics .....	308
Multiple Registration Protocol Overview .....	310
Configure Global MRP Settings .....	311

Configure MRP Port Settings .....	313
View MMRP Statistics .....	315
View MVRP Statistics .....	316

## **Chapter 5 Routing**

Manage Routes .....	319
Configure a Basic Route .....	319
Configure Advanced Routes .....	321
Specify Route Preferences .....	323
Configure the Router IP .....	325
View Statistics .....	327
Configure Routing Parameters for the Switch .....	330
View IP Statistics .....	332
Configure the IP Interface .....	336
Configure the Secondary IP Address .....	339
IPv6 .....	340
Configure IPv6 Global Settings .....	340
View the IPv6 Route Table .....	341
Configure IPv6 Interface Settings .....	343
IPv6 Prefix Configuration .....	345
View IPv6 Statistics .....	347
View the IPv6 Neighbor Table .....	351
IPv6 Static Route Configuration .....	353
Configure the IPv6 Route Table .....	354
IPv6 Route Preferences .....	355
Configure IPv6 Tunnels .....	357
VLAN Overview .....	358
Use the VLAN Static Routing Wizard .....	359
Configure VLAN Routing .....	360
Address Resolution Protocol Overview .....	361
Configure Basic ARP Cache .....	362
Add an Entry to the ARP Table .....	363
View or Configure the ARP Table .....	365
Configure RIP .....	367
Enable RIP .....	367
Configure RIP Settings .....	368
Configure Advanced RIP Interface Settings .....	370
Route Redistribution .....	372
Configure Router Discovery .....	375
Configure Virtual Router Redundancy Protocol .....	376
Configure Global VRRP Settings .....	376
Configure Advanced VRRP Settings .....	378
Configure an Advanced VRRP Secondary IP Address .....	380
Configure an Advanced VRRP Tracking Interface .....	381
View Advanced VRRP Statistics .....	383

## Chapter 6 OSPF and OSPFv3

OSPF .....	387
Configure Basic OSPF Settings .....	387
Configure the OSPF Default Route Advertise Settings .....	388
Configure OSPF Settings .....	390
Configure the OSPF Common Area ID .....	394
Configure the OSPF Stub Area .....	395
Configure the OSPF NSSA Area .....	397
Configure the OSPF Area Range .....	399
Configure the OSPF Interface .....	400
View OSPF Statistics for an Interface .....	405
View the OSPF Neighbor Table .....	408
View the OSPF Link State Database .....	410
Configure the OSPF Virtual Link .....	414
Configure the OSPF Route Redistribution .....	418
View the NSF OSPF Summary .....	420
OSPFv3 .....	422
Configure Basic OSPFv3 Settings .....	422
Configure OSPFv3 Default Route Advertise Settings .....	423
Configure the Advanced OSPFv3 Settings .....	424
Configure the OSPFv3 Common Area .....	427
Configure an OSPFv3 Stub Area .....	428
Configure the OSPFv3 NSSA Area .....	430
Configure the OSPFv3 Area Range .....	433
Configure the OSPFv3 Interface .....	434
View OSPFv3 Interface Statistics .....	437
View the OSPFv3 Neighbor Table .....	440
View the OSPFv3 Link State Database .....	442
Configure the OSPFv3 Virtual Link .....	445
Configure OSPFv3 Route Redistribution .....	448
View the NSF OSPFv3 Summary .....	449

## Chapter 7 Multicast Routing

Multicast Overview .....	453
View the Multicast Mroute Table .....	453
Configure Global Multicast Settings .....	454
Configure the Multicast Interface .....	456
Configure Global Multicast DVMRP Settings .....	457
Configure the DVMRP Interface .....	458
View the DVMRP Neighbor .....	459
View the DVMRP Next Hop Settings .....	461
View the Multicast DVMRP Prune .....	462
View the DVMRP Route .....	463
Configure Multicast IGMP Settings .....	464
Configure IGMP Global Settings .....	464
Configure the IGMP Routing Interface .....	465
View IGMP Routing Interface Statistics .....	467

View the IGMP Groups . . . . .	468
View the IGMP Membership . . . . .	470
Configure the IGMP Proxy Interface . . . . .	471
View the IGMP Proxy Interface Statistics . . . . .	473
View the IGMP Proxy Membership . . . . .	474
Configure PIM Settings . . . . .	475
Configure the Multicast PIM Global Settings . . . . .	476
Configure PIM SSM Settings . . . . .	476
Configure PIM Interface . . . . .	477
View the PIM Neighbor . . . . .	479
View the PIM Candidate Rendezvous Point . . . . .	480
View the PIM Neighbor . . . . .	481
Configure the PIM Candidate Rendezvous Point . . . . .	482
Configure the PIM Bootstrap Router Candidate . . . . .	483
Configure the PIM Static Rendezvous Point . . . . .	485
Configure Multicast Static Routes . . . . .	486
Configure the Multicast Admin Boundary . . . . .	487
Configure IPv6 Multicast Settings . . . . .	488
View the IPv6 Multicast Mroute Table . . . . .	488
Configure the IPv6 PIM Global Settings . . . . .	489
Configure IPv6 PIM SSM . . . . .	490
Configure the IPv6 PIM Interface . . . . .	491
View the IPv6 PIM Neighbor . . . . .	493
Configure the IPv6 PIM Candidate Rendezvous Point . . . . .	494
Configure the IPv6 PIM Bootstrap Router Candidate Settings . . . . .	495
Configure the IPv6 PIM Static Rendezvous Point . . . . .	496
Configure IPv6 MLD Global Settings . . . . .	497
Configure the IPv6 MLD Routing Interface . . . . .	498
View IPv6 MLD Routing Interface Statistics . . . . .	500
View the IPv6 MLD Groups . . . . .	501
View IPv6 MLD Traffic . . . . .	503
Configure the IPv6 MLD Proxy Interface . . . . .	504
View IPv6 MLD Proxy Interface Statistics . . . . .	506
View the IPv6 MLD Proxy Membership . . . . .	507
Configure IPv6 Multicast Static Routes . . . . .	508

## **Chapter 8 Configure Quality of Service**

QoS Overview . . . . .	511
Class of Service . . . . .	511
Configure Global CoS Settings . . . . .	512
Map 802.1p Priorities to Queues . . . . .	513
Map DSCP Values to Queues . . . . .	514
Configure CoS Interface Settings for an Interface . . . . .	515
Configure CoS Queue Settings for an Interface . . . . .	517
Configure CoS Drop Precedence Settings . . . . .	518
Differentiated Services Overview . . . . .	520
DiffServ Wizard Overview . . . . .	520



Use the DiffServ Wizard .....	521
Configure Basic DiffServ Settings .....	522
Configure the Global DiffServ Settings.....	524
Configure a DiffServ Class .....	526
Configure DiffServ IPv6 Class Settings.....	530
Configure DiffServ Policy .....	533
Configure the DiffServ Service Interface .....	536
View DiffServ Service Statistics.....	537

## **Chapter 9   Manage Device Security**

Management Security Settings.....	541
Configure Users.....	541
Configure a User Password .....	542
Enable Password Configuration .....	544
Configure a Line Password.....	544
RADIUS Overview .....	545
Configure Global RADIUS Server Settings .....	546
Configure a RADIUS Server.....	548
Configure RADIUS Accounting Servers.....	550
TACACS Overview.....	552
Configure Global TACACS Settings.....	553
Configure TACACS Server Settings .....	554
Configure a Login Authentication List .....	555
Configure an Enable Authentication List .....	556
Configure the Dot1x Authentication List .....	558
Configure an HTTP Authentication List .....	559
Configure an HTTPS Authentication List.....	560
View Login Sessions .....	561
Configure Management Access.....	562
Configure HTTP Server Settings .....	562
HTTPS Configuration .....	564
Manage Certificates .....	566
Download Certificates .....	567
Configure SSH Settings .....	568
Manage Host Keys .....	571
Download Host Keys.....	572
Configure Telnet Settings .....	574
Configure the Telnet Authentication List.....	574
Configure the Console Port.....	577
Configure Denial of Service Settings.....	578
Configure an Access Control Profile.....	581
Configure Access Rule Settings.....	582
Port Authentication.....	584
Configure Global 802.1X Settings.....	584
Configure 802.1X Settings.....	586
Configure Port Authentication .....	587
View the Port Summary.....	590
View the Client Summary .....	593

Traffic Control .....	594
Configure MAC Filtering .....	594
MAC Filter Summary .....	596
Port Security .....	597
Configure the Global Port Security Mode .....	597
Configure a Port Security Interface .....	598
Convert Learned MAC Addresses to Static Addresses .....	600
Configure a Static MAC Address .....	601
Configure a Private Group .....	602
Configure Private Group Membership .....	603
Configure Protected Ports .....	604
Configure a Private VLAN .....	605
Configure Private VLAN Association Settings .....	606
Configure the Private VLAN Port Mode .....	607
Configure a Private VLAN Host Interface .....	608
Configure a Private VLAN Promiscuous Interface .....	610
Storm Control .....	611
Configure Global Storm Control Settings .....	611
Configure a Storm Control Interface .....	612
DHCP Snooping .....	614
Configure DHCP Snooping Global Settings .....	614
Configure a DHCP Snooping Interface .....	615
Configure DHCP Snooping Binding .....	616
Configure Snooping Persistent Settings .....	618
View DHCP Snooping Statistics .....	619
Configure an IP Source Guard Interface .....	620
Configure IP Source Guard Binding Settings .....	621
Configure IPv6 Source Guard Interface Settings .....	623
Configure IPv6 Source Guard Binding .....	624
Configure Dynamic ARP Inspection .....	625
Configure a DAI VLAN .....	626
Configure the DAI Interface .....	628
Configure a DAI ACL .....	629
Configure a DAI ACL Rule .....	630
View DAI Statistics .....	631
Captive Portal .....	632
Configure Captive Portal Global Settings .....	632
Add a Captive Portal Instance .....	635
Configure CP Binding .....	638
View the Captive Portal Binding Table .....	639
Configure a Captive Portal Group .....	640
Configure Captive Portal User Settings .....	641
Configure the Captive Portal Trap Flag Settings .....	643
View the Captive Portal Client .....	644
Configure Access Control Lists .....	645
Use the ACL Wizard to Create a Simple ACL .....	645
Configure an ACL Based on Destination MAC Address .....	647
Use the ACL Wizard to Complete the Destination MAC ACL .....	649

Configure a Basic MAC ACL .....	649
Configure MAC ACL Rules .....	651
Configure MAC Binding .....	654
View or Delete MAC ACL Bindings in the MAC Binding Table .....	655
Configure an IP ACL .....	656
Configure Rules for an IP ACL .....	658
Configure Rules for an Extended IP ACL .....	660
Configure IPv6 ACL .....	665
Configure IPv6 Rules .....	667
Configure IP ACL Interface Bindings .....	671
View or Delete IP ACL Bindings in the IP ACL Binding Table .....	673
View or Delete VLAN ACL Bindings in the VLAN Binding Table .....	674

## **Chapter 10 Monitor the System**

View Port Statistics .....	677
View Detailed Port Statistics .....	678
View EAP Statistics .....	685
Perform a Cable Test .....	687
Manage Logs .....	688
View Buffered Logs .....	688
Configure Buffered Logs .....	689
Message Log Format .....	690
Enable or Disable the Command Log .....	690
Enable or Disable Console Logging .....	691
Configure Syslog Host Settings .....	692
View the Trap Logs .....	694
View the Event Log .....	695
Configure Persistent Logs (M5300 and M7100 only) .....	697
Format of the Messages .....	698
Configure Multiple Port Mirroring .....	699
Configure RSPAN VLAN .....	701
Configure an RSPAN Source Switch .....	702
Configure the RSPAN Destination Switch .....	704
Configure sFlow .....	705
Configure Basic sFlow Agent Information .....	705
Configure sFlow Agent Advanced Settings .....	707
Configure an sFlow Receiver .....	708
Configure the sFlow Interface .....	710

## **Chapter 11 Maintenance**

Save the Configuration .....	713
Configure Auto Save Mode .....	713
Reboot the Switch .....	714
Power Cycle the Switch .....	715
Reset the Switch to Its Factory Default Settings .....	716
Reset All User Passwords to Their Default Settings .....	717
Upload a File from the Switch .....	718

Upload a File to the TFTP Server .....	718
HTTP File Upload .....	720
Upload a File from the Switch to a USB Device .....	721
Download a File to the Switch .....	722
Download a File .....	723
Download a File to the Switch Using HTTP .....	725
Download a File from a USB Device .....	727
File Management .....	728
Copy an Image .....	729
Configure Dual Image Settings .....	729
Troubleshooting .....	731
Ping IPv4 .....	731
Ping IPv6 .....	733
Traceroute IPv4 .....	734
Traceroute IPv6 .....	737
Perform a Full Memory Dump .....	739

## **Appendix A Default Settings**

## **Appendix B Configuration Examples**

Virtual Local Area Networks (VLANs) .....	745
VLAN Configuration Examples .....	746
Access Control Lists (ACLs) .....	747
MAC ACL Sample Configuration .....	747
Standard IP ACL Sample Configuration .....	748
Differentiated Services (DiffServ) .....	749
Class .....	750
DiffServ Traffic Classes .....	750
Creating Policies .....	751
DiffServ Example Configuration .....	752
802.1X .....	753
802.1X Example Configuration .....	755
MSTP .....	756
MSTP Example Configuration .....	758

## **Appendix C Acronyms and Abbreviations**

# Getting Started

---

# 1

This chapter provides an overview of starting your NETGEAR M6100/M7100/M5300 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:

- *M6100/M7100/M5300 Chassis Hardware Installation Guide.*
- *M6100/M7100/M5300 Switch Module Installation Guide.*
- *M6100/M7100/M5300 Software Setup Manual.*
- *M6100/M7100/M5300 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**.
- *M6100/M7100/M5300 Command Line Interface Manual.*

Refer to the *M6100/M7100/M5300 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.

- *M6100/M7100/M5300 Software Administration Manual.*

When you log into the web management interface, online help is available. See [Online Help](#) on page 19.

## 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 *M6100, M5300, and M7100 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 switch 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>Update</b>	Clicking the <b>Update</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.

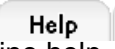


The following table describes the naming convention for all interfaces available on the switch.

**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.

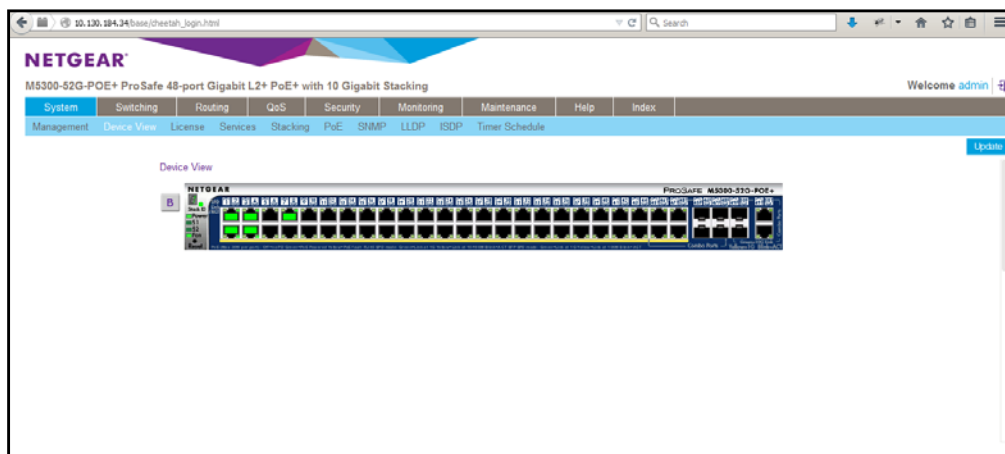
5. Enter the user name and password.

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**.

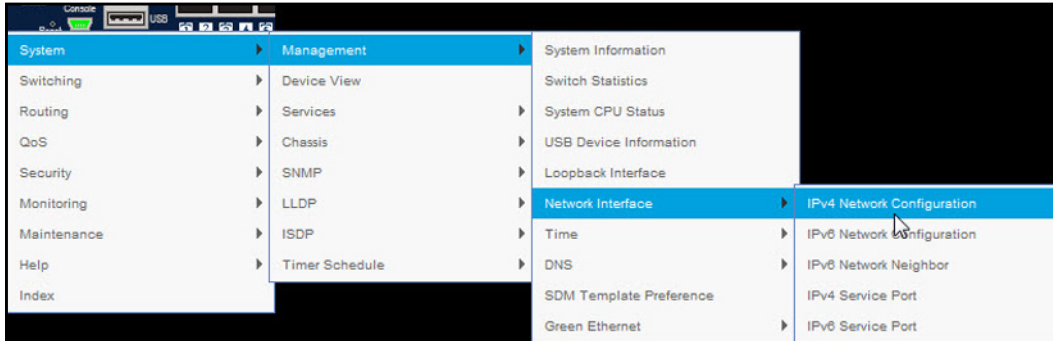


The port coloring indicates whether a port is currently active. Green indicates that the port is enabled; red indicates that an error occurred on the port, or that the link is disabled.

8. 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 use 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 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** list. 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.

## 2. Configure System Information

---

This chapter covers the following topics:

- *Initial Setup*
- *Licenses (M5300 only)*
- *Configure DHCP Server Settings*
- *Configure Basic PoE*
- *Configure SNMP*
- *LLDP Overview*
- *Configure ISDP*
- *Timer Schedule*

## Initial Setup

When you log in to a switch that has its factory settings, the Initial Setup screen displays.

➤ **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. Enter the new password for the Admin account in the **Admin Password** field.

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. In the **System Name** field, type the name to identify this switch.

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

11. In the **System Location** field, type 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** field, select **Enable** or **Disable**.

This specifies the state of the SNTP client. The default value is Disable, 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. In the **Designated Source Interface** list, select **Management VLAN** or **Service Port**.

This is the source interface that is 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 select Management VLAN as the source interface, the routing mode for the selected VLAN must be enabled.

16. Click the **Apply** button.

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

## Configure a Management VLAN

### ➤ To do the initial Management 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 **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:

Routing Mode: ☒ Enable ☐ Disable

IPv4 Address Assignment: ☒ Static ☐ DHCP

IPv6 Address Assignment: ☒ Auto Config ☐ DHCPv6 ☐ Static

IP Address:  Subnet Mask:  Gateway:

IPv6 Prefix/Length:  Gateway:

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.

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

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 VLAN1 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/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.

15. Select an **IPv6 Address Assignment** radio button.

This specifies the method for getting IPv6 network parameters (IPv6 prefix and prefix length) for the configured management VLAN interface. The possible options are **DHCPv6**, **Auto Config**, or **Static**. The default value for VLAN1 is Auto Config.

16. In the **IPv6 Prefix and Prefix Length** field, specify the prefix length for the management VLAN interface.



When Auto Config is selected, the appropriate IPv6 prefix and prefix length is displayed in this field.

17. In the IPv6 **Gateway** field, specify the default IPv6 gateway for the management VLAN interface.

18. Click the **Apply** button.

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

## Configure the Initial Service Port Settings

### ➤ To do the initial service port 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. Click **System > Management > Initial Setup**.

The Initial Setup screen displays.

8. Scroll down to the bottom of the screen to display the Service Port Configuration section.

9. Select an **IPv4 Address Assignment** radio button.

This specifies the method for getting IPv4 network parameters (IPv4 address and network mask) for the service port. Possible options are **DHCP**, **BootP**, or **Static**. The default value is Static.

10. Specify the **IP Address** for the service port.

The factory default value is 169.254.101.100.

11. Specify the **Subnet Mask** for the service port.

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. The factory default value is 255.255.255.0.

12. Specify the default **Gateway** for the service port.

The default value is 0.0.0.0.

13. In the **IPv6 Address Assignment** field, select the method for getting IPv6 network parameters (IPv6 prefix and prefix length) for the configured service port.

Possible options are **DHCPv6**, **Auto Config**, or **Static**. The default value is Auto Config.

14. Specify the **IPv6 Prefix and Prefix Length** for the service port.

When Auto Config is selected, the appropriate IPv6 prefix and prefix length are displayed in this field.

15. Specify the default IPv6 **Gateway** for the service port.

16. Click the **Apply** button.

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

## View or Define System Information

When you log in, the System Information screen displays. You can configure and view general device information.

### ➤ To view or 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.

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**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer Schedule

Management	System Information
• <b>System Information</b>	Product Name NETGEAR ProSafe M6100 Chassis Switch, 11.0.0.1, 1.0.0.9
• System CPU Status	System Name <input type="text"/>
• Switch Statistics	System Location <input type="text"/>
• USB Device Information	System Contact <input type="text"/>
• Loopback Interface	Login Timeout <input type="text" value="5"/> (0 to 160) mins
• Management Interfaces	Management Interface <input type="text" value="Different"/>
• Time	IPv4 Management VLAN Interface <a href="#">169.254.100.100/255.255.0.0</a>
• DNS	IPv6 Management VLAN Interface <a href="#">fe80::220c:c8ff:fe4d:95db/64</a>
• SDM Template Preference	Management VLAN ID <input type="text" value="1"/>
• Green Ethernet	IPv4 Service Port Network Interface <a href="#">10.130.84.23/255.255.255.128</a>
	IPv6 Service Port Network Interface <a href="#">fe80::220c:c8ff:fe4d:95db/64</a>
	IPv4 Loopback Interface
	IPv6 Loopback Interface
	System Date Jan 1 11:39:29 1970 (UTC+0:00)
	System Up Time 0 days 11 hours 39 mins 29 secs
	Current SNMP Sync Status Other
	System SNMP OID 1.3.6.1.4.1.4526.100.9.6.4
	System MAC Address 20:0C:C8:4D:95:D8
	Service Port MAC Address 20:0C:C8:4D:95:D9
	L2 MAC Address 20:0C:C8:4D:95:DA
	L3 MAC Address 20:0C:C8:4D:95:DB
	Supported Java Plugin Version 1.6
	Current SNMP Synchronized Time SNTP Last Attempt Status Is Not Successful

## 8. Define the following fields:

- **System Name.** Enter the 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 255 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 minutes. The factory default is 5. Entering 0 disables the time-out.
- **Management Interface.** Select the management interface that is 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.** For some application from the list, the source interface is configured separately. They display in the list only if this is the case.

By default VLAN 1 is used as the source interface.

9. Click the **Apply** button.

The updated configuration is sent to the switch and takes effect immediately. These changes are not retained across a power cycle unless a save is performed.

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

**Table 3. System Information**

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.
IPv6 Management VLAN Interface	The IPv6 prefix and prefix length 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 configuration screen.
IPv4 Service Port Network Interface	The IPv4 address and mask assigned to the service port interface.
IPv6 Service Port Network Interface	The IPv6 prefix and prefix length assigned to the service port interface.
IPv4 Loopback Interface	The IPv4 address and mask assigned to the loopback interface.
IPv6 Loopback Interface	The IPv6 prefix and prefix length 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	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.
Service Port MAC Address	The MAC address used for out-of-band connectivity.
L2 MAC Address	The MAC address used for communications on the Layer 2 network segment.
L3 MAC Address	The MAC address used for communications on the Layer 3 network segment.
Supported Java Plugin Version	The supported version of Java plug-in.
Current SNTP Synchronized Time	The SNTP synchronized time.

## View Backplane Information

➤ **To view backplane 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 > System Information > Backplane Information**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance		
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer Schedule

Management	Backplane Information	
• System Information	Model Identifier	XCM8903
• System CPU Status	FPGA Version	0x0
• Switch Statistics	Serial Number	00000000000000
• USB Device Information		

The following table describes the information displayed.

**Table 4. Backplane Information**

Field	Description
Model Identifier	The model identifier
FPGA Version	The FPGA version
Serial Number	The serial number

## View the Temperature Sensor Information

You can view the current temperature of the temperature sensors. The temperature is instant and can be updated with the latest information on the switch when the **Update** button is clicked. The maximum temperature of the temperature sensors depends on the actual hardware.

➤ **To view temperature 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.

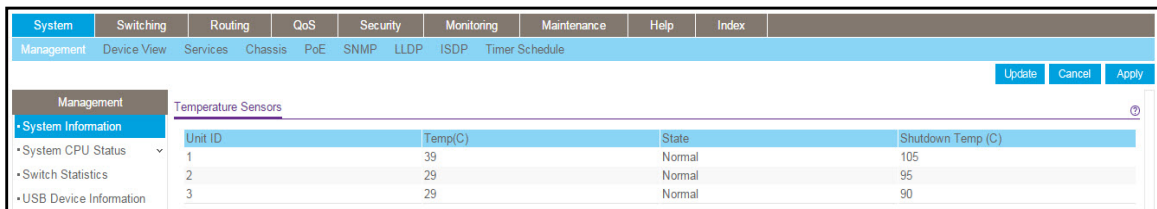
5. Enter the user name and password.

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 > System Information > Temperature Sensors**.



Unit ID	Temp(C)	State	Shutdown Temp (C)
1	39	Normal	105
2	29	Normal	95
3	29	Normal	90

To refresh the screen, click the **Update** button.

The following table describes the nonconfigurable Temperature Status information.

**Table 5. Temperature Status information**

Field	Description
Unit ID	The unit number in the chassis.
Temp (C)	The temperature of the specified unit in degrees Centigrade.
State	The unit temperature state.
Shutdown Temp (C)	The shutdown temperature value. Once the blade exceeds this limit, the chassis shuts down the the power for this blade.

## View the Fan Status

This screen shows 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 **Management > System Information > Fan Status**.

FAN	Type	Speed	Duty Level(%)	State
1	Removable	12750	30	Operational
2	Removable	12750	30	Operational
3	Removable	12750	30	Operational

Fan status has three possible values: **OK**, **Failure**, and **Not Present**.

The following table describes the nonconfigurable Fan Status information.

To refresh the screen, click the **Update** button.

**Table 6. Fan Status**

Field	Description
Fan	The fan index used to identify the fan for the given chassis member.
Type	Specifies whether the fan module is fixed or removable.
Speed	The fan speed.
Duty Level	The duty level of the fan.
State	Specifies whether the fan is running or stopped.

## 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 **Management > System Information > Device Status**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer Schedule
<div>Update Cancel Apply</div>								
Management	Device Status							
•System Information	Unit ID	1	2	3				
•System CPU Status	Firmware Version	11.0.0.1	11.0.0.1	11.0.0.1				
•Switch Statistics	Boot Version	1.0.0.9	1.0.0.9	1.0.0.9				
•USB Device Information	CPLD Version	0x3	0x2	0x2				
•Loopback Interface	Serial Number	netgg	23456789					
•Management Interfaces	Internal AC-1	Not present	Not present	Not present				
•Time	Internal AC-2	Operational	Operational	Operational				
•DNS	Internal AC-3	Not present	Not present	Not present				
•SDM Template Preference	Internal AC-4	Not present	Not present	Not present				
•Green Ethernet	EPS Power Modules	Not present	Not present	Not present				
	EPS Power Modules	Not present	Not present	Not present				
	EPS Power Modules	Not present	Not present	Not present				
	EPS Power Modules	Not present	Not present	Not present				
	PoE Version	N/A	0.0.0.0	N/A				
	MAX PoE	N/A	OFF	N/A				
	PoE D-Card Type	Not Installed	XCM89UP ProSafe UPoE daughter card	Not Installed				

To refresh the screen, click the **Update** button.

The following table describes the nonconfigurable Device Status information.

**Table 7. Device Status**

Field	Description
Unit ID	The unit number in the chassis.
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.



Table 7. Device Status (continued)

Field	Description
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.
Internal AC-1, Internal AC-2, and so on	<p>Indicates the status of the appropriate power module in each unit. Status can be any of the following:</p> <ul style="list-style-type: none"> <li>• <b>Operational.</b> Power module is present and functioning properly.</li> <li>• <b>Powering.</b> Main power is failed or disconnected but RPS provides power to the switch.</li> <li>• <b>Not Present.</b> Power module is not present in the slot.</li> <li>• <b>Not powered.</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>
EPS Power Modules	<p>Indicates the status of the appropriate power module in each unit. Status can be any of the following:</p> <ul style="list-style-type: none"> <li>• <b>Operational.</b> Power module is present and functioning properly.</li> <li>• <b>Powering.</b> Main power is failed or disconnected but RPS provides power to the switch.</li> <li>• <b>Not Present.</b> Power module is not present in the slot.</li> <li>• <b>Not powered.</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	<p>Version of the PoE controller FW image.</p> <p><b>N/A</b> indicates that the Poe is not supported by the unit.</p>
MAX PoE	<p>Indicates the status of maximum PoE power available on the switch as follows:</p> <ul style="list-style-type: none"> <li>• <b>ON.</b> Indicates less than 10W of PoE power available for another device.</li> <li>• <b>OFF.</b> Indicates at least 10W of PoE power available for another device.</li> <li>• <b>N/A.</b> Indicates that PoE is not supported by the unit.</li> </ul>

Table 7. Device Status (continued)

Field	Description
PoE D-Card Type	<p>Indicates the type of the PoE daughter card plugged in. Possible values are as follows:</p> <ul style="list-style-type: none"> <li>• <b>XCM89P.</b> PoE card supporting 802.3at standard (backward compatible with 802.3af).</li> <li>• <b>XCM89UP.</b> PoE card supporting UPOE pre-standard (backward compatible with 802.3af/802.3at).</li> <li>• <b>Not Installed.</b> PoE card is not plugged in.</li> </ul>

## View the System CPU Status

### ➤ To view the system 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**.

**CPU Memory Status**

Total System Memory 1034740 KBytes

Available Memory 485412 KBytes

**CPU Utilization**

Unit No

Memory Utilization Report

status	KBytes
free	485412
alloc	549328

CPU Utilization:

PID	Name	5 Secs	60 Secs	300 Secs
15	(kworker/1:1)	0.09%	0.09%	0.08%
16	(kworker/0:1)	0.19%	0.05%	0.03%
557	(procmgr)	0.00%	0.01%	0.02%
625	hardwareMonitorTask	0.00%	0.00%	0.01%
633	osapiTimer	0.00%	0.14%	0.14%

8. You can view the CPU Utilization information, which contains the memory information, task-related information, and percentage of CPU utilization per task.

- Select the **Unit No.** to display the CPU Utilization information.
- Select **All** to display the CPU Utilization information for all units in a chassis.

The following table describes CPU Memory Status information.

**Table 8. CPU Memory Status information**

Field	Description
Total System Memory	The total memory of the switch in KBytes.
Available Memory	The available memory space for the switch in KBytes.

## Configure the CPU Thresholds

The CPU Utilization Threshold notification feature allows you to configure thresholds that, when crossed, trigger a notification. The notification is done through SNMP trap and syslog messages.

### ➤ To configure the CPU thresholds:

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

4. Enter 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 > CPU Threshold**.

CPU Threshold		
Rising Threshold	<input type="text" value="0"/>	
Rising Interval	<input type="text" value="0"/>	secs
Falling Threshold	<input type="text" value="0"/>	
Falling Interval	<input type="text" value="0"/>	secs
Free Memory Threshold	<input type="text" value="0"/>	KB

8. Configure the **Rising Threshold** value.

Notification is generated when the total CPU utilization exceeds this threshold value over the configured time period. The range is 1 to 100.

9. Configure the **Rising Interval** value.

This utilization monitoring time period can be configured from 5 to 86400 seconds in multiples of 5 seconds.

10. Configure the **Falling Threshold**.

Notification is triggered when the total CPU utilization falls below this level for a configured period of time.

The falling utilization threshold must be equal to or less than the rising threshold value. The falling utilization threshold notification is made only if a rising threshold notification was done previously. Configuring the falling utilization threshold and time period is optional. If the Falling CPU utilization parameters are not configured, then it takes the same value as Rising CPU utilization parameters. The range is 1 to 100.

11. Configure the **Falling Interval**.

The utilization monitoring time period can be configured from 5 seconds to 86400 seconds in multiples of 5 seconds.

12. Configure the CPU **Free Memory Threshold** value in KB.

To refresh the screen, click the **Update** button.

## 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**.

Statistics	
ifIndex	163
Octets Received	0
Packets Received Without Errors	0
Unicast Packets Received	0
Multicast Packets Received	0
Broadcast Packets Received	0
Receive Packets Discarded	0
Octets Transmitted	0
Packets Transmitted Without Errors	0
Unicast Packets Transmitted	0
Multicast Packets Transmitted	0
Broadcast Packets Transmitted	0
Transmit Packets Discarded	0
Most Address Entries Ever Used	1
Address Entries in Use	1
Maximum VLAN Entries	4093
Most VLAN Entries Ever Used	1
Static VLAN Entries	1
Dynamic VLAN Entries	0
VLAN Deletes	0
Time Since Counters Last Cleared	2 day 2 hr 47 min 38 sec

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

The following table describes Switch Statistics information.

**Table 9. Switch Statistics information**

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. 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. 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 are 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 learned by this switch since the most recent reboot.

**Table 9. Switch Statistics information (continued)**

Field	Description
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.
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 USB Device Information

### ➤ 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**.

The screenshot shows the switch management interface. The top navigation bar includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, Help, and Index. Below this, a sub-navigation bar shows Management, Device View, Services, Stacking, SNMP, LLDP, ISDP, and Timer Schedule. The left sidebar under 'Management' lists options like Initial Setup, System Information, System CPU Status, Switch Statistics, USB Device Information (selected), Slot Information, Loopback Interface, Management Interfaces, Time, DNS, and SDM Template Preference. The main content area displays 'USB Device Details' with a 'Device Status' field. Below it, 'USB Memory Statistics' shows 'Total Size', 'Bytes Used', and 'Bytes Free' fields. At the bottom, 'USB Directory Details' shows a table with headers 'File Name', 'File Size', and 'Modification Time'. An 'Update' button is located in the top right corner.

The Device Status field displays the current status of the device. The status is one of the following:

- **Active.** The device is USB plugged in and recognized by the switch.
- **Inactive.** The device is not mounted.
- **Invalid.** The device is not present or an invalid device is plugged in.

To refresh the screen, click the **Update** button.

The following table describes the USB Memory Statistics information.

**Table 10. USB Memory Statistics information**

Field	Description
Total Size	The USB flash device storage size in bytes.
Bytes Used	The size of memory used on the USB flash device.
Bytes Free	The size of memory free on the USB flash device.

The following table describes the USB Directory Details information.

**Table 11. USB Directory Details information**

Field	Description
File Name	The name of the file stored in the USB flash drive.
File Size	The size of the file stored in the USB flash drive in bytes
Modification Time	The last modification time of the file stored in the USB flash drive.



## View Slot Information (M5300 only)

You can view information about the cards installed in the switch's slots. This screen also provides information about the cards and switches that are compatible with the device.

➤ **To view slot 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 > Slot Information**.

SystemSwitchingRoutingQoSSecurityMonitoringMaintenanceHelpIndex

ManagementDevice ViewLicenseServicesStackingPoESNMPLLDPISDPTimer Schedule

Management

Slot Summary

Initial Setup

System Information

System CPU Status

Switch Statistics

USB Device Information

Slot Information

Loopback Interface

Management Interfaces

Time

DNS

SDM Template Preference

Slot	Status	Administrative State	Power State	Configured Card Model ID	Configured Card Description	Inserted Card Model ID	Inserted Card Description	Card Power Down	Card Pluggable
1/0	Full	Enable	Enable	M5300-52G-POE+	ProSafe 48-port Gigabit L2+ PoE+ with 10 Gigabit Stacking	M5300-52G-POE+	ProSafe 48-port Gigabit L2+ PoE+ with 10 Gigabit Stacking	False	False

Supported Card

Card Model	Card Index	Card Type	Card Descriptor
M5300-28G	1	0x1320000	ProSafe 24-port Gigabit L2+ with 10 Gigabit Stacking
M5300-28G3	2	0x2320000	ProSafe 24-port Gigabit L3 with 10 Gigabit Stacking
M5300-28G-POE+	3	0x3320000	ProSafe 24-port Gigabit L2+ PoE+ with 10 Gigabit Stacking
M5300-28GF3	4	0x4320000	ProSafe 24-port Gigabit Fiber L3 with 10 Gigabit Stacking
M5300-52G	5	0x5320000	ProSafe 48-port Gigabit L2+ with 10 Gigabit Stacking
M5300-52G3	6	0x6320000	ProSafe 48-port Gigabit L3 with 10 Gigabit Stacking
M5300-52G-POE+	7	0x7320000	ProSafe 48-port Gigabit L2+ PoE+ with 10 Gigabit Stacking

Supported Switch

Switch Model ID	Switch Index	Management Preference
M5300-28G	1	1
M5300-28G3	2	1
M5300-28G-POE+	3	1
M5300-28GF3	4	1
M5300-52G	5	1
M5300-52G3	6	1
M5300-52G-POE+	7	1

The following table describes information in the Slot Summary table.

**Table 12. Slot Summary table**

Field	Description
Slot	The slot number.
Status	Indicates whether the slot is empty or full.
Administrative State	Indicates whether the slot is administratively enabled or disabled.
Power State	Indicates whether the device is providing power to the slot.
Configured Card Model ID	The model ID of the card configured for the slot.
Configured Card Description	The description of the card configured for the slot
Inserted Card Model ID	The model ID of the card plugged into the slot.
Inserted Card Description	The description of the card plugged into the slot.
Card Power Down	If the value is True, the power state can be administratively enabled or disabled. If the value is False, the power state cannot be configured.
Card Pluggable	If the value is True, the card can be administratively enabled or disabled. If the value is False, the administrative state cannot be configured.

The following table describes information in the Supported Card table.

**Table 13. Supported Card table**

Field	Description
Card Model	The model ID of the supported card.
Card Index	The index assigned to the card type.
Card Type	The hardware type of the supported card, which is assigned by the manufacturer.
Card Descriptor	Description of the supported card, which includes the manufacturer's product number and information about number and speed of the supported interfaces.

The following table describes information in the Supported Switch table. When preconfiguring a new stack member, the switch index identifies the type of switch that is being added to the stack.

Table 14. Supported Switch

Field	Description
Switch Model ID	The model number of the supported switch.
Switch Index	The index assigned to the supported switch.
Management Preference	The management preference of the supported switch.

## Configure a Loopback Interface

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 Type

Loopback Interface Type IPv4 ▾

IPv4 Loopback Interface Configuration

Loopback ID	Primary IP Address	Primary IP Subnet Mask	Loopback Interface Status
<span>▾</span>	<input type="text"/>	<input type="text"/>	

8. Use the **Loopback Interface Type** list to select **IPv4** or **IPv6** loopback interface.

9. In the **Loopback ID** list, select a list of currently configured loopback interfaces.
10. In the **Primary Address** field, enter the primary address for this interface in dotted-decimal notation.  
This option is visible when IPv4 loopback is selected.
11. In the **Primary Mask** field, enter the primary IPv4 subnet mask in dotted-decimal notation.  
This option is visible when IPv4 loopback is selected.
12. In the **Secondary IP Address** field, enter the secondary IP address in dotted-decimal notation.  
This input field is visible only when **Add Secondary** is selected. This option is visible when IPv4 loopback is selected.
13. In the **Secondary Subnet Mask** field, enter 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.
14. In the **IPv6 mode** field, enable IPv6 on this interface using the IPv6 address.  
This option is configurable before you specify an explicit IPv6 address. This option is visible when IPv6 loopback is selected.
15. Use the **IPv6 Address** field to enter the IPv6 address in the format prefix/length.  
This option is visible when IPv6 loopback is selected.
16. Use the **EUI64** field to optionally specify the 64-bit extended unique identifier (EUI-64).  
This option is visible when IPv6 loopback is selected.

## View the IPv6 Network Interface Neighbor Table

### ➤ To view 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 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 15. IPv6 Network Interface Neighbor Table information**

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

## Configure the IPv4 Service Port

You can configure network information on the IPv4 service port. The service port is a dedicated Ethernet port for out-of-band management of the device. Traffic on this port is segregated from operational network traffic on the switch ports and cannot be switched or routed to the operational network.

### ➤ To configure the IPv4 service 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 > Management > Management Interfaces > IPv4 Service Port Configuration**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance
Management	Device View	Services	Chassis	PoE	SNMP	LLDP
ISDP	Timer Schedule					

Management	IPv4 Service Port Configuration
• System Information	Service Port Configuration Protocol <input type="radio"/> None <input type="radio"/> Bootp <input checked="" type="radio"/> DHCP
• System CPU Status	IP Address <input type="text" value="10.130.84.23"/>
• Switch Statistics	Subnet Mask <input type="text" value="255.255.255.128"/>
• USB Device Information	Default Gateway <input type="text" value="10.130.84.1"/>
• Loopback Interface	Burned In MAC Address <input type="text" value="20:0C:C8:4D:95:D9"/>
• Management Interfaces	Interface Status <input type="text" value="Up"/>
• IPv6 Network Neighbor	DHCP Client Identifier
• IPv4 Service Port Configuration	

8. Select a Service Port Configuration Protocol radio button:

- **BootP.** During the next boot cycle, the BootP client on the device broadcasts a BootP request in an attempt to acquire information from a BootP server on the network.
- **DHCP.** During the next boot cycle, the DHCP client on the device broadcasts a DHCP request in an attempt to acquire information from a DHCP server on the network.
- **None.** The device does not attempt to acquire network information dynamically.
- This specifies how the device acquires network information on the service port.

9. In the **IP Address** field, specify the IP address of the interface.

- If the service port configuration protocol is **None**, you can manually configure a static IP address.
- If the service port configuration protocol is **BootP** or **DHCP**, this field displays the IP address that was dynamically acquired (if any).

10. In the **Subnet Mask** field, specify the IP subnet mask for the interface:

- If the service port configuration protocol is **None**, you can manually configure a static subnet mask.
- If the service port configuration protocol is **BootP** or **DHCP**, this field displays the subnet mask that was dynamically acquired (if any).

11. In the **Default Gateway** field, specify the default gateway for the IP interface:

- If the Service Port Configuration Protocol is **None**, you can manually configure the IP address of the default gateway.

- If the Service Port Configuration Protocol is **BootP** or **DHCP**, this field displays the default gateway address that was dynamically acquired (if any).

**12.** Click the **Apply** button.

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

To refresh the screen, click the **Update** button.

The following table describes the nonconfigurable fields on the Service Port Configuration screen.

**Table 16. IPv4 Service Port Configuration**

Field	Description
Burned-in MAC Address	The burned-in MAC address used for out-of-band connectivity.
Interface Status	Indicates whether the link status is up or down.
DHCP Client Identifier	The identification code assigned to the client on a network. The DHCP server uses this code to identify this device.

## Configure the IPv6 Service Port

You can configure IPv6 network information on the service port. The service port is a dedicated Ethernet port for out-of-band management of the device. Traffic on this port is segregated from operational network traffic on the switch ports and cannot be switched or routed to the operational network.

➤ **To configure the IPv6 service 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 > Management > Management Interfaces > IPv6 Service Port Configuration**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance						
Management	Device View	Services	Chassis	PoE	SNMP	LLDP						
					ISDP	Timer Schedule						
<div> <div> Management <ul style="list-style-type: none"> <li>System Information</li> <li>System CPU Status</li> <li>Switch Statistics</li> <li>USB Device Information</li> <li>Loopback Interface</li> <li>Management Interfaces <ul style="list-style-type: none"> <li>IPv6 Network Neighbor</li> </ul> </li> <li>IPv4 Service Port Configuration</li> <li>IPv6 Service Port Configuration</li> <li>IPv4 Management VLAN Configuration</li> <li>IPv6 Management VLAN Configuration</li> </ul> </div> <div> IPv6 Service Port Configuration <div> IPv6 Mode <div> <input checked="" type="radio"/> Enable <input type="radio"/> Disable </div> Service Port Configuration Protocol <div> <input checked="" type="radio"/> None <input type="radio"/> DHCP </div> IPv6 Stateless Address AutoConfig Mode <div> <input type="radio"/> Enable <input checked="" type="radio"/> Disable </div> Change IPv6 Gateway <input type="checkbox"/> IPv6 Gateway <input type="text"/> Default IPv6 Gateway Address <input type="text"/> </div> <div> Add/Delete IPv6 Address <table border="1"> <thead> <tr> <th>IPv6 Address</th> <th>EUI Flag</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td>fe80::220c:c8ff:fe4d:95d9/64</td> <td>False</td> </tr> </tbody> </table> </div> </div> </div>							IPv6 Address	EUI Flag	<input type="text"/>	<input type="text"/>	fe80::220c:c8ff:fe4d:95d9/64	False
IPv6 Address	EUI Flag											
<input type="text"/>	<input type="text"/>											
fe80::220c:c8ff:fe4d:95d9/64	False											

8. Select the IPv6 mode **Enable** or **Disable** radio button.

This specifies the IPv6 administrative mode on the service port.

9. Select the Service Port Configuration Protocol **None** or **DHCP** radio button.

This specifies whether the device acquires network information from a DHCPv6 server. Selecting **None** disables the DHCPv6 client on the service port.

10. Select the IPv6 Stateless Address AutoConfig mode **Enable** or **Disable** radio button:
  - **Enable**. The service port can acquire an IPv6 address through IPv6 Neighbor Discovery Protocol (NDP) and through the use of router advertisement messages.
  - **Disable**. The service port does not use the native IPv6 address autoconfiguration feature to acquire an IPv6 address.

This sets the IPv6 stateless address autoconfiguration mode on the service port.

11. The **DHCPv6 Client DUID** field displays the client identifier used by the DHCPv6 client (if enabled) when sending messages to the DHCPv6 server.

12. To configure the IPv6 gateway, select the **Change IPv6 Gateway** check box.

The IPv6 gateway is the default gateway for the IPv6 service port interface.

13. Use the **IPv6 Gateway** field to specify the default gateway for the IPv6 service port interface.

The **Add/Delete IPv6 Address** table lists the manually configured static IPv6 addresses on the service port interface.

14. Specify the following:

- a. In the **IPv6 Address** field, specify the IPv6 address to add or remove from the service port interface.



- b. Select the **EUI Flag** option to enable the Extended Universal Identifier (EUI) flag for IPv6 address, or clear the option to omit the flag.

15. Click the **Add** button.

The IPv6 address is added to the service port interface,

16. To delete the selected IPv6 address, click the **Delete** button.

17. Click the **Apply** button.

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

To refresh the screen, click the **Update** button.

## IPv4 Management VLAN Overview

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 gets 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 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

After 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

## Configure an IPv4 Management VLAN

➤ **To configure an 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**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance
Management	Device View	Services	Chassis	PoE	SNMP	LLDP
					ISDP	Timer Schedule

Management	IPv4 Management VLAN Configuration
• System Information	VLAN ID <input type="text" value="1"/>
• System CPU Status	Routing Mode <input checked="" type="radio"/> Enable <input type="radio"/> Disable
• Switch Statistics	Configuration Method <input type="radio"/> DHCP <input checked="" type="radio"/> Manual
• USB Device Information	IP Address <input type="text" value="169.254.100.100"/>
• Loopback Interface	Subnet Mask <input type="text" value="255.255.0.0"/>
• Management Interfaces	MAC Address <input type="text" value="20:0C:C8:4D:95:DB"/>
• IPv6 Network Neighbor	Routing Interface Status <input type="text" value="Down"/>
• IPv4 Service Port Configuration	Management VLAN ID <input type="text" value="1"/> (1 to 4093)
• IPv6 Service Port Configuration	
• IPv4 Management VLAN Configuration	
• IPv6 Management VLAN Configuration	

8. From the **VLAN ID** list, select the VLAN.  
This list displays all IDs of VLANs configured on this switch.
9. Select the Routing mode **Enable** or **Disable** radio button.  
This specifies global routing on the device.
10. Select the **Configuration Method DHCP** or **Manual** radio button:
  - **DHCP**. Transmit a DHCP request.
  - **Manual**. Do nothing.
 This specifies what the switch does on start-up.
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. It can be configured to any value in the range of 1–4093.

14. Click the **Apply** button.

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

The following table describes the nonconfigurable fields on the IPv4 Management VLAN Configuration screen.

**Table 17. IPv4 Management VLAN Configuration**

Field	Description
MAC Address	The MAC address assigned to the VLAN routing interface.
Routing Interface Status	Indicates whether the link status is up or down.

## Configure an IPv6 Management VLAN

### ➤ To configure an IPv6 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 > IPv6 Management VLAN Configuration**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance		
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer Schedule
Management	IPv6 Management VLAN Configuration							
• System Information	Admin Mode		<input checked="" type="radio"/> Enable <input type="radio"/> Disable					
• System CPU Status	IPv6 Enable Mode		<input type="radio"/> Enable <input checked="" type="radio"/> Disable					
• Switch Statistics	Address Autoconfigure Mode		<input type="radio"/> Enable <input checked="" type="radio"/> Disable					
• USB Device Information	Address DHCP Mode		<input type="radio"/> Enable <input checked="" type="radio"/> Disable					
• Loopback Interface	VLAN IPv6 Interface Status		Down					
• Management Interfaces	IPv6 VLAN Interface Configuration							
• IPv6 Network Neighbor	<input type="checkbox"/> IPv6 Prefix/Prefix Length		EUI64	State				
• IPv4 Service Port Configuration	<input type="text"/>		False	State				
• IPv6 Service Port Configuration	<input type="checkbox"/> fe80::220c:c8ff:fe4d:95db/64			TENT				
• IPv4 Management VLAN Configuration								
• IPv6 Management VLAN Configuration								
• Time								

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

This enables or disables the administration mode for the management VLAN IPv6 interface on the switch.

9. Select the IPv6 Enable mode **Enable** or **Disable** radio button.

This specifies the IPv6 mode on the management VLAN.

10. Select the Address Autoconfigure mode **Enable** or **Disable** radio button.

**Note:** The Address Autoconfigure mode option is available only if unicast routing is globally disabled.

11. Select the Address DHCP mode **Enable** or **Disable** radio button.

12. Click the **Apply** button.

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

The VLAN IP Interface Status field indicates whether the link is up or down.

## Configure an IPv6 VLAN Interface

### ➤ To configure an IPv6 VLAN 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 > Management Interfaces > IPv6 Management VLAN Configuration**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance		
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer Schedule

Management

- System Information
- System CPU Status
- Switch Statistics
- USB Device Information
- Loopback Interface
- Management Interfaces
  - IPv6 Network Neighbor
  - IPv4 Service Port Configuration
  - IPv6 Service Port Configuration
  - IPv4 Management VLAN Configuration
  - IPv6 Management VLAN Configuration
- Time

### IPv6 Management VLAN Configuration

Admin Mode ☒ Enable ☐ Disable

IPv6 Enable Mode ☐ Enable ☒ Disable

Address Autoconfigure Mode ☐ Enable ☒ Disable

Address DHCP Mode ☐ Enable ☒ Disable

VLAN IPv6 Interface Status Down

### IPv6 VLAN Interface Configuration

IPv6 Prefix/Prefix Length	EUI64	State
<input type="text"/>	False	<input type="button" value="Add"/>
fe80::220c:c8ff:fe4d:95db/64		TENT

8. In the IPv6 Prefix/Prefix Length field, specify the IPv6 address to add or remove from the management VLAN interface.

9. Select the **EUI46** option to **True** (enabled) for the Extended Universal Identifier (EUI) flag for an IPv6 address.

10. Click the **Add** button.

The IPv6 address is added to the management VLAN,

11. To delete a selected IPv6 address, click the **Delete** button.

12. Click the **Apply** button.

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

The following table describes the nonconfigurable fields on the IPv6 Management VLAN Interface Configuration screen.

**Table 18. IPv4 Management VLAN Configuration**

Field	Description
State	<p>The interface address state. Possible values are as follows:</p> <ul style="list-style-type: none"> <li>• Auto</li> <li>• DHCP</li> <li>• TENT (tentative)</li> </ul>

## Time

M6100/M7100/M5300 software supports the Simple Network Time Protocol (SNTP). As its name suggests, it is a less complicated version of Network Time Protocol, which is a system for synchronizing the clocks of networked computer systems, primarily when data transfer is handled through the Internet.

### Configure the Time Setting

➤ **To configure the time setting:**

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

8. Select the Clock Source **Local** or **SNTP** radio button.

The default is SNTP. The local clock can be set to SNTP only if the following two conditions are met:

- The SNTP server is configured.
- The SNTP last attempt status is successful.

9. In the **Date** field, specify the current date in months, days, and years.

10. In the **Time** field, specify the current time in hours, minutes, and seconds.

11. Click the **Apply** button.

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

To refresh the screen, click the **Update** button.

## Configure the SNTP Global Settings

### ➤ To configure the 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.

6. Click the **Login** button.

The web management interface menu displays.

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

When you select the **SNTP** option as the **Clock Source**, the SNTP Global Configuration section is displayed below the Time Configuration section of the screen.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance		
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer Schedule

Management	Time Configuration
<ul style="list-style-type: none"> <li>Initial Setup</li> <li>System Information</li> <li>System CPU Status</li> <li>Switch Statistics</li> <li>USB Device Information</li> <li>Loopback Interface</li> <li>Management Interfaces</li> <li>Time               <ul style="list-style-type: none"> <li><b>Time Configuration</b></li> <li>SNTP Server Configuration</li> <li>DayLight Saving Configuration</li> <li>DNS</li> <li>SDM Template Preference</li> </ul> </li> </ul>	<p>Clock Source <input type="radio"/> Local <input checked="" type="radio"/> SNTP</p> <p><b>SNTP Global Configuration</b></p> <p>Client Mode <input type="radio"/> Disable <input checked="" type="radio"/> Unicast <input type="radio"/> Broadcast</p> <p>Port <input type="text" value="123"/> (123 or 1025 to 65535) Default:123</p> <p>Source Interface <input type="text" value="vlan 1"/></p> <p>Unicast Poll Interval <input type="text" value="6"/> (6 to 10)</p> <p>Broadcast Poll Interval <input type="text" value="6"/> (6 to 10)</p> <p>Unicast Poll Timeout <input type="text" value="5"/> (1 to 30)</p> <p>Unicast Poll Retry <input type="text" value="1"/> (0 to 10)</p> <p>Time Zone Name <input type="text"/></p> <p>Offset Hours <input type="text" value="0"/> (-12 to 13)</p> <p>Offset Minutes <input type="text" value="0"/> (0 to 59)</p>

8. Select a **Client mode** radio button to specify the mode of operation of the SNTP client:
- **Disable.** SNTP is not operational. No SNTP requests are sent from the client and no received SNTP messages are 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 has a single subnet scope while a multicast address has Internet wide scope.

The default value is Unicast.

9. In the **Port** field, specify the local UDP port that the SNTP client receives server packets on. The allowed range is 1025 to 65535 and the value 123. The default value is 123. When the default value is configured, the actual client port value used in SNTP packets is assigned by the operating system.
10. Select the **Source Interface** to use for the SNTP client.

Possible values are as follows:

- None
- VLAN 1
- Routing interface
- Routing VLAN
- Routing loopback interface
- Tunnel interface
- Service port



By default VLAN 1 is used as the source interface.

**11. Specify the Unicast Poll Interval.**

This is 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.

**12. Specify the Broadcast Poll Interval.**

This is the number of seconds between broadcast poll requests expressed as a power of 2 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.

**13. Specify the Unicast Poll Timeout.**

This is 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.

**14. Specify the Unicast Poll Retry.**

This is 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.

**15. Use the Time Zone Name field to configure a time zone specifying the number of hours and, optionally, the number of minutes difference from UTC with Offset Hours and Offset Minutes.**

The time zone can affect the display of the current system time. The default value is UTC. 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), which is the same as Greenwich Mean Time (GMT). This might not be the time zone in which the switch is located.

**16. Use the Offset Hours field to specify the number of hours of difference from UTC.**

The allowed range is -12 to 13. The default value is 0.

**17. Use the Offset Minutes field to specify the number of minutes of difference from UTC.**

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

**18. Click the Apply button.**

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

To refresh the screen, click the **Update** button.

## View SNTP Global Status

When you select the **SNTP** option as the **Clock Source**, the SNTP global status is displayed below the SNTP Global Configuration section of the screen.

➤ **To view 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 > SNTP Global Status**

When you select the **SNTP** option as the **Clock Source**, the SNTP Global Status is displayed below the SNTP Global Configuration section.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance		
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer Schedule

Management	SNTP Global Status	
• Initial Setup	Version	4
• System Information	Supported Mode	Unicast and Broadcast
• System CPU Status ▾	Last Update Time	Jan 1 00:00:00 1970 (UTC+0:00)
• Switch Statistics	Last Attempt Time	Jan 1 00:00:00 1970 (UTC+0:00)
• USB Device Information	Last Attempt Status	Other
• Loopback Interface	Server IP Address	
• Management Interfaces ▾	Address Type	Unknown
• Time ▴	Server Stratum	0
• Time Configuration	Reference Clock Id	
• SNTP Server Configuration	Server Mode	Reserved
• DayLight Saving Configuration	Unicast Server Max Entries	3
	Unicast Server Current Entries	0
• DNS ▾	Broadcast Count	0
• SDM Template Preference		

The following table displays the nonconfigurable SNTP Global Status information.

**Table 19. SNTP Global Status**

Field	Description
Version	The SNTP version that the client supports.
Supported mode	The SNTP modes that the client supports. Multiple modes can be supported by a client.
Last Update Time	The local date and time (UTC) that the SNTP client last updated the system clock.
Last Attempt Time	The local date and time (UTC) of the last SNTP request or receipt of an unsolicited message.
Last Attempt Status	<p>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 <b>Other</b> is displayed. These values are appropriate for all operational modes.</p> <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 <i>leap indicator</i> 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>
Server IP Address	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	The address type of the SNTP server address for the last received valid packet.
Server Stratum	The claimed stratum of the server for the last received valid packet.
Reference Clock ID	The reference clock identifier of the server for the last received valid packet.
Server mode	The mode of the server for the last received valid packet.
Unicast Server Max Entries	The maximum number of unicast server entries that can be configured on this client.
Unicast Server Current Entries	The number of current valid unicast server entries configured for this client.
Broadcast Count	The number of unsolicited broadcast SNTP messages that were received and processed by the SNTP client since the last reboot.

## Configure an SNTP Server

SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. M6100/M7100/M5300 software operates only as an SNTP client and cannot provide time services to other systems.

Time sources are established by stratum. Stratum defines 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 stratum:

- **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.

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

### ➤ To configure the SNTP 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.

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**.

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

8. In the **Server Type** list, select the address type of the configured SNTP server address.

Possible values are as follows:

- IPv4
- IPv6
- DNS

The default value is IPv4.

9. In the **Address** field, 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 is resolved into an IP address each time an SNTP request is sent to it.

10. Enter a **Port** number on the SNTP server to which SNTP requests are sent.

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

11. 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. The priority 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 has the same priority, then the requesting order follows the lexicographical ordering of the entries in this table. The valid range is 1 to 3. The default value is 1.

- 12.** Specify the **NTP Version** running on the server.

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

- 13.** Click the **Add** button.

The SNTP server entry is added. This sends the updated configuration to the switch. Configuration changes take effect immediately.

- 14.** Repeat the previous steps to add additional SNTP servers.

You can configure up to three SNTP servers.

- 15.** 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.

- 16.** To remove an SNTP server entry, 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.

- 17.** Click the **Apply** button.

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

To refresh the screen, click the **Update** button.

The SNTP Server Status table displays status information about the SNTP servers configured on your switch. The following table displays SNTP Server Status information.

**Table 20. 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 20. SNTP Server Status (continued)

Field	Description
Last Attempt Status	<p>The status of the last S9 NTP request to this server. If no packet was received from this server, a status of Other is displayed.</p> <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 Daylight Saving Time Settings

### ➤ To configure the Daylight Saving 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 > Daylight Saving Configuration**.

The screenshot shows the 'DayLight Saving (DST) Configuration' page. The left sidebar contains a 'Management' menu with options like Initial Setup, System Information, System CPU Status, Switch Statistics, USB Device Information, Slot Information, Loopback Interface, Management Interfaces, Time, Time Configuration, SNTP Server Configuration, DayLight Saving Configuration (highlighted), and DNS. The main content area has a 'DayLight Saving (DST)' section with radio buttons for Disable (selected), Recurring, Recurring EU, Recurring USA, and Non Recurring. Below this is a 'DayLight Saving (DST) Status' section with two rows: 'DayLight Saving (DST)' set to 'Disable' and 'DayLight Saving (DST) In Effect' set to 'No'.

8. Select Daylight Saving (DST) radio button:

- **Disable.** Disable daylight saving time.
- **Recurring.** Enable Recurring daylight saving time.
- **Recurring EU.** Enable recurring EU daylight saving time.
- **Recurring USA.** Enable recurring USA daylight saving time.
- **Non Recurring.** Configure non-recurring daylight saving time.

9. Click the **Apply** button.

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

The fields in the following tables are visible only when DayLight Saving is **Recurring** or **Recurring EU** or **Recurring USA**.

**Table 21. DayLight Saving - Recurring**

Field	Description
Begins At	<p>These fields are used to configure the start values of the date and time.</p> <ul style="list-style-type: none"> <li>• <b>Week.</b> Configure the start week.</li> <li>• <b>Day.</b> Configure the start day.</li> <li>• <b>Month.</b> Configure the start month.</li> <li>• <b>Hours.</b> Configure the start hours.</li> <li>• <b>Minutes.</b> Configure the start minutes.</li> </ul>



**Table 21. DayLight Saving - Recurring**

Field	Description
Ends At	These fields are used to configure the end values of date and time. <ul style="list-style-type: none"> <li>• <b>Week.</b> Configure the end week.</li> <li>• <b>Day.</b> Configure the end day.</li> <li>• <b>Month.</b> Configure the end month.</li> <li>• <b>Hours.</b> Configure the end hours.</li> <li>• <b>Minutes.</b> Configure the end minutes.</li> </ul>
Offset	Configure recurring offset in minutes. The valid range is 1–1440 minutes.
Zone	Configure the time zone.

The fields in the following table are visible only when DayLight Saving is **Non Recurring**.

**Table 22. DayLight Saving - Non Recurring**

Field	Description
Begins At	These fields are used to configure the start values of the date and time. <ul style="list-style-type: none"> <li>• <b>Week.</b> Configure the start week.</li> <li>• <b>Day.</b> Configure the start day.</li> <li>• <b>Month.</b> Configure the start month.</li> <li>• <b>Hours.</b> Configure the start hours.</li> <li>• <b>Minutes.</b> Configure the start minutes.</li> </ul>
Ends At	These fields are used to configure the end values of date and time. <ul style="list-style-type: none"> <li>• <b>Week.</b> Configure the end week.</li> <li>• <b>Day.</b> Configure the end day.</li> <li>• <b>Month.</b> Configure the end month.</li> <li>• <b>Hours.</b> Configure the end hours.</li> <li>• <b>Minutes.</b> Configure the end minutes.</li> </ul>
Offset	Configure the non-recurring offset in minutes. The valid range is 1–1440 minutes.
Zone	Configure the time zone.

## View the DayLight Saving Time Status

### ➤ To view the DayLight Saving Time 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.

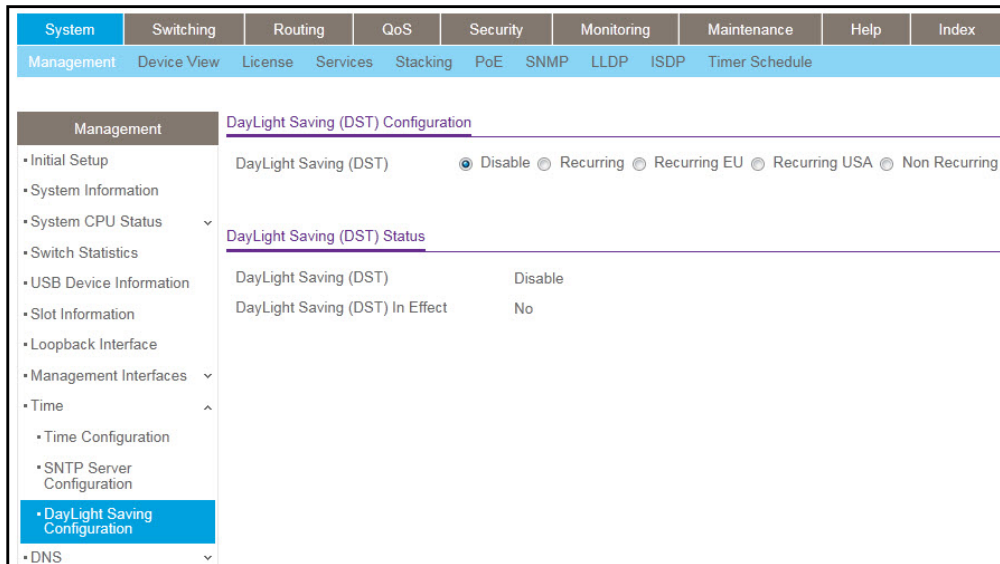
5. Enter the user name and password.

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 > DayLight Saving Configuration**.



To refresh the screen, click the **Update** button.

The following table displays the nonconfigurable Daylight Saving (DST) status information.

**Table 23. DayLight Saving Status**

Field	Description
Daylight Saving (DST)	The Daylight Saving value, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Disable</b></li> <li>• <b>Recurring</b></li> <li>• <b>Recurring EU</b></li> <li>• <b>Recurring USA</b></li> <li>• <b>Non Recurring</b></li> </ul>
Begins At	Displays when the daylight saving time begins. This field is not displayed when daylight saving time is disabled.
Ends At	Displays when the daylight saving time ends. This field is not displayed when daylight saving time is disabled.

Table 23. DayLight Saving Status (continued)

Field	Description
Offset (in Minutes)	The offset value in minutes. This field is not displayed when daylight saving time is disabled.
Zone	The zone acronym. This field is not displayed when daylight saving time is disabled.
Daylight Saving (DST) in Effect	Displays whether daylight saving time is in effect.

## Configure DNS Settings

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

### Configure Global DNS Settings

You can configure global DNS settings and DNS server information.

➤ **To configure the global DNS 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 > DNS Configuration**.

Serial No	DNS Server	Preference
1	10.130.138.20	0
2	10.130.138.21	1

8. Select the DNS Status **Disable** or **Enable** radio button:

- **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.

9. 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 provides the domain name (for example, if default domain name is netgear.com and the user enters 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.

10. 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.

11. 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.

12. Specify the **Source Interface** to use for DNS.

Possible values are as follows:

- None
- VLAN 1
- Routing interface
- Routing VLAN
- Routing loopback interface
- Tunnel interface
- Service port

By default VLAN 1 is used as the 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** field 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 its check box and click the **Delete** button.

If you click the **Delete** button without selecting a DNS server, all the DNS servers are deleted.

15. Click the **Apply** button.

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

To refresh the screen, click the **Update** button.

The following table displays DNS Server Configuration information.

**Table 24. DNS Server Configuration**

Field	Description
Serial No	The sequence number of the DNS server.
Preference	Shows the preference of the DNS server. The preference is determined by the order in which they were entered.

## Add a Static Entry to the Local DNS Table

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

### ➤ To add a static entry to the local DNS 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 > DNS > Host Configuration**.

The screenshot shows the 'DNS Host Configuration' page. It has a header 'DNS Host Configuration' and a table with two columns: 'Host Name (1 to 255 characters)' and 'IP Address'. Below this is a 'Dynamic Host Mapping' section with a table header showing columns: 'Host', 'Total', 'Elapsed', 'Type', and 'Addresses'.

8. In the **Host Name (1 to 255 characters)** field, specify the static host name to add. Its length cannot exceed 255 characters and it is a mandatory field.
9. In the **IP Address** field, enter 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 on the screen.
11. To remove an entry from the static DNS table, select its check box and click the **Delete** button.

To clear all the dynamic host name entries from the list, click the **Clear** button.

To refresh the screen, click the **Update** 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 25. DNS Dynamic Host Mapping**

Field	Description
Host	Lists the host name that 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 the Switch Database Management Template Preference

A Switch Database Management (SDM) template is a description of the maximum resources a switch or router can use for various features. Different SDM templates allow different

combinations of scaling factors, enabling different allocations of resources depending on how the device is used. In other words, SDM templates enable you to reallocate system resources to support a different mix of features based on your network requirements.

---

**Note:** If you attach a unit to a stack and its template does not match the stack's template, then the new unit automatically reboots using the template used by the other stacking members. To avoid the automatic reboot, first set the template to the SDM template used by existing members of the stack. Then power off the new unit, attach it to the stack, and power it on.

---

You can configure SDM template preferences for the switch.

➤ **To configure the SDM Template Preference 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 > SDM Template Preference**.

SDM Template	ARP Entries	IPv4 Unicast Routes	IPv6 NDP Entries	IPv6 Unicast Routes	ECMP Next Hops	IPv4 Multicast Routes	IPv6 Multicast Routes
Dual IPv4 and IPv6	6144	8160	2560	4096	4	1536	512
IPv4 Routing Default	8192	12288	0	0	4	2048	0
IPv4 Data Center	6144	8160	0	0	16	2048	0
IPv4 Data Center Plus	8192	12288	0	0	16	2048	0
Dual IPv4 and IPv6 Data Center	6144	8160	2560	4096	16	1536	512

8. Use **SDM Next Template ID** to configure the next active template.

It is active only after the next reboot. To revert to the default template after the next reboot, use the Default option. Possible values are as follows:

- Dual IPv4 and IPv6
- IPv4 Routing Default
- IPv4 Data Center
- IPv4 Data Center Plus
- Dual IPv4 and IPv6 Data Center

The following table displays Summary information.

**Table 26. SDM Template Preference Summary**

Field	Description
SDM Current Template ID	The current active SDM template. Possible values are as follows: <ul style="list-style-type: none"> <li>• Dual IPv4 and IPv6</li> <li>• IPv4-routing Default</li> <li>• IPv4 Data Center</li> </ul>
SDM Template	Identifies the template. The possible values are as follows: <ul style="list-style-type: none"> <li>• Dual IPv4 and IPv6</li> <li>• IPv4-routing Default</li> <li>• IPv4 Data Center</li> </ul>
ARP Entries	The maximum number of entries in the IPv4 Address Resolution Protocol (ARP) cache for routing interfaces.
IPv4 Unicast Routes	The maximum number of IPv4 unicast forwarding table entries.
IPv6 NDP Entries	The maximum number of IPv6 Neighbor Discovery Protocol (NDP) cache entries.
IPv6 Unicast Routes	The maximum number of IPv6 unicast forwarding table entries.
ECMP Next Hops	The maximum number of next hops that can be installed in the IPv4 and IPv6 unicast forwarding tables.
IPv4 Multicast Routes	The maximum number of IPv4 multicast forwarding table entries.
IPv6 Multicast Routes	The maximum number of IPv6 multicast forwarding table entries.

## Configure Green Ethernet Settings

### ➤ To configure the 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.

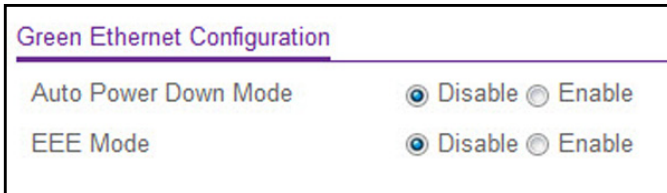
5. Enter the user name and password.

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	
Auto Power Down Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
EEE Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

8. Select the 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 autonegotiation and power consumption saving when no link partner is present.

9. Select the EEE mode **Disable** or **Enable** radio button.

Energy Efficient Ethernet (EEE) combines the MAC with a family of PHYs that support operation in a low power mode. It is defined by IEEE 802.3az Energy Efficient Task Force. Lower power mode enables both the send and receive sides of the link to disable some functionality for power savings when lightly loaded. Transition to low power mode does not change the link status. Frames in transit are not dropped or corrupted in transition to and from low power mode. Transition time is transparent to upper layer protocols and applications.

10. Click the **Apply** button.

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

## Configure Green Ethernet Interface Settings

### ➤ To configure the 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**.

Green Ethernet Interface Configuration			
1 All		Go To Interface	Go
<input type="checkbox"/>	Port	Auto Power Down Mode	EEE Mode
<input type="checkbox"/>	1/0/1	Disable	Disable
<input type="checkbox"/>	1/0/2	Disable	Disable
<input type="checkbox"/>	1/0/3	Disable	Disable
<input type="checkbox"/>	1/0/4	Disable	Disable
<input type="checkbox"/>	1/0/5	Disable	Disable

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 a short period of time, and then wakes up to check link pulses. This allows the switch to perform autonegotiation and save power consumption when no link partner is present.

11. Use the **EEE mode** menu to **Enable** or **Disable** this option.

The factory default is Disable. IF the EEE mode is not supported, then *N/A* is displayed.

12. Click the **Apply** button.

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

## Configure Green Ethernet Local and Remote Devices

➤ **To configure green Ethernet local and remote devices:**

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

Local Device Information	
Interface	1/0/1 ▾
Cumulative Energy Saved on this port due to Green Mode(s) (Watts * Hours)	0
Energy Detect Admin Mode	Disable ▾
Operational Status	Inactive
Reason	Admin Down
EEE Admin Mode	Disable ▾
EEE Transmit Idle Time	600 (600 to 4294967295)
EEE Transmit Wake Time	17 (8 to 65535)
Rx Low Power Idle Event Count	0
Rx Low Power Idle Duration (uSec)	0
Tx Low Power Idle Event Count	0
Tx Low Power Idle Duration (uSec)	0
Tw_sys_tx (uSec)	0
Tw_sys_tx Echo (uSec)	0
Tw_sys_rx (uSec)	0
Tw_sys_rx Echo (uSec)	0
Fallback Tw_sys (uSec)	0
Tx_dll_enabled	No
Tx_dll_ready	No
Rx_dll_enabled	No
Rx_dll_ready	No
Time Since Counters Last Cleared	2 days 4 hrs 10 mins 52 secs

8. Select the **Interface**.

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 a short period of time, and then wakes up to check link pulses. This allows the switch to perform autonegotiation and save 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, port transitions to low power mode during a link idle condition. The default value is Disabled.

12. Click the **Apply** button.

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

To refresh the screen, click the **Update** button.

To clear the configuration, resetting all statistics for the selected interface to default values, click the **Clear** button.

The following table describes the nonconfigurable fields.

**Table 27. Green Ethernet Local Device information**

Field	Description
Cumulative Energy Saved on this port due to Green mode(s) (Watts * Hours)	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 operational (Enabled).
Reason	The reason for the current operational status of Short Reach Admin mode.
Rx Low Power Idle Event Count	This field is incremented each time MAC RX enters low-power idle (LPI) state. Shows the total number of Rx LPI events since EEE counters were last cleared.
Rx Low Power Idle Duration (uSec)	This field indicates duration of Rx LPI state in 10 us increments. Shows the total duration of Rx LPI since the EEE counters were last cleared.
Tx Low Power Idle Event Count	This field is incremented each time MAC TX enters LPI state. Shows the total number of Tx LPI events since EEE counters were last cleared.

**Table 27. Green Ethernet Local Device information (continued)**

Field	Description
Tx Low Power Idle Duration (uSec)	This field indicates duration of Tx LPI state in 10 us 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.
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 system's 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/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/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).

## Configure Green Ethernet Remote Device Details

➤ **To configure the Green Ethernet 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.

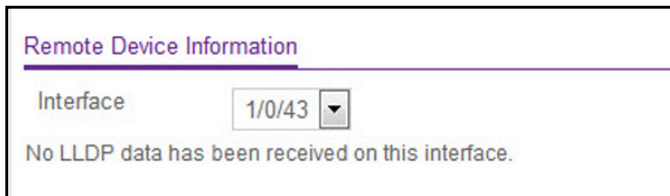
6. Click the **Login** button.

The web management interface menu displays.

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

The Green Ethernet Details screen displays.

8. Scroll down to the Remote Device Information section.



9. Select the **Interface**.

The following table describes the nonconfigurable fields.

**Table 28. Green Ethernet Remote Device Information**

Field	Description
Remote ID	The remote client identifier assigned to the remote system.
Remote Tw_sys_tx (uSec)	Integer that indicates the value of Tw_sys that the remote system can support.
Remote Tw_sys_tx Echo (uSec)	Integer that indicates the value of Transmit Tw_sys echoed back by the remote system.
Remote Tw_sys_rx (uSec)	Integer that indicates the value of Tw_sys that the remote system requests from the local system.
Remote Tw_sys_rx Echo (uSec)	Integer that indicates the value of Receive Tw_sys echoed back by the remote system.
Remote Fallback Tw_sys (uSec)	Integer that indicates the value of fallback Tw_sys that the remote system is advertising.

## View the Green Ethernet Statistics Summary

### ➤ To view the green Ethernet 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 Summary**.

Green Ethernet Statistics Summary

Current Power Consumption /Chassis (mW)	11280
Percentage Power Saving /Chassis (%)	0
Cumulative Energy Saving /Chassis (W*H)	0

Green Ethernet Feature Summary

Unit	Green Features supported on this unit
1	Energy-Detect EEE LPI-History LLDP-Cap-Exchg Pwr-Usg-Est

Green Ethernet Interface Summary

Interface	Energy Detect Admin Mode	Energy Detect Operational Status	EEE Admin Mode
1/0/1	Disable	Inactive	Disable
1/0/2	Disable	Inactive	Disable
1/0/3	Disable	Inactive	Disable
1/0/4	Disable	Inactive	Disable
1/0/5	Disable	Inactive	Disable

To refresh the screen, click the **Update** button.

The following table describes the nonconfigurable fields.

**Table 29. Green Ethernet Statistics Summary**

Field	Description
Current Power Consumption by all ports in Chassis (mWatts)	Estimated Power Consumption by all ports in chassis in mWatts.
Estimated Percentage Power Saving per chassis (%)	Estimated percentage of power saved on all ports in chassis when green modes are enabled.

Table 29. Green Ethernet Statistics Summary (continued)

Field	Description
Cumulative Energy Saving per Chassis (Watts * Hours)	Estimated cumulative energy saved per chassis in (watts * hour) when all green modes are enabled.
Unit	The Unit ID.
Green Features supported on this unit	List of green features supported on the given unit, which could be one or more of the following: Energy-Detect (Energy Detect), Short-Reach (Short Reach), 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.
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 a short period of time, then wakes up to check link pulses. This allows the switch to perform autonegotiation and save power consumption when no link partner is present.
Energy Detect Operational Status	Current operational status of the Energy Detect mode.
Short Reach Admin mode	Enable or disable Short Reach Admin mode on the port. With Short Reach mode enabled, PHY is forced to operate in low power mode irrespective of the cable length.
Short Reach Operational Status	Current operational status of the Short Reach mode.
EEE Admin mode	Enable or disable Energy Efficient Ethernet mode on the port. With EEE mode enabled, the port transitions to low power mode during link idle conditions.

## Configure the Green Ethernet EEE LPI History

### ➤ To configure 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**.

**Interface Green Mode EEE LPI History Configuration**

Interface 1/0/1

Sampling Interval 3600 (30 to 36000)

Max Samples to keep 168 (1 to 168)

Percentage LPI time per Chassis 0

**Interface Green Mode EEE LPI History**

<input type="checkbox"/>	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

8. Select the **Interface**.
9. In the **Sampling Interval** field, enter 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** field, enter the maximum number of samples to keep.  
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 update configuration is sent to the switch.

To refresh the screen, click the **Update** button.

The following table describes the nonconfigurable fields.

**Table 30. Interface Green mode EEE LPI History**

Field	Description
Percentage LPI time per Chassis	Time spent in LPI mode per chassis since EEE counters were last cleared.
Sample No.	Sample index.
Time Since The Sample Was Recorded	Each time the screen is refreshed, it shows a different time as it reflects the difference in current time and time at which the sample was recorded.

**Table 30. Interface Green mode EEE LPI History**

Field	Description
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.

## Licenses (M5300 only)

You can view license information for M5300 series switches.

### View License Keys for M5300 Series Switches

You can view information about available license keys for various features. By default, those license keys are not available. If the license key feature is available, you can configure this functionality.

➤ **To view license 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 **System > License > License Key**.

System	Switching	Routing	QoS	Security	Monitoring
Management	Device View	License	Services	Stacking	PoE SNMP LLDP
License		License Key			
• License Key		License Date	Feb-23-2015		
• License features		License Copy	1		
		License Status	Active		
		Description	License key is active.		

The following table describes the nonconfigurable information that is displayed.

**Table 31. License Key**

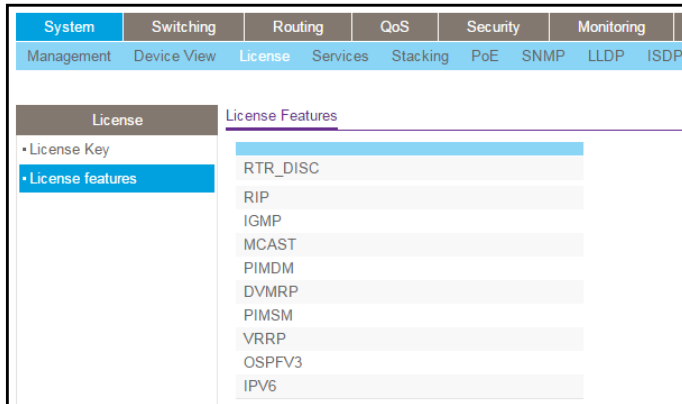
Field	Description
License Date	The date the license is purchased.
License Copy	The number of licenses.
License Status	Displays whether the license is <b>Active</b> or <b>Inactive</b> . <b>Inactive</b> means that you must download a license file and reboot the system.
Description	Shows the status of license key.

## View License Features for M5300 Series Switches

You can view a list of features that require licensing.

➤ **To view the license features:**

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



## Configure DHCP Server Settings

You can configure settings for DHCP server, DHCP pools, DHCP bindings, and DHCP relay. You can also view DHCP statistics and conflicts.

### Configure DHCP Server

➤ **To configure a 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**.

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. 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 to be enabled or disabled. The default value is Enable.
11. Select the BootP Automatic mode **Disable** or **Enable** radio button.
- This specifies whether BootP for dynamic pools is to be enabled or disabled. The default value is Disable.
12. To exclude addresses, do the following:
- In the **IP Range From** field, enter the lowest address in the range or a single address to be excluded.
  - In the **IP Range To** field, to exclude a range, enter 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.
13. Click the **Add** button.
- The exclude addresses are added to the switch
14. To delete the exclude address from the switch, click the **Delete** button.
15. Click the **Apply** button.

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

## 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**.

The screenshot shows the 'DHCP Pool Configuration' web page. It contains various configuration fields for a DHCP pool, including:
 

- Pool Name:** A text input field with a 'Create' dropdown and a note '(1 to 31 alphanumeric characters)'.
- Type of Binding:** A dropdown menu currently set to 'Unallocated'.
- Network Address:** A text input field showing '0.0.0.0'.
- Network Mask:** A text input field showing '0.0.0.0'.
- Network Prefix Length:** A text input field with a note '(0 to 32)'.
- Client Name:** A text input field.
- Hardware Address:** A text input field showing '00:00:00:00:00:00'.
- Hardware Address Type:** A dropdown menu set to 'Ethernet'.
- Client ID:** A text input field.
- Host Number:** A text input field showing '0.0.0.0'.
- Host Mask:** A text input field showing '0.0.0.0'.
- Host Prefix Length:** A text input field with a note '(1-32)'.
- Lease Time:** A dropdown menu set to 'Infinite'.
- Days:** A text input field showing '0' with a note '(0 to 59)'.
- Hours:** A text input field showing '0' with a note '(0 to 23)'.
- Minutes:** A text input field showing '0' with a note '(0 to 59)'.
- Default Router Addresses:** A dropdown menu.
- DNS Server Addresses:** A dropdown menu.
- NetBIOS Name Server Addresses:** A dropdown menu.
- NetBIOS Node Type:** A dropdown menu set to 'b-node Broadcast'.
- Next Server Address:** A text input field showing '0.0.0.0'.
- Domain Name:** A text input field with a note '(0 to 255 characters)'.
- Bootfile:** A text input field with a note '(0 to 128 characters)'.

8. Click the **Add** button.

The pool configuration is added.

9. To delete the pool, click the **Delete** button.

This field is not visible to 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 32. 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 <b>Create</b> . When the user selects <b>Create</b> , another text box <b>Pool Name</b> , appears where the user can enter a name for the pool to be created. For a user with read-only permission, this field shows names of the existing pools only.
Pool Name	The name of the pool to be created. This field appears when the user with read-write permission selects <b>Create</b> in the Pool Name list*. <b>Pool Name</b> can be up to 31 characters in length.
Type of Binding	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	The subnet address for a DHCP address of a dynamic pool.
Network Mask	The subnet number for a DHCP address of a dynamic pool. Either <b>Network Mask</b> or <b>Prefix Length</b> can be configured to specify the subnet mask but not both.
Network Prefix Length	The subnet number for a DHCP address of a dynamic pool. Either <b>Network Mask</b> or <b>Prefix Length</b> can be configured to specify the subnet mask but not both. The valid range is 0 to 32.
Client Name	The client name for DHCP manual pool.
Hardware Address	The MAC address of the hardware platform of the DHCP client.
Hardware Address Type	The protocol of the hardware platform of the DHCP client. Valid types are Ethernet and ieee802. The default value is Ethernet.
Client ID	The client identifier for DHCP manual pool.
Host Number	The IP address for a manual binding to a DHCP client. The host can be set only if Client Identifier or Hardware Address is specified. Deleting Host would delete the client name, client ID, and hardware address for the manual pool, and set the pool type to Unallocated.

Table 32. DHCP Pool Configuration (continued)

Field	Description
Host Mask	The subnet mask for a manual binding to a DHCP client. Either <b>Host Mask</b> or <b>Prefix Length</b> can be configured to specify the subnet mask but not both.
Host Prefix Length	The subnet mask for a manual binding to a DHCP client. Either <b>Host Mask</b> or <b>Prefix Length</b> can be configured to specify the subnet mask but not both. The valid range is 0 to 32.
Lease Time	Can be selected as <b>Infinite</b> to specify lease time as Infinite or <b>Specified Duration</b> to enter a specific lease period. In case of dynamic binding infinite implies a lease period of 60 days and In 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 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 the lease period. This field appears only if the user specified <b>Specified Duration</b> as the Lease time. The valid range is 0 to 22.
Minutes	The number of minutes of 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 <b>Default Router Addresses</b> for the pool. Click the arrow beside the field name to expand the screen and display a table where you can specify up to eight default router addresses in order of preference.
DNS Server Addresses	The list of <b>DNS Server Addresses</b> for the pool. Click the arrow beside the field name to expand the screen and display a table where you can specify up to eight DNS Server Addresses in order of preference.
NetBIOS Name Server Addresses	The list of <b>NetBIOS Name Server Addresses</b> for the pool. Click the arrow beside the field name to expand the screen and display a table where you can specify up to eight 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 <b>Next Server Address</b> for the pool.
Domain Name	The domain name for a DHCP client. <b>Domain Name</b> can be up to 255 characters in length.
Bootfile	The name of the default boot image for a DHCP client. File Name can be up to 128 characters in length.



## Configure DHCP Pool Options

➤ **To configure 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**.

The screenshot shows the web management interface with the following structure:

- Top Navigation Bar:** System, Switching, Routing, QoS, Security, Monitoring, Maintenance.
- Sub-Navigation Bar:** Management, Device View, Services, Chassis, PoE, SNMP, LLDP, ISDP, Timer Schedule.
- Left Sidebar (Services):**
  - DHCP Server
    - DHCP Server Configuration
    - DHCP Pool Configuration
    - DHCP Pool Options** (selected)
    - DHCP Server Statistics
- Main Content Area (DHCP Pool Options):**

Pool Name	Option Code	Option Type	Option Value
test	150	IP Address	192.168.10.4

8. In **Pool Name** list, 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. Click the **Add** button.
 

The Option Code is added for the selected pool.
13. To delete the Option Code for the selected pool, click the **Delete** button.

## View DHCP Server Statistics

➤ **To view the 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**.

<b>Binding Details</b>	
Automatic Bindings	0
Expired Bindings	0
Malformed Messages	0
<b>Message Received</b>	
DHCPDISCOVER	0
DHCPREQUEST	0
DHCPDECLINE	0
DHCPRELEASE	0
DHCPINFORM	0
<b>Message Sent</b>	
DHCPOFFER	0
DHCPACK	0
DHCPNAK	0

The following table describes the DHCP Server Statistics fields.

**Table 33. DHCP Server Statistics**

Field	Description
Automatic Bindings	The number of automatic bindings on the DHCP Server.
Expired Bindings	The number of expired bindings on the DHCP Server.
Malformed Messages	The number of the malformed messages.
DHCPDISCOVER	The number of DHCPDISCOVER messages received by the DHCP Server.
DHCPREQUEST	The number of DHCPREQUEST messages received by the DHCP Server.
DHCPDECLINE	The number of DHCPDECLINE messages received by the DHCP Server.
DHCPRELEASE	The number of DHCPRELEASE messages received by the DHCP Server.
DHCPINFORM	The number of DHCPINFORM messages received by the DHCP Server.
DHCPOFFER	The number of DHCPOFFER messages sent by the DHCP Server.
DHCPACK	The number of DHCPACK messages sent by the DHCP Server.
DHCPNAK	The number of DHCPNAK messages sent by the DHCP Server.

## View DHCP Bindings Information

### ➤ To view the DHCP 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 **System > Services > DHCP Server > DHCP Bindings Information**.

8. To display DHCP Bindings Information, select one of the following radio buttons:
- **All Dynamic Bindings.** Specify all dynamic bindings to be deleted.
  - **Specific Dynamic Binding.** Specify specific dynamic binding to be deleted.

The following table describes the DHCP Bindings Information fields.

**Table 34. DHCP Bindings Information**

Field	Description
IP Address	The client's IP address.
Hardware Address	The client's hardware address.
Lease Time Left	The Lease Time Left in Days, Hours and Minutes dd:hh:mm format.
Type	The Type of Binding: Dynamic or Manual.

## View DHCP Conflicts

You can view information on hosts with address conflicts, such as when the same IP address is assigned to two or more devices on the network.

➤ **To view the DHCP conflicts:**

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

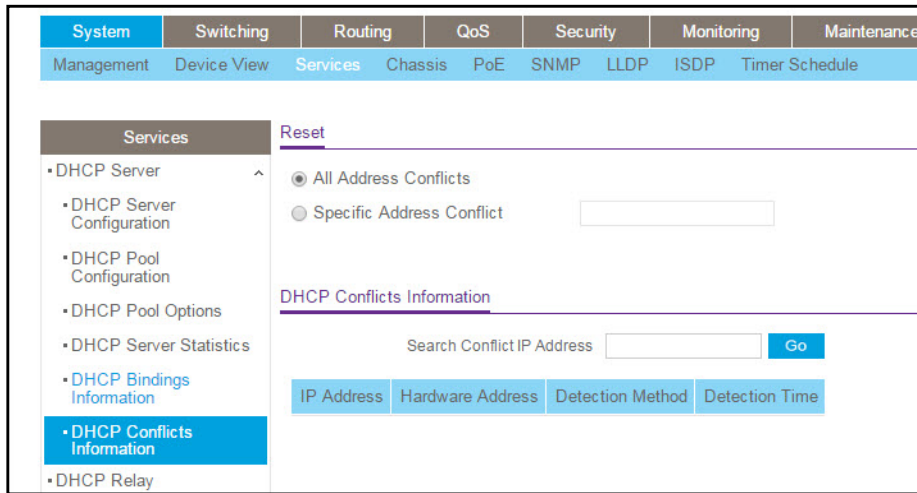
5. Enter the user name and password.

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 Conflicts Information**.



8. To display DHCP conflicts information, select one of the following radio buttons:

- **All Address Conflicts.** Specify all address conflicts to be deleted.
- **Specific Address Conflict.** Specify a specific dynamic binding to be deleted.

The following table describes the DHCP Conflicts Information fields.

**Table 35. DHCP Conflicts Information**

Field	Description
IP Address	The IP address of the host as recorded on the DHCP server.
Hardware Address	The client's hardware address.
Detection Method	The manner in which the IP address of the hosts were found on the DHCP server.
Detection Time	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 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' field.

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, which represents 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.

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 Statistics fields.

**Table 36. 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.

## DHCP L2 Relay

### Configure Global DHCP L2 Relay Settings

➤ **To configure global DHCP L2 Relay 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 > DHCP L2 Relay > DHCP L2 Relay Global Configuration**.

DHCP L2 Relay Global Configuration			
Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable		

DHCP L2 Relay VLAN Configuration			
VLAN ID	Admin Mode	Circuit ID Mode	Remote ID String
1	Disable	Disable	

8. Select the Admin mode **Disable** or **Enable** radio button.  
For global configuration, this enables or disables the DHCP L2 Relay on the switch. The default is Disable.
9. For VLAN configuration, **VLAN ID** shows the VLAN ID configured on the switch.
  - a. Use **Admin mode** to enable or disable the DHCP L2 Relay on the selected VLAN.
  - b. Use **Circuit ID mode** to enable or disable the Circuit ID suboption of DHCP Option-82.
  - c. Use **Remote ID String** to specify the Remote ID when Remote ID mode is enabled.
10. Click the **Apply** button.

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

- Pagination Navigation Menu
  - Rows per page. Select how many table entries are displayed per screen. Possible values are 20, 50, 100, 200, and All.

**Note:** If you select All, the browser might be slow to display the information.

- < Display the previous page of the table data entries.
- > Display the next page of the table data entries.

## Configure a DHCP L2 Relay Interface

### ➤ To configure DHCP L2 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 L2 Relay > DHCP L2 Relay Interface Configuration**.

Interface	Admin Mode	82 Option Trust Mode
<input type="checkbox"/> 1/0/1	Disable	Disable
<input type="checkbox"/> 1/0/2	Disable	Disable
<input type="checkbox"/> 1/0/3	Disable	Disable
<input type="checkbox"/> 1/0/4	Disable	Disable
<input type="checkbox"/> 1/0/5	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.

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 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
1/0/1	0	0	0	0
1/0/2	0	0	0	0
1/0/3	0	0	0	0
1/0/4	0	0	0	0
1/0/5	0	0	0	0

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

**Table 37. DHCP L2 Relay Interface Statistics**

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

## Configure UDP Relay Global Settings

- **To configure 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				
<input type="checkbox"/>	Server Address	UDP Port	UDP Port Other Value	Hit Count
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>	

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

This enables or disables 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 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 Routing Image Protocol (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. Click the **Add** button.

This creates an entry in UDP Relay Table with the specified configuration.

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

14. Click the **Apply** button.

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

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

To refresh the screen, click the **Update** button.

## Configure UDP Relay Interface Settings

### ➤ To configure UDP Relay 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 > Services > UDP Relay > UDP Relay Interface Configuration**.

UDP Relay Interface Configuration						
<input type="checkbox"/>	Interface	Server Address	UDP Port	UDP Port Other Value	Discard	Hit Count
	▼		▼		▼	

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 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 the user to enter their 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/disable dropping of matched packets.

Enable can be chosen only when a user enters 0.0.0.0 IP address. Discard mode can be set to Disable when user adds a new entry with a non-zero IP address.

13. Click the **Add** button.

This creates an entry in UDP Relay Table with the specified configuration.

14. Click the **Apply** button.

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

To remove all entries or a specified one from UDP Relay Interface Configuration Table, click the **Delete** button.

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

To refresh the screen, click the **Update** button.

## Enable or Disable DHCPv6 Server

You can configure the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server settings on the device. The device can act as a DHCPv6 server or DHCPv6 relay agent to help assign network configuration information to IPv6 clients.

➤ **To enable or disable DHCP 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.

The Login screen displays.

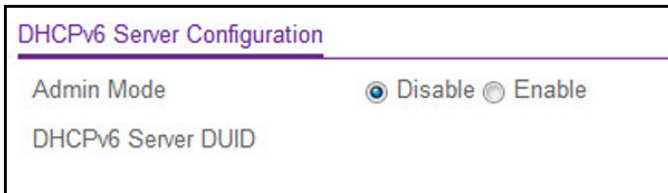
5. Enter the user name and password.

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 > DHCPv6 Server > DHCPv6 Server Configuration**.



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

This specifies whether the DHCPv6 Service administrative mode is enabled or disabled. The default value is Disable.

9. Use the **DHCPv6 Server DUID** field to specify the DHCP Unique Identifier (DUID) of the DHCPv6 server.

10. Click the **Apply** button.

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

## Configure the DHCPv6 Pool

You can view the currently configured DHCPv6 server pools as well as to add and remove pools. A DHCPv6 server pool is a set of network configuration information available to DHCPv6 clients that request the information.

➤ **To configure DHCPv6 pool 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 > DHCPv6 Server > DHCPv6 Pool Configuration**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance		
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP	Timer Schedule

Services	DHCPv6 Pool Configuration
• DHCP Server	Pool Name <input type="text"/> Create
• DHCP Relay	Pool Name <input type="text"/>
• DHCP L2 Relay	DNS Server Addresses
• UDP Relay	Domain Name
• DHCPv6 Server	
• DHCPv6 Server Configuration	
• DHCPv6 Pool Configuration	
• DHCPv6 Prefix Delegation Configuration	

The **Pool Name** field shows the names of all the existing pools and the **Create** option.

**Note:** If you are logged in as a user with read-only permission, the **Pool Name** field displays only the existing pool names. To create a pool, you must log in with the admin user name, which has read/write permissions.

8. To create a pool, select **Create**, and enter a unique name that identifies the DHCPv6 server pool to be created.

The name can be up to 31 alphanumeric characters in length.

9. Use the **Default Router Addresses** field to specify the list of default router addresses for the pool.

The user can specify up to eight default router addresses in order of preference.

10. Use the **Domain Name** field to specify the domain name for a DHCPv6 client in the pool.

The domain name can be up to 255 alphanumeric characters in length.

To delete the selected pool on the switch, click the **Delete** button.

11. Click the **Apply** button.

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

## Configure the DHCPv6 Prefix Delegation

### ➤ To configure the DHCPv6 Prefix delegation 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 > DHCPv6 Server > DHCPv6 Prefix Delegation Configuration**.



DHCPv6 Prefix Delegation Configuration							
<input type="checkbox"/>	Pool Name	Prefix	Prefix Length	DUID	Client Name	Valid Lifetime	Prefer Lifetime
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

8. Select from the list of configured **Pool Names**.
9. In the **Prefix** and **Prefix Length** fields, specify the delegated IPv6 prefix.
10. In the **DUID** field, specify the DUID identifier used to identify the client's unique DUID value.
11. Specify the **Client Name**, which is useful for logging or tracing only.  
The name can be up to 31 alphanumeric characters.
12. Specify the **Valid Lifetime** in seconds for the delegated prefix.  
Valid values are 0 to 4294967295.
13. Specify the **Prefer Lifetime** in seconds for the delegated prefix.  
Valid values are 0 to 4294967295.
14. Click the **Add** button.  
The delegated prefix is added for the selected pool.
15. To delete the delegated prefix for the selected pool, click the **Delete** button.
16. Click the **Apply** button.  
The updated configuration is sent to the switch. Configuration changes take effect immediately.

## Configure DHCPv6 Interface Settings

You can configure the per-interface settings for DHCPv6. The DHCPv6 interface modes are mutually exclusive. The fields that can be configured on this screen depend on the selected mode for the interface.

### ➤ To configure DHCPv6 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 > Services > DHCPv6 Server > DHCPv6 Interface Configuration**.

DHCPv6 Interface Configuration					
1 All		Go To Interface <input type="text"/>		Go	
<input type="checkbox"/>	Interface	Admin mode	Pool Name	Rapid Commit	Preference
<input type="checkbox"/>		<input type="text" value="v"/>	<input type="text" value="v"/>	<input type="text" value="v"/>	<input type="text"/>
<input type="checkbox"/>	1/0/1	Disable			
<input type="checkbox"/>	1/0/2	Disable			
<input type="checkbox"/>	1/0/3	Disable			
<input type="checkbox"/>	1/0/4	Disable			
<input type="checkbox"/>	1/0/5	Disable			

8. Select the Interface with the information to view or configure. You can either:
  - a. In the **Go To Interface** field, enter the interface in unit/slot/port format and click the **Go** button. The entry corresponding to the specified interface is selected.
  - b. Select the check box from the list of **Interfaces** configured for DHCPv6 server functionality.
9. In the **Admin mode** list, select to **Enable** or **Disable** DHCPv6 mode to configure server functionality.

DHCPv6 server and DHCPv6 relay functions are mutually exclusive.

10. In the **Pool Name** field, specify the DHCPv6 pool containing stateless and/or prefix delegation parameters.
11. **Rapid Commit** is an optional parameter. In the **Rapid Commit** list, select to **Enable** or **Disable** allowing an abbreviated exchange between the client and server.
12. In the **Preference** field, specify the preference value used by clients to determine the preference between DHCPv6 servers.

Valid values are 0 to 4294967295. The default value is 0.

13. Click the **Apply** button.

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

## View DHCPv6 Bindings Information

You can view entries in the DHCP Bindings table. After a client acquires IPv6 configuration information from the DHCPv6 server, the server adds an entry to its database. The entry is called a binding.

➤ **To view DHCPv6 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.

The Login screen displays.

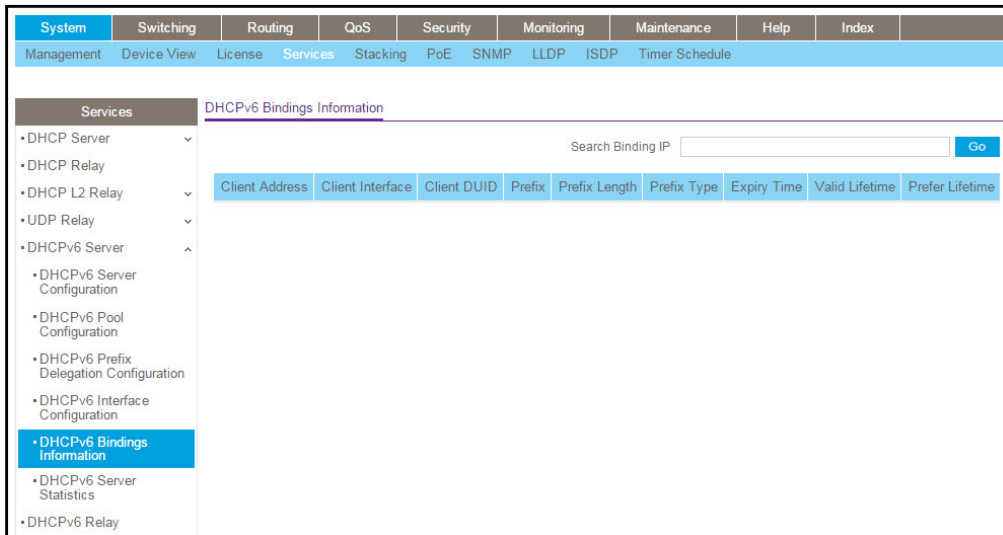
5. Enter the user name and password.

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 > DHCPv6 Server > DHCPv6 Bindings Information**.



To refresh the screen, click the **Update** button.

The following table describes the nonconfigurable fields that are displayed.

**Table 38. DHCPv6 Binding Information**

Field	Description
Client Address	The IPv6 address of the client associated with the binding.
Client Interface	The interface number where the client binding occurred.

**Table 38. DHCPv6 Binding Information (continued)**

Field	Description
Client DUID	The DHCPv6 Unique Identifier (DUID) of the client. The DUID is a combination of the client's hardware address and client identifier.
Prefix	The IPv6 address for the delegated prefix associated with this binding.
Prefix Length	The IPv6 mask length for the delegated prefix associated with this binding.
Prefix Type	The type of IPv6 prefix associated with this binding.
Expiry Time	The number of seconds until the prefix associated with a binding expires.
Valid Lifetime	The maximum amount of time in seconds that the client is allowed to use the prefix.
Prefer Lifetime	The preferred amount of time in seconds that the client is allowed to use the prefix.

## View DHCPv6 Server Statistics

You can view the DHCPv6 server statistics for the device, including information about the DHCPv6 messages, sent, received, and discarded globally and on each interface. The values on the screen indicate the various counts that accumulated since they were last cleared.

### ➤ To view DHCPv6 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 > DHCPv6 Server > DHCPv6 Server Statistics**.

DHCPv6 Interface Selection

Interface
1/0/1

Messages Received:

Total DHCPv6 Packets Received	0
DHCPv6 Solicit Packets Received	0
DHCPv6 Request Packets Received	0
DHCPv6 Confirm Packets Received	0
DHCPv6 Renew Packets Received	0
DHCPv6 Rebind Packets Received	0
DHCPv6 Release Packets Received	0
DHCPv6 Decline Packets Received	0
DHCPv6 Inform Packets Received	0
DHCPv6 Relay-forward Packets Received	0
DHCPv6 Relay-reply Packets Received	0
DHCPv6 Malformed Packets Received	0
Received DHCPv6 Packets Discarded	0

Messages Sent:

Total DHCPv6 Packets Sent	0
DHCPv6 Advertisement Packets Transmitted	0
DHCPv6 Reply Packets Transmitted	0
DHCPv6 Reconfig Packets Transmitted	0
DHCPv6 Relay-forward Packets Transmitted	0
DHCPv6 Relay-reply Packets Transmitted	0

8. To view detailed DHCPv6 statistics for an interface, from the **Interface** list select the entry for which data is to be displayed.

If you select **All**, data is shown for all interfaces.

To reset the DHCPv6 counters for one or more interface, select each interface with the statistics to reset and click the **Clear** button.

To refresh the screen, click the **Update** button.

The following table describes the nonconfigurable fields that are displayed.

**Table 39. DHCPv6 Server Statistics**

Field	Description
Messages Received	The aggregate of all interface level statistics for received messages.
Total DHCPv6 Packets Received	The number of DHCPv6 messages received on the interface. The DHCPv6 messages sent from a DHCP v6 client to a DHCP v6 server include solicit, request, confirm, renew, rebind, release, decline, and information-request messages. Additionally, a DHCP v6 relay agent can forward relay-forward messages to a DHCP v6 server.
DHCPv6 Solicit Packets Received	The number of DHCPv6 Solicit messages received on the interface. This type of message is sent by a client to locate DHCPv6 servers.

**Table 39. DHCPv6 Server Statistics (continued)**

Field	Description
DHCPv6 Request Packets Received	The number of requests.
DHCPv6 Confirm Packets Received	The number of DHCPv6 Confirm messages received on the interface. This type of message is sent by a client to all DHCPv6 servers to determine whether its configuration is valid for the connected link.
DHCPv6 Renew Packets Received	The number of DHCPv6 Renew messages received on the interface. This type of message is sent by a client to extend and update the configuration information provided by the DHCPv6 server.
DHCPv6 Rebind Packets Received	The number of DHCPv6 Rebind messages received on the interface. This type of message is sent by a client to any DHCPv6 server when it does not receive a response to a Renew message.
DHCPv6 Release Packets Received	The number of DHCPv6 Release messages received on the interface. This type of message is sent by a client to indicate that it no longer needs the assigned address.
DHCPv6 Decline Packets Received	The number of DHCPv6 Decline messages received on the interface. This type of message is sent by a client to the DHCPv6 server to indicate that an assigned address is already in use on the link.
DHCPv6 Inform Packets Received	The number of DHCP v6 information-request messages received on the interface. This type of message is sent by a client to request configuration information other than IP address assignment.
DHCPv6 Relay-forward Packets Received	The number of DHCPv6 relay-forward messages received on the interface. This type of message is sent by a relay agent to forward messages to servers.
DHCPv6 Relay-reply Packets Received	The number of DHCP v6 relay-reply messages received on the interface. This type of message is sent by a server to a DHCP v6 relay agent and contains the message for the relay agent to deliver to the client.
DHCPv6 Malformed Packets Received	The number of DHCPv6 messages that were received on the interface but were dropped because they were malformed.
Received DHCPv6 Packets Discarded	The number of Packets Discarded.
Messages Sent	The aggregate of all interface level statistics for messages sent.
Total DHCPv6 Packets Sent	The number of DHCPv6 messages sent by the interface. The DHCPv6 messages sent from a DHCPv6 server to a DHCPv6 client include Advertise, Reply, Reconfigure, and Relay-Reply messages.
DHCPv6 Advertisement Packets Transmitted	The number of DHCPv6 Advertise messages sent by the interface. This type of message is sent by a server to a DHCPv6 client in response to a Solicit message and indicates that it is available for service.
DHCPv6 Reply Packets Transmitted	The number of DHCPv6 Reply messages sent from the interface to a DHCPv6 client in response to a solicit, request, renew, rebind, information-request, confirm, release, or decline message.

Table 39. DHCPv6 Server Statistics (continued)

Field	Description
DHCPv6 Reconfig Packets Transmitted	The number of DHCPv6 reconfigure messages sent by the interface. This type of message is sent by a server to a DHCPv6 client to inform the client that the server has new or updated information. The client then typically initiates a renew/reply or Information-request/reply transaction with the server to receive the updated information.
DHCPv6 Relay-forward Packets Transmitted	The number of DHCPv6 Relay-Forward messages sent by the interface. This type of message is sent by a relay agent to forward messages to servers.
DHCPv6 Relay-reply Packets Transmitted	The number of DHCPv6 Relay-Reply messages sent by the interface. This type of message is sent by a server to a DHCPv6 relay agent and contains the message for the relay agent to deliver to the client.

## Configure DHCPv6 Relay for an Interface

### ➤ To configure DHCPv6 Relay 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 **System > Services > DHCPv6 Relay**.

**DHCPv6 Relay Configuration**

1 2 3 All      Go To Interface  **Go**

<input type="checkbox"/>	Interface	Admin Mode	Relay Interface	Destination IP Address	Remote ID
<input type="checkbox"/>		<input type="text"/> ▼	<input type="text"/> ▼	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	1/0/1	Disable			
<input type="checkbox"/>	1/0/2	Disable			
<input type="checkbox"/>	1/0/3	Disable			
<input type="checkbox"/>	1/0/4	Disable			
<input type="checkbox"/>	1/0/5	Disable			

8. Select the Interface with the information to view or configure. You can either:
  - In the **Go To Interface** field, enter the interface in unit/slot/port format and click the **Go** button. The entry corresponding to the specified interface is selected.
  - Select the check box from the list of **Interfaces** configured for DHCPv6 Relay functionality.
9. In the **Admin mode** field, specify the DHCPv6 mode, either Enable or Disable, to configure DHCPv6 Relay functionality.

The default is Disable. DHCPv6 server and DHCPv6 relay functions are mutually exclusive.

10. From the **Relay Interface** list, select an interface to reach a relay server.
11. In the **Destination IP Address**, specify an IPv6 address to reach a relay server.
12. In the **Remote ID** field, specify the relay agent information option.

The remote ID is derived from the DHCPv6 server DUID and the relay interface number, or it can be specified as a user-defined string.

13. Click the **Apply** button.

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

## Configure Basic PoE

### ➤ To configure basic 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.

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**.

Unit	Model	Host	Status	Firmware Version	Power Status	Total Power (Main AC) Watt	Total Power (RPS) Watt	Power Source	Threshold Power mW	Consumed Power mW	System Usage Threshold (1% to 99%)
1	XCM8948							PD (0/2)			90

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

8. To change the PoE unit, select another unit from the list.
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. The **Power Management mode** describes or controls 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. To set the traps, select **Enable** to activate the PoE traps.

Select **Disable** to deactivate 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 40. PoE Configuration nonconfigurable Fields**

Field	Description
Units	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.

**Table 40. PoE Configuration nonconfigurable Fields (continued)**

Field	Description
Total Power (Main AC)	The total power provided by the MAIN AC power source.
Total Power (RPS)	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. 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 a power which is currently being delivered to all ports.

## Congure PoE Settings

### ➤ To configure 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.  
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 Configuration**.

1 All	Unit	Model	Host	Status	Firmware Version	Power Status	Total Power (Main AC) Watt	Total Power (RPS) Watt	Power Source	Threshold Power mW	Consumed Power mW	System Usage Threshold (1% to 99%)
1	1	XCM8948							PD (0/2)			90

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

8. To change the PoE unit, select another unit from the list.
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.** The **Power Management mode** describes or controls 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.** To set the traps, select **Enable** to activate the PoE traps.

Select **Disable** to deactivate 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 41. PoE Configuration**

Field	Description
Units	The current PoE Unit. You can change the PoE Unit by selecting another unit ID listed here.
Firmware Version	The version of the PoE controller's FW image.
Power Status	Indicates the power status.
Total Power (Main AC)	The total power provided by the MAIN AC power source.
Total Power (RPS) Total Power (PD) for GSM5212P switches only	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. i.e. 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 which is currently being delivered to all ports.

## Configure PoE Ports

### ➤ To configure PoE 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 **System > PoE > Advanced > PoE Port Configuration**.

8. Select the **Admin mode (Enable or Disable)** to determine the ability of the port to deliver power.
9. **Port Priority** is used to determine which ports can deliver power when the total power delivered by the system crosses a specific threshold.

If the switch cannot supply power to all connected devices, the priority determines which ports can supply power. The lowest numbered ports with the same Port Priority setting are given 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** indicates that the port power limit is equal to the class of the PD attached.

- **User** indicates that the port power limit is equal to the value specified by Power Limit.
  - **None** indicates that the port draws up to class 0 maximum power in low power mode and up to class 4 maximum power in high power mode.
12. Select the **Power Limit** to define the maximum power (in watts) which 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 is sent to the switch. Configuration changes take effect immediately.

The following table describes the PoE Configuration nonconfigurable fields.

**Table 42. PoE Configuration**

Field	Description
Port	The interface for which data is to be displayed or configured.
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 42. PoE Configuration (continued)

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

## Configure SNMP

You can configure SNMP settings for SNMP V1/V2 and SNMPv3.

### Configure the SNMP V1/V2 Community

By default, two SNMP communities exist:

- 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 defaults or to add other communities. Only the communities that you define can access to the switch using the SNMP V1 and SNMP V2 protocols. Only those communities with read/write level access can be used to change the configuration using SNMP.

---

**Note:** If you want to use SNMP v3, use the User Accounts menu.

---

#### ➤ To configure the SNMP V1/V2 community:

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

3. Launch a web browser.
4. Enter 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**.

Community Configuration					
<input type="checkbox"/>	Community Name	Client Address	Client IP Mask	Access Mode	Status
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="v"/>	<input type="text" value="v"/>
<input type="checkbox"/>	public	0.0.0.0	0.0.0.0	Read-Only	Enable
<input type="checkbox"/>	private	0.0.0.0	0.0.0.0	Read-Write	Enable

8. Use **Community Name** to reconfigure an existing community, or to create a new one.

Use this menu to select one of the existing community names, or select 'Create' to add a new one. A valid entry is a case-sensitive string of up to 16 characters.

9. **Client Address.** Taken together, the Client Address and Client IP Mask denote a range of IP addresses from which SNMP clients can use that community to access this device.

If either (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 Client Address.

10. **Client IP Mask.** Taken together, the Client Address and Client IP Mask denote a range of IP addresses from which SNMP clients can use that community to access this device.

If either (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 IP 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 Client Address.

11. In the **Access mode** menu, select **Read-Write** or **Read-Only**.

This specifies the access level for this community.

12. 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 are rejected. If you select disable, the Community Name becomes invalid.

13. Click the **Add** button.

This adds the selected community to the switch.

14. To delete the selected Community Name, click the **Delete** button.

## Configure SNMP V1/V2 Trap Settings

### ➤ To configure the SNMP V1/V2 trap 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 > Trap Configuration**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help
Management	Device View	Services	Chassis	PoE	SNMP	LLDP	ISDP
Timer Schedule							

SNMP	Trap Source Interface Configuration
• SNMP V1/V2 ^	Source Interface: vlan 1
• Community Configuration	
• <b>Trap Configuration</b>	Trap Configuration
• Trap Flags	
• Supported MIBS	
• SNMP V3 v	

Community Name	Version	Protocol	Address	Status
	SNMP V1	IPv4		Disable

8. In the **Source Interface** list, select the source interface to use for SNMP Trap receiver.



Possible values are as follows:

- Routing interface
- Routing VLAN
- Routing loopback interface
- Tunnel interface
- Service port

VLAN 1 is used as source interface by default.

9. To add a host that receives SNMP traps, do the following steps:
  - a. **Community Name.** Enter the community string for the SNMP trap packet to be sent to the trap manager. This name can be up to 16 characters and is case-sensitive.
  - b. **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.
  - c. **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.
  - d. **Address.** Enter the IPv4 address in x.x.x.x format or the IPv6 address in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx to receive SNMP traps from this device. The length of the address cannot exceed 39 characters.
  - e. **Status.** Select the receiver's status:
    - **Enable.** Send traps to the receiver
    - **Disable.** Do not send traps to the receiver.
  - f. Click the **Add** button.
10. To modify information about an existing SNMP recipient, select the check box for the recipient, and change the desired fields.
11. To delete a recipient, select the check box for the recipient and click the **Delete** button.
12. Click the **Apply** button.

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

## Configure SNMP V1/V2 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 the 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**.

Trap Flags	
Authentication	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Link Up/Down	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Multiple Users	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Spanning Tree	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
ACL	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Captive Portal	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
DVMRP	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
PIM	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
PoE	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
OSPFv2 Traps:	
errors:	
authentication-failure	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
bad-packet	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
config-error	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
virt-authentication-failure	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
virt-bad-packet	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
virt-config-error	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Isa:	
Isa-maxage	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Isa-originate	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
overflow:	
Isdb-overflow	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Isdb-approaching-overflow	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
retransmit:	
packets	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

8. Select the Authentication **Disable** or **Enable** radio button.

This enables or disables activation of authentication failure traps. The factory default is Enable.

9. Select the Link Up/Down **Disable** or **Enable** radio button

This enables or disables activation of link status traps. The factory default is Enable.

10. Select the Multiple Users **Disable** or **Enable** radio button

This enables or disables activation of multiple user traps. The factory default is Enable. This trap is triggered when the same user ID is logged into the switch more than once at the same time (either through Telnet or the serial port).

11. Select the Spanning Tree **Disable** or **Enable** radio button.

This enables or disables activation of spanning tree traps. The factory default is Enable.

12. Select the ACL **Disable** or **Enable** radio button.

This enables or disables activation of ACL traps. The factory default is Disable.

13. Select the PoE **Disable** or **Enable** radio button.

This enables or disables activation of PoE traps. The factory default is Enable. 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 the Supported MIBs

### ➤ To view all the MIBs supported by 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.

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

Status	
Name	Description
RFC 1907 - SNMPv2-MIB	The MIB module for SNMPv2 entities
RFC 2819 - RMON-MIB	Remote Network Monitoring Management Information Base
HC-RMON-MIB	The original version of this MIB, published as RFC3273.
HC-ALARM-MIB	Initial version of the High Capacity Alarm MIB module. This version published as RFC 3434.
HCNUM-TC	A MIB module containing textual conventions for high capacity data types.
NETGEAR-REF-MIB	NETGEAR 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.
NETGEAR-POWER-ETHERNET-MIB	NETGEAR Power Ethernet Extensions MIB
POWER-ETHERNET-MIB	Power Ethernet MIB
SFLOW-MIB	sFlow MIB
NETGEAR-SFLOW-MIB	The NETGEAR Private MIB for NETGEAR SFLOW
NETGEAR-ISDP-MIB	Industry Standard Discovery Protocol MIB
NETGEAR-UDLD-MIB	UDLD MIB
NETGEAR-BOXSERVICES-PRIVATE-MIB	The NETGEAR Private MIB for NETGEAR Box Services Feature.
DIFFSERV-DSCP-TC	The Textual Conventions defined in this module should be used whenever a Differentiated Services Code Point is used in a MIB.
IANA-ADDRESS-FAMILY-NUMBERS-MIB	The MIB module defines the AddressFamilyNumbers textual convention.
NETGEAR-DHCPSEVER-PRIVATE-MIB	The NETGEAR Private MIB for NETGEAR DHCP Server
NETGEAR-DHCPCLIENT-PRIVATE-MIB	The NETGEAR Private MIB for NETGEAR DHCP Client
NETGEAR-DNS-RESOLVER-CONTROL-MIB	Defines a portion of the SNMP MIB under the NETGEAR Corporation enterprise OID pertaining to DNS Client control configuration
NETGEAR-DENIALOFSERVICE-PRIVATE-MIB	The NETGEAR Private MIB for NETGEAR Denial of Service.
NETGEAR-GREENETHERNET-PRIVATE-MIB	The MIB definitions for NETGEAR Green Ethernet Feature.
NETGEAR-KEYING-PRIVATE-MIB	The NETGEAR Private MIB for NETGEAR Keying Utility

The following table describes the SNMP Supported MIBs Status fields.

**Table 43. SNMP Supported MIBs**

Field	Description
Name	The RFC number if applicable and the name of the MIB.
Description	The RFC title or MIB description.

## Configure SNMP V3 Users

### ➤ To configure SNMPv3 settings for the user account:

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

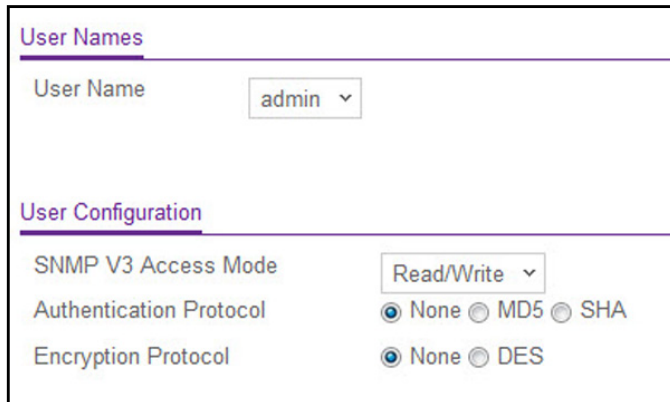
5. Enter the user name and password.

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 for SNMP V3. It has two main sections: 'User Names' and 'User Configuration'. In the 'User Names' section, there is a 'User Name' dropdown menu currently showing 'admin'. In the 'User Configuration' section, there are three settings: 'SNMP V3 Access Mode' is a dropdown menu set to 'Read/Write'; 'Authentication Protocol' has three radio buttons: 'None' (selected), 'MD5', and 'SHA'; 'Encryption Protocol' has two radio buttons: 'None' (selected) and 'DES'.

8. In the **User Name** list, select the user account to be configured.

The **SNMP v3 Access mode** field indicates the SNMPv3 access privileges for the user account. The admin account has read/write access, and all other accounts are assigned read-only access.

9. Select an **Authentication Protocol** radio button.

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 SNMPv3 authentication password, and you must therefore specify a password, and it must be eight characters long.

This specifies the SNMPv3 Authentication Protocol setting for the selected user account.

10. Select a **Encryption Protocol** radio button.

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.

This specifies the SNMPv3 Encryption Protocol setting for the selected user account.

11. If you selected **DES** in the **Encryption Protocol** field, enter the encryption key in the **SNMPv3 Encryption Key** field.

If you did not select DES, this field is ignored. Valid keys are 0 to 15 characters long. You must select the **Apply** check box to change the Encryption Protocol and Encryption Key.

12. 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/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/asset number).

## Configure LLDP Global Settings

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

### ➤ To configure global LLDP 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	<input type="text" value="30"/>	(5 to 32768 secs)
Transmit Hold Multiplier	<input type="text" value="4"/>	(2 to 10 secs)
Re-Initialization Delay	<input type="text" value="2"/>	(1 to 10 secs)
Notification Interval	<input type="text" value="5"/>	(5 to 3600 secs)

8. In the **Transmit Interval** field, enter the interval in seconds to transmit LLDP frames.  
The range is from 5 to 32768 secs. The default value is 30 seconds.
9. In the **Transmit Hold Multiplier** field, enter the multiplier on Transmit Interval to assign TTL.  
The range is from 2 to 10 secs. The default value is 4.
10. In the **Re-Initialization Delay** field, enter the delay before re-initialization.  
The range is from 1 to 10 secs. The default value is 2 seconds.
11. In the **Notification Interval** field, enter 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 updated configuration is sent to the switch. The changes take effect immediately but are not retained across a power cycle unless a save is performed.

## Configure the LLDP Interface

➤ **To configure the 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.  
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 > Interface Configuration**.

Interface Configuration

1 All Go To Port  **Go**

	Port	Link Status	Transmit	Receive	Notify	Operational TLV(s)				Transmit Management Information
						Port Description	System Name	System Description	System Capabilities	
<input type="checkbox"/>			<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	1/0/1	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	1/0/2	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	1/0/3	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	1/0/4	Down	Enable	Enable	Disable	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	1/0/5	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.  
The **Link Status** field indicates whether the link is up or down.
10. Use **Transmit** to specify the LLDP - 802.1AB transmit mode for the selected interface.
11. Use **Receive** to specify the LLDP - 802.1AB receive mode for the selected interface.
12. Use **Notify** to specify the LLDP - 802.1AB notification mode for the selected interface.
13. Optional TLV(s):
- Use **Port Description** to include port description TLV in LLDP frames.
  - Use **System Name** to include system name TLV in LLDP frames.
  - Use **System Description** to include system description TLV in LLDP frames.
  - Use **System Capabilities** to include system capability TLV in LLDP frames.
14. Use **Transmit Management Information** to specify whether 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 Update0 Days 00:00:00

Total Inserts0

Total Deletes0

Total Drops0

Total Ageouts0

LLDP Statistics

Interface	Transmit Total	Receive Total	Discards	Errors	Ageouts	TLV Discards	TLV Unknowns	TLV MED	TLV 802.1	TLV 802.3	TLV UPOE
1/0/1	0	0	0	0	0	0	0	0	0	0	0
1/0/2	0	0	0	0	0	0	0	0	0	0	0
1/0/3	0	0	0	0	0	0	0	0	0	0	0
1/0/4	0	0	0	0	0	0	0	0	0	0	0
1/0/5	0	0	0	0	0	0	0	0	0	0	0

The following table describes the LLDP Statistics fields.

**Table 44. LLDP Statistics**

Field	Description
Last Update	The time when an entry was created, modified or deleted in the tables associated with the remote system.
Total Inserts	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.
Total Deletes	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	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	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	The unit/slot/port for the interfaces.
Transmit Total	The number of LLDP frames transmitted by the LLDP agent on the corresponding port.

Table 44. LLDP Statistics (continued)

Field	Description
Receive Total	The number of valid LLDP frames received by this LLDP agent on the corresponding port, while the LLDP agent is enabled.
Discards	The number of LLDP TLVs discarded for any reason by the LLDP agent on the corresponding port.
Errors	The number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
Age outs	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 expired.
TLV Discards	The number of LLDP TLVs discarded for any reason by the LLDP agent on the corresponding port.
TLV Unknowns	The number of LLDP TLVs received on the local ports which were not recognized by the LLDP agent on the corresponding port.
TLV MED	The total number of LLDP-MED TLVs received on the local ports.
TLV 802.1	The total number of LLDP TLVs received on the local ports which are of type 802.1.
TLV 802.3	The total number of LLDP TLVs received on the local ports which 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 Interface Selection

Interface: 1/0/1

Local Device Information

Chassis ID Subtype	MAC Address
Chassis ID	C4:04:15:AD:7F:00
Port ID Subtype	Local
Port ID	1/0/1
System Name	
System Description	ProSafe 48-port Gigabit blade, 6.2.13.24, 1.0.0.5
Port Description	
System Capabilities Supported	bridge, router
System Capabilities Enabled	bridge
Management Address Type	IPv4
Management Address	10.27.65.73

8. In **Interface** list, select the ports on which LLDP - 802.1AB frames can be transmitted. The following table describes the LLDP Local Device Information fields.

**Table 45. LLDP Local Device Information**

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

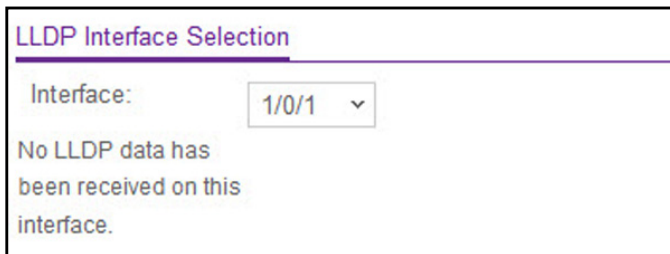
5. Enter the user name and password.

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 which can receive LLDP frames.

The following table describes the LLDP Remote Device Information fields.

**Table 46. 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 port identifier.
System Name	The system name of the remote system.

**Table 46. LLDP Remote Device Information (continued)**

Field	Description
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 which 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. The advertised management address of the remote system.</li> <li>Type. 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.  
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 > Remote Device Inventory**.

LLDP Remote Device Inventory

Search By Interface

Port	Remote Device ID	Management Address	MAC Address	System Name	Remote Port ID
------	------------------	--------------------	-------------	-------------	----------------

The following table describes the LLDP Remote Device Inventory fields.

**Table 47. LLDP Remote Device Inventory**

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

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 > Global Configuration**.

**Global Configuration**

---

Fast Start Repeat Count  (1 to 10)

Device Class

8. In the **Fast Start Repeat Count** field, enter the number of LLDP PDUs that are transmitted when the protocol is enabled.

The range is from (1 to 10). Default value of fast repeat count is 3.

The **Device Class** field specifies 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 Network Connectivity Device, which is typically a LAN Switch/Router, IEEE 802.1 Bridge, IEEE 802.11 Wireless Access Point and so on

## Configure LLDP-MED Interface

### ➤ To configure 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**.

Interface Configuration											
1 All		Go To Port <input type="text"/> <input type="button" value="Go"/>									
	Interface	Link Status	Med Status	Operational Status	Notification Status	Transmit Type Length Values					
						MED Capabilities	Network Policy	Location Identification	Extended Power via MDI-PSE	Extended Power via MDI-PD	Inventory Information
<input type="checkbox"/>	1/0/1	Down	Enable	Disable	Enable	Enable	Enable	Enable	Disable	Disable	Enable
<input type="checkbox"/>	1/0/2	Down	Enable	Disable	Enable	Enable	Enable	Enable	Disable	Disable	Enable
<input type="checkbox"/>	1/0/3	Down	Enable	Disable	Enable	Enable	Enable	Enable	Disable	Disable	Enable
<input type="checkbox"/>	1/0/4	Down	Enable	Disable	Enable	Enable	Enable	Enable	Disable	Disable	Enable
<input type="checkbox"/>	1/0/5	Down	Enable	Disable	Enable	Enable	Enable	Enable	Disable	Disable	Enable

The **Link Status** field displays the link status of the port (up or down).

The **Operational Status** field displays whether the LLDP-MED TLVs are transferred 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 is transmitted in the LLDP PDUs frames for the selected interface:
  - **MED Capabilities.** To transmit the capabilities TLV in LLDP frames.
  - **Network Policy.** To transmit the network policy TLV in LLDP frames.
  - **Location Identification.** To transmit the location TLV in LLDP frames.
  - **Extended Power via MDI - PSE.** To transmit the extended PSE TLV in LLDP frames.
  - **Extended Power via MDI - PD.** To 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 Interface Selection

Interface: 1/0/1

Network Policies Information

Media Application Type	VLAN ID	Priority	DSCP	Unknown Bit Status	Tagged Bit Status
------------------------	---------	----------	------	--------------------	-------------------

Inventory Information

Hardware Revision  
Firmware Revision  
Software Revision  
Serial Number  
Manufacturer Name  
Model Name  
Asset Id

Location Information

Sub Type	Location Information
Coordinate Based	
Civic Address	
ELIN	

Extended PoE

Device Type	Power Source	Power Priority	Power Value
None	Primary		

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 48. LDP-MED Local Device Information**

Field	Description
<b>Network Policy Information: Specifies if network policy TLV is present in the LLDP frames.</b>	
Media Application Type	<p>The application type. Types of application types are <b>unknown</b>, <b>voicesignaling</b>, <b>guestvoice</b>, <b>guestvoicesignalling</b>, <b>softphonevoice</b>, <b>videoconferencing</b>, <b>streammingvideo</b>, <b>vidoesignalling</b>.</p> <p>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.</p> <p>If a network policy TLV was transmitted, only then would this information be displayed</p>
<b>Inventory: Specifies if inventory TLV is present in LLDP frames</b>	
Hardware Revision	Specifies hardware version.

Table 48. LDP-MED Local Device Information (continued)

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

LLDP-MED Interface Selection					
Interface:		1/0/1			
Remote ID					
Capability Information					
Supported Capabilities					
Enabled Capabilities					
Device Class					
Network Policies Information					
Media Application Type	VLAN ID	Priority	DSCP	Unknown Bit Status	Tagged Bit Status
Inventory Information					
Hardware Revision					
Firmware Revision					
Software Revision					
Serial Number					
Manufacturer Name					
Model Name					
Asset Id					
Location Information					
Sub Type	Location Information				
Extended PoE					
Device Type					

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 49. LLDP-MED Remote Device Information**

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

Table 49. LLDP-MED Remote Device Information (continued)

Field	Description
Media Application Type	The application type. Types of application types are <b>unknown</b> , <b>voicesignaling</b> , <b>guestvoice</b> , <b>guestvoicesignalling</b> , <b>softphonevoice</b> , <b>videoconferencing</b> , <b>streamingvideo</b> , <b>vidoesignalling</b> . 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. If a network policy TLV was received on this port, only then would this information be displayed.
VLAN Id	The VLAN ID associated with a particular policy type.
Priority	The priority associated with a particular policy type.
DSCP	The DSCP associated with a particular policy type.
Unknown Bit Status	The unknown bit associated with a particular policy type.
Tagged Bit Status	The tagged bit associated with a particular policy type.
<b>Inventory Information: Specifies if inventory TLV is received in LLDP frames on this port.</b>	
Hardware Revision	Specifies hardware version of the remote device.
Firmware Revision	Specifies Firmware version of the remote device.
Software Revision	Specifies Software version of the remote device.
Serial Number	Specifies serial number of the remote device.
Manufacturer Name	Specifies manufacturers name of the remote device.
Model Name	Specifies model name of the remote device.
Asset ID	Specifies asset ID of the remote device.
<b>Location Information: Specifies if location TLV is received in LLDP frames on this port.</b>	
Sub Type	Specifies type of location information.
Location Information	The location information as a string for given type of location ID.
<b>Extended POE: Specifies if remote device is a PoE device.</b>	
Device Type	Specifies remote device's PoE device type connected to this port.
<b>Extended POE PSE: Specifies if extended PSE TLV is received in LLDP frame on this port</b>	
Available	The remote ports PSE power value in tenths of watts.
Source	The remote ports PSE power source.
Priority	The remote ports PSE power priority.
<b>Extended POE PD: Specifies if extended PD TLV is received in LLDP frame on this port.</b>	
Required	The remote port's PD power requirement.
Source	The remote port's PD power source.

Table 49. LLDP-MED Remote Device Information (continued)

Field	Description
Priority	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.  
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 > Remote Device Inventory**.

LLDP-MED Remote Device Inventory				
Port	Management Address	MAC Address	System Model	Software Revision

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

Table 50. 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.
MAC Address	The MAC address associated with the remote system.

Table 50. LLDP-MED Remote Device Inventory (continued)

Field	Definition
System Model	Specifies model name of the remote device.
Software Revision	Specifies Software version of the remote device.

## Configure ISDP

You can configure ISDP global and interface settings.

### Configure ISDP Basic Global Settings

➤ **To configure ISDP basic 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 > ISDP > Basic > Global Configuration**.

Global Configuration

Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Timer	<input type="text" value="30"/> (5 to 254 secs)
Hold Time	<input type="text" value="180"/> (10 to 255 secs)
Version 2 Advertisements	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Neighbors table last time changed	
Device ID	1234222
Device ID Format Capability	Serial Number, Host Name
Device ID Format	Serial Number

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

This specifies whether the ISDP Service is 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 must 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 Enabled.

The following table describes the ISDP Basic Global Configuration fields.

**Table 51. ISDP Basic Global Configuration**

Field	Description
Neighbors table last time changed	Specifies if
Device ID	The device ID of this switch.
Device ID Format Capability	The device ID format capability.
Device ID Format	The device ID format.

## 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.  
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 > Global Configuration**.

Global Configuration

Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Timer	<input type="text" value="30"/> (5 to 254 secs)
Hold Time	<input type="text" value="180"/> (10 to 255 secs)
Version 2 Advertisements	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Neighbors table last time changed	
Device ID	1234222
Device ID Format Capability	Serial Number, Host Name
Device ID Format	Serial Number

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

This specifies whether the ISDP Service is enabled or disabled. The default value is Enable.

9. 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.

10. 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 must 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.

The following table describes the ISDP Advanced Global Configuration fields.

**Table 52. ISDP Advanced Global Configuration**

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



## Configure an ISDP Interface

### ➤ To configure an 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.

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 > Interface Configuration**.

Interface Configuration		
1 All	Go To Port	Go
<input type="checkbox"/>	Port	Admin Mode
<input type="checkbox"/>	1/0/1	Enable
<input type="checkbox"/>	1/0/2	Enable
<input type="checkbox"/>	1/0/3	Enable
<input type="checkbox"/>	1/0/4	Enable
<input type="checkbox"/>	1/0/5	Enable

8. Use **Port** to select the port on which the admin mode is configured.
9. Use **Admin mode** to enable or disable ISDP on the port.

The default value is Enable.

## View an ISDP Neighbor

### ➤ To view an ISDP neighbor:

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



**Table 53. ISDP Neighbor (continued)**

Field	Description
Advertisement Version	The ISDP version sending from the neighbor.
Entry Last Changed Time	The time since last entry is changed.
Software Version	The software version on 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 Packets Received	0
ISDP Packets Transmitted	0
ISDPv1 Packets Received	0
ISDPv1 Packets Transmitted	0
ISDPv2 Packets Received	0
ISDPv2 Packets Transmitted	0
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 54. ISDP Statistics**

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

## Timer Schedule

You can configure the global timer settings and the timer schedule.

### Configure the Global Timer Settings

➤ **To configure the global timer 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**.

Timer Schedule Name			
<input type="checkbox"/>	Timer Schedule Name	Timer Schedule Status	ID
<input type="checkbox"/>			

8. Use the **Timer Schedule Name** to specify the name of a timer schedule.

9. Click the **Add** button.

The timer is added. The configuration changes take effect immediately.

10. To delete the selected timer schedules, click the **Delete** button.

The configuration changes take 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.

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 > Timer Schedule > Advanced > Schedule Configuration**.

8. In the **Timer Schedule Name** list, select the timer schedule.
9. In the **Timer Schedule Type** list, select **Absolute** or **Periodic**.
10. In the **Timer Schedule Entry** list, select the number of the timer schedule entries to be configured or added.
- If you are adding an entry, select **new**.
11. In the **Time Start** field, enter the time of the day in format (HH:MM) when the schedule operation is started.
- This field is required. If no time is specified, the schedule does not start running.
12. In the **Time End** field, enter the time of the day in format (HH:MM) when the schedule operation is terminated.
13. Use the **Date Start** to set the schedule start date.
- If no date is specified, the schedule starts running immediately.
14. Use the **Date Stop** to set the schedule termination date.
- If No End Date selected, the schedule operates indefinitely.
15. Use the **Recurrence Pattern** to show with what period the event repeats.
- If recurrence is not needed (a timer schedule must be triggered just once), then set Date Stop as equal to Date Start. There are the following possible values of recurrence:
- **Daily.** The timer schedule works with daily recurrence
- Daily mode.** Every WeekDay selection means that the schedule is triggered every day from Monday to Friday. Every Day(s) selection means that the schedule is triggered every defined number of days. If 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  
**Monthly mode.** Show the day of the month when the schedule is triggered. Field Every Month(s) means that the schedule is triggered every defined number of months.

**16.** Click the **Apply** button.

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

## 3. Chassis and Stacking

---

The chassis features apply only to the M6100 series switches. Stacking features apply only to the M5300 series switches

This chapter covers the following topics:

- *M6100 Series Switch Chassis Overview*
- *M5300 Series Switch Stacking Overview*



## M6100 Series Switch Chassis Overview

You can move the primary management unit (supervisor) functionality from one blade to another. When this change is applied, the entire chassis (including all interfaces in the chassis) is unconfigured and reconfigured with the configuration on the new primary management unit. After the reload is complete, all chassis management capability must be performed on the new primary management unit. To preserve the current configuration across a chassis move, save the current configuration to the NVRAM before performing the chassis move. A chassis move causes all routes and Layer 2 addresses to be lost. The system prompts the administrator to confirm the management move before the changes are applied.

### Configure Basic Chassis Settings

➤ **To configure the global status management mode and sample size:**

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

Unit ID	Switch Type	Hardware Management Preference	Management Status	Standby Status	Switch Status
1	XCM8944-PoE+	Unassigned	Management	None	OK
2	XCM8924X	Unassigned	ChassisMember	Oper Standby	OK
3	XCM8944F	Unassigned	ChassisMember	None	OK

Unit ID	Switch Description	Serial Number	Uptime	Plugged-in Model Identifier	Detected Code Version	Detected Code
1	XCM8944-PoE+	12345	0 days, 13 hours, 24 minutes, 58 secs	XCM8944-PoE+	Q.2.15.1	Q.2.15.1
2	XCM8924X	FSDWFSDFVSDKFVJDJFVDFJHDGJHDG	0 days, 13 hours, 25 minutes, 0 secs	XCM8924X	Q.2.15.1	Q.2.15.1

**Note:** You can also navigate to this screen by selecting **Advanced > Chassis Configuration**.

8. Select the **Management Unit**.

This field displays the current primary management unit. You can change it by selecting another blade ID listed here.

9. Click the **Apply** button to send the updated configuration to the switch.

Configuration changes take effect immediately.

**Note:** The Move Management operation might cause a change in the system IP address when the IP address is assigned by a DHCP server.

10. Select the **Chassis Sample Mode**.

The global status management mode, which can be one of the following:

- **Cumulative.** This tracks the sum of received time-stamp offsets cumulatively.
- **History.** This tracks the history of received timestamps.

11. Enter a value for **Max Samples** – the maximum number of samples to keep.

The valid range is 100 to 500. **Max Samples** applies to **History** mode.

12. Click the **Apply** button.

The updated configuration is sent to the switch. The mode and sample size parameters are applied globally to all units in the chassis. Configuration changes take effect immediately.

13. Select the **Unit ID** from the displayed list of blades.

14. Specify the **Switch Type**.

This specifies the type of blade hardware when you are creating a new blade in the chassis.

15. Select the **Management Status**. Indicates whether the selected switch is the management unit, or a normal chassis member, or on standby.

16. Click the **Apply** button.

The system prompts you to confirm the management move. Upon administrator confirmation, the entire chassis, including all interfaces in the chassis, is unconfigured and reconfigured with the configuration on the new primary management unit. Configuration changes take place immediately.

17. After the reload is complete, all chassis management capability must be performed on the new primary management unit.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable fields on the Chassis Configuration section.

**Table 55. Chassis Configuration section**

Field	Description
Hardware Management Preference	The hardware management preference of the blade. The hardware management preference can be disabled or unassigned.
Standby Status	Identifies the switch that is configured as the standby unit. The possible values are as follows: <ul style="list-style-type: none"> <li>• <b>Cfg Standby</b>. Indicates that the blade is configured as the standby blade. The blade configured as the Standby blade becomes the supervisor if the current supervisor fails.</li> <li>• <b>Opr Standby</b>. Indicates that this blade is operating as the standby.</li> </ul>
Switch Status	The status of the selected unit. The possible values are as follows: <ul style="list-style-type: none"> <li>• OK</li> <li>• Unsupported</li> <li>• Code Mismatch</li> <li>• Config Mismatch</li> <li>• Not Present</li> <li>• SDM Mismatch</li> <li>• Updating Code</li> </ul>

The following table describes the nonconfigurable fields displayed in the Basic Chassis Status.

**Table 56. Basic Chassis Status section**

Field	Description
Unit ID	The unit ID of the specific blade.
Switch Description	The description for the blade that can be configured by the user.
Serial Number	The unique box serial number for this blade.
Uptime	The relative time since the last reboot of the blade.

**Table 56. Basic Chassis Status section**

Field	Description
Plugged-in Model Identifier	The model type assigned by the device manufacturer to identify the plugged-in device.
Detected Code Version	Indicates the detected version of code on this blade.
Detected Code in Flash	The release number and version number of the code stored in flash.
SFS Last Attempt Status	The stack firmware synchronization last attempt status.

## View the Chassis Protocol Information

### ➤ To view chassis protocol 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 > Chassis > Advanced > Chassis Status**.

Unit ID	Neighbor Unit ID	Current	Average	Min	Max	Dropped
1	2	2000	2000	1964	2035	2
1	3	2000	2000	1980	2032	0

Unit ID	Watchdog Counter
1	0
2	0
3	0

8. Select either the **Unit ID** or **All**.

- Select the **Unit ID** to display information for the selected unit.
- Select **All** to display information for all units.

The following table describes the nonconfigurable Advanced Chassis Status data that is displayed.

**Table 57. Advanced Chassis Status**

Field	Description
Unit ID	The unit ID of the specific blade.
Neighbor Unit ID	The neighboring blade with which data is exchanged.
Current	Current time of heartbeat message reception.
Average	Average time of heartbeat messages received.
Min	Minimum time of heartbeat messages received.
Max	Maximum time of heartbeat messages received.
Dropped	Heartbeat messages dropped or lost counter.

➤ **To clear the sampling 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. Click **System > Chassis > Advanced > Chassis Status**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance
Management	Device View	Services	Chassis	PoE	SNMP	LLDP
					ISDP	Timer Schedule

Chassis		Chassis Status						
• Basic	▼	1 2 3 All						
• Advanced	▲							
• Chassis Configuration								
• Chassis Status								
• Backplane-port Configuration								
• Backplane-port Diagnostics								
• Chassis Power Configuration								
• Chassis Power Rebalance								
• Chassis Firmware Synchronization								
• NSF	▼							

Unit ID	Neighbor Unit ID	Current	Average	Min	Max	Dropped
1	2	2000	2000	1964	2035	2
1	3	2000	2000	1980	2032	0

1 2 3 All

Clear sampling information

Clear counters

Watchdog Status

Unit ID	Watchdog Counter
1	0
2	0
3	0

8. In the **Clear sampling information > Clear counters** field, select the unit to clear the counters.

Possible choices are **None**, a **unit ID** number, or **All**.

9. To display watchdog status, scroll down to the Watchdog Status section.

The following table describes the nonconfigurable **Watchdog Status** data that is displayed.

**Table 58. Watchdog Status**

Field	Description
Unit ID	The unit ID of the specific blade.
Watchdog Counter	The watchdog reset counter for the corresponding unit.

## View Chassis Backplane-Port Configuration

➤ **To view backplane-port 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 > Chassis > Advanced > Backplane-port Configuration**.

Unit ID	Port	Link Status	Link Speed (Gbps)	Transmit Data Rate (Mbps)	Transmit Error Rate (Errors/s)	Total Transmit Errors	Receive Data Rate (Mbps)	Receive Error Rate (Errors/s)	Total Receive Errors	Link Flaps
1	0/45	Down	11	0	0	0	0	0	0	0
1	0/46	Down	11	0	0	0	0	0	0	0
1	0/47	Down	11	0	0	0	0	0	0	0
1	0/48	Down	11	0	0	0	0	0	0	0
1	0/49	Down	11	0	0	0	0	0	0	0
1	0/50	Down	11	0	0	0	0	0	0	0
1	0/51	Down	11	0	0	0	0	0	0	0
1	0/52	Down	11	0	0	0	0	0	0	0

8. Select either the **Unit ID** or **All**.
  - Select the **Unit ID** to display information for the selected unit.
  - Select **All** to display information for all units.

The following table describes the nonconfigurable Backplane-port Configuration data that is displayed.

**Table 59. Backplane-Port Configuration**

Field	Description
Unit ID	The unit ID of the specific blade.
Port	The backplane-port on the given blade.
Link Status	The link status (Up/Down) of the port.
Link Speed (Gbps)	The maximum speed of the backplane-port.

**Table 59. Backplane-Port Configuration (continued)**

Field	Description
Transmit Data Rate (Mbps)	The approximate transmit rate on the backplane-port.
Transmit Error Rate (Error/s)	The number of errors in transmit packets per second.
Total Transmit Errors	The total number of errors in transmit packets since bootup. The counter might wrap.
Receive Data Rate (Mbps)	The approximate receive rate on the backplane-port.
Receive Error Rate (Error/s)	The number of errors in receive packets per second.
Total Receive Errors	The total number of errors in receive packets since bootup. The counter might wrap.
Link Flaps	Displays a backplane-port counter that increments whenever a backplane-port link transitions to the down state.

## View the Chassis Backplane-Port Packet-Path

You can view low-level statistics such as APT counts and RPC counts, and so on for all the backplane-ports in the given chassis.

➤ **To view the backplane-port packet-path:**

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

Backplane-port Diagnostics

Backplane-port Diagnostics

1 2 3 All

Unit ID	Port	Port Diagnostics Info
1	0/45	RBYT:0 RPKT:0 TBYT:0 TPKT:0RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0TFCS:0 TERR:0
1	0/46	RBYT:0 RPKT:0 TBYT:0 TPKT:0RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0TFCS:0 TERR:0
1	0/47	RBYT:0 RPKT:0 TBYT:0 TPKT:0RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0TFCS:0 TERR:0
1	0/48	RBYT:0 RPKT:0 TBYT:0 TPKT:0RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0TFCS:0 TERR:0
1	0/49	RBYT:0 RPKT:0 TBYT:0 TPKT:0RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0TFCS:0 TERR:0
1	0/50	RBYT:0 RPKT:0 TBYT:0 TPKT:0RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0TFCS:0 TERR:0
1	0/51	RBYT:0 RPKT:0 TBYT:0 TPKT:0RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0TFCS:0 TERR:0
1	0/52	RBYT:0 RPKT:0 TBYT:0 TPKT:0RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0TFCS:0 TERR:0

Backplane-port packet-path

Direction	Packet-path
-----------	-------------

1 2 3 All

8. Select either the **Unit ID** or **All**.
- Select the **Unit ID** to display information for the selected unit.
  - Select **All** to display information for all units.
9. Select **System > Chassis > Advanced > Backplane-port Diagnostics** to display the Backplane-port packet-path fields.
10. To navigate, select either the **Unit ID** or **All**.
- Select the **Unit ID** to display the packet path starting from the selected blade.
  - Select **All** to display the packet path starting from all the blades of the chassis.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable **Backplane-port Diagnostics** data that is displayed.

**Table 60. Backplane-Port Diagnostics**

Field	Description
Unit ID	The slot number of the blade.
Port	The backplane-port on the given blade.
Port Diagnostics Info	Displays three text fields (character strings) populated by the driver containing debug and status information. The port Diagnostics information contains hardware counters; counter values are displayed in hexadecimal digits.

The following table describes the nonconfigurable **Backplane-port packet-path** data that is displayed.

**Table 61. Backplane-port Packet-path**

Field	Description
Direction	The path direction.
Packet-path	The packet path.

## Configure the Chassis Power Settings

### ➤ To configure the chassis power 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. Click **System > Chassis > Advanced > Chassis Power Configuration**.

Chassis Power Configuration

Power Module Redundancy (N+1)	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Total Available Power (W)	1540
Total Required System Power (W)	470
Total Power Consumption(W)	20
System Power (W)	<input type="text" value="470"/> (0 to 2550)
Power Auto-rebalance	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Power Module AC Input (V)	220

8. Select the Power Module Redundancy **Enable** or **Disable** radio button.  
This specifies whether power redundancy mode is enabled or disabled.
9. Click the **Apply** button.

If you enabled this feature, power redundancy mode is applied.

## Configure the System Power

### ➤ To configure the system power:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 **System > Chassis > Advanced > Chassis Power Configuration**.

Chassis Power Configuration	
Power Module Redundancy (N+1)	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Total Available Power (W)	1540
Total Required System Power (W)	470
Total Power Consumption(W)	20
System Power (W)	<input type="text" value="470"/> (0 to 2550)
Power Auto-rebalance	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Power Module AC Input (V)	220

8. To configure system power, in the **System Power** field, specify the power reserved for the system, excluding PoE power.

This provides a way to reserve power for blades. The remaining power can be used by a PoE sub system. System Power must be less than or equal to 2550W. Use 0 to reset System Power to defaults.

9. Click the **Apply** button.

The system power is applied.

## Configure the Power Auto-Rebalance

➤ **To configure the power auto-rebalance:**

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

Chassis Power Configuration	
Power Module Redundancy (N+1)	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Total Available Power (W)	1540
Total Required System Power (W)	470
Total Power Consumption(W)	20
System Power (W)	<input type="text" value="470"/> (0 to 2550)
Power Auto-rebalance	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Power Module AC Input (V)	220

8. In the **Power Auto-rebalance** field, specify whether power auto-rebalance mode is **Enabled** or **Disabled**.
9. Click the **Apply** button.

Power is applied in auto-rebalance mode. When enabled, the system automatically shuts down low priority ports to power up higher priority ports, even if they were spread across different blades on the chassis.

The following table describes the nonconfigurable Chassis Power Configuration data that is displayed.

**Table 62. Chassis Power Configuration**

Field	Description
Total Available Power	Total available power for chassis in watts.
Total Required System Power	Total required system power in watts. The value depends on the type of blades on the chassis. Refer to the Power Matrix or Blade Power Consumption table for power requirements of each blade type.
Total Power Consumption	Total power consumption in watts measured at PSU.
Power Module AC Input	Power module input voltage in volts. Possible values are 110 and 220.

## View Blade Power Consumption

### ➤ To view blade power consumption:

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

Blade Power Consumption					
Unit ID	Blade Type	Blade Model	Current Power Consumption (W)	Blade Power Required (W)	Blade Status
1	3	XCM8948	50	60	OK
2	4	XCM8924X	370	200	OK
3	2	XCM8944F	310	150	OK

The following table describes the Blade Power Consumption data that is displayed.

**Table 63. Chassis Power Modules**

Field	Description
Unit ID	The unit ID that identifies the blade slot.
Blade Type	Displays blade type number.
Blade Model	Displays blade model.
Current Power Consumption	Displays amount of power required by blade (excluding PoE power) in watts.
Blade Power Required	Displays amount of power required by blade (excluding PoE power) in watts.
Blade Status	Displays blade status. The possible values are as follows: <ul style="list-style-type: none"> <li>• <b>OK</b></li> <li>• <b>Booting up</b></li> <li>• <b>Bootup Failed</b></li> <li>• <b>Thermal Shutdown</b></li> <li>• <b>SW Power Down</b></li> <li>• <b>Not Enough Power</b></li> <li>• <b>Unknown Blade</b></li> <li>• <b>Absent</b></li> </ul>

## View Power Redundancy

### ➤ To view power redundancy:

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

The Chassis Power Configuration screen displays.

8. Scroll down to the Power Redundancy section.

Unit ID	Blade Type	Blade Model	Current Power Consumption (W)	Blade Power Required (W)	Blade Status
1	1	XCM8944	43	70	OK
2	4	XCM8924X	106	200	OK
3	2	XCM8944F	43	150	OK

Power Redundancy	
N+1 Configuration	Disable
N+1 Active	No
Number of PSU	2
Effective Power	2

The following table describes the Power Redundancy data that is displayed.

**Table 64. Power Redundancy**

Field	Description
N+1 Configuration	Power redundancy configuration. Possible values are <b>Enable</b> and <b>Disable</b> .
N+1 Active	Displays whether power supply N+1 redundancy is active on the chassis.
Number of PSU	Total number of active PSUs in chassis.
Effective Power	Effective number of PSUs in the chassis after factoring N+1 active state. The value is one less than number of PSU when N+1 is active on the chassis.

## View the Power Modules

➤ **To view the power modules:**

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

The Chassis Power Configuration screen displays.

Scroll down to the Power Module section..

Power Modules			
Slot	Type	State	AC (V)
1	Removable	Operational	220V
2	Removable	Not Present	N/A
3	Removable	Operational	220V
4	Removable	Not Present	N/A

The following table describes the nonconfigurable Power Module data that is displayed.

**Table 65. Power Modules**

Field	Description
Slot	Power module number counted from left to right.
Type	Power module type. Valid values are <b>Fixed</b> and <b>Removable</b> .
State	Power module state. Possible states are as follows: <ul style="list-style-type: none"> <li>• <b>Operational</b></li> <li>• <b>Failed</b></li> <li>• <b>Not Present</b></li> <li>• <b>Not Powered</b></li> <li>• <b>Not Applicable</b></li> </ul>
AC	Power module input voltage category in volts. Possible values are <b>110V</b> , <b>220V</b> , and <b>N/A</b> . <b>N/A</b> specifies that power source input voltage cannot be obtained.

## View EPS Power Modules and EPS Ports

### ➤ To display EPS 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 **System > Chassis > Advanced > Chassis Power Configuration**.

The Chassis Power Configuration screen displays.

8. Scroll down to the EPS Power Module section.

EPS Power Modules			
Slot	Type	State	AC (V)
1	Removable	Not present	N/A
2	Removable	Not present	N/A
3	Removable	Not present	N/A
4	Removable	Not present	N/A

9. Scroll down to the EPS Ports section..

EPS Ports				
Port	State	Sharing Status	Device Type	EPS/RPS Port Group
1	Not present	No	Unknown	
2	Not present	No	Unknown	

The following tables describes the EPS power module data and the EPS ports data that is displayed.

**Table 66. EPS Power Modules**

Field	Description
Slot	EPS power module number counted from left to right.
Type	EPS power module type. Valid value is Removable.
State	EPS power module state. Possible states are as follows: <ul style="list-style-type: none"> <li>• <b>Operational</b></li> <li>• <b>Not Present</b></li> </ul>
AC	EPS power module input voltage category in volts. Possible values are <b>110V</b> , <b>220V</b> , and <b>N/A</b> . <b>N/A</b> specifies that power source input voltage cannot be obtained.

The following table describes the non configurable EPS Ports data that is displayed.

**Table 67. EPS Ports**

Field	Description
Ports	EPS port number counted from left to right while facing rear side of the chassis.
State	EPS port state. Possible state is <b>Not present</b> or <b>Operational</b> .
Sharing Status	EPS power sharing status.
Device Type	Device type. Possible values are as follows: <ul style="list-style-type: none"> <li>• <b>RPS4000v1</b></li> <li>• <b>RPS4000v2</b></li> <li>• <b>Unknown</b></li> </ul>
EPS/RPS Port Group	Group of EPS slots connected to this port. Possible values are as follows: <ul style="list-style-type: none"> <li>• <b>1,2</b></li> <li>• <b>3,4</b></li> </ul>

## View the Power Matrix

### ➤ To view the power matrix:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > Chassis > Advanced > Chassis Power Configuration**.  
The Chassis Power Configuration screen displays.

8. Scroll down to the Power Matrix section.

Power Matrix		
Blade Type	Blade Model	Power Required (W)
1	XCM8944	70
2	XCM8944F	150
3	XCM8948	60
4	XCM8924X	200

The following table describes the nonconfigurable Power Matrix data that is displayed.

**Table 68. Power Matrix**

Field	Description
Blade Type	The 4-bit identification number assigned to a blade.
Blade Model	Blade model.
Power Required	Maximum consumption by blade in watts (excluding PoE power).

## Rebalance the Chassis Power

### ➤ To rebalance the chassis power:

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

Chassis Power Rebalance	
Check this box and click Apply button to power down the low priority PD device until enough power is obtained to power up new blade.	<input type="checkbox"/>

8. Select the check box.

9. Click the **Apply** button.

The low-priority PD device powers down until enough power is obtained to power up a new blade or higher-priority PoE port on a different blade.

## Configure Chassis Firmware Synchronization

### ➤ To configure chassis firmware synchronization:

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

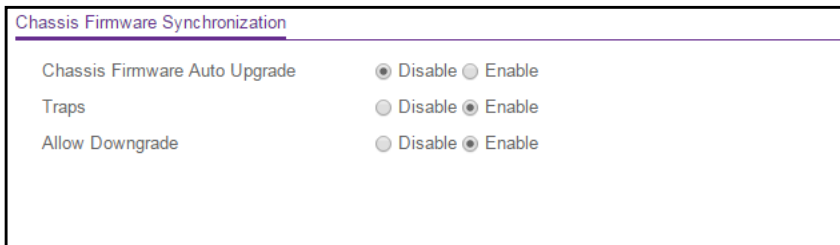
5. Enter the user name and password.

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 > Chassis > Advanced > Chassis Firmware Synchronization**.



Chassis Firmware Synchronization	
Chassis Firmware Auto Upgrade	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Traps	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Allow Downgrade	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

8. Select the Chassis Firmware Auto Upgrade **Disable** or **Enable** radio button.

This specifies whether the firmware synchronization feature enabled or disabled. The default is Disable.

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

This enables or disables the sending of traps during chassis firmware synchronization start, failure, and finish. The default is Enable.

10. Select the Allow Downgrade **Disable** or **Enable** radio button.

This enables or disables downgrading the image on a chassis member if the chassis member's version is newer. The default is Enable.

11. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

## View NSF Summary Data

➤ **To display NSF Summary data:**

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

- For M6100 switches, select **System > Chassis > NSF > NSF Summary**.

- For M5300 and M7100 switches, select **System > Stacking > NSF > NSF Summary**.

NSF Summary	
Operational Status	Enable
Last Startup Reason	Power On
Time Since Last Restart	2 days 3 hrs 2 mins 14 secs
Restart In Progress	No
Warm Restart Ready	No
Copy of Running Configuration to Backup Unit	
Status	No Backup Unit
Backup Configuration Age	Not yet copied
Time Until Next Backup	No Backup Unit
NSF Support on Unit	
Unit ID	NSF Support
1	Enable

- To cause the supervisor unit to fail over to the backup blade, click the **Initiate Failover** button on the top right corner of the screen.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable NSF Summary data that is displayed.

**Table 69. NSF Summary**

Field	Description
Operational Status	Indicates whether NSF is enabled on the chassis. NSF is enabled by default.
Last Startup Reason	<p>The type of activation that caused the software to start the last time. The possible values are as follows:</p> <ul style="list-style-type: none"> <li><b>Power On.</b> The switch is rebooted. A power cycle or an administrative reload command might caused this</li> <li><b>Cold Admin Move.</b> The system resets all hardware tables without a reboot and the application begins from a pre-initialized state, but no data is retained from before the failover.</li> <li><b>Warm Admin Move.</b> The administrator issued a command for the standby manager to take over.</li> <li><b>Auto Warm.</b> The primary management card restarted due to a failure, and the system executed a nonstop forwarding failover.</li> <li><b>Auto Cold.</b> The system switched from the active manager to the backup manager and could not maintain user data traffic. This is usually caused by multiple failures occurring close together.</li> </ul>

Table 69. NSF Summary (continued)

Field	Description
Time Since Last Restart	Time since the current management card because the active management card. For the backup manager, the value is set to 0d:00:00:00.
Restart In Progress	Indicates whether a restart is in progress. A restart is not considered complete until all hardware tables are fully reconciled.
Warm Restart Ready	Indicates whether the initial full checkpoint finished.
<b>Copy of Running Configuration to Backup Unit</b>	
Status	Status of copying the running configuration to backup blades.
Backup Configuration Age	Indicates the time since the running configuration was last copied to the backup blade.
Time Until Next Backup	Indicates the number of seconds until the running configuration is copied to the backup blade.
NSF Support on Unit	
Unit ID	The slot number for the blade.
NSF Support	Displays whether the switch supports the nonstop forwarding (NSF) feature.

## View NSF Checkpoint Statistics

### ➤ To view NSF checkpoint 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 > Chassis > NSF > Checkpoint Statistics**.

NSF Checkpoint Statistics	
Messages Checkpointed	58
Bytes Checkpointed	31786
Time Since Counters Cleared	0 days 0 hrs 11 mins 28 secs
Checkpoint Message Rate	0.084 msg/sec
Last 10-second Message Rate	0.0 msg/sec
Highest 10-second Message Rate	3.4 msg/sec

To reset the statistics on the screen, click the **Clear** button.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 70. NSF Checkpoint Statistics**

Field	Description
Messages Checkpoint	The number of messages sent from the supervisor to the backup blade.
Bytes Checkpointed	How much data was sent from the supervisor until to the backup blade.
Time Since Counters Cleared	The amount of time since the counters were reset.
Checkpoint Message Rate	The number of seconds between measurements.
Last 10-second Message Rate	How many messages were sent in the last measurement interval.
Highest 10-second Message Rate	The highest number of messages that were sent in a measurement interval.

## M5300 Series Switch Stacking Overview

A stackable switch is a switch that is fully functional operating as a stand-alone unit but can also be set-up to operate together with up to seven other switches. This group of switches shows the characteristics of a single switch while having the port capacity of the sum of the combined switches.

One of the switches in the stack controls the operation of the stack. This switch is called the stack *master*. The remaining switches in the stack are stack *members*. The stack members use stacking technology to behave and work together as a unified system. Layer 2 and higher protocols present the entire switch stack as a single entity to the network.

The stack master is the single point of stack-wide management. From the stack master, you configure the following:

- System-level (global) features that apply to all stack members



- Interface-level features for all interfaces on any stack member

A switch stack is identified in the network by its network IP address. The network IP address is assigned according to the MAC address of the stack master. Every stack member is uniquely identified by its own stack member number, which is from 1 to 6. The stack master can be any number within that range.

Stacking supports the following:

- Up to eight switches per stack, which can be any combination of the following switch models:
  - M6100
  - M7100
  - M5300
- Single IP address management through a web browser, the CLI, or SNMP.
- Master-slave configuration:
  - The master retains configuration for entire stack.
  - Automatic detection of new members, with synchronization of firmware (upgrade or downgrade as needed).
- Configuration updates across the stack through a single operation.
- Automatic master failover. Fully resilient stack with chain and ring topology.
- Hot swapping (insertion and removal) of stack members.

## Firmware Synchronization and Upgrade

All stack members must run the same software version to ensure compatibility within the stack. By default, if a unit is added to the stack and its software version is not the same as the stack master, that unit is not allowed to join the stack. You can enable the Stack Firmware Auto Upgrade feature, which automatically synchronizes the firmware version on the new unit with the version running on the stack master. The synchronization operation might result in either upgrade or downgrade of firmware on the mismatched stack member.

Upgrading the firmware on a stack of switches is the same as upgrading the firmware on a single switch. After you download a new image by using the File Download screen or SCC, the downloaded image is distributed to all the connected units of the stack.

---

**Note:** NETGEAR recommends that you set the active image for all stack members the same as the active image of the stack master. In other words, if image1 is the active image on the stack master, all units must use image1 as the active image. For information about configuring the active image, see [Configure Dual Image Settings](#) on page 729.

---

## Stack Configuration Maintenance

The stack master stores and maintains the saved and running configuration files for the switch stack. The configuration files include the system-level settings for the switch stack and the interface-level settings for all stack members. Each stack member retains a copy of the saved file for backup purposes. If the master is removed from the stack or becomes unavailable, another member is elected master and then runs from that saved configuration.

The switch master copies its running configuration to the stack member configured as the *standby* unit whenever it changes (subject to some restrictions to reduce overhead). This enables the standby unit to take over the stack operation with minimal interruption if the stack master becomes unavailable. The running-config synchronization also occurs when the running configuration is auto-saved on the stack master or when the standby unit changes.

## Stack Master Election

All stack members are eligible stack masters. If the stack master becomes unavailable, the remaining stack members participate in electing a new stack master from among themselves. The following factors determine which switch is elected the stack master:

- The switch that is master always has priority to retain the role of master.
- Assigned priority.
- MAC address.

When the stack is powered up and completes the boot process or the original stack master becomes unavailable, the stack master is determined through an election process.

The rules for stack master election are as follows:

- If a unit was elected stack master previously, then it remains the stack master and other units are stack members.
- If no units were stack masters, or more than one unit was a stack master, then the unit with the highest management preference is elected stack master. The management preference can be assigned by the administrator. However, if all units are assigned the same management preference, then the unit with the highest MAC address is assigned as the stack master.

## Stack Factory Defaults Reset Behavior

If the stack master is reset to the factory default settings (see [Reset the Switch to Its Factory Default Settings](#) on page 716), the stack master applies the default settings to all the stack members and resets the stack, including all participating stack members. When the stack boots, the stack master election process begins.

A switch can be described in terms of three semi-independent functions called the forwarding plane, the control plane, and the management plane. The forwarding plane forwards data packets. The forwarding plane is implemented in hardware. The control plane is the set of protocols that determine how the forwarding plane forwards packets, deciding which data packets are allowed to be forwarded and where they go. Application software on the

management unit acts as the control plane. The management plane is application software running on the management unit that provides interfaces allowing a network administrator to configure and monitor the device.

## Stack NSF

Nonstop forwarding (NSF) allows the forwarding plane of stack units to continue to forward packets while the control and management planes restart as a result of a power failure, hardware failure, or software fault on the management unit. A nonstop forwarding failover can also be manually initiated by clicking the Initiate Failover button on the NSF Summary screen. Traffic flows that enter and exit the stack through physical ports on a unit other than the management continue with at most sub-second interruption when the management unit fails.

To prepare the backup management unit in case of a failover, applications on the management unit continuously checkpoint some state information to the backup unit. Changes to the running configuration are automatically copied to the backup unit. MAC addresses stay the same across a nonstop forwarding failover so that neighbors are not required to relearn them.

When a nonstop forwarding failover occurs, the control plane on the backup unit starts from a partially initialized state and applies the checkpointed state information. While the control plane is initializing, the stack cannot react to external changes, such as network topology changes. Once the control plane is fully operational on the new management unit, the control plane ensures that the hardware state is updated as necessary. Control plane failover time depends on the size of the stack, the complexity of the configuration, and the speed of the CPU.

The management plane restarts when a failover occurs. Management connections must be reestablished.

For NSF to be effective, adjacent networking devices must not reroute traffic around the restarting device. The switch uses three techniques to prevent traffic from being rerouted:

- A protocol can distribute a part of its control plane to stack units so that the protocol can give the appearance that it is still functional during the restart. Spanning tree and port channels use this technique.
- A protocol can enlist the cooperation of its neighbors through a technique known as graceful restart. OSPF uses graceful restart if it is enabled.
- A protocol can restart after the failover if neighbors react slowly enough that they cannot normally detect the outage. The IP multicast routing protocols are a good example of this behavior.

To take full advantage of nonstop forwarding, Layer 2 connections to neighbors must be through port channels that span two or more stack units, and Layer 3 routes must be ECMP routes with next hops through physical ports on two or more units. The hardware can quickly move traffic flows from port channel members or ECMP paths on a failed unit to a surviving unit.

## Stack Configuration

You can move the primary management unit functionality from one unit to another. Upon execution, the entire stack (including all interfaces in the stack) is unconfigured and reconfigured with the configuration on the new primary management unit. After the reload is complete, all stack management capability must be performed on the new primary management unit. To preserve the current configuration across a stack move, save the current configuration to the NVRAM before performing the stack move. A stack move causes all routes and Layer 2 addresses to be lost. The administrator is prompted to confirm the management move.

### Select a New Stack Master

➤ **To select a new stack master:**

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

The screenshot shows the 'Stacking' configuration page. The 'Management Unit Selection' section has a dropdown menu for 'Management Unit Selected' with the value '4'. The 'Stack Sample Mode' section has a dropdown for 'Sample Mode' set to 'Cumulative'. The 'Stack Configuration' table lists stack members with columns: Unit ID, Change Switch ID to, Switch Type, Hardware Management Preference, Switch Priority, Management Status, Standby Status, and Switch Status. The table shows one member with Unit ID '4', Switch Type 'M5300-52G-POE+', and Management Status 'Management'. Below this is the 'Basic Stack Status' table with columns: Unit ID, Switch Description, Serial Number, Uptime, Preconfigured Model Identifier, Plugged-in Model Identifier, Detected Code Version, and Detected Code. It shows the same member with details like 'M5300-52G-POE+', '2XN129520001C', and uptime '0 days, 2 hours, 15 minutes, 15 secs'.

The **Management Unit Selected** menu displays the current primary management unit.

8. To change the primary management unit, select another unit ID of the stack member to become the stack master.

A message displays to notify you that moving stack management unconfigures the entire stack including all interfaces.

9. Click the **OK** button to confirm the selection and reload the stack.

The stack is unavailable until the boot process completes.

## Specify the Stack Sample Mode

Use the Stack Sample mode section of the screen to configure global status management mode, and sample size. The mode and sample size parameters are applied globally to all units in the stack.

In the **Sample mode** list, select one of the following:

- **Cumulative.** Tracks the sum of received time-stamp offsets cumulatively.
- **History.** Tracks the history of received timestamps.

In the **Max Samples** field, configure the maximum number of samples to keep. The valid range is 100 to 500.

## Configure a Stack Member

- **To configure a stack member before adding it to the stack:**

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

4. Enter 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 > Stacking > Stack Configuration**.

Unit ID	Change Switch ID to	Switch Type	Hardware Management Preference	Switch Priority	Management Status	Standby Status	Switch Status
1		M5300-52G-POE+	Unassigned	10	StackMember	None	OK
2		M5300-52G3	Unassigned	5	StackMember	None	OK
3		M5300-52G	Unassigned	Unassigned	StackMember	None	OK
6		M5300-28GF3	Unassigned	15	StackMember	Op Standby	OK
7		M5300-52G3	Unassigned	14	Management	None	OK

Unit ID	Switch Description	Serial Number	Uptime	Pre-configured Model Identifier	Plugged-in Model Identifier	Detected Code Version	Detected Code in Flash	SFS Last Attempt Status
1	M5300-52G-POE+	2XN1245BF001D	4 days, 16 hours, 12 minutes, 9 secs	M5300-52G-POE+	M5300-52G-POE+	11.0.0.4	11.0.0.4	None
2	M5300-52G3	2XR1245RF0032	4 days, 16 hours, 12 minutes, 12 secs	M5300-52G3	M5300-52G3	11.0.0.4	11.0.0.4	None
3	M5300-52G	33J1245TF0011	4 days, 16 hours, 12 minutes, 14 secs	M5300-52G	M5300-52G	11.0.0.4	11.0.0.4	None
6	M5300-28GF3	2X61245TF0035	4 days, 16 hours, 12 minutes, 12 secs	M5300-28GF3	M5300-28GF3	11.0.0.4	11.0.0.4	None
7	M5300-52G3	2XR1245TF0018	4 days, 16 hours, 12 minutes, 12 secs	M5300-52G3	M5300-52G3	11.0.0.4	11.0.0.4	None

8. Select the **Unit ID** of the stack member to add.
9. Select the switch model number of the new unit from the **Switch Type** field.
10. Optionally, specify the **Switch Priority** to select whether this unit becomes a management unit in preference to another unit.

The default value for this setting is undefined. If the preference level is set to zero, then the device cannot become a management unit. A higher value indicates a higher priority. The maximum value is 15.

11. Use the **Management Status** field to indicate whether the selected switch is the stack master, a normal stacking member, or the standby unit.

A standby unit takes over the stack master responsibilities if the stack master becomes unavailable.

12. Click the **Add** button.

The preconfigured unit is added to the stack.

➤ **To change the settings for an existing stack member:**

1. Select the check box next to the stack member to configure.
2. If desired, specify a new unit ID for the stack member in the **Change to Switch ID** field.

The renumbering process causes the unit to reload.

3. Specify the switch type, priority, or management status from the available fields.
4. Click the **Apply** button.

The changes to the stack member are saved.

**Note:** If you configured a new unit number for an existing stack member, you are asked to confirm the change. Click the **OK** button to continue or click the **Cancel** button to retain the original settings.

5. Click the **Delete** button to remove the selected unit from the stack.
6. Click **Refresh** to update the screen with the latest information from the switch.

**Note:** In the case of adding or removing a dummy unit with POE for preconfiguration, you must log in again to an actual web session to apply changes and observe relevant POE web pages.

7. Click the **Add** button.

This adds the unit to the stack with the specific switch type.

8. To remove the selected unit from the stack, click the **Delete** button.
9. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable Stack Configuration fields.

**Table 71. Stack Configuration**

Field	Description
Hardware Management Preference	The hardware management preference of the switch. The hardware management preference can be disabled or unassigned.

**Table 71. Stack Configuration (continued)**

Field	Description
Standby Status	Identifies the switch that is configured as the standby unit. The possible values are as follows: <ul style="list-style-type: none"> <li>• <b>Cfg Standby.</b> Indicates that the unit is configured as the standby unit. The unit configured as the standby switch becomes the stack manager if the current manager fails.</li> <li>• <b>Opr Standby.</b> Indicates that this unit is operating as the standby unit and the configured standby unit is not part of the stack.</li> <li>• <b>None.</b> The switch is not configured as the standby unit.</li> </ul>
Switch Status	The status of the selected unit. The possible values are as follows: <ul style="list-style-type: none"> <li>• OK</li> <li>• Unsupported</li> <li>• Code Mismatch</li> <li>• Config Mismatch</li> <li>• Not Present</li> </ul>

The following table describes the nonconfigurable Stack Status information that is displayed.

**Table 72. Stack Status nonconfigurable fields**

Field	Description
Hardware Management Preference	The hardware management preference of the switch, which can be disabled or unassigned.
Standby Status	Identifies the switch that is configured as the standby unit: <ul style="list-style-type: none"> <li>• <b>Cfg Standby.</b> The unit is configured as the standby unit. The unit configured as the standby switch becomes the stack manager if the current manager fails.</li> <li>• <b>Opr Standby.</b> This unit is operating as the standby unit and the configured standby Unit is not part of the stack.</li> <li>• <b>None.</b> The switch is not configured as the standby unit.</li> </ul>
Switch Status	The status of the selected unit. Possible values are as follows: <ul style="list-style-type: none"> <li>• <b>OK.</b> The unit is connected and works properly.</li> <li>• <b>Unsupported.</b> The type of inserted unit is not supported.</li> <li>• <b>Code Mismatch.</b> The code version is not identical to the master/management unit.</li> <li>• <b>Config Mismatch.</b> The inserted device type is different from the configured devices.</li> <li>• <b>Not Present.</b> The unit is not connected.</li> <li>• <b>SDM Mismatch.</b> SDM template mismatch.</li> <li>• <b>Updating Code.</b> A code update is in progress.</li> <li>• <b>STM Mismatch.</b> STM template mismatch.</li> </ul>
Unit ID	The unit ID of the specific switch.
Switch Description	The description for the unit that is configured by the user.
Serial Number	The unique box serial number for this switch.



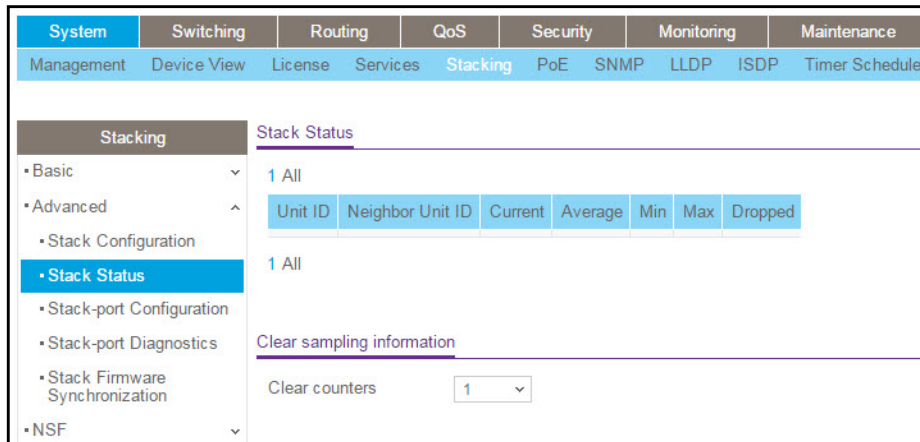
**Table 72. Stack Status nonconfigurable fields (continued)**

Field	Description
Up Time	The relative time since the last reboot of the switch.
Preconfigured Model Identifier	The model type assigned by the device manufacturer to identify the device.
Plugged-In Model Identifier	The model type assigned by the device manufacturer to identify the plugged-in device.
Detected Code Version	The detected version of code on this unit.
Detected Code in Flash	The release number and version number of the code stored in flash.
SFS Last Attempt Status	The stack firmware synchronization last attempt status.

## View the Stack Status

### ➤ To view the stack 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 > Stacking > Advanced > Stack Status**.



8. Select the units.
  - Select the **Unit ID** to display information for the selected unit.
  - Select **All** to display information for all units.
9. To refresh the screen with the latest information on the switch, click the **Update** button.
10. To clear the sampling information, in the **Clear Counters** list, select the unit.

The following table displays the nonconfigurable information.

**Table 73. Stack Status**

Field	Description
Unit ID	The unit ID of the specific switch.
Neighbor Unit ID	The neighboring unit with which data is exchanged.
Current	The current time of heartbeat message reception.
Average	The average time of heartbeat messages received.
Min	Minimum time of heartbeat messages received.
Max	Maximum time of heartbeat messages received.
Dropped	Heartbeat message dropped/lost counter.

## Configure the mode of the Stack Ports

By default, the stack ports on each switch are configured for stacking. However, you can use these ports as standard Ethernet ports. Use the Stack Port Configuration screen to configure the mode of the stack ports and to view information about the ports.

### ➤ To configure the mode of the stack 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 **System > Stacking > Advanced > Stack Port Configuration**.

The screen is shown in two parts.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management	Device View	License	Services	Stacking	PoE	SNMP	LLDP	ISDP
Timer Schedule								

Stacking									
Stack-port Configuration									
Basic	1 All								
Advanced									
Stack Configuration									
Stack Status									
Stack-port Configuration									
Stack-port Diagnostics									
Stack Firmware Synchronization									

Unit ID	Port	Type	Product name	Configured Stack Mode	Running Stack Mode	Link Status	Link Speed (Gbps)	Transmit Data Rate (Mbps)
<input type="checkbox"/> 1	0/49			Ethernet	Ethernet	Down	10	0
<input type="checkbox"/> 1	0/50			Ethernet	Ethernet	Down	10	0
<input type="checkbox"/> 1	0/51			Stack	Stack	Down	12	0
<input type="checkbox"/> 1	0/52			Stack	Stack	Down	12	0

Transmit Error Rate (Errors/s)	Total Transmit Errors	Receive Data Rate (Mbps)	Receive Error Rate (Errors/s)	Total Receive Errors	Link Flaps
0	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0

8. Select the check box associated with the unit and port to configure:
9. From the **Configured Stack mode** field, select the operating mode of the port to be either:
  - **Stack**. The port connects to the stack port on another stack member. This is the default value for back panel stack mode.
  - **Ethernet**. The port operates as a standard switch port that receives and transmits network traffic. This is the default value for front panel stack mode.
10. Click the **Apply** button to apply the new settings to the system.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes Stack Port Configuration fields.

**Table 74. Stack Port Configuration**

Field	Description
Unit ID	The unit.
Port	The stackable interfaces on the given unit.
Slot ID	The slot ID in the format unit/slot.
Type	The type of stackable interfaces on the given unit.
Product Name	The name of the XFP/SFP+ adapter.
Running Stack mode	The run-time mode of the stackable interface.
Link Status	The link status (UP/DOWN) of the port.
Link Speed (Gbps)	The maximum speed of the stacking port.
Transmit Data Rate (Mbps)	The approximate transmit rate on the stacking port.
Transmit Error Rate	The number of errors in transmit packets per second.
Total Transmit Errors	The total number of errors in transmit packets since boot. The counter might wrap.
Receive Data Rate (Mbps)	The approximate receive rate on the stacking port.
Receive Error Rate	The number of errors in receive packets per second.
Total Receive Errors	The total number of errors in receive packets since boot. The counter might wrap.
Link Flaps	The total number of link flaps.

## Run Stack Port Diagnostics

### ➤ To run stack port diagnostics:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > Stacking > Advanced > Stack Port Diagnostics**.

SystemSwitchingRoutingQoSSecurityMonitoringMaintenanceHelpIndex

ManagementDevice ViewLicenseServicesStackingPoESNMPLLDPISDPTimer Schedule

Stacking

Basic

Advanced

Stack Configuration

Stack Status

Stack-port Configuration

Stack-port Diagnostics

Stack Firmware Synchronization

NSF

Stack-port Diagnostics

1 All

Unit ID	Port	Port Diagnostics Info
1	0/49	
1	0/50	
1	0/51	RBYT:0 RPKT:0 TBYT:0 TPKT:0 RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0 TFCS:0 TERR:0
1	0/52	RBYT:0 RPKT:0 TBYT:0 TPKT:0 RFCS:0 RFRG:0 RJBR:0 RUND:0 RUNT:0 TFCS:0 TERR:0

Stack-port packet-path

Direction	Packet-path
1 All	

8. Select **Unit ID** to display the packet path starting from the selected unit.
9. Select **All** to display the packet path from all the units in the stack.
10. To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the Stack Port Diagnostics fields.

### Table 75. Stack Port Diagnostics

Field	Definition
Unit ID	The unit.
Port	The stackable interface on the given unit.
Port Diagnostics Info	Displays three text fields (80 character strings) populated by the driver containing debug and status information.

The following table describes the nonconfigurable Stack Port Packet Path fields.

### Table 76. Stack Port Packed Path

Field	Definition
Direction	The path direction.
Packet Path	The packet path.

## Configure Stack Firmware Synchronization

➤ **To configure the stack firmware synchronization features:**

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

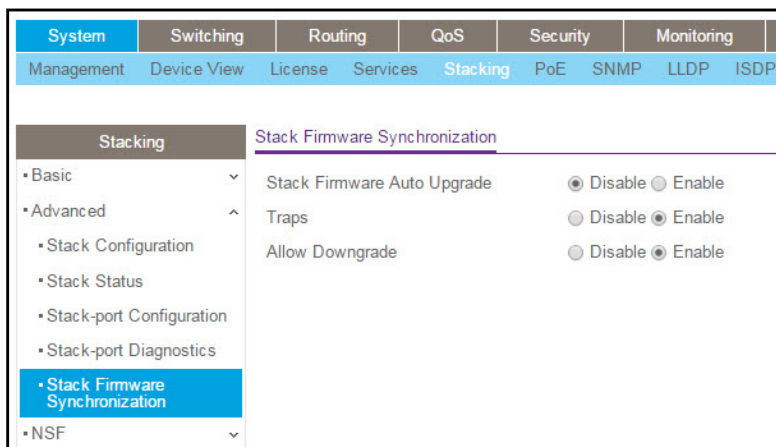
5. Enter the user name and password.

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 > Stacking > Advanced > Stack Firmware Synchronization**.



8. Specify whether **Stack Firmware Auto Upgrade** is enabled or disabled.

This feature determines what to do when a new member attempts to join the stack, and its firmware does not match the version running on the master.

- **Enable.** The stack master upgrades the version on the new member to match the version running on the rest of the stack.
- **Disable.** The new member is not allowed to join.

9. Use the **Traps** field to enable or disable sending of traps during stack firmware synchronization start, failure, or finish.

10. Use the **Allow Downgrade** field to determine whether the stack master downgrades the firmware version on a new member that attempts to join the stack if the new member has a firmware version that is more recent than the stack.

11. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

## 4. Configure Switching Information

---

This chapter covers the following topics:

- *Configure VLANs*
- *Auto-VoIP*
- *iSCSI Overview*
- *Spanning Tree Protocol*
- *Multicast*
- *Configure MVR*
- *MAC Address Table*
- *Port Settings*
- *Link Aggregation Groups*
- *Multiple Registration Protocol Overview*



## Configure VLANs

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 is assigned 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.

You can define VLAN groups stored in the VLAN membership table. Each switch in the M6100/M7100/M5300 family supports up to 1024 VLANs. VLAN 1 is created by default and is the default VLAN of which all ports are members.

### Configure Basic VLAN Settings

The internal VLAN is reserved by a port-based routing interface and invisible to the end user. Once these internal VLANs are allocated by the 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 > Basic > VLAN Configuration**.

**Reset**

Reset Configuration ☐

**Internal VLAN Configuration**

Internal VLAN Allocation Base: 4093

Internal VLAN Allocation Policy: ☐ Ascending ☒ Descending

**VLAN Configuration**

<input type="checkbox"/>	VLAN ID	VLAN Name	VLAN Type	Make Static
<input type="checkbox"/>				Disable ▾
<input checked="" type="checkbox"/>	1	default	Default	Disable

8. To reset VLAN settings to their default values, select the **Reset Configuration** check box.

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.

All VLANs, except for the default VLAN, are deleted.

9. Specify the internal VLAN settings.

The Internal VLAN Configuration section displays the allocation base and the allocation mode of internal VLAN.

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

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

- b. Select the Internal VLAN Allocation Policy **Ascending** or **Descending** radio button.

This specifies a policy for the internal VLAN allocation.

10. Use **VLAN ID** to specify the VLAN identifier for the new VLAN.

The range of the VLAN ID is 1 to 4093.

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

The VLAN name can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always uses the name Default.

The **VLAN Type** field identifies the type of the VLAN 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 uses a type of Dynamic. When configuring a dynamic VLAN, you can change its type to Static.

12. Click the **Add** button.

The VLAN is added to the switch.

13. To delete a selected VLAN from the switch, click the **Delete** button .

14. Click the **Apply** button.

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

## Configure an Advanced VLAN

### ➤ To configure an advanced 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 > VLAN Configuration**.

**Reset**

Reset Configuration ☐

**Internal VLAN Configuration**

Internal VLAN Allocation Base: 4093

Internal VLAN Allocation Policy: ☐ Ascending ☒ Descending

**VLAN Configuration**

<input type="checkbox"/>	VLAN ID	VLAN Name	VLAN Type	Make Static
<input type="checkbox"/>				Disable ▾
<input checked="" type="checkbox"/>	1	default	Default	Disable

- 8. Reset Configuration** - If you select this button 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 an Internal VLAN

The Internal VLAN section displays the allocation base and the allocation mode of internal VLAN. The internal VLAN is reserved by a port-based routing interface and invisible to the end user. Once these internal VLANs are allocated by the 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.

6. Click the **Login** button.

The web management interface menu displays.

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

Reset				
Reset Configuration <input type="checkbox"/>				
Internal VLAN Configuration				
Internal VLAN Allocation Base		<input type="text" value="4093"/>		
Internal VLAN Allocation Policy		<input type="radio"/> Ascending <input checked="" type="radio"/> Descending		
VLAN Configuration				
<input type="checkbox"/>	VLAN ID	VLAN Name	VLAN Type	Make Static
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>		Disable ▾
<input type="checkbox"/>	1	default	Default	Disable

8. In the **Internal VLAN Allocation Base** field, specify the VLAN allocation base for the routing interface.

You can enter a value from 1 to 4093.

9. Select the Internal VLAN Allocation Policy **Ascending** or **Descending** radio button.

This specifies a policy for the internal VLAN allocation.

## 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 constraints 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.

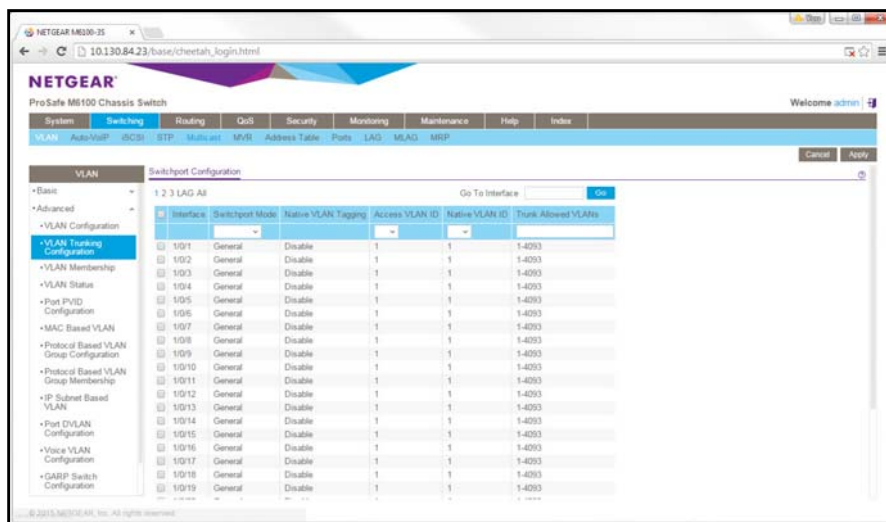
5. Enter the user name and password.

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**.



8. Select the interface:
  - Select the **Unit ID** field to display physical port information for the selected unit.
  - Use **LAG** to display LAGs only.
  - Use **All** to display all physical ports.
  - Use **Go To Interface** to select an interface by entering its number.
  - Use **Interface** to select the interface for which data is to be displayed or configured.
9. In the **Switchport Mode** list, select one of the following:
  - **Access**. This mode is suitable for ports connected to end stations or end users. Access ports participate in only one VLAN. They accept both tagged and untagged packets, but always transmit untagged packets.
  - **Trunk**. This 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.
  - **General**. This mode enables custom configuration of a port. You configure 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.

- **Host.** This mode is used for private VLAN configuration.
- **Promiscuous.** This mode is used for private VLAN configuration.

**10. Select from the list 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 list 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**.**

This is 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 the allowed VLANs. An **All** value sets all VLANs in the range (1 to 4093).

**13. Click the **Apply** button.**

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

The **Native VLAN Tagging** field displays enabled or disabled:

- When VLAN tagging is enabled, if the trunk port receives untagged frames, it forwards them on the native VLAN with no VLAN tag.
- When VLAN tagging is disabled, if the trunk port receives untagged frames, it includes the native VLAN ID in the VLAN tag when forwarding

## 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.

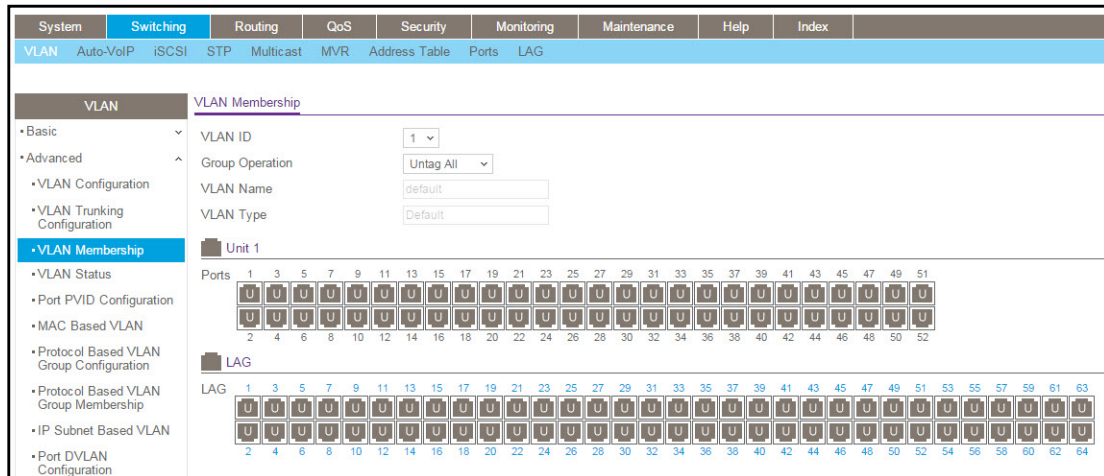
5. Enter the user name and password.

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

6. Click the **Login** button.

The web management interface menu displays.

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



8. In the **VLAN ID** list, select the VLAN ID.
9. In the **Group Operation** list, 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.** All the ports that can be dynamically registered in this VLAN through GVRP. This selection excludes all ports from the selected VLAN.
10. In the **Port** display, select port numbers to add them to this VLAN.

Each port can use one of 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 excludes a port from the selected VLAN.



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

**Table 77. Advanced 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 uses the name Default.
VLAN Type	The type of the VLAN you selected: <ul style="list-style-type: none"> <li>• <b>Default</b> (VLAN ID = 1). Always present</li> <li>• <b>Static</b>. A VLAN that 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 ID	VLAN Name	VLAN Type	Routing Interface	Member Ports
1	default	Default		1/0/1 - 1/0/48, lag 1 - lag 64

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

**Table 78. 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 VLAN type: <ul style="list-style-type: none"> <li>• <b>Default</b> (VLAN ID = 1). Always present</li> <li>• <b>Static</b>. A VLAN that 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 Settings

You can assign a port VLAN ID (PVID) to an interface. There are certain requirements for a PVID:

- You must define a PVID for all ports.
- If no other value is specified, the default VLAN PVID is used.
- To change the port's 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 PVID 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 > Port PVID Configuration**.

Interface	PVID	VLAN Member	VLAN Tag	Acceptable Frame Types	Configured Ingress Filtering	Current Ingress Filtering	Port Priority (0 to 7)
<input type="checkbox"/> 1/0/1	1	1	None	Admit All	Disable	Disable	0
<input type="checkbox"/> 1/0/2	1	1	None	Admit All	Disable	Disable	0
<input type="checkbox"/> 1/0/3	1	1	None	Admit All	Disable	Disable	0
<input type="checkbox"/> 1/0/4	1	1	None	Admit All	Disable	Disable	0
<input type="checkbox"/> 1/0/5	1	1	None	Admit All	Disable	Disable	0
<input type="checkbox"/> 1/0/6	1	1	None	Admit All	Disable	Disable	0
<input type="checkbox"/> 1/0/7	1	1	None	Admit All	Disable	Disable	0
<input type="checkbox"/> 1/0/8	1	1	None	Admit All	Disable	Disable	0
<input type="checkbox"/> 1/0/9	1	1	None	Admit All	Disable	Disable	0
<input type="checkbox"/> 1/0/10	1	1	None	Admit All	Disable	Disable	0

8. To display information for all physical ports and LAGs, click the **ALL** button.
9. Select the interfaces.  
Select the **Interface** check box next to the interfaces. You can select multiple interfaces. To select all the interfaces, select the **Interface** check box in the heading row.
10. In the **PVID** field, specify the VLAN ID to assign to untagged or priority-tagged frames received on this port.  
The factory default is 1.
11. In the **VLAN Member** field, specify the VLAN ID or list of VLANs of a member port.  
VLAN IDs range from 1 to 4093. The factory default is 1. Use a hyphen (-) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted.
12. In the **VLAN Tag** field, specify the VLAN ID or list of VLANs of a tagged port.  
VLAN IDs range from 1 to 4093. Use a hyphen (-) to specify a range or a comma (,) to separate VLAN IDs in a list. Spaces and zeros are not permitted. To reset the VLAN tag configuration to the defaults, use the **None** keyword. Port tagging for the VLAN can be set only if the port is a member of this VLAN.
13. In the **Acceptable Frame Types** list, specify the types of frames that can be received on this port.  
The options are **VLAN only** and **Admit All**:
  - When set to **VLAN only**, untagged frames or priority-tagged frames received on this port are discarded.
  - When set to **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.
14. In the **Configured Ingress Filtering** field, select **Enabled** or **Disabled**.
  - 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.

15. In the **Port Priority** field, specify the default 802.1p priority assigned to untagged packets arriving at the port.

You can enter a number from 0 to 7.

## Configure a MAC-Based VLAN

The MAC-Based VLAN feature allows incoming untagged packets to be assigned to a VLAN and thus classify traffic based on the source MAC address of the packet.

You define a 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 (that is, there is a system-wide table with 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 was not created on the system.

### ➤ To configure a MAC-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.

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 Configuration		
<input type="checkbox"/>	MAC Address	VLAN ID
	00:00:00:00:00:00	

8. In the **MAC Address** field, type a valid MAC address to be bound to a VLAN ID.  
This field is configurable only when a MAC-based VLAN is created.
9. In the **VLAN ID** field, specify a VLAN ID in the range of 1 to 4093.
10. Click the **Add** button.  
The MAC address is added to the VLAN mapping.
11. To delete a MAC address from VLAN mapping, click the **Delete** button.

## Configure Protocol-Based VLAN Groups

You can use a protocol-based VLAN to define filtering criteria for untagged packets. By default, if you do not configure any port-based (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 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 specify 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**.

Protocol Based VLAN Group Configuration					
<input type="checkbox"/>	Group ID	Group Name	Protocol	VLAN ID	Ports
<input type="checkbox"/>					

8. In the **Group Name** field, type a name for the new group.

You can enter up to 16 characters.

9. In the **Protocol** field, select the protocols to be associated with the group.

There are three configurable protocols:

- **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. In the **VLAN ID** field, select the VLAN ID.

It can be any number in the range of 1 to 4093. All the ports in the group assigns this VLAN ID to untagged packets received for the protocols that you included in this group.

11. Click the **Add** button.

The protocol-based VLAN group is added to the switch.

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 79. Protocol Based VLAN Group**

Field	Description
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 configure 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.

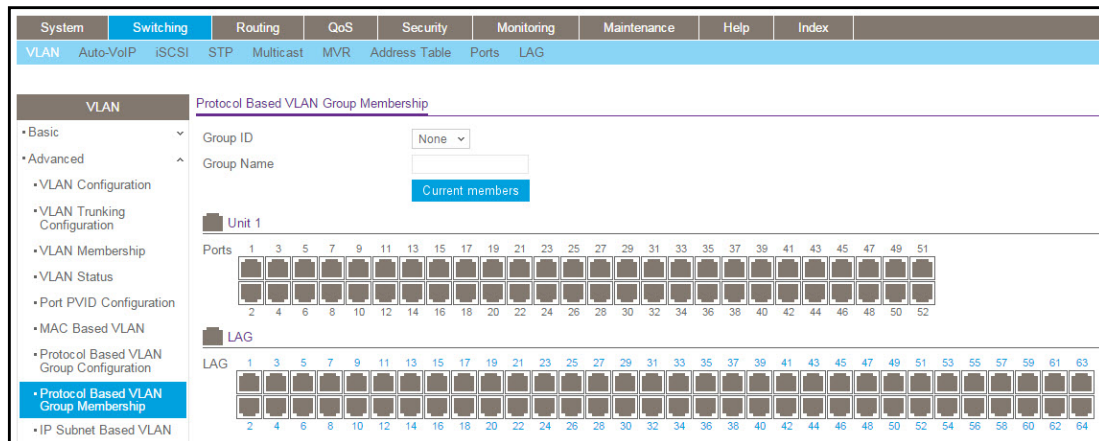
5. Enter the user name and password.

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. In the **Group ID** list, select the protocol-based VLAN group ID.
9. Select port numbers (1, 2, 3, and so on) to select ports to add to this protocol-based VLAN group.

An 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 can add it to a new group for IPX.

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

**Table 80. Protocol-Based VLAN Group Membership**

Field	Description
Group Name	This field identifies the name for the protocol-based VLAN that 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 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.

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 > IP Subnet Based VLAN**.

IP Subnet Based VLAN Configuration			
<input type="checkbox"/>	IP Address	Subnet Mask	VLAN ID
	<input type="text"/>	<input type="text"/>	<input type="text"/>

8. In the **IP Address** field, specify a valid IP address bound to the VLAN ID.  
Enter the IP address in dotted-decimal notation.
9. In the **Subnet Mask** field, specify a valid subnet mask of the IP address.



Enter the subnet mask in dotted-decimal notation.

10. In the **VLAN ID** field, specify a VLAN ID in the range of (1 to 4093).

11. Click the **Add** button.

The IP subnet-based VLAN is added.

12. To delete the selected IP subnet-based VLAN, click the **Delete** button.

## Configure a Port DVLAN

### ➤ To configure a 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.

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 DVLAN Configuration**.

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
1/0/7	Disable
1/0/8	Disable
1/0/9	Disable
1/0/10	Disable
1/0/11	Disable
1/0/12	Disable

8. Select **Interface** check boxes to select the physical interface.  
To select all ports, select the Interface check box at the top of the column.
9. In the **Admin Mode** field, select **Enabled** or **Disabled**.  
This specifies the administrative mode through which double VLAN tagging can be enabled or disabled. The default value for this is Disabled.
10. In the **Global EtherType** field, specify 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 voice VLAN configuration. Only users 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**.

**Voice VLAN Global Admin**

Admin Mode ☒ Disable ☐ Enable

---

**Voice VLAN Configuration**

1 All Go To Interface

	Interface	Interface Mode	Value	CoS Override Mode	Operational State	Authentication Mode	DSCP Value
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>		<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	1/0/1	Disable	0	Disable	Disable	Enable	0
<input type="checkbox"/>	1/0/2	Disable	0	Disable	Disable	Enable	0
<input type="checkbox"/>	1/0/3	Disable	0	Disable	Disable	Enable	0
<input type="checkbox"/>	1/0/4	Disable	0	Disable	Disable	Enable	0
<input type="checkbox"/>	1/0/5	Disable	0	Disable	Disable	Enable	0

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

This specifies the administrative mode for voice VLAN for the switch. The default is Disable.

9. Use **Interface** to select the physical interface.

10. Use **Interface Mode** to select the voice VLAN mode for selected interface:

- **Disable**. This is 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 the interface mode.

12. In the **CoS Override Mode** field, select **Disable** or **Enable**.

The default is Disable.

13. In the **Authentication Mode** field, select **Enable** or **Disable**.

The default is **Enable**. When the authentication mode is enabled, voice traffic is allowed on an unauthorized voice VLAN port. When the authentication mode is disabled, devices are authorized through dot1x.

**Note:** Authentication through dot1x is possible only if dot1x is enabled.

14. In the **DSCP Value** field, configure the Voice VLAN DSCP value for the port.

The valid range is 0 to 64. The default value is 0.

The Operational State field displays the operational status of the voice VLAN on the given interface.

## 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.

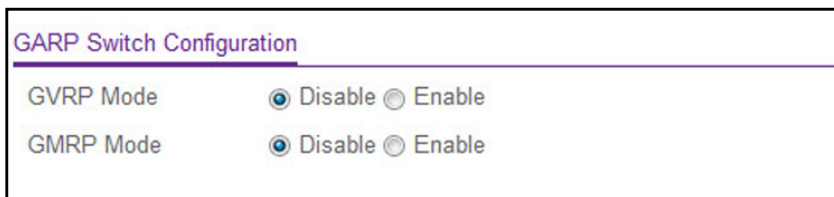
5. Enter the user name and password.

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**.



GARP Switch Configuration	
GVRP Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
GMRP Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

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

This selects 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 selects the GARP multicast registration protocol administrative mode for the switch. The factory default is Disable.

## Configure GARP Port

---

**Note:** It can take up to 10 seconds for GARP configuration changes to take effect.

---

➤ **To configure GARP 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 **Switching > VLAN > Advanced > GARP Port Configuration**.

<input type="checkbox"/>	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

8. Use **Interface** to select the physical interface for which data is to be displayed or configured.
9. In the **Port GVRP Mode** field, select **Enable** or **Disable**.  
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 **Enable** or **Disable**

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 re-registering) 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 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. Use **Leave All Time (centiseconds)** to control how frequently LeaveAll PDUs are generated.

A LeaveAll PDU indicates that all registrations will be deregistered soon. To maintain registration, participants must rejoin. 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

You can configure protocol-based port settings and OUI settings.

### 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 web management interface for configuring Auto-VoIP settings. It is divided into two main sections: 'Protocol Based Global Settings' and 'Protocol Based Port Settings'.

**Protocol Based Global Settings:**

- Prioritization Type:** A dropdown menu set to 'Traffic Class'.
- Class Value:** A dropdown menu set to '6'.

**Protocol Based Port Settings:**

- At the top, there is a filter '1 LAGS All' and a 'Go To Interface' field with a 'Go' button.
- Below is a table with the following columns: 'Interface', 'Auto VoIP Mode', and 'Operational Status'.
- The table lists five interfaces: 1/0/1, 1/0/2, 1/0/3, 1/0/4, and 1/0/5. Each interface has a checkbox in the 'Interface' column, a 'Disable' option in the 'Auto VoIP Mode' column, and a 'DOWN' status in the 'Operational Status' column.

8. In the **Prioritization Type** field, select **Traffic Class** or **Remark**.

This specifies the type of prioritization.

9. In the **Class Value** list, 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 switch is updated with the values you entered. For the switch to retain the new values across a power cycle you must perform a save.

## Configure Auto-VoIP OUI-Based Properties

### ➤ To configure auto-VoIP OUI-based 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.

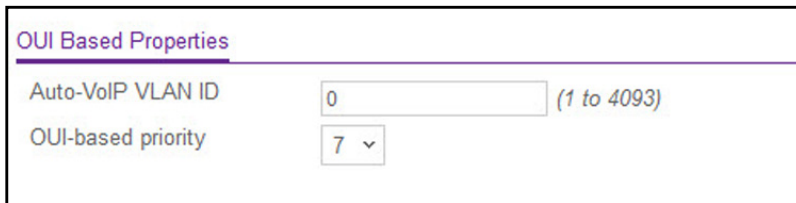
5. Enter the user name and password.

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 **VoIP VLAN ID** field, type the VoIP VLAN ID of the switch.

There is no default VLAN for auto-VoIP, you must create a VLAN for it first.

9. In the **OUI-based priority** list, select the OUI-based priority of the switch.

The default value is 7.

10. Click the **Apply** button.

The switch is updated with the values you entered. For the switch to retain the new values across a power cycle, you must perform a save.

## OUI-Based Port Settings

### ➤ To configure auto-VoIP OUI-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 > OUI-based > Port Settings**.

<input type="checkbox"/>	Interface	Auto VoIP Mode	Operational Status
<input type="checkbox"/>	1/0/1	Disable	DOWN
<input type="checkbox"/>	1/0/2	Disable	DOWN
<input type="checkbox"/>	1/0/3	Disable	DOWN
<input type="checkbox"/>	1/0/4	Disable	DOWN
<input type="checkbox"/>	1/0/5	Disable	DOWN

The Operational Status field displays the current operational status of each interface.

8. Use **Interface** check boxes to select the interfaces.
9. In the **Auto VoIP Mode** field, select **Disable** or **Enable**.  
Auto-VoIP is disabled by default.
10. Use **Go To Interface** to select an interface by entering its number.
11. Click the **Apply** button.

The switch is updated with the values you entered. For the switch to retain the new values across a power cycle, you must perform a save.

## Configure the OUI Table

### ➤ To configure the OUI 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 > Auto-VoIP > OUI-based > OUI Table**.

OUI Table		
<input type="checkbox"/>	Telephony OUI(s)	Description
<input type="checkbox"/>		
<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
<input type="checkbox"/>	00:04:13	SNOM

8. In the **Telephony OUI(s)** field, specify the VoIP OUI prefix to be added in the format AA:BB:CC.

Up to 128 OUIs can be configured.

9. In the **Description** field, 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. Click the **Add** button.

The telephony OUI entry is added.

11. To delete a created entry, click the **Delete** button.

## View the Auto-VoIP Status

➤ **To view 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**.

System	Switching	Routing	QoS	Security	Monitoring
VLAN	Auto-VoIP	iSCSI	STP	Multicast	MVR
		Address Table	Ports	LAG	
Auto-VoIP		Auto-VoIP Status			
• Protocol-based		Auto-VoIP VLAN ID		0	
• OUI-based		Maximum Number of Voice Channels Supported		20	
• Auto-VoIP Status		Number of Voice Channels Detected		0	

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable Auto-VoIP status information.

**Table 81. Auto-VoIP Status**

Field	Description
Auto-VoIP VLAN ID	The auto-VoIP VLAN ID.
Maximum Number of Voice Channels Supported	The maximum number of voice channels supported.
Number of Voice Channels Detected	The number of VoIP channels prioritized successfully.

## iSCSI Overview

The Internet Small Computer System Interface (iSCSI) feature helps network administrators track iSCSI traffic between iSCSI initiators and target systems. This is accomplished by monitoring or snooping traffic to detect packets used by iSCSI stations in establishing iSCSI sessions and connections. Data from these exchanges is used to create classification rules that assign the traffic between the stations to a configured traffic class. Packets in the flow are queued and scheduled for egress on the destination port based on these rules.

In networks containing iSCSI initiators and targets, iSCSI helps to monitor iSCSI sessions or give iSCSI traffic preferential Quality of Service (QoS) treatment. Dynamically-generated classifier rules are used to direct the iSCSI data traffic to queues that can be given the desired preference characteristics over other data traveling through the switch. This might help to avoid session interruptions during times of congestion that would otherwise cause iSCSI packets to be dropped. However, in systems where a large proportion of traffic is iSCSI, it might also interfere with other network control-plane traffic, such as ARP or LACP.

The preferential treatment of iSCSI traffic must be balanced against the needs of other critical data in the network.

You can view and manage iSCSI Optimization settings on the device. iSCSI Optimization provides a means of giving traffic between iSCSI initiator and target systems special Quality of Service (QoS) treatment.

In addition, if configured, the packets can be updated with IEEE 802.1 or IP-DSCP values. This is done by enabling Remark. Remarking packets with priority data provides special QoS treatment as the packets continue through the network.

## Configure Global iSCSI Settings

### ➤ To configure the global iSCSI settings 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.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > iSCSI > Basic > Global Configuration**.

The screenshot shows the 'iSCSI Global Configuration' page. The top navigation bar includes 'System', 'Switching', 'Routing', 'QoS', 'Security', 'Monitoring', and 'Maintenance'. Under 'Switching', there are sub-tabs: 'VLAN', 'Auto-VoIP', 'iSCSI', 'STP', 'Multicast', 'MVR', 'Address Table', 'Ports', and 'LAG'. The 'iSCSI' tab is selected, and the left sidebar shows a tree structure with 'Basic' (selected), 'Global Configuration', 'Sessions', and 'Advanced'. The main content area is titled 'iSCSI Global Configuration' and contains the following settings:

- iSCSI Status:** Radio buttons for 'Disable' (selected) and 'Enable'.
- QoS Profile:** Radio buttons for 'VLAN Priority Tag' (selected) and 'DSCP'.
- VLAN Priority Tag:** A dropdown menu showing '5'.
- DSCP:** A dropdown menu showing '46'.
- Remark:** Radio buttons for 'Disable' and 'Enable' (selected).
- iSCSI Aging Time:** A text input field showing '10' with a note '(1 to 43200 minutes)'.

8. In the **iSCSI Status** field, select **Enable** or **Disable**.

This globally enables or disables the iSCSI Optimization feature. By default, iSCSI Optimization is disabled.

9. Select the QoS Profile **VLAN Priority Tag** or **DSCP** radio button.

This specifies the Quality of Service (QoS) profile that is applied to iSCSI flows. By default, iSCSI flows are assigned to the highest VLAN Priority tag (VPT)/DSCP mapped to the highest queue not used for chassis management or voice VLAN.

Setting the VLAN Priority tag/DSCP sets the QoS profile which determines the egress queue to which the frame is mapped. The switch default setting for egress queues scheduling is Weighted Round Robin (WRR). Complete the QoS setting by configuring the relevant ports to work in other scheduling and queue management modes through the Class of Service settings. Depending on the platform, these choices might include strict priority for the queue used for iSCSI traffic. The downside of strict priority is that, in certain circumstances (under heavy high priority traffic), other lower priority traffic might get starved. In WRR, the queue to which the flow is assigned to can be set to get the required percentage.

10. Configure the global traffic class mapping in Class of Service.

The global traffic class mapping configuration determines the traffic class used to transmit iSCSI packets. The traffic mapping configuration options are as follows:

- IEEE 802.1P
- IP-DSCP

The configuration of the CoS component determines changes in the mapping of IEEE 802.1p or IP-DSCP values to traffic classes. For more information, see [Class of Service](#) on page 511.

11. If you are using VLAN Priority as the QoS profile, in the **VLAN Priority Tag** field, select the iSCSI session packets.

The range is 0 to 7. The default is 5.

12. If you are using DSCP as the QoS profile, in the **DSCP** list, select a value to assign iSCSI session packets.

The range is 0 to 63. The default is 46.

13. Select the Remark **Enable** or **Disable** radio button.

This enables or disables the marking of iSCSI frames with the configured VLAN Priority tag/DSCP when egressing the switch. Enabling remarks updates the packets with IEEE 802.1p or IP-DSCP values. Remarking packets with priority data provides special QoS treatment as the packets continue through the network. Remark is enabled by default.

14. In the **iSCSI Aging Time** field, set the number of minutes a session can be inactive prior to If using DSCP as the QoS profile, userremoval.

The iSCSI Aging Time must be a whole number in the range of 1 to 43200 minutes. The default is 10 minutes.

15. Click the **Apply** button.

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

## View iSCSI Sessions

### ➤ To view active iSCSI session 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. click **Switching > iSCSI > Basic > Sessions**.

iSCSI Sessions		
Target Name	Initiator Name	ISID (Initiator Session ID)

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable iSCSI Sessions information.

**Table 82. iSCSI Sessions**

Field	Description
Target Name	The target's name.
Initiator Name	The initiator's name.
Initiator Session ID (ISID)	The iSCSI identifier.

## Control iSCSI Target Settings

You can view iSCSI targets and assign target ports/port IP address combinations for iSCSI optimization on the switch.

### ➤ To configure iSCSI target 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 > iSCSI > Advanced > iSCSI Targets**.

The screenshot shows the web management interface with the following structure:

- Top Navigation Bar:** System, Switching (selected), Routing, QoS, Security, Monitoring, Maintenance.
- Sub-Navigation Bar:** VLAN, Auto-VoIP, iSCSI (selected), STP, Multicast, MVR, Address Table, Ports, LAG.
- Left Sidebar (iSCSI menu):**
  - Basic (expanded)
  - Advanced (expanded)
  - Global Configuration
  - iSCSI Targets** (selected)
  - Sessions
  - Sessions Detailed
- Main Content Area:**
  - iSCSI Targets Configuration** (Title)
  - Table:**

<input type="checkbox"/>	TCP Port	IP Address	Target Name
<input type="checkbox"/>	860	0.0.0.0	
<input type="checkbox"/>	3260	0.0.0.0	

8. In the **TCP Port** field, specify the TCP port for the target that monitors iSCSI traffic.  
Up to 16 TCP ports can be defined in the system. The well-known iSCSI ports 860 and 3260 are configured as defaults but you can remove them as any other configured target.
9. In the **IP address** field, specify an IP address for the target that monitors iSCSI traffic.  
The default is 0.0.0.0.
10. In the **Target Name** field, specify a name to assign to the target.  
The iSCSI **Target Name** can be up to 233 characters in length.
11. Click the **Add** button.  
The iSCSI targets configuration is added.
12. To delete a selected iSCSI targets configuration, click the **Delete** button.

## View iSCSI Sessions

### ➤ To view information about active iSCSI 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 **Switching > iSCSI > Advanced > Sessions**.

iSCSI Sessions		
Target Name	Initiator Name	ISID (Initiator Session ID)
iqn.2012-05.cbu-80-06-02:disk177	iqn.1991-05.com.microsoft:admin-pc	400001370000
iqn.2012-05.cbu-80-06-02:test	iqn.1991-05.com.microsoft:admin-pc	400001370000



The following describes the nonconfigurable iSCSI Sessions information that is displayed.

**Table 83. iSCSI Sessions**

Field	Description
Target Name	The target's name.
Initiator Name	The initiator's name.
Initiator Session ID (ISID)	The unique identifier an initiator assigns to its session endpoint which, when combined with the iSCSI initiator name, provides a unique name for the iSCSI initiator port.

## View iSCSI Session Details

You can view detailed information about active iSCSI sessions.

➤ **To view the iSCSI session details:**

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

iSCSI Sessions Detailed			
Session Index	0 ▾		
Target Name	iqn.2012-05.cbu-80-06-02:disk118		
Initiator Name	iqn.1991-05.com.microsoft:admin-pc		
Up Time	00:00:02:03 (DD:HH:MM:SS)		
Time for aging out (in Seconds)	599		
ISID (Initiator Session ID)	400001370000		
Initiator IP address	Initiator TCP Port	Target IP Address	Target TCP Port
172.26.2.193	53179	172.26.2.116	3260

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable iSCSI Sessions Detailed information.

**Table 84. iSCSI Sessions Detailed**

Field	Description
Session Index	The list of session indices.
The rest of the fields on this screen correspond to the currently selected Session Index.	
Target Name	The target's name.
Initiator Name	The initiator's name.
Up Time	The time elapsed since the creation of the current session.
Time for Aging Out (in Seconds)	The time left for the current session to expire in seconds.
Initiator Session ID (ISID)	The unique identifier an initiator assigns to its session endpoint which, when combined with the iSCSI initiator name, provides a unique name for the iSCSI initiator port.
Initiator IP Address	The initiator's IP address.
Initiator TCP Port	The initiator's TCP port number of one of the connections between the target and initiator.
Target IP Address	The IP address of the target.
Target TCP Port	The target's TCP port number of one of the connections between the target and initiator.

## Spanning Tree Protocol

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 on configuring Common STP, see [Configure CST Port Settings](#) on page 236.

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 which 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 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.

---

**Note:** For two bridges to be in the same region, the force version must be 802.1s and their configuration name, digest key, and revision level must match. For additional information about regions and their effect on network topology, refer to the IEEE 802.1Q standard.

---

## Configure Basic STP Settings

### ➤ To configure STP basic 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 > Basic > STP Configuration**.

**STP Configuration**

Spanning Tree Admin Mode: ☐ Disable ☒ Enable

Force Protocol Version: ☐ IEEE 802.1d ☒ IEEE 802.1w ☐ IEEE 802.1s ☐ PVST ☐ RPVST

Configuration Name:

Configuration Revision Level:  (0 to 65535)

Forward BPDU while STP Disabled: ☒ Disable ☐ Enable

BPDU Guard: ☒ Disable ☐ Enable

BPDU Filter: ☒ Disable ☐ Enable

Configuration Digest Key:

Configuration Format Selector:

Fast Backbone: ☒ Disabled ☐ Enabled

Fast Uplink: ☒ Disabled ☐ Enabled

Max Update Rate:  (0 to 32000 packets/sec. Default: 150.)

**STP Status**

MST ID	VID	FID
0	1	1
0	4093	4093

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, IEEE 802.1s, PVST, and RPVST.
10. Use **Configuration Name** to specify an identifier used to identify the configuration currently being used.  
It can be up to 32 alphanumeric characters.
11. Use **Configuration Revision Level** to 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 are 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 do not 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 disable 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. 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 then it drops the BPDUs received on this port.
15. Select the e **Fast Backbone Mode Disable** or **Enable** radio button. (*PVSTP only*)  
Use this option to choose a new indirect link when an indirect link fails. The system does not ignore inferior BPDUs, as is done in 802.1d. Rather the system uses the BPDUs to age out on the port it received the BPDUs. Later the system sends out root link queries on other non-designated ports. Based on the replies, if there is a positive response to at least one of them, it chooses a new indirect link. Fast Backbone mode is disabled by default.
16. Select the **Fast Uplink Mode Disable** or **Enable** radio button. (*PVSTP only*)  
This option reduces the recovery time in selecting a new root port when the primary root port goes down. Fast Uplink mode is disabled by default.
17. Use the **Max Update Rate** field to configure the Fast Uplink Maximum Update Rate.  
This field is enabled for configuration when Fast Uplink mode is enabled. Allowed values are 0 to 32000 packets per second. The default value is 150.

**18.** Click the **Apply** button.

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

The following table describes the nonconfigurable fields.

**Table 85. STP Configuration**

Field	Description
Configuration Digest Key	Identifier used to identify the configuration currently being used.
Configuration Format Selector	The version of the configuration format being used in the exchange of BPDUs.
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**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
VLAN	Auto-VoIP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG
								MLAG
								MRP

STP	STP Configuration
• Basic	Spanning Tree Admin Mode <input type="radio"/> Disable <input checked="" type="radio"/> Enable
• Advanced	Force Protocol Version <input type="radio"/> IEEE 802.1d <input checked="" type="radio"/> IEEE 802.1w <input type="radio"/> IEEE 802.1s <input type="radio"/> PVST <input type="radio"/> RPVST
• STP Configuration	Configuration Name <input type="text" value="C4-04-15-AD-7F-18"/>
• CST Configuration	Configuration Revision Level <input type="text" value="0"/> (0 to 65535)
• CST Port Configuration	Forward BPDU while STP Disabled <input checked="" type="radio"/> Disable <input type="radio"/> Enable
• CST Port Status	BPDU Guard <input checked="" type="radio"/> Disable <input type="radio"/> Enable
• MST Configuration	BPDU Filter <input checked="" type="radio"/> Disable <input type="radio"/> Enable
• MST Port Status	Configuration Digest Key <input type="text" value="0xac36177f50283cd4b83821d8ab26de62"/>
• STP Statistics	Configuration Format Selector <input type="text" value="0"/>
• PVST VLAN	Fast Backbone <input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
• PVST Interface	Fast Uplink <input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
• PVST Statistics	Max Update Rate <input type="text" value="150"/> (0 to 32000 packets/sec. Default: 150.)

STP Status		
MST ID	VID	FID
0	1	1

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

This specifies whether spanning tree operation is enabled on the switch. The default is Enable.

9. Use **Force Protocol Version** to specify the Force Protocol Version parameter for the switch.

The options are IEEE 802.1d, IEEE 802.1w, IEEE 802.1s, PVST, and RPVST. The default is IEEE 802.1w.

10. Use **Configuration Name** to specify the identifier used to identify the configuration currently being used.

It can be up to 32 alphanumeric characters.

11. Use **Configuration Revision Level** to 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 are forwarded while spanning-tree is disabled on the switch. The default is Disable.

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 do not 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 disable 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. 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 then it drops the BPDUs received on this port.

**15. Select the Fast Backbone Mode **Disable** or **Enable** radio button. (PVSTP only.)**

Use this option to choose a new indirect link when an indirect link fails. The system does not ignore inferior BPDUs, as is done in 802.1d. Rather the system uses the BPDUs to age out on the port it received the BPDUs. Later the system sends out root link queries on other non-designated ports. Based on the replies, if there is a positive response to at least one of them, it chooses a new indirect link. Fast Backbone mode is disabled by default.

**16. Select the Fast Uplink Mode **Disable** or **Enable** radio button. (PVSTP only.)**

This option reduces the recovery time in selecting a new root port when the primary root port goes down. Fast Uplink mode is disabled by default.

**17. Use the **Max Update Rate** field to configure the Fast Uplink Maximum Update Rate.**

This field is enabled for configuration when Fast Uplink mode is enabled. Allowed values are 0 to 32000 packets per second. The default value is 150.

**18. 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 86. STP Configuration**

Field	Description
Configuration Digest Key	The 16-byte signature of type HMAC-MD5 created from the MST Configuration Table (a VLAN ID-to-MST ID mapping) which is used to identify the configuration currently being used.
Configuration Format Selector	The version of the configuration format being used in the exchange of BPDUs.
STP Status	
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 CST Settings

You can configure Common Spanning Tree (CST) and Internal Spanning Tree on the switch.

➤ **To configure CST 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 > CST Configuration**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance		
VLAN	Auto-VoIP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG
<div> <div>STP</div> <div>CST Configuration</div> </div>								
<div> <div>Basic</div> <div>Advanced</div> <div>STP Configuration</div> <div><b>CST Configuration</b></div> <div>CST Port Configuration</div> <div>CST Port Status</div> <div>MST Configuration</div> <div>MST Port Status</div> <div>STP Statistics</div> <div>PVST VLAN</div> <div>PVST Interface</div> <div>PVST Statistics</div> </div>		<div> <div>Bridge Priority</div> <div>32768</div> <div>(0 to 61440)</div> </div> <div> <div>Bridge Max Age (secs)</div> <div>20</div> <div>(6 to 40)</div> </div> <div> <div>Bridge Hello Time (secs)</div> <div>2</div> <div></div> </div> <div> <div>Bridge Forward Delay (secs)</div> <div>15</div> <div>(4 to 30)</div> </div> <div> <div>Spanning Tree Maximum Hops</div> <div>20</div> <div>(6 to 40)</div> </div> <div> <div>Spanning Tree Tx Hold Count</div> <div>6</div> <div>(1 to 10)</div> </div>						
		<div>CST Status</div> <div> <div>Bridge Identifier</div> <div>80:00:20:E5:2A:51:0A:CE</div> </div> <div> <div>Time Since Topology Change</div> <div>0 day 10 hr 8 min 23 sec</div> </div> <div> <div>Topology Change Count</div> <div>0</div> </div> <div> <div>Topology Change</div> <div>False</div> </div> <div> <div>Designated Root</div> <div>80:00:20:E5:2A:51:0A:CE</div> </div> <div> <div>Root Path Cost</div> <div>0</div> </div> <div> <div>Root Port Identifier</div> <div>00:00</div> </div> <div> <div>Max Age (secs)</div> <div>20</div> </div> <div> <div>Forward Delay (secs)</div> <div>15</div> </div> <div> <div>Hold Time (secs)</div> <div>6</div> </div> <div> <div>CST Regional Root</div> <div>80:00:20:E5:2A:51:0A:CE</div> </div> <div> <div>CST Path Cost</div> <div>0</div> </div> <div> <div>Port Triggered TC</div> <div></div> </div>						



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 BPDUs, the switch with the lowest priority value becomes the root bridge. Specifies 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).** 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).** 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).** 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 seconds.
- **Spanning Tree Maximum Hops.** The maximum number of bridge hops the information for a particular CST instance can travel before being discarded. The valid range is 6–40. The default is 20 hops.
- **Spanning Tree Tx Hold Count.** Configures the maximum number of bpdus the bridge is allowed to send within the hello time window. The valid range is 1–10. The default value is 6.

9. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the CST Status information that is displayed.

**Table 87. STP Advanced CST Configuration**

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 changed for the CST.

**Table 87. STP Advanced CST Configuration**

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 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 Port Settings

You can configure the Common Spanning Tree (CST) and Internal Spanning Tree on a specific port on the switch.

A port can become *Diagnostically Disabled* (D-Disable) when DOT1S experiences a severe error condition. The most common cause is when the DOT1S software experiences BPDU flooding. The flooding criteria is such that DOT1S receives more than 15 BPDUs in a 3-second interval. The other causes for DOT1S D-Disable are extremely rare.

### ➤ To configure CST 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 > 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	BPDU Filter	BPDU Forwarding	BPDU Guard Effect	Auto Edge	Root Guard	Loop Guard	TCN Guard	Port Mode	Port Forwarding State
1/0/1	128	Disable	0	Enabled	2	0	Enabled	Disable	Disable	Disable	Enable	Disable	Disable	Disable	Enable	Disabled
1/0/2	128	Disable	0	Enabled	2	0	Enabled	Disable	Disable	Disable	Enable	Disable	Disable	Disable	Enable	Disabled
1/0/3	128	Disable	0	Enabled	2	0	Enabled	Disable	Disable	Disable	Enable	Disable	Disable	Disable	Enable	Disabled
1/0/4	128	Disable	0	Enabled	2	0	Enabled	Disable	Disable	Disable	Enable	Disable	Disable	Disable	Enable	Disabled
1/0/5	128	Disable	0	Enabled	2	0	Enabled	Disable	Disable	Disable	Enable	Disable	Disable	Disable	Enable	Disabled

8. Select an **Interface**.

You can select a physical or port channel interface associated with VLANs associated with the CST.

9. 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 attempted to be set to any value between 0 and 15, it is set to 0. If it is tried to be set to any value between 16 and (2\*16-1) it is set to 16 and so on. The default value is 128.

10. Use **Admin Edge Port** to specify if the specified port is an Edge Port within the CIST.

Use the menu to select **Disable** or **Enable**. The default value is Disable.

11. 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. The default is 0.

12. 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. The default is 0.

13. Use **BPDU Filter** to configure the BPDU Filter, which filters the BPDU traffic on this port when STP is enabled on this port.

The possible values are **Enable** or **Disable**. The default value is Disable.

14. Use **BPDU Flood** to configure the BPDU Flood, which floods the BPDU traffic arriving on this port when STP is disabled on this port.

The possible values are **Enable** or **Disable**. The default value is Disable.

15. Use **Auto Edge** to configure 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.

The possible values are **Enable** or **Disable**. The default value is Enable.

16. Use **Root Guard** to configure the root guard mode, which sets a port to discard any superior information received by the port and thus protect against root of the device from changing.

The port gets put into discarding state and does not forward any packets. The possible values are **Enable** or **Disable**. The default value is Disable.

17. Use **Loop Guard** to enable or disable 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. The default value is Disable

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**. The default value is 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 default value is **Disable**.

20. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

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

**Table 88. 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	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	Display the BPDU Guard Effect, it 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 CST Port Status

You can view the Common Spanning Tree (CST) and Internal Spanning Tree on a specific port on the switch.

### ➤ To view the 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								
1 LAGS All								
Interface	Port ID	Port Forwarding State	Port Role	Designated Root	Designated Cost	Designated Bridge	Designated Port	Topology Change Acknowledge
1/0/1	80:01	Disabled	Disabled	80:00:C4:04:15:AD:7F:09	0	80:00:C4:04:15:AD:7F:09	00:00	False
1/0/2	80:02	Disabled	Disabled	80:00:C4:04:15:AD:7F:09	0	80:00:C4:04:15:AD:7F:09	00:00	False
1/0/3	80:03	Disabled	Disabled	80:00:C4:04:15:AD:7F:09	0	80:00:C4:04:15:AD:7F:09	00:00	False
1/0/4	80:04	Disabled	Disabled	80:00:C4:04:15:AD:7F:09	0	80:00:C4:04:15:AD:7F:09	00:00	False
1/0/5	80:05	Disabled	Disabled	80:00:C4:04:15:AD:7F:09	0	80:00:C4:04:15:AD:7F:09	00:00	False

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
Disabled	False	80:00:C4:04:15:AD:7F:09	0	0 day 1 hr 5 min 24 sec	False	0	0
Disabled	False	80:00:C4:04:15:AD:7F:09	0	0 day 1 hr 5 min 24 sec	False	0	0
Disabled	False	80:00:C4:04:15:AD:7F:09	0	0 day 1 hr 5 min 24 sec	False	0	0
Disabled	False	80:00:C4:04:15:AD:7F:09	0	0 day 1 hr 5 min 24 sec	False	0	0
Disabled	False	80:00:C4:04:15:AD:7F:09	0	0 day 1 hr 5 min 24 sec	False	0	0

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the CST Status information displayed on the screen.

**Table 89. 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.

Table 89. CST Port Status (continued)

Field	Description
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: <b>Root Port</b> , <b>Designated Port</b> , <b>Alternate Port</b> , <b>Backup Port</b> , <b>Master Port</b> or <b>Disabled Port</b> .
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.
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 topology change acknowledgement flag is set for the next BPDU to be transmitted for this port. 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 Regional 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 transitioned into loop inconsistent state.
Transitions Out Of Loop Inconsistent State	The number of times this interface transitioned out of loop inconsistent state.

## Configure MST Settings

You can configure Multiple Spanning Tree (MST) on the switch.

### ➤ To configure an MST instance:

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

3. Launch a web browser.

4. Enter 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 Configuration**.

MST Configuration										
<input type="checkbox"/>	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:C4:04:15:AD:7F:09	1	0 day 1 hr 12 min 47 sec	0	False	80:00:C4:04:15:AD:7F:09	0	00:00

8. Configure the MST values:

- **MST ID.** Specify the ID of the MST to create. The valid values for this are 1 to 4094. This is only visible when the select option of the MST ID select box is selected.
- **Priority.** The bridge priority value for the MST. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. The 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 gives a combo box of each VLAN on the switch. These can be selected or unselected for re-configuring the association of VLANs to MST instances.

9. Click the **Add** button

This creates the new MST that you configured.

10. To modify an MST instance:

- a. Select the check box next to the instance (You can select multiple check boxes to apply the same setting to all selected ports.)
- b. Update the values
- c. click the **Apply** button.

11. To delete an MST instance, select the check box for the instance and click the **Delete** button.

To refresh the screen with the latest information on the switch, click the **Update** button.



For each configured instance, the information described in the following table displays on the screen.

**Table 90. 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 changed for the selected MST instance.
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 of 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 Port Identifier	Port to access the Designated Root for this MST instance.

## View the Spanning Tree MST Port Status

You can configure and display Multiple Spanning Tree (MST) settings on a specific port on the switch.

A port can become *Diagnostically Disabled* (D-Disable) when DOT1S experiences a severe error condition. The most common cause is when the DOT1S software experiences BPDU flooding. The flooding criteria is such that DOT1S receives more than 15 BPDUs in a 3-second interval. The other causes for DOT1S D-Disable are extremely rare.

### ➤ 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**.

Interface	Port Priority	Port Path Cost	Auto Calculated Port Path Cost	Port ID	Port Uptime Since Last Clear Counters	Port Mode	Port Forwarding State	Port Role	Designated Root
1/0/1	128	0	Enabled	80 01	0 day 0 hr 0 min 4 sec	Enabled	Disabled	Disabled	80 01 6C B0 CE
1/0/2	128	0	Enabled	80 02	0 day 0 hr 0 min 4 sec	Enabled	Disabled	Disabled	80 01 6C B0 CE
1/0/3	128	0	Enabled	80 03	0 day 0 hr 0 min 4 sec	Enabled	Disabled	Disabled	80 01 6C B0 CE
1/0/4	128	0	Enabled	80 04	0 day 0 hr 0 min 4 sec	Enabled	Disabled	Disabled	80 01 6C B0 CE
1/0/5	128	0	Enabled	80 05	0 day 0 hr 0 min 4 sec	Enabled	Disabled	Disabled	80 01 6C B0 CE
1/0/6	128	0	Enabled	80 06	0 day 0 hr 0 min 4 sec	Enabled	Disabled	Disabled	80 01 6C B0 CE
1/0/7	128	0	Enabled	80 07	0 day 0 hr 0 min 4 sec	Enabled	Disabled	Disabled	80 01 6C B0 CE

**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 attempted to be set to any value between 0 and 15, it is set to 0. If it is tried to be set to any value between 16 and (2\*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.

12. Click the **Apply** button.

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

The following table describes the read-only MST port configuration information displayed on the Spanning Tree CST Configuration screen.

**Table 91. MST Port Status**

Field	Description
Auto Calculated Port Path Cost	Displays whether the path cost is automatically calculated ( <b>Enable</b> ) or not ( <b>Disable</b> ). 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 <b>Enable</b> or <b>Disable</b> .
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: <b>Root Port</b> , <b>Designated Port</b> , <b>Alternate Port</b> , <b>Backup Port</b> , <b>Master Port</b> or <b>Disabled Port</b> .
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 STP 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.

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 Statistics**.

STP Statistics						
1 LAGS All						
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	0	0	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

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the information available on the STP Statistics screen.

**Table 92. 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 PVST VLAN Settings

You can view and configure Per VLAN Spanning Tree Protocol (PVST)/Per VLAN Rapid Spanning Tree Protocol (RPVST) VLAN settings for the device.

- **To configure PVST/RPVST VLAN settings for the 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 **Switching > STP > Advanced > PVST VLAN** in the navigation menu.

PVST/RPVST VLAN Configuration						
VLAN ID	Root	Hello Time	Forward Time	Max Age	Priority	
1	None	2	15	20	32768	

8. Select a **VLAN ID**, a unique VLAN identifier, from the list of VLANs with enabled STP Admin mode and PVST or RPVST.

9. In the **Root** list, select **None**, **Primary**, or **Secondary**.

The default value is None. This setting configures the switch to become the root bridge or standby root bridge by modifying the bridge priority from the default value of 32768 to a lower value calculated to ensure the bridge is the root (or standby) bridge.

10. In the **Hello Time** field, configure the spanning tree hello time interval for the specified VLAN

The hello time is the interval between sending successive BPDUs. Allowed values range from 1 to 10 seconds. The default value is 2 seconds.

11. In the **Forward Time** field, configure the spanning tree forward delay time for a specified VLAN.

The range is 4 to 30 seconds. The default value is 15 seconds. This interval is a time for listening and learning states before transitioning a port to the forwarding state.

12. Use the **Max Age** field to configure the spanning tree maximum age time for a specified VLAN.

Max age is the maximum age time before a bridge port saves its configuration information. The range is 6 to 40 seconds. The default value is 20 seconds.

13. Configure the bridge **Priority** of a VLAN.

The allowed values are between 0 and 61440. The valid values are listed in the following table.

**Table 93. PVST/RPVST VLAN Configuration - VLAN Bridge Priority**

0	4096	8192
12288	16384	20480
24576	28672	32768 (default)
36864	40960	45056
49152	53248	57344
61440	—	—

The default value is 32768. If the value configured is not among the specified values, then it is rounded off to the nearest valid value.

14. Click the **Add** button.

PVST/RPVST is enabled for the selected VLAN.

15. To disable PVST/RPVST for the specified VLAN entry, click the **Delete** button.

16. Click the **Apply** button.

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

## Configure the PVST Interface Settings

You can view and configure Per VLAN Spanning Tree Protocol (PVST)/Per VLAN Rapid Spanning Tree Protocol (RPVST) Interface settings for the device.

### ➤ To configure the PVST/RPVST 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 > STP > Advanced > PVST Interface**.

System Switching Routing QoS Security Monitoring Maintenance Help																																																														
VLAN Auto-VoIP iSCSI STP Multicast MVR Address Table Ports LAG MLAG MRP																																																														
STP PVST/RPVST Interface Configuration																																																														
• Basic • Advanced		VLAN ID: 1																																																												
• STP Configuration • CST Configuration • CST Port Configuration • CST Port Status • MST Configuration • MST Port Status • STP Statistics • PVST VLAN • <b>PVST Interface</b> • PVST Statistics		1 2 3 LAG All <table border="1"> <thead> <tr> <th>Interface</th> <th>Priority</th> <th>Cost</th> <th>Role</th> <th>Status</th> </tr> </thead> <tbody> <tr><td><input type="checkbox"/> 1/0/1</td><td>128</td><td>0</td><td>Disabled</td><td>Disabled</td></tr> <tr><td><input type="checkbox"/> 1/0/2</td><td>128</td><td>0</td><td>Disabled</td><td>Disabled</td></tr> <tr><td><input type="checkbox"/> 1/0/3</td><td>128</td><td>0</td><td>Disabled</td><td>Disabled</td></tr> <tr><td><input type="checkbox"/> 1/0/4</td><td>128</td><td>0</td><td>Disabled</td><td>Disabled</td></tr> <tr><td><input type="checkbox"/> 1/0/5</td><td>128</td><td>0</td><td>Disabled</td><td>Disabled</td></tr> <tr><td><input type="checkbox"/> 1/0/6</td><td>128</td><td>0</td><td>Disabled</td><td>Disabled</td></tr> <tr><td><input type="checkbox"/> 1/0/7</td><td>128</td><td>0</td><td>Disabled</td><td>Disabled</td></tr> <tr><td><input type="checkbox"/> 1/0/8</td><td>128</td><td>0</td><td>Disabled</td><td>Disabled</td></tr> <tr><td><input type="checkbox"/> 1/0/9</td><td>128</td><td>0</td><td>Disabled</td><td>Disabled</td></tr> <tr><td><input type="checkbox"/> 1/0/10</td><td>128</td><td>0</td><td>Disabled</td><td>Disabled</td></tr> </tbody> </table>						Interface	Priority	Cost	Role	Status	<input type="checkbox"/> 1/0/1	128	0	Disabled	Disabled	<input type="checkbox"/> 1/0/2	128	0	Disabled	Disabled	<input type="checkbox"/> 1/0/3	128	0	Disabled	Disabled	<input type="checkbox"/> 1/0/4	128	0	Disabled	Disabled	<input type="checkbox"/> 1/0/5	128	0	Disabled	Disabled	<input type="checkbox"/> 1/0/6	128	0	Disabled	Disabled	<input type="checkbox"/> 1/0/7	128	0	Disabled	Disabled	<input type="checkbox"/> 1/0/8	128	0	Disabled	Disabled	<input type="checkbox"/> 1/0/9	128	0	Disabled	Disabled	<input type="checkbox"/> 1/0/10	128	0	Disabled	Disabled
Interface	Priority	Cost	Role	Status																																																										
<input type="checkbox"/> 1/0/1	128	0	Disabled	Disabled																																																										
<input type="checkbox"/> 1/0/2	128	0	Disabled	Disabled																																																										
<input type="checkbox"/> 1/0/3	128	0	Disabled	Disabled																																																										
<input type="checkbox"/> 1/0/4	128	0	Disabled	Disabled																																																										
<input type="checkbox"/> 1/0/5	128	0	Disabled	Disabled																																																										
<input type="checkbox"/> 1/0/6	128	0	Disabled	Disabled																																																										
<input type="checkbox"/> 1/0/7	128	0	Disabled	Disabled																																																										
<input type="checkbox"/> 1/0/8	128	0	Disabled	Disabled																																																										
<input type="checkbox"/> 1/0/9	128	0	Disabled	Disabled																																																										
<input type="checkbox"/> 1/0/10	128	0	Disabled	Disabled																																																										

8. Select a **VLAN ID** from the list of VLANs with enabled STP Admin mode and PVST or RPVST.

**Note:** The Other option is used for configuring a VLAN which is not yet created. Specify the required value for VLAN ID and click the **Apply** button to observe actual values.

9. Configure the **Priority** value used to allow the operator to select the relative importance of the port in the selection process for forwarding.

Set this value to a lower number to prefer a port for forwarding of frames. This priority configuration is used when the port is configured as a point-to-point link type. The allowed values are between 0 and 240. The priority values are listed in the following table. All other values are rounded off. The default value is 128.

**Note:** The value must be a multiple of 16.

**Table 94. PVST/RPVST Interface Configuration Priority Values**

0	16	32
48	64	80
96	112	128 (default)

**Table 94. (continued)PVST/RPVST Interface Configuration Priority Values**

144	160	176
192	208	224
240	—	—

- 10.** The Per VLAN **Cost** is the path cost from the port to the root bridge.

The values allowed are between 1 and 200,000,000. By default, cost is not configured. Use the value 0 to unconfigure the setting. If per VLAN cost is not configured, the path cost value is set based on Link Speed.

- 11.** Click the **Apply** button.

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

The following table describes the nonconfigurable data that the PVST/RPVST Interface Configuration screen displays.

**Table 95. PVST/RPVST Interface Configuration**

Field	Description
Interface	The list of physical interfaces and LAGs.
Role	Indicates the role of the interface. Possible values are as follows: Disabled, Root, Designated, Alternate, Backup, and Master.  <b>Note:</b> The blank field is displayed for the interface which is not included for the specified VLAN.
Status	Indicates the status of the interface. Possible values are as follows: Discarding, Learning, Forwarding, and Disabled.  <b>Note:</b> The blank field is displayed for the interface which is not included for the specified VLAN.

## View PVST Statistics

You can view and configure Per VLAN Spanning Tree Protocol (PVST)/Per VLAN Rapid Spanning Tree Protocol (RPVST) Statistics settings for the device.

➤ **To view the PVST/RPVST 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.

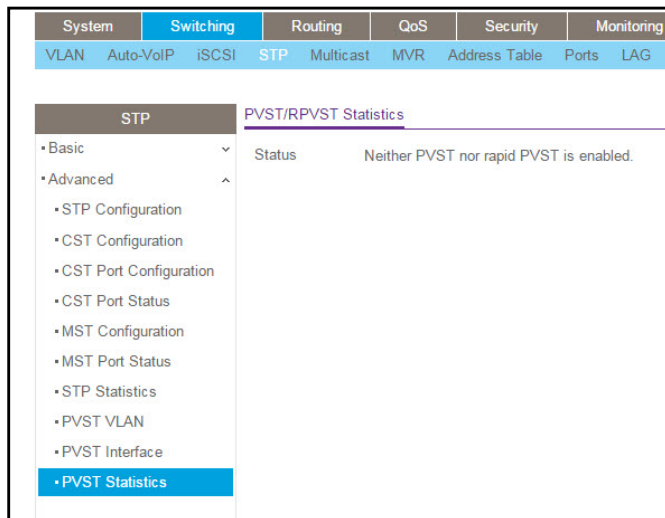
5. Enter the user name and password.

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 > STP > Advanced > PVST Statistics**.



To refresh the screen with the latest information on the switch, click the **Update** button.

The **Status** field displays Neither PVST nor Rapid-PVST is enabled.

To display statistic information, change STP mode to PVST or to RPVST.

## Multicast

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.

### 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**.

The screenshot shows the 'MFDB Table' page in a web browser. At the top, there's a search section with the text 'Search By MAC Address' and a text input field. To the right of the input field is a blue button labeled 'Go'. Below the search section is a table with six columns: 'MAC Address', 'VLAN ID', 'Component', 'Type', 'Description', and 'Forwarding Interfaces'. The table is currently empty.

8. Use **Search by MAC Address** to enter a MAC address.

Enter six two-digit hexadecimal numbers separated by colons, for example 00:01:23:43:45:67.

9. Click the **GO** button.

If the address exists, that entry is displayed. An exact match is required.

**Table 96. 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.

Table 96. MFDB Table

Field	Description
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 the MFDB Statistics

### ➤ To view the 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	
Max MFDB Table Entries	1024
Most MFDB Entries Since Last Reset	0
Current Entries	0

The following table describes the MFDB Statistics fields.

**Table 97. MFDB Statistics**

Field	Description
Max MFDB Table Entries	The maximum number of entries that the Multicast Forwarding Database table can hold.
Most MFDB Entries Since Last Reset	The largest number of entries that were present in the Multicast Forwarding Database table since last reset. This value is also known as the MFDB high-water mark.
Current Entries	The current number of entries in the Multicast Forwarding Database table.

## IGMP Snooping

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 is receptive to the packet. While nodes rarely incur any processing overhead to filter packets addressed to unrequested group addresses, they cannot 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 receive packets directed to the group address.

## Configure IGMP Snooping

You can configure the parameters for IGMP snooping, which is used to build forwarding lists for multicast traffic.

---

**Note:** You must log in as the admin user, which has read/write access privileges to change the data on this screen.

---

➤ **To configure IGMP 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 > IGMP Snooping > Configuration**.

IGMP Snooping Configuration	
Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Multicast Control Frame Count	0
Validate IGMP IP header	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Interfaces Enabled for IGMP Snooping	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Proxy Querier Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
VLAN IDs Enabled for IGMP Snooping	

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

This specifies the administrative mode for IGMP snooping for the switch. The default is Disable.

9. Use the **Validate IGMP IP header** option to **Enable** or **Disable** header validation for all IGMP versions.

If Validate IGMP IP Header is enabled, then IGMP IP header checks for Router Alert option, ToS and TTL. The default value is Enable.

10. Select the Proxy Querier Mode **Enable** or **Disable** radio button.

This enables or disables IGMP proxy querier on the system. If disabled, then the IGMP proxy query with source IP 0.0.0.0 is not sent in response to IGMP leave packet. the default value is Enable.

11. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table displays information about the global IGMP snooping status and statistics on the screen.

**Table 98. IGMP Snooping Configuration**

Field	Description
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.
Interfaces Enabled for IGMP Snooping	A list of all the interfaces currently enabled for IGMP snooping.
VLAN IDs Enabled For IGMP Snooping	Displays VLAN IDs enabled for IGMP snooping.

## Configure IGMP Snooping for Interfaces

### ➤ To configure IGMP snooping for interfaces:

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

<input type="checkbox"/>	Interface	Admin Mode	Group Membership Interval(secs)	Max Response Time(secs)	Present Expiration Time(secs)	Fast Leave Mode	Proxy Querier Mode
<input type="checkbox"/>	1/0/1	Disable	260	10	0	Disable	Enable
<input type="checkbox"/>	1/0/2	Disable	260	10	0	Disable	Enable
<input type="checkbox"/>	1/0/3	Disable	260	10	0	Disable	Enable
<input type="checkbox"/>	1/0/4	Disable	260	10	0	Disable	Enable
<input type="checkbox"/>	1/0/5	Disable	260	10	0	Disable	Enable
<input type="checkbox"/>	1/0/6	Disable	260	10	0	Disable	Enable

The screen lists all physical, VLAN, and LAG interfaces.

8. Use the **Interface** check boxes to select interfaces.
9. In the **Admin Mode** field, select **Disable** or **Enable**.

This specifies the interface mode for the selected interface for IGMP snooping for the switch. The default is Disable.

10. Use **Group Membership Interval** to specify the amount of time the switch waits 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. Use **Max Response Time** to 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 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. Use **Present Expiration Time** to 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, i.e. no expiration.

13. Use **Fast Leave Admin Mode** to select the fast leave mode for a particular interface.

The default is Disable.

14. Use **Proxy Querier Mode** to select the proxy querier mode for a particular interface.

If it is disabled, then IGMP proxy query with source IP 0.0.0.0 is not sent in response to IGMP leave packet. The default value is Enable.

15. Click the **Apply** button.

The settings are applied to the switch. Configuration changes take effect immediately.

## Configure IGMP Snooping for VLANs

### ➤ 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.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Switching > Multicast > IGMP Snooping > IGMP VLAN Configuration**.

	VLAN ID	Admin Mode	Fast Leave Mode	Group Membership Interval	Maximum Response Time	Multicast Router Expiry Time	Report Suppression Mode	Proxy Querier Mode
	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

8. To enable IGMP snooping on a VLAN, enter the VLAN ID and configure the IGMP snooping values:
  - Use **Admin Mode** to enable or disable IGMP snooping for the specified VLAN ID.
  - Use **Fast Leave Admin Mode** to enable or disable the IGMP snooping fast leave mode for the specified VLAN ID.
  - Use **Group Membership Interval** to 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.
  - Use **Maximum Response Time** to set the value for maximum response time of IGMP snooping for the specified VLAN ID. The valid range is 1 to Group Membership Interval - 1. Its value must be greater than group membership interval value.
  - Use **Multicast Router Expiry Time** to set the value for multicast router expiry time of IGMP snooping for the specified VLAN ID. The valid range is 0 to 3600 seconds.

- Use **Report Suppression Mode** to enable or disable IGMP snooping report suppression mode for the specified VLAN ID. IGMP snooping report suppression allows the suppression of the IGMP reports sent by the multicast hosts by building a Layer 3 membership table, thereby sending only the very needed reports to the IGMP Routers to receive the multicast traffic. As a result, the multicast report traffic being sent to the IGMP Routers is reduced.
  - **Enable** or **Disable** the **Proxy Querier Mode** for the specified VLAN ID. If proxy querier mode is disabled, then IGMP proxy query with source IP 0.0.0.0 is not sent in response to an IGMP leave packet. The default is Enable.
9. To disable IGMP snooping on a VLAN and remove it from the list:
    - a. Select the check box next to the VLAN ID
    - b. Click the **Delete** button.
  10. To modify IGMP snooping settings for a VLAN:
    - a. Select the check box next to the VLAN ID
    - b. Update the values
    - c. Click the **Apply** button.

The settings are sent to the switch.

## Configure 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 since the switch automatically detects the multicast router and forwards IGMP packets accordingly. It is needed only if you want to make sure that the multicast router always receives IGMP packets from the switch in a complex network.

### ➤ 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.  
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**.

Multicast Router Configuration		
1 LAGS All Go To Interface <input type="text"/> <input type="button" value="Go"/>		
<input type="checkbox"/>	Interface	Multicast Router
		<input type="text"/>
<input type="checkbox"/>	1/0/1	Disable
<input type="checkbox"/>	1/0/2	Disable
<input type="checkbox"/>	1/0/3	Disable
<input type="checkbox"/>	1/0/4	Disable
<input type="checkbox"/>	1/0/5	Disable

8. Use **Interface** to select the physical interface.
9. In the **Multicast Router** field, select **Enable** or **Disable**.
10. Click the **Apply** button.

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

## Configure a Multicast Router VLAN

You can configure the interface to only forward 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 since the switch automatically detects a multicast router and forwards the 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 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

Interface 1/0/1 ▾

Multicast Router VLAN Configuration

	VLAN ID	Multicast Router
<input type="checkbox"/>	<input type="text"/>	<span>▾</span>

8. Use **Interface** to select the interface.
9. Use **VLAN ID** to select the VLAN ID.
10. In the **Multicast Router** field, select **Enable** or **Disable**.
11. Click the **Apply** button.

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

## IGMP Snooping Querier Overview

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 on IGMP snooping queriers on the network and, separately, on VLANs.

## Configure IGMP Snooping Querier

You can configure the parameters for IGMP snooping querier. Only a user with read/write access privileges can change the data on this screen.

### ➤ To configure IGMP snooping querier 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 > Querier Configuration**.

**Querier Configuration**

Querier Admin Mode ☒ Disable ☐ Enable

Snooping Querier Address

IGMP Version  (1 to 2)

Query Interval(secs)  (1 to 1800)

Querier Expiry Interval(secs)  (60 to 300)

**VLAN IDs Enabled for IGMP Snooping Querier**

8. Use **Querier Admin Mode** to select the administrative mode for IGMP snooping for the switch.  
The default is Disable.
9. In the **Snooping Querier IP Address** field, type an IP address.  
This specifies 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.  
The range is 1 to 2. The default value is 2.
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.

13. Click the **Apply** button.

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

The screen displays the VLAN IDs enabled for IGMP snooping querier.

## Configure IGMP Snooping Querier for VLANs

You can configure IGMP queriers for use with VLANs on the network.

### ➤ To configure querier 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 > Multicast > IGMP Snooping > Querier VLAN Configuration**.

IGMP Snooping Querier VLAN Configuration								
<input type="checkbox"/>	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="text"/>	<input type="text"/>	<input type="text"/>					

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.** 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 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.

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

**Table 99. Querier VLAN Configuration**

Field	Description
Operational State	<p>The operational state of the IGMP snooping querier on a VLAN. It can be in any of the following states:</p> <ul style="list-style-type: none"> <li>• <b>Querier:</b> 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 finds a better querier in the VLAN, it moves to non-querier mode.</li> <li>• <b>Non-Querier:</b> The snooping switch is in non-querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch moves into querier mode.</li> <li>• <b>Disabled:</b> The 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	The operational IGMP protocol version of the querier.
Last Querier Address	The IP address of the last querier from which a query was snooped on the VLAN.
Last Querier Version	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. 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.

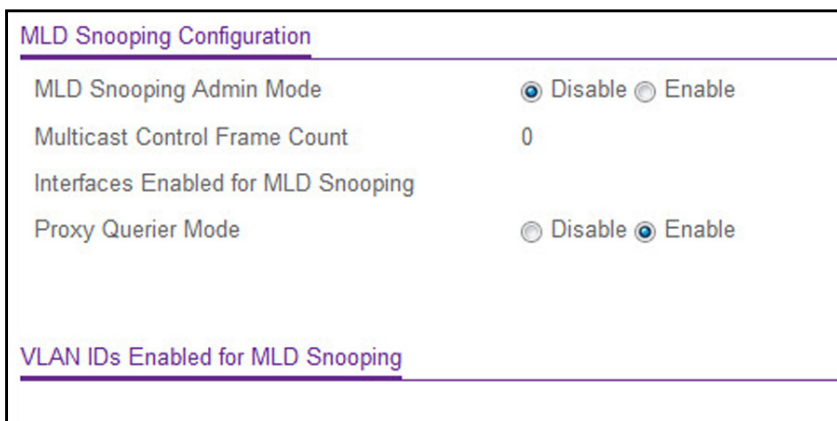
5. Enter the user name and password.

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**.



The screenshot shows the 'MLD Snooping Configuration' page. It has a title bar 'MLD Snooping Configuration' with a purple underline. Below the title bar, there are four configuration items: 'MLD Snooping Admin Mode' with radio buttons for 'Disable' (selected) and 'Enable'; 'Multicast Control Frame Count' with a text input field containing '0'; 'Interfaces Enabled for MLD Snooping' with a text input field; and 'Proxy Querier Mode' with radio buttons for 'Disable' and 'Enable' (selected). At the bottom, there is a section titled 'VLAN IDs Enabled for MLD Snooping' with a purple underline, followed by a table with two columns: 'VLAN ID' and 'Status'. The table is currently empty.

8. Use **MLD Snooping Admin Mode** to select the administrative mode for MLD snooping for the switch.

The default is Disable.

9. Select the Proxy Querier Mode **Enable** or **Disable** radio button.

This enables or disables an MLD proxy querier on the system. If it is disabled, then an MLD proxy query with source IP 0::0 is not sent in response to an MLD leave packet. If it is enabled, then MLD proxy queries are sent. The default value is Enable.

10. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable MLD Snooping Configuration fields.

**Table 100. MLD Snooping Configuration**

Field	Definition
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU.
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 a MLD Snooping Interface

### ➤ To configure a MLD 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 **Switching > Multicast > MLD Snooping > Interface Configuration**.

MLD Snooping Interface Configuration							
1 LAGS All				Go To Interface <input type="text"/>		<b>Go</b>	
<input type="checkbox"/>	Interface	Admin Mode	Group Membership Interval(secs)	Max Response Time(secs)	Present Expiration Time(secs)	Fast Leave Mode	Proxy Querier Mode
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	1/0/1	Disable	260	10	0	Disable	Enable
<input type="checkbox"/>	1/0/2	Disable	260	10	0	Disable	Enable
<input type="checkbox"/>	1/0/3	Disable	260	10	0	Disable	Enable
<input type="checkbox"/>	1/0/4	Disable	260	10	0	Disable	Enable
<input type="checkbox"/>	1/0/5	Disable	260	10	0	Disable	Enable

All physical, VLAN, and LAG interfaces are displayed.

8. Use the **Interface** check boxes to select the interface.
9. Use **Admin Mode** to select the interface mode for the selected interface for MLD snooping for the switch.

The default is Disable.

10. Use **Group Membership Interval(secs)** to specify the amount of time the switch waits 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. Use **Max Response Time (secs)** to 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 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. Use **Present Expiration Time** to 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, that is, no expiration.

13. Use **Fast Leave Admin Mode** to select the fast leave mode for a particular interface. The default is Disable.

14. Select the **Proxy Querier Mode** to **Enable** or **Disable** MLD proxy querier on the system.

If it is disabled, then an MLD proxy query with source IP 0::0 is not sent in response to an MLD leave packet. If it is enabled, then MLD proxy queries are sent. The default value is Enable.

## Configure MLD VLAN Settings

### ➤ To configure MLD 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 > Multicast > MLD Snooping > MLD VLAN Configuration**.

MLD VLAN Configuration						
<input type="checkbox"/>	VLAN ID	Fast Leave Mode	Group Membership Interval	Maximum Response Time	Multicast Router Expiry Time	Proxy Querier Mode
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

8. Use **VLAN ID** to set the VLAN IDs for which MLD snooping is enabled.
9. Use **Admin Mode** 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. Use **Group Membership Interval** to 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. Use **Maximum Response Time** to set the value for the maximum response time of MLD snooping for the specified VLAN ID.  
The valid range is 1 to (Group Membership Interval – 1). Its value must be less than group membership interval value.
13. Use **Multicast Router Expiry Time** to set the value for the multicast router expiry time of MLD snooping for the specified VLAN ID.  
The valid range is 0 to 3600.
14. Click the **Apply** button.

The updated configuration is sent to the switch.

## Enable or Disable a Multicast Router on an Interface

### ➤ To enable or disable a multicast router 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 **Switching > Multicast > MLD Snooping > Multicast Router Configuration**.

Multicast Router Configuration		
1 LAGS All Go To Interface <input type="text"/> <input type="button" value="Go"/>		
<input type="checkbox"/>	Interface	Multicast Router
<input type="checkbox"/>	1/0/1	Disable
<input type="checkbox"/>	1/0/2	Disable
<input type="checkbox"/>	1/0/3	Disable
<input type="checkbox"/>	1/0/4	Disable
<input type="checkbox"/>	1/0/5	Disable

8. **Interface:** Select the interface.

9. Use **Multicast Router** to enable or disable s multicast router on the selected interface.

10. Click the **Apply** button.

The updated configuration is sent to the switch.

## Configure Multicast Router VLAN Settings

### ➤ To configure multicast router 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 > Multicast > MLD Snooping > Multicast Router VLAN Configuration**.

Multicast Router VLAN Configuration	
Interface	1/0/1
Multicast Router VLAN Configuration	
VLAN ID	Multicast Router
<input type="text"/>	<input type="text"/>

8. Use **Interface** to select the interface.
9. Use **VLAN ID** to select the VLAN ID.
10. Use **Multicast Router** to enable or disable the multicast router for the VLAN ID.
11. Click the **Apply** button.

The updated configuration is sent to the switch.

## Configure MLD Snooping Querier

You can configure the parameters for an MLD snooping querier. Only a user with read/write access privileges can change the data on this screen.

### ➤ To configure an MLD 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 > MLD Snooping > Querier Configuration**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help
VLAN	Auto-VoIP	iSCSI	STP	Multicast	MVR	Address Table	Ports
<div> <div>Multicast</div> <div> <div>• MFDB</div> <div>• IGMP Snooping</div> <div>• MLD Snooping</div> <div>• Configuration</div> <div>• Interface Configuration</div> <div>• MLD VLAN Configuration</div> <div>• Multicast Router Configuration</div> <div>• Multicast Router VLAN Configuration</div> <div>• Querier Configuration</div> <div>• Querier VLAN Configuration</div> </div> </div> <div> <div>MLD Snooping Querier Configuration</div> <div> <div>Querier Admin Mode</div> <div> <input checked="" type="radio"/> Disable           <input type="radio"/> Enable         </div> <div>Querier Address</div> <div> <input type="text"/> <small>(x::x::x::x::x and x::x)</small> </div> <div>MLD Version</div> <div> <input type="text"/> <small>(1 to 1800)</small> </div> <div>Query Interval (secs)</div> <div> <input type="text"/> <small>(1 to 1800)</small> </div> <div>Querier Expiry Interval (secs)</div> <div> <input type="text"/> <small>(60 to 300)</small> </div> </div> <div> <div>VLAN Ids Enabled for MLD Snooping Querier</div> <div></div> </div> </div>							

8. Use **Querier Admin Mode** to select the administrative mode for MLD snooping for the switch.

The default is Disable.

9. Use **Querier Address** to 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. Use **MLD Version** to specify the MLD protocol version used in periodic MLD 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 to 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 to 300. The default value is 60.

The screen displays VLAN IDs enabled for the MLD snooping querier.

## Configure MLD Snooping Querier VLAN Settings

➤ **To configure MLD snooping querier 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 > Multicast > MLD Snooping > Querier VLAN Configuration**.

MLD Snooping Querier VLAN Configuration								
<input type="checkbox"/>	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="text"/>	<input type="text"/>	<input type="text"/>					

8. Use **VLAN ID** to select the VLAN ID on which the MLD snooping querier is administratively enabled and a VLAN exists in the VLAN database.
9. Use **Querier Election Participate Mode** to enable or disable the MLD snooping querier participation in election mode.

When this mode is disabled, on detecting another querier of same version in the VLAN, the snooping querier moves to a non-querier state. When this mode is enabled, the snooping querier participates in querier election where 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. Use **Querier VLAN Address** to 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 101. Querier VLAN Configuration**

Field	Description
Operational State	<p>The operational state of the MLD snooping querier on a VLAN. It can be in any of the following states:</p> <ul style="list-style-type: none"> <li>• <b>Querier:</b> 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>• <b>Non-Querier:</b> 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>• <b>Disabled:</b> 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	The operational MLD protocol version of the querier.
Last Querier Address	The IP address of the last querier from which a query was snooped on the VLAN.
Last Querier Version	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

You can configure basic, advanced, group, interface or group membership settings.

### Configure Basic MVR Settings

#### ➤ To configure basic MVR 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 > MVR > Basic > MVR Configuration**.

MVR Configuration	
MVR Running	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
MVR Multicast Vlan	<input type="text" value="1"/> (1 to 4093)
MVR Max Multicast Groups	<input type="text" value="256"/>
MVR Current Multicast Groups	<input type="text" value="0"/>
MVR Global query response time	<input type="text" value="5"/> (1 to 100)
MVR Mode	<input checked="" type="radio"/> compatible <input type="radio"/> dynamic

8. Use **MVR Running** to **Enable** or **Disable** the MVR feature.

The factory default is **Disable**.

9. Use **MVR Multicast VLAN** to 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.

10. Use **MVR Global Query Response Time** to 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.

11. Use **MVR Mode** to specify the MVR mode of operation.

Possible values are compatible or dynamic. The factory default is compatible.

12. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

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

**Table 102. MVR Configuration**

Field	Definition
MVR Max Multicast Groups	The maximum number of multicast groups that MVR supports.
MVR Current Multicast Groups	Displays current number of the MVR groups allocated.

## Configure Advanced MVR Settings

### ➤ To configure advanced MVR 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 > MVR > Advanced > MVR Configuration**.

MVR Configuration	
MVR Running	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
MVR Multicast Vlan	<input type="text" value="1"/> (1 to 4093)
MVR Max Multicast Groups	<input type="text" value="256"/>
MVR Current Multicast Groups	<input type="text" value="0"/>
MVR Global query response time	<input type="text" value="5"/> (1 to 100)
MVR Mode	<input checked="" type="radio"/> compatible <input type="radio"/> dynamic

8. Select the MVR Running **Enable** or **Disable** radio button.

The factory default is Disable.



9. Use the **MVR Multicast VLAN** to 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. Use the **MVR Global query response time** to 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. Select a **MVR Mode** radio button to specify the MVR mode of operation.

The factory default is compatible.

12. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

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

**Table 103. Advanced MVR Configuration**

Field	Definition
MVR Max Multicast Groups	The maximum number of multicast groups that MVR supports.
MVR Current Multicast Groups	Displays the current number of MVR groups allocated.

## Configure an MVR Group

### ➤ To configure an MVR 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 > MVR > Advanced > MVR Group Configuration**.

MVR Group IP	Status	Members	Count
<input type="text"/>	<input type="button" value="Add"/>	<input type="button" value="Delete"/>	<input type="button" value="Count"/>

8. Use the **MVR Group IP** to specify the IP address for the new MVR group.
9. Use the **Count** to specify the number of contiguous MVR groups.

This helps you to create multiple MVR groups through a 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. Click the **Add** button.

The MVR group is added.

11. To delete a selected MVR group, click the **Delete** button.

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

**Table 104. MVR Group Configuration**

Field	Definition
Status	The status of the specific MVR group.
Members	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					
1 All					
Go To Interface <input type="text"/> <input type="button" value="Go"/>					
<input type="checkbox"/>	Interface	Admin Mode	Type	Immediate Leave	Status
<input type="checkbox"/>	1/0/1	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	1/0/2	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	1/0/3	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	1/0/4	Disable	none	Disable	INACTIVE/InVLAN
<input type="checkbox"/>	1/0/5	Disable	none	Disable	INACTIVE/InVLAN

The status of each port displays.

8. Use **Interface** to select the interface.

9. Use **Admin Mode** to **Enable** or **Disable** MVR on a port.

The factory default is **Disable**.

10. Use **Type** to configure the port as an MVR **receiver** port or a **source** port.

The default port type is **none**.

11. Use **Immediate Leave** to **Enable** or **Disable** the **Immediate Leave** feature of the MVR on a port.

The factory default is **Disable**.

12. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

## 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. Use the **Group IP** to specify the IP multicast address of the MVR group.
9. Use the **Port List** to view 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**.

MVR Statistics	
IGMP Query Received	0
IGMP Report V1 Received	0
IGMP Report V2 Received	0
IGMP Leave Received	0
IGMP Query Transmitted	0
IGMP Report V1 Transmitted	0
IGMP Report V2 Transmitted	0
IGMP Leave Transmitted	0
IGMP Packet Receive Failures	0
IGMP Packet Transmit Failures	0

To refresh the screen with the latest information on the switch, click the **Update** button.

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

**Table 105. MVR Statistics**

Field	Definition
IGMP Query Received	The number of received IGMP queries.
IGMP Report V1 Received	The number of received IGMP reports V1.
IGMP Report V2 Received	The number of received IGMP reports V2.
IGMP Leave Received	The number of received IGMP leaves.
IGMP Query Transmitted	The number of transmitted IGMP queries.
IGMP Report V1 Transmitted	The number of transmitted IGMP reports V1.
IGMP Report V2 Transmitted	The number of transmitted IGMP reports V2.
IGMP Leave Transmitted	The number of transmitted IGMP leaves.
IGMP Packet Receive Failures	The number of IGMP packet receive failures.
IGMP Packet Transmit Failures	The number of IGMP packet transmit failures.

## MAC Address Table

You can view or configure 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.

### Configure the MAC Address Table

➤ **To configure 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 > Basic > Address Table**.

VLAN ID	MAC Address	Port	status
1	00:10:18:99:F5:55	1/0/4	Learned
1	20:0C:C8:4D:95:31	1/0/4	Learned
1	84:44:01:82:75:57	1/0/4	Learned
1	C4:04:15:AD:7F:18	0/5/1	Management
1	C4:04:15:AD:7F:19	1/0/4	Learned
1	C4:04:15:AD:7F:1B	vlan 1	Management
1	DC:7B:94:D6:2A:C6	1/0/4	Learned

8. Use **Search By** to search for MAC addresses by MAC address, VLAN ID, or port:
  - **Searched by MAC Address.** Select **MAC Address**, 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**, 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**, 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 106. Basic 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 and/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 upon 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>• Static. The value of the corresponding instance was added by the system or a user and cannot be relearned.</li> <li>• Learned. The value of the corresponding instance was learned, and is being used.</li> <li>• Management. The value of the corresponding instance is also the value of an existing instance of dot1dStaticAddress.</li> </ul>

## Set the Dynamic Address 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)	<input type="text" value="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 static 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**.



The screenshot shows a web interface for configuring a switch. At the top, there is a 'Port List' section with a dropdown menu for 'Interface' set to '1/0/1'. Below this is the 'Static MAC Address Table' section, which contains a table with two columns: 'Static MAC Address' and 'VLAN ID'. The 'Static MAC Address' column has an input field, and the 'VLAN ID' column has a dropdown menu.

Port List	
Interface	1/0/1

Static MAC Address Table	
<input type="checkbox"/>	Static MAC Address
<input type="text"/>	VLAN ID

8. Use **Interface** to select the physical interface/LAGs.
9. In the **Static MAC Address** field, type the MAC address.
10. Select the **VLAN ID** associated with the MAC address.
11. Click the **Add** button.

The static MAC address is added to the switch.

12. To delete a existing static MAC address from the switch, click the **Delete** button.

## Port Settings

You can view and monitor the physical port information for the ports available on the switch.

## 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**.

The screenshot shows the 'Port Configuration' page for '1 LAG All'. It features a table with columns for Port, Media Type, Port Type, STP mode, Admin Mode, LACP Mode, Auto-negotiation, Speed, Duplex Mode, Admin Status, Physical Status, Link Status, Link Trap, Frame Size, Debounce Time, Flow Control, and Index. The table lists five ports (1/0/1 to 1/0/5) with their respective configurations.

Port	Media Type	Port Type	STP mode	Admin Mode	LACP Mode	Auto-negotiation	Speed	Duplex Mode	Admin Status	Physical Status	Link Status	Link Trap	Frame Size	Debounce Time	Flow Control	Index
1/0/1		Normal	Enable	Enable	Enable	Enable	Auto	Auto	Normal	Unknown	Link Down	Enable	1518	0	Disable	1
1/0/2		Normal	Enable	Enable	Enable	Enable	Auto	Auto	Normal	Unknown	Link Down	Enable	1518	0	Disable	2
1/0/3		Normal	Enable	Enable	Enable	Enable	Auto	Auto	Normal	Unknown	Link Down	Enable	1518	0	Disable	3
1/0/4		Normal	Enable	Enable	Enable	Enable	Auto	Auto	Normal	Unknown	Link Down	Enable	1518	0	Disable	4
1/0/5		Normal	Enable	Enable	Enable	Enable	Auto	Auto	Normal	Unknown	Link Down	Enable	1518	0	Disable	5

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.

The default is Enable.

10. In the **Admin Mode** list, select **Enable** or **Disable**.

This sets the port control administrative mode. For the port to participate in the network, you must select **Enable**. The factory default is Enable.

11. From the **LACP Mode** list, select **Enable** or **Disable**.

This selects the Link Aggregation Control Protocol administrative mode. The mode must be enabled in order for the port to participate in link aggregation. The factory default is Enable.

12. From the **Auto-negotiation** list, select **Enable** or **Disable**.

This specifies the auto-negotiation mode for this port. The default is Enable.

**Note:** After you change the auto-negotiation mode, the switch might be inaccessible for a number of seconds while the new settings take effect.

13. From the **Speed** list, select the speed value for the selected port.

Possible field values are as follows:

- **Auto**. All supported speeds.
- **100**. 100 Mbits/second
- **10G**. 10 Gbits/second.

The delimiter characters for setting different speed values are a comma (,), a period (.) and a space ( ). For you to set the auto-negotiation speed, the auto-negotiation mode must be set to **Enable**. The default is **Auto**.

**Note:** After you change the speed value, the switch might be inaccessible for a number of seconds while the new settings take effect.

14. From the **Duplex Mode** list, select the duplex mode for the selected port.

Possible values are as follows:

- **Auto.** Indicates that speed is set by the auto-negotiation process.
- **Full.** Indicates that the interface supports transmission between the devices in both directions simultaneously.
- **Half.** Indicates that the interface supports transmission between the devices in only one direction at a time.

The default is **Auto**.

**Note:** After you change the duplex mode, the switch might be inaccessible for a number of seconds while the new settings take effect.

15. Use the **Link Trap object** to determine whether to send a trap when link status changes.

The factory default is enabled.

16. Use **Frame Size** to specify the maximum Ethernet frame size the interface supports or is configured to use , including Ethernet header, CRC, and payload.

The range is 1518 to 12288. The default maximum frame size is 1518.

17. Use **Debounce Time** to specify the timer value for port debouncing in a multiple of 100 milliseconds (msec) in the range to 100 to 5000.

The default debounce timer value is 0, which means that debounce is disabled.

18. From the **Flow Control** list, select to **Enable** or **Disable** IEEE 802.3 flow control.

The default is Disable. The switch does not send pause frames if the port buffers become full. 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 the 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. For LAG interfaces, flow control mode is displayed as *blank* because flow control is not applicable.

19. Click the **Apply** button.

The switch is updated with the values you entered. For the switch to retain the new values across a power cycle, you must save the configuration.

The following table describes the nonconfigurable data that is displayed.

**Table 107. Port Configuration**

Field	Description
Media Type	The media type.
Port Type	For normal ports this field is <b>Normal</b> . Otherwise the possible values are as follows: <ul style="list-style-type: none"> <li>• <b>Mirrored</b>. The port is a mirrored port on which all the traffic is copied to the probe port.</li> <li>• <b>Probe</b>. Use this port to monitor a mirrored port.</li> <li>• <b>Trunk Member</b>. The port is a member of a link aggregation trunk. Look at the LAG screens for more information.</li> </ul>
Admin Status	When the port's admin mode is D-Disable, this field indicates the reason. Possible reasons are as follows: <ul style="list-style-type: none"> <li>• <b>STP</b>. Spanning Tree Protocol violation.</li> <li>• <b>UDLD</b>. UDLD protocol violation.</li> <li>• <b>XCEIVER</b>. Unsupported SFP/SFP+ inserted.</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.

## Configure Port Descriptions

### ➤ To configure and display the description for all ports in the 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 **Switching > Ports > Port Description**.

Port	Description	MAC Address	PortList Bit Offset	ifindex
1/0/1		C4:04:15:AD:7F:1A	1	1
1/0/2		C4:04:15:AD:7F:1A	2	2

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 108. Port Description**

Field	Description
Port	Selects the interface for which data is to be displayed or configured.
MAC Address	The physical address of the specified interface.
PortList Bit Offset	The bit offset value that corresponds to the port when the MIB object type PortList is used to manage in SNMP.
ifIndex	The interface index associated with the port.

## View Port Transceiver Information

You can view the transceiver information for all fiber ports in the box.

### ➤ To view port transceiver 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 **Switching > Ports > Port Transceiver**.

Port Transceiver Information								
1 All								
Port	Vendor Name	Link Length 50µm	Link Length 62.5µm	Serial Number	Part Number	Nominal Bit Rate	Revision	Compliance
1/0/1								
1/0/2								
1/0/3								
1/0/4								
1/0/5								

8. Select **Unit ID** to display physical ports of the selected unit or select **All** to display physical ports of all units.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following describes the nonconfigurable data that is displayed.

**Table 109. Port Transceiver**

Field	Description
Port	The interface for which data is to be displayed.
Vendor Name	Vendor name of the SFP.
Link Length 50 µm	Link length supported for 50 µm fiber.
Link Length 62, 5 µm	Link length supported for 62, 5 µm fiber.
Serial Number	Serial number of the SFP.
Part Number	Part number of the SFP.
Nominal Bit Rate	Nominal signalling rate for SFP.
Revision	Vendor revision of the SFP.
Compliance	Compliance of the SFP.

## Link Aggregation Groups

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 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 Name	Description	LAG ID	Admin Mode	Hash Mode	STP Mode	Static Mode	Link Trap	Configured Ports	Active Ports	LAG State	Local Preference Mode
<input type="text"/>			<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>				
<input type="checkbox"/> <b>ch1</b>		lag 1	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Disable	Disable			DOWN	Disable
<input type="checkbox"/> <b>ch2</b>		lag 2	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Disable	Disable			DOWN	Disable
<input type="checkbox"/> <b>ch3</b>		lag 3	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Disable	Disable			DOWN	Disable
<input type="checkbox"/> <b>ch4</b>		lag 4	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Disable	Disable			DOWN	Disable
<input type="checkbox"/> <b>ch5</b>		lag 5	Enable	3 Src/Dest MAC, VLAN, EType, incoming port	Enable	Disable	Disable			DOWN	Disable

8. Use **LAG Name** to enter the name to be 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 **Admin Mode** to select enable or disable.

When the LAG is disabled, no traffic flows and LACPDUs are dropped, but the links that form the LAG are not released. The factory 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 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/Dest MAC, VLAN, EType, incoming port** is the default.
  - **Src IP** and **Src TCP/UDP Port** fields. Source IP and Source TCP/UDP fields of the packet.
  - **Dest IP** and **Dest TCP/UDP Port** fields. Destination IP and Destination TCP/UDP Port fields of the packet.
  - **Src/Dest IP** and **TCP/UDP Port Fields.** 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. Enable is the default.
- 12. Use **Static Mode** to select **Enable** or **Disable**.**
- When the LAG is enabled, it does not transmit or process received LACPDUs that is, the member ports do not transmit LACPDUs and all the LACPDUs it can receive are dropped. The factory default is Disable.
- 13. Use **Link Trap** to specify whether to send a trap when the link status changes.**
- The factory default is Enable, which causes the trap to be sent.
- 14. Use **Local Preference Mode** to **Enable** or **Disable** the LAG interface's local preference mode.**
- The default is Disable.
- 15. Click the **Delete** button to remove the currently selected configured LAG.**
- All ports that were members of this LAG are removed from the LAG and included in the default VLAN.
- 16. Click the **Apply** button.**



The switch is updated with the values you entered. Configuration changes take effect immediately.

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

**Table 110. 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.
LAG State	Indicates whether the link is up or down.
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.

## 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**.

8. Use **LAG ID** to select the identification of the LAG.
9. Use **LAG Name** to enter the name to be 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. Use **Admin Mode** to select **Enable** or **Disable**.  
When the LAG is disabled, no traffic flows and LACPDUs are dropped, but the links that form the LAG are not released. The factory default is Enable.
12. Use **Link Trap** to specify whether to send a trap when the 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. Enable is the default.
14. Use **Static Mode** to select enable or disable.  
When the LAG is enabled, it does not transmit or process received LACPDUs that is, 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. This option is the default.
- **Src IP and Src TCP/UDP Port** fields. Source IP and Source TCP/UDP fields of the packet.
- **Dest IP and Dest TCP/UDP Port** fields. Destination IP and Destination TCP/UDP Port fields of the packet.
- **Src/Dest IP and TCP/UDP Port** fields. 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.

## Configure the Virtual Port-Channel Global Settings

---

**Note:** Only switch series M6100 and M7100 support this feature.

---

You can view and manage global virtual port-channel (VPC) settings on the device. VPCs are also known as multichassis or multiswitch link aggregation groups (MLAGs). Like port-channels (also known as link aggregation groups or LAGs), VPCs allow one or more Ethernet links to be aggregated together to increase speed and provide redundancy. With port-channels, the aggregated links must be on the same physical device, but VPCs do not share that requirement. The VPC feature allows links on two different switches to pair with links on a partner device. The partner device is unaware that it is pairing with two different devices to form a port channel.

---

**Note:** Virtual port-channel configuration is supported by the M6100 and M7100 platforms.

---

### ➤ To configure the virtual port-channel 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 **Switching > MLAG > Basic > VPC Global Configuration**.

**Note:** You can navigate to the same screen by selecting **Switching > MLAG > Advanced > VPC Global Configuration**.

The screenshot shows the web management interface with the following structure:

- Top Navigation Bar:** System, Switching (selected), Routing, QoS, Security, Monitoring, Maintenance.
- Sub-Navigation Bar:** VLAN, Auto-VoIP, iSCSI, STP, Multicast, MVR, Address Table, Ports, LAG, MLAG (selected), MRP.
- Left Sidebar:**
  - MLAG
    - Basic (expanded)
      - VPC Global Configuration (selected)
    - Advanced
- Main Content Area:** VPC Global Configuration
  - VPC Mode: ☒ Disable ☐ Enable
  - Domain ID:  (1 to 255)
  - Remove Domain ID: ☐
  - Operational VPC Mode: Disabled
  - VPC State: Disabled
  - VPC MAC Mode: ☒ Auto ☐ Manual
  - VPC MAC:  (xx:xx:xx:xx:xx:xx)
  - Operational VPC MAC:
  - VPC System Priority:  (1 to 65535)
  - Operational VPC System Priority:
  - Self Role: None
  - Local System MAC: 20:0C:C8:4D:95:D8

8. In the **VPC Mode** field, select **Enable** or **Disable** to globally enable or disable the VPC feature.

By default, the VPC feature is disabled.

9. In the **Domain ID** field, enter the ID of the VPC domain.

Possible values are 1 to 255. The VPC domain ID must be equal to the domain ID of the peer for a VPC pair to be formed. The domain IDs are exchanged during role election and, if they are different, VPC does not become operational.

10. If you select the **Remove Domain ID** option, the current VPC domain ID is deleted.

11. Select **Auto** or **Manual** in the **VPC MAC Mode** field to indicate the administrative mode of VPC on the system.

The default is Auto.

12. Use the **VPC MAC** field to configure the MAC address of the VPC domain.

The VPC MAC must be the same on both the MLAG peer devices. The MAC address must be a unicast MAC address in the format XX:XX:XX:XX:XX:XX and must not be equal to the physical MAC address of either the primary or secondary VPC system device. A VPC MAC is auto-generated using the VPC domain ID or it can be configured manually. The configured VPC domain MAC address is exchanged during role election and, if configured differently on the peer device, then VPC does not become operational. The configured domain MAC address is present in the LACP PDUs and STP BPDUs that are sent on VPC member ports if VPC primary device election takes place after the VPC MAC address is configured. When the VPC MAC address is configured after the VPC primary device is elected, the already agreed upon operational VPC MAC address is used in the LACP PDUs and STP BPDUs, instead of the configured VPC MAC address. By default, the domain uses a preconfigured MAC address. The VPC MAC address range is C0:FF:D4:A7:DA:00 to C0:FF:D4:A7:DA:FF.

13. Configure the **VPC System Priority** for the VPC domain.

The system priority must be the same on both peer devices for VPC to become operational. If the configured VPC system priority is different on VPC peers, then VPC does not come up. The system priority is present in the LACP PDUs that are sent out on VPC member ports if the VPC primary device election takes place after the VPC system priority is configured. When VPC system priority is configured after the VPC primary device is elected, the already agreed upon operational VPC system priority is used in the LACP PDUs, instead of the configured VPC system priority. By default, the VPC system priority is 32767. The possible range is 1–65535.

The following table describes the nonconfigurable VPC Global Configuration fields.

**Table 111. VPC Channel Global Configuration**

Field	Description
Operational VPC MAC	The VPC MAC address agreed upon by both peers during role election. This field is present in the keep-alive message only if the transmitting peer is either primary or secondary.
VPC State	The global MLAG state, which is one of the following: <ul style="list-style-type: none"> <li>• <b>Disable.</b> The VPC mode is not operational.</li> <li>• <b>Listen.</b> The keep-alive component does not advertise any packets. It listens for advertisements from a peer.</li> <li>• <b>Ready.</b> The keep-alive component starts sending periodic keep-alive messages.</li> <li>• <b>Primary.</b> Traffic over VPC interfaces is allowed to be forwarded in this state. The keep-alive component continues to advertise keep-alive messages with the state as primary and monitors the health of the secondary device.</li> <li>• <b>Secondary.</b> Traffic over VPC interfaces is allowed to be forwarded in this state. The keep-alive component continues to advertise keep-alive messages with the state as secondary and monitors the health of the primary device.</li> </ul>
Operational VPC MAC	The VPC MAC address agreed upon by both peers during role election. This field is present in the keep-alive message only if the transmitting peer is either primary or secondary.
Operational VPC System Priority	The VPC system priority agreed upon by both peers during role election. This field is present in the keep-alive message only if the transmitting peer is either primary or secondary.
Self Role	The role of the local device in the VPC domain, which is either <b>Primary</b> , <b>Secondary</b> , or <b>None</b> . The default is None. The role is determined by an election between the two devices after a keep-alive link is established. The primary device owns the VPC member ports on the secondary device and handles the control plane functionality of supported protocols for the VPC member ports on the secondary device.
Local System MAC	The MAC address of the local system.

## Configure the Keep-Alive Parameters

The VPC feature sends periodic keep-alive messages over the peer link between the primary and secondary devices in the VPC domain to determine the device roles (primary and secondary) and to monitor the health of the link.

### ➤ To configure the keep-alive parameters:

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

2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > MLAG > Basic > VPC Global Configuration > Keepalive Parameters**.

Keepalive Parameters		
Keepalive Priority	<input type="text" value="100"/>	(1 to 255) secs
Keepalive Timeout	<input type="text" value="5"/>	(2 to 15) secs
Keepalive Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
Keepalive Operational Mode	Disabled	

8. Enter the **Keepalive Priority**.  
Use this field to configure the priority value that is used on a switch for primary and secondary role selection. The primary switch is responsible for maintaining and propagating the spanning tree and link aggregation states to the secondary switch. The range is 1 to 255 seconds. The default is 100. The device with a lower priority value becomes the primary device in the VPC role election.
9. Enter the **Keepalive Timeout**.  
Use this field to configure the number of seconds that must pass without receiving a keep-alive message before the peer device is considered to be down. If an MLAG switch does not receive keep-alive messages from the peer for this time-out value, it then transitions its role (if required). The range is 2 to 15 seconds. The default is 5 seconds.
10. Use the **Keepalive Admin Mode** field to **Enable** or **Disable** the administrative mode of the keep-alive component on the device.  
If a VPC switch does not receive keep-alive messages from the peer within the time-out value, it begins the process of transitioning its role to primary (if standby). By default, the keep-alive admin mode is disabled.
11. Click the **Apply** button.  
The switch is updated with the values you entered. Configuration changes take effect immediately.

## View the VPC Peer Link Settings

### ➤ To configure the peer 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 > VPC Global Configuration
8. Select **Switching > MLAG > Basic > VPC Global Configuration**.

MLAG	Peer
• Basic ^	Domain ID Not configured
• VPC Global Configuration	VPC MAC 00:00:00:00:00:00
• Advanced v	Operational VPC MAC 00:00:00:00:00:00
	VPC System Priority 0
	Operational VPC System Priority 0
	Peer Role None
	Local System MAC 00:00:00:00:00:00

**Note:** You can also navigate to this screen by selecting **Switching > MLAG > Advanced > VPC Global Configuration**.

The following table describes the nonconfigurable VPC peer settings.

**Table 112. VPC Peer Settings**

Field	Description
Domain ID	The ID of the peer VPC domain.
VPC MAC	The MAC address of the peer VPC domain.



Table 112. VPC Peer Settings

Field	Description
Operational VPC MAC	The VPC MAC address agreed upon by both peers during the role election.
VPC System Priority	The system priority of the peer VPC domain.
Operational VPC System Priority	The VPC system priority agreed upon by both peers during role election.
Peer Role	The role of the peer device in the VPC domain, which is Primary, Secondary, or None.
Local System MAC	The MAC address of the peer system.

## Configure the Peer Link Settings

The peer link is a port-channel that serves as the link between the two devices in the VPC domain. Using a multimember port-channel as the peer link helps protect it from link-level failures. The peer link is used to do the following:

- Carry the keep-alive messages between the two peer devices.
- Carry the BPDUs and LACPDUs between the secondary and primary VPC devices.
- Carry control messages like VPC member port-related events, FDB/MFDB entries, and configuration details.
- Carry data traffic over the peer's VPC member ports when the member ports of the VPC interface on the local device are all down.

### ➤ To configure the peer link 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 >

8. Select **Switching > MLAG > Basic > VPC Global Configuration**.

The VPC Global Configuration screen displays.

9. Scroll down to the Peer Link section.

Peer Link	
Enable Modification	<input type="checkbox"/>
Port Channel	None ▾
Peer Link Status	Down
Peer Keepalive Priority	0
Peer Link STP Mode	

10. Select the **Enable Modification** option to enable port-channel modification.
11. Use the **Port Channel** list to configure a LAG interface as the VPC peer link and enable/disable the peer link protocol.

The peer link protocol is disabled by default. Select **None** to remove the lag from a port channel. The port channel cannot be changed or reset when the operational VPC mode is Enabled.

12. Click the **Apply** button.

The switch is updated with the values you entered. Configuration changes take effect immediately.

The following table describes the nonconfigurable Peer Link fields.

**Table 113. Peer Link**

Field	Description
Peer Link Status	The operational status of the peer link, which is either Up or Down.
Peer Keepalive Priority	The peer keep-alive priority.
Peer Link STP Mode	The Spanning Tree Protocol (STP) administrative mode of the port channel. When enabled, the port channel participates in the STP operation to help prevent network loops.

## Configure the Peer Detection Settings

The peer detection feature uses the Dual Control Plane Detection Protocol (DCPDP), a UDP-based protocol, to detect peer links. You must configure peer detection on an IP interface with a VLAN that is not shared by any of the VPC interfaces.

➤ **To configure the peer detection 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 > MLAG > Basic > VPC Global Configuration**.

The VPC Global Configuration screen displays.

8. Scroll down to the Peer Detection section.

MLAG	
• Basic	Peer Detection
• VPC Global Configuration	Peer Detection Mode <input type="radio"/> Disable <input type="radio"/> Enable
• Advanced	Peer Detection Status
	Peer IP Address <input type="text"/> (X.X.X.X)
	Source IP Address <input type="text"/> (X.X.X.X)
	UDP Port <input type="text"/> (1 to 65535)
	Tx Interval <input type="text"/> (200 to 4000)
	Operational Tx Interval
	Rx Timeout <input type="text"/> (700 to 14000)
	Operational Rx Timeout

9. Select the **Peer Detection Mode** option to **Enable** or **Disable** the Dual Control Plane Detection Protocol (DCPDP).

The mode is disabled by default. This configuration is used to enable the detection of peer VPC switches (and suppress state transitions out of the secondary state) in the presence of peer link failure.

10. In the **Peer IP Address** field, enter the IP address of the peer VPC device.

This is the destination IP address in the DCPDP messages. The default value is 0.0.0.0.

11. Enter the local **Source IP Address** to be used by DCPDP.

The default value is 0.0.0.0.

12. Enter the local **UDP Port** number that is used to listen for peer DCPDP packets.

The range is 1 to 65535 seconds. The default is 50000.

13. Configure the **Tx Interval** in milliseconds between the DCPDP messages transmitted.

The range is 200 to 4000 milliseconds.

14. Configure the **Rx Timeout**, which is the DCPDP reception time-out in milliseconds.

The range is 700 to 14000 milliseconds.

15. Click the **Apply** button.

The switch is updated with the values you entered. Configuration changes take effect immediately.

The following table describes the nonconfigurable Peer Detection field.

**Table 114. Peer Detection**

Field	Description
Peer Detection Status	Displays whether peer detection is enabled or disabled.
Operational Tx Interval	The operational transmit interval in milliseconds.
Operational Rx Timeout	The operational time-out value in milliseconds.

## Configure the Virtual Port Channel Interface

You can configure the VPC interfaces on the device. You create a VPC interface by combining a port channel on the local device with a port channel on the peer device. The VPC interface on the local and peer devices share a common VPC identifier. You can configure multiple instances of VPC interfaces on each peer device in the VPC domain.

### ➤ Configure the VPC 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 > MLAG > Advanced > VPC Interface Configuration**.

VPC Interface Configuration		
LAG Interface	State	VPC Identifier
<input type="text" value="▼"/>		<input type="text"/>

8. From the **LAG Interface** list, select the ID of the local port channel to configure as a VPC interface.
9. Enter a VPC interface identifier value in the **VPC Identifier** field.

The possible range is 1 to 63. To form a VPC interface with a port channel on the peer device, the port channel on the peer device must use the same VPC identifier.

10. Click the **Add** button.

The interface configuration is added.

11. To delete the selected interface configuration, click the **Delete** button.

12. Click the **Apply** button.

The switch is updated with the values you entered. Configuration changes take effect immediately.

The following table describes the nonconfigurable VPC Interface Configuration fields.

**Table 115. VPC Interface Configuration**

Field	Description
State	<p>The VPC interface's operational mode, which is one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Disabled.</b> VPC functionality is operationally disabled on the VPC interface.</li> <li>• <b>Wait.</b> The port channel is waiting for VPC functionality to be enabled on a port channel on the peer device.</li> <li>• <b>Error.</b> VPC functionality is enabled on a port channel on both peer devices, but not all entry criteria are met for the port channel to be operational. For example, if the combined number of member ports for the VPC interface is more than the maximum allowed, then the state is set to Error on both devices.</li> <li>• <b>Active.</b> VPC functionality is enabled on a port channel on both peer devices, and all entry criteria are satisfied. The VPC interface is operationally enabled, and traffic is allowed to flow through the VPC member ports.</li> <li>• <b>Inactive.</b> The links connected to the VPC member ports are down, but the VPC interface on the peer remains active.</li> </ul>

## View Virtual Port Channel Interface Details

➤ **To view the virtual port channel interface details:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > MLAG > Advanced > VPC Interface Details**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance				
VLAN	Auto-VoIP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAG	MRP

MLAG	VPC Interface Details	
• Basic	LAG Interface	lag 1
• Advanced	Status	Disabled
• VPC Global Configuration	State	Wait
• VPC Interface Configuration	VPC Identifier	1
	Configured VLANs	1
• VPC Interface Details	Egress Tagging	None
• VPC Keepalive Statistics	Peer Link STP Mode	Enable
• VPC Peer Link Statistics		

8. From the list of **LAG Interfaces**, select the ID of the local port channel that is configured as a VPC interface.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable VPC details that are displayed.

**Table 116. VPC Interface Details**

Field	Description
Status	The status of the VPC identifier.
State	<p>The VPC interface's operational mode, which is one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Disabled.</b> VPC functionality is operationally disabled on the VPC interface.</li> <li>• <b>Wait.</b> The port channel is waiting for VPC functionality to be enabled on a port channel on the peer device.</li> <li>• <b>Error.</b> VPC functionality is enabled on a port channel on both peer devices, but not all entry criteria are met for the port channel to be operational. For example, if the combined number of member ports for the VPC interface is more than the maximum allowed, then the state is set to Error on both devices.</li> <li>• <b>Active.</b> VPC functionality is enabled on a port channel on both peer devices, and all entry criteria are satisfied. The VPC interface is operationally enabled, and traffic is allowed to flow through the VPC member ports.</li> <li>• <b>Inactive.</b> The links connected to the VPC member ports are down, but the VPC interface on the peer remains active.</li> </ul>
VPC Identifier	The VPC interface identifier value. The range is 1 to 63.
Configured VLANs	<p>The VLAN ID or list of VLAN IDs in which the LAG is a member.</p> <p><b>Note:</b> If the VLAN Member or the VLAN Tag field exceeds the maximum number of displayable VLANs, an <i>Exceeded data limit to display</i> message is shown. Editing the values of these fields is prevented when at least one port reaches the maximum limit of VLANs during port multiselection.</p>
Egress Tagging	The VLAN ID or list of VLAN IDs on which the LAG is tagged.
Peer Link STP Mode	The Spanning Tree Protocol administrative mode associated with the LAG.

## View Virtual Port Channel Interface Details

### ➤ To configure virtual port channel interface details:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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. To view self members, select an ID in the **Self Port** field, which lists the ID of each port that is a member of the port channel configured as a VPC interface on the current switch.

Self Members	
Self Port	Status

The operational status of the self port is displayed in the **Status** field. The Self Member fields on the VPC Interface Details screen, provide information about the VPC member ports on the local device

To refresh the screen with the latest information on the switch, click the **Update** button.

8. To view peer members, select an ID in the **Peer Port** list.

This list includes the ID of each port that is a member of the port channel configured as a VPC interface.

Peer Members	
Peer Port	Status

The operational status of the peer port is displayed in the **Status** field. The Peer Member fields, on the VPC Interface Details screen, provide information about the VPC member ports on the peer device

To refresh the screen with the latest information on the switch, click the **Update** button.

## View Virtual Port Channel Keep-Alive Statistics

The VPC feature sends periodic keep-alive messages over the peer link between the primary and secondary devices in the VPC domain to determine the device roles (primary and secondary) and to monitor the health of the link.

### ➤ To view the virtual port channel keep-alive 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 > MLAG > Advanced > VPC Keepalive Statistics**.

Keepalive Statistics	
Total transmitted	0
Tx successful	0
Tx errors	0
Total received	0
Rx successful	0
Rx errors	0
Timeout counter	0

To clear all the counters and reset all switch summary statistics to the default values, click the **Clear** button.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable VPC Keepalive Statistics that are displayed.

**Table 117. VPC Keepalive Statistics**

Field	Description
Total Transmitted	The total number of keep-alive messages that the local device sent to the peer device.
Tx Successful	The number of keep-alive messages transmitted from the local device.

Table 117. VPC Keepalive Statistics (continued)

Field	Description
Tx Errors	The number of keep-alive messages that the local device attempted to send to the peer device that were not transmitted due to an error.
Total Received	The total number of keep-alive messages that the local device received from the peer device.
Rx Successful	The number of successful keep-alive messages that the local device received from the peer device.
Rx Errors	The number of keep-alive messages that the local device received from the peer device that contained errors.
Timeout Counter	The number of times the keep-alive time-out timer expired.

## View Virtual Port Channel Peer Link Statistics

In addition to keep-alive messages, the peer link is used to send and receive control messages, data messages, BPDUs, and LACPDUs between the peer devices.

### ➤ To view the virtual port channel peer link 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 > MLAG > Advanced > VPC Peer Link Statistics**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance				
VLAN	Auto-VoIP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAG	MRP
MLAG		Peer Link Statistics								
• Basic	▼	Peer Link Control Messages Transmitted						0		
• Advanced	▲	Peer Link Control Messages Tx Errors						0		
• VPC Global Configuration		Peer Link Control Messages Tx Timeout						0		
• VPC Interface Configuration		Peer Link Control Messages ACK Transmitted						0		
• VPC Interface Details		Peer Link Control Messages ACK Tx Errors						0		
• VPC Keepalive Statistics		Peer Link Control Messages Received						0		
• VPC Peer Link Statistics		Peer Link Data Messages Transmitted						0		
		Peer Link Data Messages Tx Errors						0		
		Peer Link Data Messages Tx Timeout						0		
		Peer Link Data Messages Received						0		
		Peer Link BPDU's Transmitted To Peer						0		
		Peer Link BPDU's Tx Errors						0		
		Peer Link BPDU's Received From Peer						0		
		Peer Link BPDU's Rx Errors						0		
		Peer Link LACPDU's Transmitted To Peer						0		
		Peer Link LACPDU's Tx Errors						0		
		Peer Link LACPDU's Received From Peer						0		
		Peer Link LACPDU's Rx Errors						0		

To refresh the screen with the latest information on the switch, click the **Update** button.

To clear all the counters and reset all switch summary statistics to the default values, click the **Clear** button.

The following table describes the nonconfigurable VPC peer link statistics that are displayed.

**Table 118. VPC Peer Link Statistics**

Field	Description
Peer Link Control Messages Transmitted	The total number of control messages successfully sent from the local device to the peer device over the peer link.
Peer Link Control Messages Tx Errors	The total number of errors encountered when sending peer link control messages from the local device to the peer device over the peer link.
Peer Link Control Messages Tx Timeout	The total number of peer link control messages that did not receive an ACK from the peer device.
Peer Link Control Messages ACK Transmitted	The total number of ACKs sent to the peer device in response to peer link control messages that were received.
Peer Link Control Messages ACK Tx Errors	The total number of errors encountered when sending ACKs in response to peer link control messages.
Peer Link Control Messages Received	The total number of control messages successfully received by the local device from the peer device over the peer link.
Peer Link Data Messages Transmitted	The total number of data messages successfully sent from the local device to the peer device over the peer link.

**Table 118. VPC Peer Link Statistics (continued)**

Field	Description
Peer Link Data Messages Tx Errors	The total number of error encountered when sending peer link data messages from the local device to the peer device over the peer link.
Peer Link Data Messages Tx Timeout	The total number of peer link data messages that did not receive an ACK from the peer device.
Peer Link Data Messages Received	The total number of data messages successfully received by the local device from the peer device over the peer link.
Peer Link BPDU's Transmitted To Peer	The total number of BPDUs successfully sent to the peer device over the peer link.
Peer Link BPDU's Tx Errors	The total number of errors encountered when sending BPDUs to the peer device.
Peer Link BPDU's Received From Peer	The total number of BPDUs successfully received from the peer device over the peer link.
Peer Link BPDU's Rx Errors	The total number of errors encountered when receiving BPDUs from the peer device.
Peer Link LACPDU's Transmitted To Peer	The total number of LACPDU's successfully sent to the peer device over the peer link.
Peer Link LACPDU's Tx Errors	The total number of errors encountered when sending LACPDU's to the peer device.
Peer Link LACPDU's Received From Peer	The total number of LACPDU's successfully received from the peer device over the peer link.
Peer Link LACPDU's Rx Errors	The total number of errors encountered when receiving LACPDU's from the peer device.

## Multiple Registration Protocol Overview

---

**Note:** Only M6100 series switches support this feature.

---

Like 802.1AS, Multiple Registration Protocol (MRP) is an audio video bridging (AVB) feature that is available on some FASTPATH platforms. MVR is a base registration protocol that enables devices running an MRP application to register attributes to other devices in a network. MRP provides an application to register attributes such as bandwidth for a given AV stream and MAC address information. It is used by various applications to propagate the registration. Blade switches support the following MRP applications:

- Multiple MAC Registration Protocol (MMRP)
- Multiple Stream Reservation Protocol (MSRP)
- Multiple VLAN Registration Protocol (MVRP)

**MMRP** allows for the propagation MAC address information in the network, and allows for the registration and deregistration of both individual MAC address information and group MAC address membership. End stations can request to join or leave a multicast group, or to register an individual MAC address with a specific VLAN. MAC address entries can be dynamically registered and deregistered if MMRP is administratively enabled on the switch.

**MSRP** reserves necessary resources in the network to facilitate time-sensitive traffic to flow end to end. In a typical network, there are multiple talkers (those who transmit streams) and multiple Listeners (those who receive streams from one or many talkers). Each flow requires specific bandwidth, frame rate, and time sync values. With the use of MSRP these resources are guaranteed through all intermediate devices that are between any talker and listener.

**MVRP** registers VLANs in the network, enabling automatic VLAN configuration on the switch. In a typical network, VLAN tagging is common. Many nodes require ingress traffic to be tagged with a specific VLAN ID, and other nodes require egress traffic to be transmitted with a specific VLAN ID. With the use of MVRP on both ingress and egress, no manual VLAN configuration is required to pass tagged traffic through the network.

---

**Note:** MRP framework must be available and enabled in all intermediate devices to ensure that the propagation of the attributes occurs throughout the network.

---

With MRP, network attributes are declared, registered, withdrawn, and removed completely dynamically without any user intervention. This dynamic nature is especially useful in networks where the following is true:

- Network attributes are likely to change frequently, requiring reconfiguration of the intermediate devices.
- Recipients of these attributes frequently increase or decrease in number.
- Each of these changes without a dynamic self-adjusting framework would require constant attention from the network administrator.

## Configure Global MRP Settings

You can configure global MRP settings for the switch.

### ➤ To configure global MRP 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.

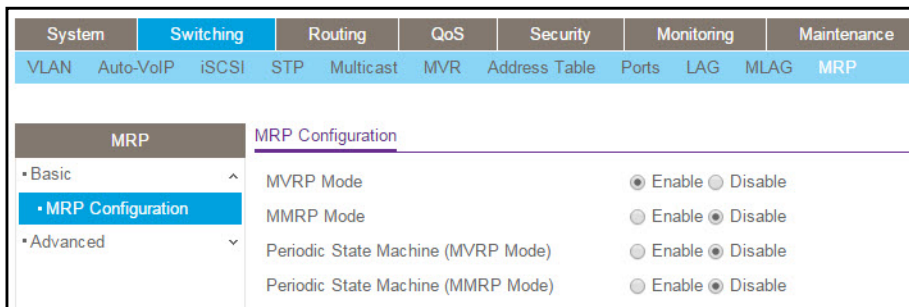
5. Enter the user name and password.

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 > MRP > Basic > MRP Configuration**.



**Note:** The fields available on the MRP Configuration screen vary based on the platform and its supported features.

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

This specifies the global administrative mode of MVRP on the device. The default is Disable.

Multiple VLAN Registration Protocol (MVRP) registers VLANs in the network, enabling automatic VLAN configuration on the device. In a typical network, VLAN tagging is common. Many nodes require ingress traffic to be tagged with a specific VLAN ID, and other nodes require egress traffic to be transmitted with a specific VLAN ID. With the use of MVRP on both ingress and egress, no manual VLAN configuration is required to pass tagged traffic through the network.

9. Select the MMRP **Enable** or **Disable** radio button.

This specifies the global administrative mode of MMRP on the device. The default is Disable.

Multiple MAC Registration Protocol (MMRP) allows the propagation of MAC address information in the network, and allows for the registration and deregistration of both individual MAC address information and group MAC address membership. End stations can request to join or leave a multicast group, or to register an individual MAC address with a specific VLAN. MAC address entries can be dynamically registered and deregistered if MMRP is administratively enabled on the device.

10. Select the Periodic State Machine (MVRP) **Enable** or **Disable** radio button.

When enabled, the state machine can help limit the effect of topology changes and reduce the number of protocol data units (PDUs) transmitted between devices. The default is Disable.

11. Select the Periodic State Machine (MMRP) **Enable** or **Disable** radio button.

When enabled, the state machine can help limit the effect of topology changes and reduce the number of protocol data units (PDUs) transmitted between devices. The default is Disable.

12. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

## Configure MRP Port Settings

You can configure the per-port MRP mode and timer settings. The timers control when and how often various messages are transmitted on each interface.

### ➤ To configure MRP 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 > MRP > Advanced > Port Settings**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index		
VLAN	Auto-VoIP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAG	MRP

MRP	MRP Port Settings
• Basic	1 2 3 LAG All
• Advanced	Go To Interface <input type="text"/> <input type="button" value="Go"/>
• MRP Configuration	
• MRP Port Settings	
• MMRP Statistics	
• MVRP Statistics	

	Interface	MVRP Mode	MMRP Mode	Join Timer (10-100)	Leave Timer (20-600)	Leave All Timer (200-6000)
<input type="checkbox"/>	1/0/1	Disable	Disable	20	300	2000
<input type="checkbox"/>	1/0/2	Disable	Disable	20	300	2000
<input type="checkbox"/>	1/0/3	Disable	Disable	20	300	2000

8. To configure one or more ports or LAGs, select the check box next to each port or LAG to configure.

You can select multiple ports to apply the same settings to the selected interfaces.

9. In the **MVRP Mode** field, select **Enable** or **Disable**.

This specifies the administrative mode of Multiple VLAN Registration Protocol (MVRP) on the interface. MVRP registers VLANs in the network, enabling automatic VLAN configuration on the device.

10. In the **MMRP Mode** field, select **Enable** or **Disable**.

This specifies the administrative mode of Multiple MAC Registration Protocol (MMRP) on the interface. MMRP allows the propagation of MAC address information in the network and allows for the registration and deregistration of both individual MAC address information and group MAC address membership.

11. Use the MRP **Join Timer** field to configure the amount of time in centiseconds to wait for JoinIn messages from other MRV participants after the interface sends a Join message.

If the amount of time specified in this field passes before the interface receives a JoinIn message, the interface resends the Join message. The range is 10 to 100 centiseconds. The default value is 20.

12. Use the MRP **Leave Timer** field to configure the amount of time in centiseconds to wait before the interface deregisters attributes from other MRV participants.

If the interface receives Join messages from other participants before the Leave timer expires, the attributes are not deregistered. The range is 20 to 600 centiseconds. The default value is 300.

13. Use the MRP **Leave All Timer** field to configure the amount of time to wait, after the interface starts the MRP registration process, before the participants refresh and reregister their attributes.

The range is 200 to 6000 centiseconds. The default value is 2000.

14. Click the **Apply** button.

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



## View MMRP Statistics

You can view information regarding the MMRP frames transmitted and received by the switch and by each interface.

➤ **To view MMRP 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 > MRP > Advanced > MMRP Statistics**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index		
VLAN	Auto-VoIP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAG	MRP

MRP

• Basic

• Advanced

• MRP Configuration

• MRP Port Settings

• **MMRP Statistics**

• MVRP Statistics

MMRP Global Statistics

Frames Received0

Bad Header0

Bad Format0

Frames Transmitted0

Transmission Failures0

MMRP Statistics

123LAGAll

Go To Interface

Go

<input type="checkbox"/>	Interface	Frames Received	Bad Header	Bad Format	Frames Transmitted	Transmission Failures
<input type="checkbox"/>	1/0/1	0	0	0	0	0
<input type="checkbox"/>	1/0/2	0	0	0	0	0

To refresh the screen with the latest information on the switch, click the **Update** button.

To clear the statistics for one or more ports, select the check box next to the interface or interfaces, and click the **Clear** button.

The following table describes the nonconfigurable data that the MMRP Global Statistics screen displays.

**Table 119. MMRP Global Stastics**

Field	Description
Interface	In the MMRP Statistics table, this field identifies the interface associated with the rest of the data in the row.
Frames Received	The number of MMRP frames that were received on the device or on the particular interface.
Bad Header	The number of MMRP frames with bad headers that were received on the switch.
Bad Format	The number of MMRP frames with bad PDUs body formats that were received on the switch.
Frames Transmitted	The number of MMRP frames that were transmitted on the switch.
Transmission Failures	The number of MMRP frames that the switch failed to transmit.

## View MVRP Statistics

You can view information about the MVRP frames transmitted and received by the switch and by each interface.

### ➤ To view MVRP 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 > MRP > MVRP Statistics**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index		
VLAN	Auto-VoIP	iSCSI	STP	Multicast	MVR	Address Table	Ports	LAG	MLAG	MRP

MRP

• Basic

• Advanced

• MRP Configuration

• MRP Port Settings

• MMRP Statistics

• MVRP Statistics

MVRP Global Statistics

Frames Received

0

Bad Header

0

Bad Format

0

Frames Transmitted

0

Transmission Failures

0

Message Queue Failures

0

MVRP Statistics

123LAGAll

Go To Interface

Go

<input type="checkbox"/>	Interface	Frames Received	Bad Header	Bad Format	Frames Transmitted	Transmission Failures	Registration Failures
<input type="checkbox"/>	1/0/1	0	0	0	0	0	0
<input type="checkbox"/>	1/0/2	0	0	0	0	0	0

To clear the statistics for one or more ports, select the check box next to the interface or interfaces, and click the **Clear** button.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that the MVRP Global Statistics screen displays.

**Table 120. MVRP Statistics**

Field	Description
Interface	In the MVRP Statistics table, this field identifies the interface associated with the rest of the data in the row.
Frames Received	The number of MVRP frames that were received on the switch.
Bad Header	The number of MVRP frames with bad headers that were received on the switch.
Bad Format	The number of MVRP frames with bad PDUs body formats that were received on the switch.
Frames Transmitted	The number of MVRP frames that were transmitted on the switch.
Transmission Failures	The number of MVRP frames that the switch failed to transmit.
Message Queue Failures	The number of messages that failed to be added to the queue.
Registration Failures	The number of MVRP frames that failed to register on a device or particular interface.

## 5. Routing

---

This chapter covers the following topics:

- *Manage Routes*
- *Configure the Router IP*
- *Configure Routing Parameters for the Switch*
- *IPv6*
- *VLAN Overview*
- *Address Resolution Protocol Overview*
- *Configure RIP*
- *Configure Router Discovery*
- *Configure Virtual Router Redundancy Protocol*

## Manage Routes

The Routing Table collects routes from multiple sources: static routes and local routes. The Routing Table can learn multiple routes to the same destination from multiple sources. The Routing Table lists all routes.

### Configure a Basic Route

➤ **To configure a basic route:**

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

Configure Routes						
Route Type	Network Address	Subnet Mask	Next Hop Address	Preference	Description	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	

Learned Routes							
Network Address	Subnet Mask	Protocol	Route Type	Next Hop Interface	Next Hop Address	Preference	Metric

8. In the **Route Type** list, select one of the following route types.
  - **Default.** To create a default route, all that must be specified is the next hop address, and preference.
  - **Static.** To create a static route, specify the network address, subnet mask, next hop address, and preference.
  - **Static Reject.** To create a static reject route, specify the network address, subnet mask, and preference.
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 that identifies the route.

Description must consist of alphanumeric, hyphen, or underscore characters and can be up to 31 characters in length.

- 14. Click the Add button.**

The static route is added to the switch.

- 15. To delete an existing static route entry from the switch, click the Delete button.**

- 16. Click the Apply button.**

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

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 121. Routing Table Basic Route Configuration**

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 one of the following: <ul style="list-style-type: none"> <li>Local</li> <li>Static</li> </ul>
Route Type	This field can be <b>Connected</b> or <b>Static</b> or <b>Dynamic</b> based on the protocol.

Table 121. Routing Table Basic Route Configuration (continued)

Field	Description
Next Hop Interface	The outgoing router interface to use when forwarding traffic to the destination.
Next Hop 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.
Preference	The preference is an integer value from (0 to 255). The user can specify the preference value (sometimes called <i>administrative distance</i> ) 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 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.  
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 Configuration**.

Configure Routes						
<input type="checkbox"/>	Route Type	Network Address	Subnet Mask	Next Hop IP Address	Preference	Description
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Learned Routes							
Network Address	Subnet Mask	Protocol	Route Type	Next Hop Interface	Next Hop IP Address	Preference	Metric

8. Use the **Route Type** field to specify Default or static reject route.

If you are creating a default route, all that must be specified is the next hop IP address; otherwise, each field must be completed.

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 that identifies the route.

The description must consist of alphanumeric, hyphen or underscore characters and can be up to 31 characters in length.

14. Click the **Add** button.

The static route is added to the switch.

15. To delete the selected static route entry from the switch, click the **Delete** button.

To refresh the screen with the latest information on the switch, click the **Update** button.



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

**Table 122. 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 one of the following: <ul style="list-style-type: none"> <li>Local</li> <li>Static</li> </ul>
Route Type	This field can be either default or static.
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.
Preference	The preference is an integer value from 0 to 255. The user 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.

## Specify Route Preferences

You can configure the default preference for each protocol, for example, 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 (such as RIP and Open Shortest Path First [OSPF] metrics, which are not directly comparable) you must configure different preference values for each of the protocols.

➤ **To specify 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	<input type="text" value="0"/>	
Static	<input type="text" value="1"/>	(1 to 255)
RIP	<input type="text" value="120"/>	(1 to 255)
OSPF Intra	<input type="text" value="110"/>	(1 to 255)
OSPF Inter	<input type="text" value="110"/>	(1 to 255)
OSPF External	<input type="text" value="110"/>	(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.

9. Specify the **RIP** route preference value in the router.

The default value is 120. The range is 1 to 255.

10. Specify the **OSPF Intra** route preference value in the router.

The default value is 110. The range is 1 to 255. The OSPF specification (RFC 2328) requires that preferences must be given to the routes learned through OSPF in the following order: intra < inter < type-1 < type-2.

11. Specify the **OSPF Inter** route preference value in the router.

The default value is 110. The range is 1 to 255. The OSPF specification (RFC 2328) requires that preferences must be given to the routes learned through OSPF in the following order: intra < inter < type-1 < type-2.

12. Specify the **OSPF External** route preference value in the router.

The default value is 110. The range is 1 to 255. The OSPF specification (RFC 2328) requires that preference value must be the same for all the OSPF external route types, such as type1/type2/nssa1/nssa2.

**13. Click the **Apply** button.**

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

The Local field displays the local route preference value.

## Configure the Router IP

You can configure routing parameters for the switch, as opposed to an interface.

➤ **To configure the router IP:**

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

IP Configuration	
Default Time to Live	64
Routing Mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
ICMP Echo Replies	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
ICMP Redirects	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
ICMP Rate Limit Interval	<input type="text" value="1000"/> (0 to 2147483647 ms)
ICMP Rate Limit Burst Size	<input type="text" value="100"/> (1 to 200)
Maximum Next Hops	4
Maximum Routes	8160
Select to configure Global Default Gateway	<input type="checkbox"/>
Global Default Gateway	<input type="text" value="0.0.0.0"/>

**8. Use `Routing Mode` to select `Enable` or `Disable`.**

You must enable routing for the switch before you can route through any of the interfaces. The default value is `Disable`.

**9. Use `ICMP Echo Replies` to select `Enable` or `Disable`.**

If you select `Enable`, then only the router can send ECHO replies. By default ICMP Echo Replies are sent for echo requests.

**10. Use `ICMP Redirects` to select `Enable` or `Disable`.**

If this is enabled globally and on an 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 (the burst interval is 1000 msec). To disable ICMP Rate limiting, set this field to 0. The valid rate Interval is from 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 range is 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 123. Routing 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 Statistics

The statistics reported on this screen are as specified in RFC 1213.

➤ **To view 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 > Basic > Statistics**.

IP Statistics			
IpInReceives	49066	IcmpInTimeExcds	0
IpInHdrErrors	0	IcmpInParmProbs	0
IpInAddrErrors	0	IcmpInSrcQuenchs	0
IpForwDatagrams	0	IcmpInRedirects	0
IpInUnknownProtos	0	IcmpInEchos	0
IpInDiscards	0	IcmpInEchoReps	0
IpInDelivers	26277	IcmpInTimestamps	0
IpOutRequests	10134	IcmpInTimestampReps	0
IpOutDiscards	0	IcmpInAddrMasks	0
IpOutNoRoutes	0	IcmpInAddrMaskReps	0
IpReasmTimeout	0	IcmpOutMsgs	3
IpReasmReqds	0	IcmpOutErrors	0
IpReasmOKs	0	IcmpOutDestUnreachs	3
IpReasmFails	0	IcmpOutTimeExcds	0
IpFragOKs	0	IcmpOutParmProbs	0
IpFragFails	0	IcmpOutSrcQuenchs	0
IpFragCreates	0	IcmpOutRedirects	0
IpRoutingDiscards	0	IcmpOutEchos	0
IcmpInMsgs	3	IcmpOutEchoReps	0
IcmpInErrors	0	IcmpOutTimestamps	0
IcmpInDestUnreachs	3	IcmpOutTimestampReps	0
		IcmpOutAddrMasks	0

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

**Table 124. IP Basic Statistics**

Field	Description
IpInReceives	The total number of input datagrams received from interfaces, including those received in error.
IpInHdrErrors	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.
IpInAddrErrors	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 (for example, 0.0.0.0) and addresses of unsupported classes (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.
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 (for lack of buffer space). 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 for reasons such as lack of buffer space. 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. 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 for which received fragments are held while they are awaiting reassembly at this entity.

Table 124. IP Basic Statistics (continued)

Field	Description
IpReasmReqds	The number of IP fragments received that were 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 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, for reasons such as 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 were 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.
IcmpInSrcQuenchs	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. This counter includes all those counted by icmpOutErrors.

Table 124. IP Basic Statistics (continued)

Field	Description
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 might 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.
IcmpOutSrcQuenchs	The number of ICMP source quench messages sent.
IcmpOutRedirects	The number of ICMP redirect messages sent. For a host, this 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.
IcmpOutAddrMasks	The number of ICMP address mask request messages sent.

## Configure Routing Parameters for the Switch

You can configure routing parameters for the switch as opposed to an interface.

### ➤ To configure routing parameters for 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.

**7. Select **Routing > IP > Advanced > IP Configuration**.**

**8. Use **Routing Mode** to select **Enable** or **Disable**.**

You must enable routing for the switch before you can route through any of the interfaces. The default value is Disable.

**9. Use **ICMP Echo Replies** to select **Enable** or **Disable**.**

If you select Enable, then only the router can send ECHO replies. By default ICMP echo replies are sent for echo requests.

**10. Use **ICMP Redirects** to select **Enable** or **Disable**.**

If it is enabled globally and on 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, (the 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 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 updated configuration is sent to the switch. Configuration changes take effect immediately.

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

**Table 125. Routing 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.
Maximum Static Routes	The maximum number of static routes supported by the switch.

## 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. Select **Routing > IP > Advanced > Statistics**.

IP Statistics	
IpInReceives	51627
IpInHdrErrors	0
IpInAddrErrors	0
IpForwDatagrams	0
IpInUnknownProtos	0
IpInDiscards	0
IpInDelivers	27781
IpOutRequests	10714
IpOutDiscards	0
IpOutNoRoutes	0
IpReasmTimeout	0
IpReasmReqds	0
IpReasmOKs	0
IpReasmFails	0
IpFragOKs	0
IpFragFails	0
IpFragCreates	0
IpRoutingDiscards	0
IcmpInMsgs	3
IcmpInErrors	0
IcmpInDestUnreachs	3
IcmpInTimeExcds	0

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

**Table 126. IP Statistics**

Field	Description
IpInReceives	The total number of input datagrams received from interfaces, including those received in error.
IpInHdrErrors	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
IpInAddrErrors	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 (for example, 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 126. IP Statistics (continued)

Field	Description
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 which were discarded for reasons such as lack of buffer space. 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 for reasons such as lack of buffer space. 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. 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 for which 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 reassembled.
IpReasmFails	The number of failures detected by the IP reassembly algorithm (for whatever reason: timed out, errors, etc). 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 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, for example this can occur 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.

Table 126. IP Statistics (continued)

Field	Description
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.
IcmpInSrcQuenchs	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. 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 might 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.
IcmpOutSrcQuenchs	The number of ICMP source quench messages sent.
IcmpOutRedirects	The number of ICMP redirect messages sent. For a host, this is 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.

Table 126. IP Statistics (continued)

Field	Description
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.
IcmpOutAddrMaskReps	The number of ICMP address mask reply messages sent.

## Configure the IP Interface

You can update IP interface data for this switch.

### ➤ To configure the 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.

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 Interface Configuration**.

The screen is shown in three parts.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index			
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast

IP

• Basic

• Advanced

• IP Configuration

• Statistics

• IP Interface Configuration

• Secondary IP

1 VLANs All

<div></div>	Port	Description	VLAN ID	IP Address Configuration Method	IP Address	Subnet Mask	Routing Mode
<div></div>							
<div></div>	1/0/1			None	0.0.0.0	0.0.0.0	Disable
<div></div>	1/0/2			None	0.0.0.0	0.0.0.0	Disable
<div></div>	1/0/3			None	0.0.0.0	0.0.0.0	Disable
<div></div>	1/0/4			None	0.0.0.0	0.0.0.0	Disable

Administrative Mode	Link Speed Data Rate	OSPF Admin Mode	Forward Net Directed Broadcasts	Active State	MAC Address	Encapsulation Type	Proxy Arp
<input type="text"/>			<input type="text"/>			<input type="text"/>	<input type="text"/>
Enable	1000 Mbps	Disable	Disable	Active	20:E5:2A:51:0A:D0	Ethernet	Enable
Enable	1000 Mbps	Disable	Disable	Active	20:E5:2A:51:0A:D0	Ethernet	Enable
Enable	1000 Mbps	Disable	Disable	Active	20:E5:2A:51:0A:D0	Ethernet	Enable
Enable	1000 Mbps	Disable	Disable	Active	20:E5:2A:51:0A:D0	Ethernet	Enable

Go To Interface <input type="text"/> <input type="button" value="Go"/>						
Local Proxy Arp	Bandwidth	ICMP Destination Unreachables	ICMP Redirects	IP MTU	Link State	Routing Interface Status
<input type="text"/>		<input type="text"/>	<input type="text"/>			
Disable	1000000	Enable	Disable	1500	Link Up	Down
Disable	1000000	Enable	Disable	1500	Link Up	Down
Disable	1000000	Enable	Disable	1500	Link Up	Down
Disable	1000000	Enable	Disable	1500	Link Up	Down

8. Use **Go To Interface** to enter the interface in unit/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. Use the **None** method 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. In the **Routing Mode** list, select **Enable** or **Disable**.

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 are 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 (kbps)** 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 destination unreachables mode is enabled.

22. Use **ICMP Redirects** to enable or 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.

24. To delete the IP address from the selected interface, click the **Delete** button.

25. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 127. IP Interface Configuration**

Field	Description
VLAN ID	The VLAN ID for the interface.
OSPF Admin Mode	Displays the OSPF admin mode of the interface. The default value is Disable.
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 forwarding state.
Routing Interface Status	Indicates whether the link status is up or down.



## Configure the Secondary IP Address

➤ **To configure the 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**.

System		Switching		Routing		QoS		Security		Monitoring		Maintenance		Help	
Routing Table		IP		IPv6		VLAN		ARP		RIP		OSPF		OSPFv3	
Router Discovery		VRRP		Multicast		IPv6 Multicast									

IP

- Basic
- Advanced
- IP Configuration
- Statistics
- IP Interface Configuration
- Secondary IP

Routing Interface

Interface: vlan 1

Secondary IP Address

VLAN ID	Primary IP Address	Secondary IP Address	Secondary IP Subnet Mask

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 associated with the secondary IP address.

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. Click the **Add** button.

The secondary IP address for the selected interface is added.

12. To delete the secondary IP address from the selected interface, click the **Delete** button.

The following table describes the nonconfigurable data that is displayed.

**Table 128. Secondary IP**

Field	Description
VLAN ID	The VLAN ID associated with the displayed or configured interface.
Primary IP Address	The primary IP address for the interface.

## IPv6

Only the following switches support IPv6:

- M6100
- M5300-28G3
- M5300-52G3
- M5300-28GF3

The following switches support IPv6 with an L3 license:

- M5300-28G
- M5300-52G
- M5300-28G-POE+
- M5300-52G-POE+

## Configure IPv6 Global Settings

You can configure IPv6 routing parameters for the switch, as opposed to an interface.

### ➤ To configure IPv6 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 **Routing > IPv6 > Basic > Global Configuration**.

IPv6 Global Configuration		
IPv6 Unicast Routing	<input checked="" type="radio"/> Disable <input type="radio"/> Enable	
Hop Limit	<input type="text" value="64"/>	(1 to 255)
ICMPv6 Rate Limit Error Interval	<input type="text" value="1000"/>	(0 to 2147483647 msec)
ICMPv6 Rate Limit Burst Size	<input type="text" value="100"/>	(1 to 200)

8. In the **IPv6 Unicast Routing** field, select the option to globally **Enable** or **Disable** IPv6 unicast routing.
9. In the **Hop Limit** field, enter a value for the unicast hop count used in IPv6 packets originated by the node.

The value is also included in router advertisements. The valid values for hops are 1 to 255, inclusive. The default is Not Configured, which means that a value of zero is sent in router advertisements.

10. In the **ICMPv6 Rate Limit Error Interval** field, specify the number of ICMP error packets allowed per burst interval.

This value controls the ICMPv6 error packets. The default rate limit is 100 packets per second, meaning that the burst interval is 1000 mseconds. To disable ICMP rate limiting, set this field to 0. The valid rate interval must be in the range 0 to 2147483647 mseconds.

11. In the **ICMPv6 Rate Limit Burst Size** field, specify the number of ICMP error packets allowed per burst interval.

This value controls the ICMP error packets. The 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 is 1 to 200.

12. Click the **Apply** button.

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

## View the IPv6 Route Table

### ➤ To view the IPv6 Route 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 > IPv6 > Basic > Route Table**.

IPv6 Route Table

Routes Displayed: All Routes (dropdown)

Number of Routes: 0

IPv6 Prefix	Prefix Length	Protocol	Next Hop Interface	Next Hop IP Address	Preference
-------------	---------------	----------	--------------------	---------------------	------------

8. In the **Routes Displayed** list, select from the following:
  - **All Routes**. Shows all active IPv6 routes.
  - **Best Routes Only**. Shows only the best active routes.
  - **Configured Routes Only**. Shows the routes configured by the user.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 129. IPv6 Route Table**

Field	Description
Number of Routes	The total number of active routes in the route table.
IPv6 Prefix	The network prefix for the active route.
Prefix Length	The prefix length for the active route.
Protocol	The type of protocol for the active route.
Next Hop Interface	The interface over which the route is active. For a reject route, the next hop would be a <i>Null0</i> interface.
Next Hop IP Address	The next hop IPv6 address for the active route.
Preference	The route preference of the configured route.

## Configure IPv6 Interface Settings

### ➤ Configure IPv6 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 **Routing > IPv6 > Advanced > Interface Configuration**.

IPv6 Interface Configuration

1 2 3 VLANs All

<input type="checkbox"/>	Interface	IPv6 Mode	DHCPv6 Client Mode	Stateless Address AutoConfig Mode	Routing Mode	Admin Mode	Operational Mode	MTU	Duplicate Address Detection Transmits
<input type="checkbox"/>	1/0/1	Disable	Disable	Disable	Disable	Enable	Disable	1500	1
<input type="checkbox"/>	1/0/2	Disable	Disable	Disable	Disable	Enable	Disable	1500	1
<input type="checkbox"/>	1/0/3	Disable	Disable	Disable	Disable	Enable	Disable	1500	1
<input type="checkbox"/>	1/0/4	Disable	Disable	Disable	Disable	Enable	Disable	1500	1
<input type="checkbox"/>	1/0/5	Disable	Disable	Disable	Disable	Enable	Disable	1500	1

Go To Interface  **Go**

Life Time Interval	Adv NS Interval	Adv Reachable Interval	Adv Interval	Adv Managed Config Flag	Adv Other Config Flag	Adv Suppress Flag	Destination Unreachables	Link State
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
1800	0	0	600	Disable	Disable	Disable	Enable	Link Down
1800	0	0	600	Disable	Disable	Disable	Enable	Link Down
1800	0	0	600	Disable	Disable	Disable	Enable	Link Down
1800	0	0	600	Disable	Disable	Disable	Enable	Link Down
1800	0	0	600	Disable	Disable	Disable	Enable	Link Down

8. Use **Go To Interface** to enter the interface in unit/slot/port format and click the **Go** button.  
The entry corresponding to the specified interface is selected.
9. Select the check box next to the **interface** to select it.

All physical interfaces are valid.

10. Select **Enable** or **Disable** in the **IPv6 Mode** list.

When IPv6 mode is enabled, the interface is capable of IPv6 operation without a global address. In this case, an EUI-64 based link-local address is used. The default value is Disable.

11. In the **DHCPv6 Client Mode** list, select to **Enable** or **Disable** DHCPv6 client mode on an interface.

At any point in time, only one interface can act as a client. The default value is Disable.

12. In the **Stateless Address AutoConfig Mode** list, select to **Enable** or **Disable** Stateless Address AutoConfig mode on an interface.

The default value is Disable.

13. In the **Routing Mode** list, select to **Enable** or **Disable** the routing mode of an interface.

The default is Disable.

14. In the **Admin Mode** list, select to **Enable** or **Disable** IPv6 mode.

The default is Disable. When IPv6 mode is enabled, the interface is capable of IPv6 operation without a global address. In this case, an EUI-64 based link-local address is used.

15. In the **MTU** field, specify the maximum transmit unit on an interface.

If the value is 0, then this interface is not enabled for routing. It is not valid to set this value to 0 if routing is enabled. The MTU range 1280 to 1500. The default is 1500.

16. In the **Duplicate Address Detection Transmits** field, specify the number of duplicate address detection (DAD) transmits on an interface.

DAD transmits values must be in the range 0 to 600. The default is 1.

17. Specify the router advertisement **Life Time Interval** sent from the interface.

This value must be greater than or equal to the maximum advertisement interval. 0 means do not use the router as the default router. The range of router life time is 0 to 9000. The default is 1800.

18. In the **Adv NS Interval** field, specify the retransmission time field of router advertisements sent from the interface.

A value of 0 means the interval is not specified for the router. The range of the neighbor solicit interval is 1000 to 4294967295. The default is 0.

19. In the **Adv Reachable Interval** field, specify the router advertisement time.

This is the amount of time allocated to consider the neighbors reachable after ND confirmation. The range of reachable time is 0 to 3600000. The default is 0.

20. Use the **Adv Interval** field to specify the maximum time allowed between sending router advertisements from the interface.

The range of the maximum advertisement interval is 4 to 1800. The default value is 600.

21. In the **Adv Other Config Flag** list, select **Enable** or **Disable** to specify the router advertisement other stateful configuration flag.

Default value of other config flag is Disable.

22. In the **Adv Suppress Flag** list, select to **Enable** or **Disable** router advertisement suppression on an interface.

The default value of the suppress flag is Disable.

23. In the **Destination Unreachables** list, select to **Enable** or **Disable** the mode of sending ICMPv6 destination unreachables on this interface.

If disabled, then this interface does not send ICMPv6 destination unreachables. By default, the IPv6 destination unreachables mode is enabled.

24. Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 130. IPv6 Advanced Interface Configuration**

Field	Description
Operational Mode	Specifies the operational state of an interface. The default value is Disable.
Link State	Indicates whether the link is up or down.

## IPv6 Prefix Configuration

### ➤ Configure IPv6 prefix 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 > IPv6 > Advanced > Prefix Configuration**.

IPv6 Interface Selection							
Interface <span>1/0/1</span>							
IPv6 Interface Configuration							
Ipv6 Prefix	Prefix Length	EUI64	Valid Life Time	Preferred Life Time	Onlink Flag	Autonomous Flag	Current State
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

8. From the **Interface** list, select the interface.

When the selection is changed, a screen update occurs, causing all fields to be updated for the newly selected port. All physical interfaces are valid.

9. In the **IPv6 Prefix** field, specify the IPv6 prefix for an interface.

10. In the **Prefix Length** field, specify the IPv6 prefix length for an interface.

11. In the **EUI64** list, select to **Enable** or **Disable** the specified 64-bit unicast prefix.

12. In the **Valid Life Time** field, specify the router advertisement per prefix time.

This is the amount of time allowed to consider the prefix valid for the purpose of on-link determination. The valid life time is 0 to 4294967295.

13. In the **Preferred Life Time** field, specify the router advertisement per prefix time.

An autoconfigured address generated from this prefix is preferred. The preferred life time must be in the range 0 to 4294967295.

14. From the **Onlink Flag** list, select **Enable** or **Disable**.

This specifies whether the selected prefix can be used for on-link determination. The default is Enable.

15. In the **Autonomous Flag** list, select **Enable** or **Disable**.

This specifies whether the selected prefix can be used for autonomous address configuration. The default value is Enable.

16. Click the **Add** button.

The IPv6 address is added to the interface.

17. To delete a existing IPv6 address entry from the interface, click the **Delete** button.

18. Click the **Apply** button.

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

The **Current State** field displays the state of the IPV6 address. The state is TENT if routing is disabled or DAD fails. The state is Active if the interface is active and DAD is successful.



## View IPv6 Statistics

➤ **To view IPv6 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.

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 > IPv6 > Advanced > Statistics**.

IPv6 Interface Selection	
Interface	1/0/1
IPv6 Statistics	
Total Datagrams Received	0
Received Datagrams Locally Delivered	0
Received Datagrams Discarded Due To Header Errors	0
Received Datagrams Discarded Due To MTU	0
Received Datagrams Discarded Due To No Route	0
Received Datagrams With Unknown Protocol	0
Received Datagrams Discarded Due To Invalid Address	0
Received Datagrams Discarded Due To Truncated Data	0
Received Datagrams Discarded Other	0
Received Datagrams Reassembly Required	0
Datagrams Successfully Reassembled	0
Datagrams Failed To Reassemble	0
Datagrams Forwarded	0
Datagrams Locally Transmitted	0
Datagrams Transmit Failed	0
Datagrams Successfully Fragmented	0
Datagrams Failed To Fragment	0
Datagrams Fragments Created	0
Multicast Datagrams Received	0
Multicast Datagrams Transmitted	0

8. From the **Interface** list, select the interface.

When the selection is changed, a screen refresh occurs, causing all fields to be updated for the newly selected port.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 131. IPv6 Advanced Interface Statistics**

Field	Description
Total Datagrams Received	The total number of input datagrams received by the interface, including those received in error.
Received Datagrams Locally Delivered	The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed, which might not be the input interface for some of the datagrams.
Received Datagrams Discarded Due To Header Errors	The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IPv6 options, and so on
Received Datagrams Discarded Due To MTU	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.
Received Datagrams Discarded Due To No Route	The number of input datagrams discarded because no route could be found to transmit them to their destination
Received Datagrams With Unknown Protocol	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed, which might not be the input interface for some of the datagrams.
Received Datagrams Discarded Due To Invalid Address	The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example, ::0) and unsupported addresses (such as addresses with unallocated prefixes). For entities that are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Received Datagrams Discarded Due To Truncated Data	The number of input datagrams discarded because datagram frame didn't carry enough data.
Received Datagrams Discarded Other	The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but that were discarded for reasons such as lack of buffer space. This counter does not include any datagrams discarded while awaiting re-assembly.
Received Datagrams Reassembly Required	The number of IPv6 fragments received that needed to be reassembled at this interface. This counter is incremented at the interface to which these fragments were addressed, which might not be the input interface for some of the fragments.

**Table 131. IPv6 Advanced Interface Statistics (continued)**

Field	Description
Datagrams Successfully Reassembled	The number of IPv6 datagrams successfully reassembled. This counter is incremented at the interface to which these datagrams were addressed, which might not be necessarily the input interface for some of the fragments.
Datagrams Failed To Reassemble	The number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, and so on). This is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed, which might not be the input interface for some of the fragments.
Datagrams Forwarded	The number of output datagrams that this entity received and forwarded to their final destinations. In entities that do not act as IPv6 routers, this counter includes only those packets that were source-routed through this entity, and the source-route processing was successful. For a successfully forwarded datagram the counter of the outgoing interface is incremented.
Datagrams Locally Transmitted	The number of datagrams that this entity successfully transmitted from this output interface.
Datagrams Transmit Failed	The number of datagrams that this entity failed to transmit successfully.
Datagrams Successfully Fragmented	The number of IPv6 datagrams that were fragmented at this output interface.
Datagrams Failed To Fragment	The number of output datagrams that could not be fragmented at this interface.
Datagrams Fragments Created	The number of output datagram fragments that were generated as a result of fragmentation at this output interface.
Multicast Datagrams Received	The number of multicast packets received by the interface.
Multicast Datagrams Transmitted	The number of multicast packets transmitted by the interface.

The following table describes the nonconfigurable data that is displayed.

**Table 132. ICMPv6 Statistics**

Field	Description
Total ICMPv6 Messages Received	The total number of ICMP messages received by the interface, which includes all those counted by IPv6IfIcmpInErrors. This interface is the interface to which the ICMP messages were addressed, which might not be the input interface for the messages.
ICMPv6 Messages With Errors Received	The number of ICMP messages that the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so on).
ICMPv6 Destination Unreachable Messages Received	The number of ICMP Destination Unreachable messages received by the interface.

**Table 132. ICMPv6 Statistics (continued)**

Field	Description
ICMPv6 Messages Prohibited Administratively Received	The number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
ICMPv6 Time Exceeded Messages Received	The number of ICMP Time Exceeded messages received by the interface.
ICMPv6 Parameter Problem Messages Received	The number of ICMP Parameter Problem messages received by the interface.
ICMPv6 Packet Too Big Messages Received	The number of ICMP Packet Too Big messages received by the interface.
ICMPv6 Echo Request Messages Received	The number of ICMP Echo (request) messages received by the interface.
ICMPv6 Echo Reply Messages Received	The number of ICMP Echo Reply messages received by the interface.
ICMPv6 Router Solicit Messages Received	The number of ICMP Router Solicit messages received by the interface.
ICMPv6 Router Advertisement Messages Received	The number of ICMP Router Advertisement messages received by the interface.
ICMPv6 Neighbor Solicit Messages Received	The number of ICMP Neighbor Solicit messages received by the interface.
ICMPv6 Neighbor Advertisement Messages Received	The number of ICMP Neighbor Advertisement messages received by the interface.
ICMPv6 Redirect Messages Received	The number of ICMPv6 Redirect messages received by the interface.
ICMPv6 Group Membership Query Messages Received	The number of ICMPv6 Group Membership Query messages received by the interface.
ICMPv6 Group Membership Response Messages Received	The number of ICMPv6 Group Membership Response messages received by the interface.
ICMPv6 Group Membership Reduction Messages Received	The number of ICMPv6 Group Membership Reduction messages received by the interface.
Total ICMPv6 Messages Transmitted	The total number of ICMP messages that this interface attempted to send. This counter includes all those counted by icmpOutErrors.
ICMPv6 Messages Not Transmitted Due To Error	The number of ICMP messages that this interface 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 IPv6 to route the resultant datagram. In some implementations there might be no types of error that contribute to this counter's value.
ICMPv6 Destination Unreachable Messages Transmitted	The number of ICMP Destination Unreachable messages sent by the interface.

**Table 132. ICMPv6 Statistics (continued)**

Field	Description
ICMPv6 Messages Prohibited Administratively Transmitted	Number of ICMP Destination Unreachable/Communication Administratively Prohibited messages sent.
ICMPv6 Time Exceeded Messages Transmitted	The number of ICMP Time Exceeded messages sent by the interface.
ICMPv6 Parameter Problem Messages Transmitted	The number of ICMP Parameter Problem messages sent by the interface.
ICMPv6 Packet Too Big Messages Transmitted	The number of ICMP Packet Too Big messages sent by the interface.
ICMPv6 Echo Request Messages Transmitted	The number of ICMP Echo (request) messages sent by the interface.
ICMPv6 Echo Reply Messages Transmitted	The number of ICMP Echo Reply messages sent by the interface.
ICMPv6 Router Solicit Messages Transmitted	The number of ICMP Neighbor Solicitation messages sent by the interface.
ICMPv6 Router Advertisement Messages Transmitted	The number of ICMP Router Advertisement messages sent by the interface.
ICMPv6 Neighbor Solicit Messages Transmitted	The number of ICMP Neighbor Solicitation messages sent by the interface.
ICMPv6 Neighbor Advertisement Messages Transmitted	The number of ICMP Neighbor Advertisement messages sent by the interface.
ICMPv6 Redirect Messages Transmitted	The number of Redirect messages sent.
ICMPv6 Group Membership Query Messages Transmitted	The number of ICMPv6 Group Membership Query messages sent.
ICMPv6 Group Membership Response Messages Transmitted	The number of ICMPv6 Group Membership Response messages sent.
ICMPv6 Group Membership Reduction Messages Transmitted	The number of ICMPv6 Group Membership Reduction messages sent.
ICMPv6 Duplicate Address Detects	The number of duplicate addresses detected by the interface.

## View the IPv6 Neighbor Table

### ➤ To view the IPv6 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 **Routing > IPv6 > Advanced > Neighbor Table**.

8. Use the **Search By** field to search for IPv6 routes by **IPv6 Address** or **Interface**.

- To search by IPv6 address, select **IPv6 Address** from the **Search By** list. Enter the 128-byte hexadecimal IPv6 address in four-digit groups separated by colons, for example, 2001:231F:::1. Then click the **Go** button. If the address exists, that entry is displayed. An exact match is required.
- To search by Interface, select **Interface** from the **Search By** list, enter the interface ID in unit/slot/port format, for example, 2/1/1. Then click the **Go** button. If the address exists, that entry is displayed.

To clear the IPv6 neighbors on a selected interface or on all interfaces, click the **Clear** button.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 133. IPv6 Advanced Neighbor Table**

Field	Description
Interface	The interface whose settings are displayed in the current table row.
IPv6 Address	The IPv6 address of the neighbor or interface.
MAC Address	Specifies MAC address associated with an interface.
isRtr	Indicates whether the neighbor is a router. If the neighbor is a router, the value is <b>True</b> . If the neighbor is not a router, the value is <b>False</b> .

Table 133. IPv6 Advanced Neighbor Table (continued)

Field	Description
Neighbor State	<p>The state of the neighbor cache entry. Following are the states for dynamic entries in the IPv6 neighbor discovery cache:</p> <ul style="list-style-type: none"> <li>• <b>Incmp.</b> Address resolution is being performed on the entry. A neighbor solicitation message was sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received.</li> <li>• <b>Reach.</b> Positive confirmation was received within the last Reachable Time milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent.</li> <li>• <b>Stale.</b> More than ReachableTime milliseconds elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent.</li> <li>• <b>Delay.</b> More than ReachableTime milliseconds elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE.</li> <li>• <b>Probe.</b> A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.</li> </ul>
Last Updated	Time since the address was confirmed to be reachable.

## IPv6 Static Route Configuration

### ➤ Configure the IPv6 static route:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > IPv6 > Advanced > Static Route Configuration**.

Configure Routes						
<input type="checkbox"/>	IPv6 Prefix	Prefix Length	Next Hop IPv6 Address Type	Next Hop IPv6 Address	Interface	Preference
	<input type="text"/>	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>	<input type="text" value="v"/>	<input type="text"/>

8. In the **IPv6 Prefix** field, specify the IPv6 prefix for the configured route.
9. In the **Prefix Length** field, specify the IPv6 prefix length for the configured route.
10. In the **Next Hop IPv6 Address Type** list, select one of the following options:
- **Global IPv6 Address.**
  - **Link-Local IPv6 address.** If the next hop IPv6 address specified is a link-local IPv6 address, then specify the interface for the link-local IPv6 next hop address.
  - **Static-Reject.** Select **Static-Reject** to create a static-reject route for a destination prefix. No next hop address is specified in that case.
11. Enter the **Next Hop IPv6 Address** for the configured route.
12. Select from the **Interface** list to specify in unit/slot/port format, the link-local IPv6 next hop address.
- This field is enabled only if Link-Local is selected.
13. Specify the route **Preference** of the configured route.
14. Click the **Add** button.
- The route is added.
15. To delete the selected route, click the **Delete** button.

## Configure the IPv6 Route Table

### ➤ To configure the IPv6 Route 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 > IPv6 > Advanced > Route Table**.

IPv6 Route Table

Routes Displayed: All Routes (dropdown)

Number of Routes: 0

IPv6 Prefix	Prefix Length	Protocol	Next Hop Interface	Next Hop IP Address	Preference
-------------	---------------	----------	--------------------	---------------------	------------

8. In the **Routes Displayed** field, select which routes to display from the following list:

- **All Routes.** Show all active IPv6 routes.
- **Best Routes Only.** Show only the best active routes.
- **Configured Routes Only.** Show the routes configured by the user.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 134. IPv6 Advanced Route Table**

Field	Description
Number of Routes	The total number of active routes in the route table.
IPv6 Prefix	The network prefix for the active route.
Prefix Length	The prefix length for the active route.
Protocol	The type of protocol for the active route.
Next Hop Interface	The interface over which the route is active. For a reject route, the next hop would be a <i>Null0</i> interface.
Next Hop IP Address	The next hop IPv6 address for the active route.
Preference	The route preference of the configured route.

## IPv6 Route Preferences

Use this screen to configure the default preference for each protocol. 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 you must configure different preference values for each of the protocols.

➤ **Configure the IPv6 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 > IPv6 > Advanced > Route Preference**.

IPv6 Route Preferences		
Local	<input type="text" value="0"/>	
Static	<input type="text" value="1"/>	(1 to 255)
OSPFv3 Intra	<input type="text" value="110"/>	(1 to 255)
OSPFv3 Inter	<input type="text" value="110"/>	(1 to 255)
OSPFv3 External	<input type="text" value="110"/>	(1 to 255)

8. In the **Static** field, specify the static route preference value for the router.  
The range is 1 to 255. The default value is 1.
9. In the **OSPFv3 Intra** field, specify the OSPFv3 intra route preference value in the router.  
The range is 1 to 255. The default value is 110.
10. In the **OSPFv3 Inter** field, specify the OSPFv3 inter route preference value in the router.  
The range is 1 to 255. The default value is 110.
11. In the **OSPFv3 External** field, specify the OSPFv3 external route preference value in the router.  
The range is 1 to 255. The default value is 110.
12. Click the **Apply** button.

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

The **Local** field displays the local preference.

## Configure IPv6 Tunnels

You can create, configure, and delete tunnels.

### ➤ To configure an IPv6 tunnel:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > IPv6 > Advanced > Tunnel Configuration**.

Tunnel Configuration									
Tunnel ID	Mode	IPv6 Mode	IPv6 Unreachables	IPv6 Address/Prefix Length	EUI64	Source Address	Source Interface	Destination Address	Interface Link Status
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

8. In the **Tunnel ID** field, select from the list of available tunnel IDs.

9. In the **Mode** list, select a supported mode:

- 6-in-4-configured
- 6-to-4

10. Select the **IPv6 Mode** from the list.

11. **Enable** IPv6 on this interface using the IPv6 address.

This option is configurable only until you specify an explicit IPv6 address.

12. From the **IPv6 Unreachables** list, select to **Enable** or **Disable**.

This specifies the mode of sending ICMPv6 Destination Unreachables on this interface. If you select Disable, then this interface does not send ICMPv6 destination unreachables. By default IPv6 destination unreachables mode is enabled.

13. In the **IPv6 Address/Prefix Length** field, enter a configured IPv6 address for the selected interface.

The address must be entered in the format prefix/length.

14. From the **EUI64** list, select to **Enable** or **Disable** the 64-bit extended unique identifier (EUI-64).

For 6to4 tunnels, configure the IPv6 address with first 48-bits in the format 2002:tunnel-source-IPv4-address::/48.

15. Specify the desired **Source Address** for this tunnel.

This value must be entered in dotted-decimal notation.

16. Select the **Source Interface** for this tunnel.

The address associated with the selected interface is used as the source address.

17. Enter the **Destination Address** for this tunnel in dotted-decimal notation.

18. Click the **Add** button.

The tunnel is added.

19. To delete the selected tunnel, click the **Delete** button.

20. Click the **Apply** button.

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

The **Interface Link Status** field indicates whether the tunnel interface is up or down.

## VLAN Overview

You can configure M6100/M7100/M5300 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 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 Static Routing Wizard gives you the option to add the selected ports as a link aggregation (LAG). 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, add selected ports to a LAG, then adds a 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 Static Routing 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 **Routing > VLAN > VLAN Static Routing Wizard**.

8. 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.
13. Click the **Apply** button.  
The updated configuration is sent to the switch. Configuration changes take effect immediately.

## Configure VLAN Routing

### ➤ 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**.

8. Select the **VLAN ID**.

This field displays the IDs of all the VLANs configured on this switch.

9. Use **IP Address** to enter the IP address to be configured for the VLAN routing interface.

10. Use **Subnet Mask** to enter the subnet mask to be configured for the VLAN routing interface.

11. Click the **Add** button.

The VLAN routing interface is added for the selected VLAN ID.

12. To remove the VLAN routing interface selected in the **VLAN ID** field, click the **Delete** button.

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

**Table 135. VLAN Routing Configuration**

Field	Description
Port	The interface assigned to the VLAN for routing.
MAC Address	The MAC Address assigned to the VLAN routing interface

## Address Resolution Protocol Overview

The Address Resolution Protocol (ARP) associates a Layer 2 MAC address with a Layer 3 IPv4 address. M6100/M7100/M5300 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), each recipient has the opportunity to store the sender's IP and MAC address in its 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, or it disappeared from the network altogether (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 was identified as a sender of an ARP packet during the course of an ageout interval, usually specified through configuration.

## Configure Basic ARP Cache

Use this screen to show ARP entries in the ARP cache.

### ➤ To display ARP entries in the 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.

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**.

System	Switching		Routing	QoS	Security	Monitoring		
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery

ARP

ARP Cache

• Basic

• ARP Cache

• Advanced

Rows per page

20

1 of 1

IP Address	Port	MAC Address
10.130.166.129		DC:7B:94:D6:2A:C6

8. **IP Address** displays the IP address associated with the system's MAC address.

It must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.

9. The **Port** field displays the associated unit/slot/port of the connection.

**MAC Address** displays the unicast MAC address of the device. The address is six 2-digit hexadecimal numbers separated by colons, for example, 00:06:29:32:81:40.

To refresh the screen with the latest information on the switch, click the **Update** button.

### Pagination Navigation Menu

- Rows per screen — Select how many table entries are displayed per screen. Possible values are 50, 100, 500, 1000 and All.

**Note:** If you select All, the browser might be slow to display the information.

- < Display the previous screen of the table data entries.
- > Display the next screen of the table data entries.

## Add an Entry to the ARP Table

You can add an entry to the Address Resolution Protocol (ARP) table.

➤ **To add an entry to 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 Create**.

The screenshot shows the 'ARP Static Configuration' and 'ARP Cache' sections of a web management interface. The 'ARP Static Configuration' section has a table with two columns: 'IP Address' and 'MAC Address'. The 'IP Address' column has a checkbox and a text input field. The 'MAC Address' column has a text input field. The 'ARP Cache' section has a table with five columns: 'IP Address', 'Port', 'MAC Address', 'Type', and 'Age'.

8. Use **IP Address** to enter the IP address to add.

It must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.

9. Use **MAC Address** to specify the unicast MAC address of the device.

Enter the address as six 2-digit hexadecimal numbers separated by colons, for example, 00:06:29:32:81:40.

10. Click the **Add** button.

The static ARP entry is added to the switch.

11. To delete the selected static ARP entry from the switch, click the **Delete** button.

12. Click the **Apply** button.

The MAC address mapping to the IP changes. Configuration changes take effect immediately.

To refresh the screen with the latest information on the switch, click the **Update** button.

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

**Table 136. ARP Cache**

Field	Description
Port	The associated unit/slot/port of the connection.
IP Address	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.

Table 136. ARP Cache (continued)

Field	Description
Port	The associated unit/slot/port of the connection.
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.
Type	The type of ARP entry. Possible values are as follows: <ul style="list-style-type: none"> <li>• <b>Local.</b> An ARP entry associated with one of the switch's routing interface's MAC addresses.</li> <li>• <b>Gateway.</b> A dynamic ARP entry whose IP address is that of a router.</li> <li>• <b>Static.</b> An ARP entry configured by the user.</li> <li>• <b>Dynamic.</b> An ARP entry that was learned by the router.</li> </ul>
Age	Age since the entry was last refreshed in the ARP table (in seconds).

## View or Configure the ARP Table

You can change the configuration parameters for the Address Resolution Protocol (ARP) table. You can also use this screen to display the contents of the table.

### ➤ To 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**.

ARP Table Configuration		
Age Time(secs)	<input type="text" value="1200"/>	(15 to 21600)
Response Time(secs)	<input type="text" value="10"/>	(1 to 10)
Retries	<input type="text" value="10"/>	(0 to 10)
Cache Size	<input type="text" value="6144"/>	(384 to 6144)
Dynamic Renew	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	
Total Entry Count	0	
Peak Total Entries	0	
Active Static Entries	0	
Configured Static Entries	0	
Maximum Static Entries	128	
Remove From Table	<input type="text" value="None"/> ▼	

8. Use **Age Time** to enter the value for the switch to use for the ARP entry age-out time.  
You must enter a valid integer that 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.
9. Use **Response Time** to enter the value for the switch to use for the ARP response time-out.  
You must enter a valid integer that 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 is 1 second.
10. 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 4.
11. Use **Cache Size** to enter an integer that specifies the maximum number of entries for the ARP cache.  
The range for this field is 64 to 512. The default value for Cache Size is 1664.
12. 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.
13. 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.

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

**Table 137. 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 RIP

Only the following switches support RIP:

- M6100
- M5300-28G3
- M5300-52G3
- M5300-28GF3

The following switches support RIP with an L3 license:

- M5300-28G
- M5300-52G
- M5300-28G-POE+
- M5300-52G-POE+

## Enable RIP

### ➤ To enable RIP:

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

4. Enter 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.

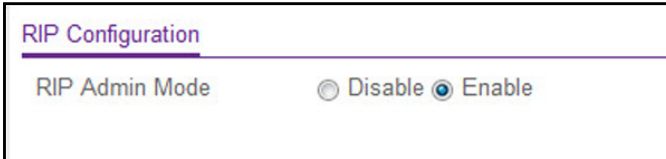
5. Enter the user name and password.

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 > RIP > Basic > RIP Configuration**.



RIP Configuration	
RIP Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable

8. In the **RIP Admin Mode** field, select the **Enable** or **Disable** option.

If you select **Enable**, RIP is activated for the switch. The default is Enable.

## Configure RIP Settings

### ➤ To configure advanced RIP 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 > RIP > Advanced > RIP Configuration**.

RIP Configuration	
RIP Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Split Horizon Mode	<input type="radio"/> None <input checked="" type="radio"/> Simple <input type="radio"/> Poison Reverse
Auto Summary Mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Host Routes Accept Mode	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Global Route Changes	0
Global Queries	0
Default Information Originate	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Default Metric	<input type="text" value="0"/> (1 to 15)

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

If you select **Enable**, RIP is activated for the switch. By default, RIP is enabled.

9. Select a **Split Horizon Mode** radio button:

- **None.** No special processing for this case.
- **Simple.** A route is not included in updates sent to the router from which it was learned. The default is Simple.
- **Poison Reverse.** A route is included in updates sent to the router from which it was learned, but the metric is set to infinity.

Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned

10. In the **Auto Summary Mode** field, select the **Enable** or **Disable** option.

If you select **Enable**, groups of adjacent routes are summarized into single entries reduce the total number of entries. The default is Disable.

11. In the **Host Routes Accept Mode** field, select the **Enable** or **Disable** option.

If you select Enable, the router accepts host routes. The default is Enable.

12. In the **Default Information Originate** field, select to **Enable** or **Disable** default route advertisement.

13. In the **Default Metric** field, specify a default value for the metric of redistributed routes.

This field displays the default metric if one has already been set, or 0 if one was not configured earlier. The valid values are 1 to 15.

14. Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 138. RIP Advanced Configuration**

Field	Description
Global Route Changes	The number of route changes made to the IP route database by RIP. This does not include the refresh of a route's age.
Global Queries	The number of responses sent to RIP queries from other systems.

## Configure Advanced RIP Interface Settings

➤ **To configure advanced RIP 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 **Routing > RIP > Advanced > Interface Configuration**.

RIP Interface Configuration						
1 2 3 VLANs All						
<input type="checkbox"/>	Interface	Send Version	Receive Version	RIP Mode	Authentication Type	Authentication Key
<input type="checkbox"/>	1/0/1	RIP-2	Both	Disable	None	
<input type="checkbox"/>	1/0/2	RIP-2	Both	Disable	None	
<input type="checkbox"/>	1/0/3	RIP-2	Both	Disable	None	



Go To Interface <input type="text"/> <input type="button" value="Go"/>					
Authentication Key ID	Bad Packets Received	Bad Routes Received	Updates Sent	IP Address	Link State
<input type="text"/>					
0				0.0.0.0	
0				0.0.0.0	
0				0.0.0.0	
0				0.0.0.0	
0				0.0.0.0	

8. Select the check box next to the **Interface**.
9. In the **Go To Interface** field, enter the Interface in unit/slot/port format and click the **Go** button.

The entry corresponding to the specified interface is selected.

10. From the **Send Version** list, select the version of RIP control packets that the interface will send.

The value is one of the following:

- **None**. No RIP control packets are sent.
- **RIP-1**. Send RIP version 1 formatted packets through broadcast.
- **RIP-1c**. RIP version 1–compatibility mode. Send RIP version 2–formatted packets through broadcast.
- **RIP-2**. Send RIP version 2 packets using multicast. The default is RIP-2.

11. From the **Receive Version** list, select which RIP control packets the interface accepts.

The value is one of the following:

- **RIP-1**. Accept only RIP version 1–formatted packets.
- **RIP-2**. Accept only RIP version 2–formatted packets.
- **Both**. Accept packets in either format. The default is Both.
- **None**. No RIP control packets are accepted.

12. Select **Enable** or **Disable** from the **RIP Mode** list.

Before you enable RIP version 1 or version 1c on an interface, you must first enable network directed broadcast mode on the corresponding interface. The default value is Disable.

13. Select the **Authentication Type** from the list.

The types are as follows:

- **None**. This is the initial interface state. If you select this option, no authentication protocols are run.
- **Simple**. If you select **Simple**, you are prompted to enter an authentication key. This key is included, in the clear, in the RIP header of all packets sent on the network. All routers on the network must be configured with the same key.

- **Encrypt.** If you select **Encrypt**, you are prompted to enter both an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.

**14.** Enter the **RIP Authentication Key** for the specified interface.

If you selected **Authentication Type None**, you are not prompted to enter a key. If you selected **Simple** or **Encrypt**, the key can be up to 16 octets long. The key value is displayed only if you are logged on with read/write privileges.

**15.** Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 139. RIP Advanced Interface Configuration**

Field	Description
Bad Packets Received	The number of RIP response packets received by the RIP process that were subsequently discarded for any reason.
Bad Routes Received	The number of routes in valid RIP packets that were ignored for any reason (for example, unknown address family, or invalid metric).
Updates Sent	The number of triggered RIP updates actually sent on this interface. This explicitly does <i>not</i> include full updates sent containing new information.
IP Address	The IP address of the router interface.
Link State	Indicates whether the RIP interface is up or down.

## Route Redistribution

Use this screen to configure the RIP route redistribution parameters. The allowable values for each field are displayed next to the field. If any invalid values are entered, an alert message is displayed with the list of all the valid values.

➤ **To configure advanced RIP route redistribution 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 > RIP > Advanced > Route Redistribution**.

**Configuration**

Source:    
 Redistribute Mode:    
 Metric:  (0 to 15, 0 to unconfigure)   
 Distribute List:  (0 to 199, 0 to unconfigure)

**Summary**

Source Protocol	Redistribute Mode	Metric	Distribute List	Match Internal	Match External Type 1	Match External Type 2	Match NSSA External Type 1	Match NSSA External Type 2
Connected	Disable	0	0					
Static	Disable	0	0					
OSPF	Disable	0	0	Enable	Disable	Disable	Disable	Disable

The **Source** list is populated by only those source routes that are already configured for redistribution by RIP. This allows you to configure another source route among the available source routes.

8. In the Source list, select a value.

The valid values are as follows:

- Connected
- Static
- OSPF

9. From the **Redistribute Mode** list, select to **Enable** or **Disable** RIP redistribute mode.

The default is Disable.

10. Enter the **Metric** of redistributed routes for the given source route.

The valid values are is 0 to 15; 0 means unconfigure.

11. Use the **Distribute List** field to set the access list that filters the routes to be redistributed by the destination protocol.

Only permitted routes are redistributed. If this command refers to a non-existent access list, all routes are permitted. The valid values for Access List IDs are 0 to 199. When used for route filtering, the only fields in an access list that get used are as follows:

- Source IP address and netmask
- Destination IP address and netmask
- Action (permit or deny)

All other fields (such as Source and Destination Port, Precedence, Tos, and so on) are ignored.

The source IP address is compared to the destination IP address of the route. The source IP netmask in the access list rule is treated as a wildcard mask, indicating which bits in the source IP address must match the destination address of the route.

**Note:** A 1 in the mask indicates a *do not care* in the corresponding address bit.

When an access list rule includes a destination IP address and netmask (an extended access list), the destination IP address is compared to the network mask of the destination of the route. The destination netmask in the access list serves as a wildcard mask, indicating which bits in the route's destination mask are significant for the filtering operation.

**12.** Click the **Apply** button.

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

The following table describes the RIP Route Redistribution nonconfigurable data that is displayed.

**Table 140. RIP Route Redistribution Summary**

Field	Description
Source Protocol	The source route to be redistributed by RIP. The valid values are as follows: <ul style="list-style-type: none"> <li>Connected</li> <li>Static</li> <li>OSPF</li> </ul>
Redistribute Mode	The route redistribution mode for a particular source protocol. By default this is disabled.
Metric	The metric of redistributed routes for the given source route. The field displays 0 when the metric is not configured.
Distribute List	The access list that filters the routes to be redistributed by the destination protocol. The field displays 0 when not configured.
The following list of redistributed routes is valid when <b>OSPF</b> is selected as source. The list can include one or more of:	
Match Internal	Sets internal OSPF routes to be redistributed.
Match External Type 1	Sets external type 1 OSPF routes to be redistributed.
Match External Type 2	Sets external type 2 OSPF routes to be redistributed.
Match NSSA External Type 1	Sets NSSA external type 1 OSPF routes to be redistributed.
Match NSSA External Type 2	Sets NSSA external type 2 OSPF routes to be redistributed.

## 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 Configuration**.

Interface	Advertise Mode	Advertise Address	Maximum Advertise Interval	Minimum Advertise Interval	Advertise Lifetime	Preference Level
<input type="checkbox"/> 1/0/1	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/2	Disable	224.0.0.1	600	450	1800	0
<input type="checkbox"/> 1/0/3	Disable	224.0.0.1	600	450	1800	0

8. Use **Interface** to select 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. Use **Apply** to send the updated configuration to the switch. Configuration changes take effect immediately.

## Configure Virtual Router Redundancy Protocol

Only the following switches support Virtual Redundancy Protocol (VRRP):

- M7100
- M6100
- M5300-28G3
- M5300-52G3
- M5300-28GF3

The following switches support VRRP with an L3 license:

- M5300-28G
- M5300-52G
- M5300-28G-POE+
- M5300-52G-POE+

## Configure Global VRRP Settings

### ➤ To configure the global VRRP 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 > VRRP > Basic > VRRP Configuration**.

The screenshot shows the VRRP Configuration page. Under 'Global Configuration', the 'Admin Mode' is set to 'Disable'. Below this, the 'Table Configuration' section contains a table with the following columns: 'VRID (1 to 255)', 'Interface', 'Interface IP Address', 'Primary IP Address', 'Mode', and 'State'. The table is currently empty, with input fields for each column.

8. In the Global Configuration **Admin Mode** field, set the administrative status of VRRP in the router to either **Enable** or **Disable** option.

By default, VRRP is disabled.

9. The **VRID** field is configurable only if you are creating a new virtual router.

Enter the VRID. The valid values are 1 to 255.

10. Select the unit/slot/port for the new virtual router from the **Interface** list.

11. Enter the **Primary IP Address** of the virtual router.

12. From the **Mode** list, select **Active** or **Inactive** mode for the new virtual router.

13. Click the **Add** button.

The virtual router is added to the switch configuration.

14. To delete the selected virtual router, click the **Delete** button.

**Note:** The router cannot be deleted if there are secondary addresses configured.

15. Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 141. VRRP Global Configuration**

Field	Description
Interface IP Address	Indicates the IP address associated with the selected interface.
State	The current state of the virtual router. Possible values are as follows: <ul style="list-style-type: none"> <li>• Initialize</li> <li>• Master</li> <li>• Backup</li> </ul>

## Configure Advanced VRRP Settings

➤ To configure the advanced VRRP 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 **Routing > VRRP > Advanced > VRRP Configuration**.

Global Configuration

Admin Mode ☒ Disable ☐ Enable

Table Configuration

<input type="checkbox"/>	VRID (1 to 255)	Interface	Pre-empt Mode	Accept Mode	Configured Priority (1 to 254)	Operational Priority	Advertisement Interval (secs) (1 to 255)
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>		<input type="text"/>

Interface IP Address	Owner	VMAC Address	Primary IP Address	Authentication Type	Authentication Data	Status	State
			<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	

8. In the Global Configuration **Admin Mode** field, set the administrative status of VRRP in the router to either **Enable** or **Disable**.

By default, VRRP is disabled.

9. Enter the **VRID**.



The **VRID** field is configurable only if you are creating a new virtual router. The valid values are 1 to 255.

10. Select the unit/slot/port for the new virtual router from the **Interface** list.

11. In the **Preempt Mode** field, select the **Enable** or **Disable** option.

If you select **Enable**, a backup router preempts the master router if it has a priority greater than the master virtual router's priority, provided the master is not the owner of the virtual router IP address. The default is Enable.

12. In the **Accept Mode** field, select the **Enable** or **Disable** option.

If you select **Enable**, the VRRP master accepts all types of data packets addressed to IP addresses associated with the virtual router. If you select **Disable**, the VRRP master discards all types of data packets addressed to IP addresses associated with the virtual router, if it is not the IP address owner. The default is Disable.

13. Enter the **Configured Priority value** to be used by the VRRP router in the election for the master virtual router.

The valid values are 1 to 254. If the virtual IP address is the same as the interface IP address, the priority gets set to 254, no matter what you enter.

14. In the **Advertisement Interval** field, enter the time, in seconds, between the transmission of advertisement packets by this virtual router.

Enter a number from 1 to 255. The default value is 1 second.

15. Enter the **Primary IP Address**, the IP address associated with the virtual router.

The default is 0.0.0.0.

16. From the **Authentication Type** list, select the type of authentication for the virtual router.

The options are as follows:

- **0-None.** No authentication is performed. The default is None.
- **1-Simple.** Authentication is performed using a text password.

17. If you selected simple authentication, enter the password in the **Authentication Data** field.

18. In the **Status** field, select the **Active** or **Inactive** option to start or stop the operation of the virtual router.

The default is inactive.

19. Click the **Add** button.

The virtual router is added to the switch configuration.

20. To delete the selected virtual router, click the **Delete** button.

**Note:** The router cannot be deleted if there are secondary addresses configured.

21. Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 142. Advanced VRRP Global Configuration**

Field	Description
Operational Priority	<p>Indicates the priority to be used for the virtual router master election process. Higher values imply higher priority.</p> <ul style="list-style-type: none"> <li>A priority of 0 is sent by the master router to indicate that this router has ceased to participate in VRRP and a backup virtual router transitions to become a new master.</li> <li>A priority of 255 is used for the router that owns the associated IP addresses.</li> </ul>
Interface IP Address	Indicates the IP address associated with the selected interface.
Owner	Set to <b>True</b> if the virtual IP address and the interface IP address are the same, otherwise set to <b>False</b> . If this parameter is set to True, the virtual router is the owner of the virtual IP address, and always wins an election for master router when it is active.
VMAC Address	The virtual MAC address associated with the virtual router, composed of a 24-bit organizationally unique identifier, the 16-bit constant identifying the VRRP address block and the 8-bit VRID.
State	<p>The current state of the virtual router. Possible values are as follows:</p> <ul style="list-style-type: none"> <li>Initialize</li> <li>Master</li> <li>Backup</li> </ul>

## Configure an Advanced VRRP Secondary IP Address

### ➤ To configure the advanced VRRP secondary IP address 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 > VRRP > Advanced > VRRP Secondary IP Address Configuration**.

Routing Interface	
VRRP Interface	<input type="text"/>
VRRP ID	<input type="text"/>
VRRP Secondary IP Address Configuration	
Primary IP Address	Secondary IP Address
<input type="checkbox"/> <input type="text"/>	<input type="text"/>

8. In the **VRRP Interface - VRRP ID** field, select one of the existing virtual routers, listed by interface number and VRRP ID.
9. In the **Secondary IP Address** field, enter the IP address for the interface.  
This address must be a member of one of the subnets currently configured on the interface. This value is read-only once configured.

10. Click the **Add** button.

The secondary IP address is added to the selected VRRP interface.

11. To delete the selected secondary IP address interface., click the **Delete** button

12. Click the **Apply** button.

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

The **Primary IP Address** field displays the primary IP address of the virtual router.

## Configure an Advanced VRRP Tracking Interface

### ➤ To configure an advanced VRRP tracking 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 **Routing > VRRP > Advanced > VRRP Tracking Configuration**.

**Routing Interface**

VRRP Interface

VRRP ID

**VRRP Tracking Interface Configuration**

Tracked Interface		
<input type="checkbox"/> Tracked Interface	Priority Decrement	Tracked Interface State
<input type="text" value="▼"/>	<input type="text"/>	

8. In the **VRRP Interface - VRRP ID** field, select a virtual router.

The virtual routers are listed by interface number and VRRP ID.

9. Select a routing interface from the **Tracked Interface** field.

This lists all routing interfaces that are not yet tracked for this VRRP ID and interface configuration. The exceptions to this list are loopback and tunnels that could not be tracked.

10. Enter the **Priority Decrement** for the tracked interface.

The valid range is 1 to 254. The default value is 10.

The nonconfigurable field, **Tracked Interface State**, displays the state of the tracked interface.

**VRRP Tracking Route Configuration**

Tracked Route			
<input type="checkbox"/> Tracked Route Prefix	Tracked Route Prefix Length	Priority Decrement	Reachable
<input type="text"/>	<input type="text"/>	<input type="text"/>	

11. In the **Tracked Route Prefix** field, enter the prefix of the route.

12. In the **Tracked Route Prefix Length** field, enter the prefix length of the route.

13. Enter the **Priority Decrement** for the route.

The valid range is 1 to 254. The default value is 10.

The nonconfigurable **Reachable** field displays the reachability of the tracked route.

14. Click the **Add** button.

The traced interface or tracked route is added to the VRRP.

15. To delete the selected tracked interface or tracked route, click the **Delete** button.

16. Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 143. Advanced VRRP Tracking Configuration**

Field	Description
Tracked Interface State	The state of the tracked interface.
Reachable	The reachability of the tracked route.

## View Advanced VRRP Statistics

### ➤ To view advanced VRRP 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 > VRRP > Advanced > VRRP Statistics**.

Global Statistics						
Router Checksum Errors	0					
Router Version Errors	0					
Router VRID Errors	0					
Statistics						
VRRP ID	Interface	Up Time	State Transitioned to Master	Advertisement Received	Advertisement Interval Errors	Authentication Failure

IP TTL Errors	Zero Priority Packets Received	Zero Priority Packets Sent	Invalid Type Packets Received	Address List Errors	Invalid Authentication Type	Authentication Type Mismatch	Packet Length Errors
---------------	--------------------------------	----------------------------	-------------------------------	---------------------	-----------------------------	------------------------------	----------------------

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 144. Advanced VRRP Statistics**

Field	Description
Global Statistics	
Router Checksum Errors	The total number of VRRP packets received with an invalid VRRP checksum value.
Router Version Errors	The total number of VRRP packets received with an unknown or unsupported version number.
Router VRID Errors	The total number of VRRP packets received with an invalid VRID for this virtual router.
Statistics	
VRRP ID	The VRID for the selected virtual router.
Interface	The unit/slot/port for the selected virtual router.
Up Time	The time, in days, hours, minutes and seconds, that elapsed since the virtual router transitioned to the initialized state.
State Transitioned to Master	The total number of times that this virtual router's state transitioned to Master.
Advertisement Received	The total number of VRRP advertisements received by this virtual router.

**Table 144. Advanced VRRP Statistics (continued)**

Field	Description
Advertisement Interval Errors	The total number of VRRP advertisement packets received for which the advertisement interval was different from the one configured for the local virtual router.
Authentication Failure	The total number of VRRP packets received that did not pass the authentication check.
IP TTL Errors	The total number of VRRP packets received by the virtual router with IP Time-To-Live (TTL) not equal to 255.
Zero Priority Packets Received	The total number of VRRP packets received by the virtual router with a priority of 0.
Zero Priority Packets Sent	The total number of VRRP packets sent by the virtual router with a priority of 0.
Invalid Type Packets Received	The number of VRRP packets received by the virtual router with an invalid value in the Type field.
Address List Errors	The total number of packets received for which the address list does not match the locally configured list for the virtual router.
Invalid Authentication Type	The total number of packets received with an unknown authentication type.
Authentication Type Mismatch	The total number of packets received with an authentication type different from the locally configured authentication method.
Packet Length Errors	The total number of packets received with a packet length less than the length of the VRRP header.

## 6. OSPF and OSPFv3

---

This chapter covers the following topics:

- *OSPF*
- *OSPFv3*



## OSPF

Only the following switches support OSPF:

- M6100
- M5300-28G3
- M5300-52G3
- M5300-28GF3

The following switches support OSPF with an L3 license:

- M5300-28G
- M5300-52G
- M5300-28G-POE+
- M5300-52G-POE+

## Configure Basic OSPF Settings

### ➤ To configure basic OSPF 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 > OSPF > Basic > OSPF Configuration**.



OSPF Configuration	
Admin Mode	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Router ID	<input type="text" value="0.0.0.0"/>

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

If you select Enable, OSPF is activated for the switch. By default, OSPF is enabled. You must configure a router ID before OSPF can become operational. Use the IP Configuration screen to configure a router ID or issue the CLI command **config router id**. For more information, see [Configure the Router IP](#) on page 325.

The **Router ID** displays the 32-bit integer in dotted-decimal format that uniquely identifies the router within the autonomous system (AS).

To change the router ID, you must first disable OSPF. After you set the new router ID, you must reenabling OSPF for the change to take effect. The default value is 0.0.0.0, although this is not a valid router ID.

9. Click the **Apply** button.

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

## Configure the OSPF Default Route Advertise Settings

### ➤ To configure default route advertise 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 > OSPF > Advanced > OSPF Configuration**.

Default Route Advertise Configuration	
Default Information Originate	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Always	<input type="radio"/> True <input checked="" type="radio"/> False
Metric	<input type="text" value="0"/> (0 to 16777214)
Metric Type	<input type="radio"/> External Type 1 <input checked="" type="radio"/> External Type 2

OSPF Configuration		
Router ID	<input type="text" value="0.0.0.0"/>	
Admin Mode	<input type="button" value="Enable"/>	
ASBR Mode	<input type="button" value="Disable"/>	
RFC 1583 Compatibility	<input type="button" value="Enable"/>	
ABR Status	<input type="button" value="Enable"/>	
Opaque LSA Status	<input type="button" value="Enable"/>	
Exit Overflow Interval (secs)	<input type="text" value="0"/>	(0 to 2147483647)
SPF Delay Time(secs)	<input type="text" value="5"/>	(0 to 65535)
SPF Hold Time(secs)	<input type="text" value="10"/>	(0 to 65535)
External LSA Count	<input type="text" value=""/>	
External LSA Checksum	<input type="text" value=""/>	
AS_OPAQUE LSA Count	<input type="text" value=""/>	
AS_OPAQUE LSA Checksum	<input type="text" value=""/>	
New LSAs Originated	<input type="text" value=""/>	
LSAs Received	<input type="text" value=""/>	
External LSDB Limit	<input type="text" value="-1"/>	(-1 to 2147483647)
Default Metric	<input type="text" value="0"/>	(0 to 16777214)
Maximum Paths	<input type="text" value="4"/>	(1 to 4)
AutoCost Reference Bandwidth	<input type="text" value="100"/>	(1 to 4294967)
Default Passive Setting	<input type="button" value="Disable"/>	

8. In the **Default Information Originate** field, select the **Enable** or **Disable** option.

If you select **Enable**, OSPF originates an external LSA advertising a default route (0.0.0.0/0.0.0.0). Default Information Originate is disabled by default.

9. In the **Always** field, select **True** or **False**.

If **Default Information Originate** is enabled, but the **Always** option is **False**, OSPF originates a default route only if a default route is already in the router's routing table.

Set **Always** to **True** to force OSPF to originate a default route regardless of whether a default route already exists. The default is **False**.

10. In the **Metric** field, specify the metric of the default route.

The valid values range from 0 to 16777214. The default is 0.

11. In the **Metric Type** field, select the OSPF metric type of the default route.

Two types are supported: **External Type 1** and **External Type 2**. The default is **External Type 2**.

12. Click the **Apply** button.

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

??? Does this need to be a separate procedure? What should I put in for the navigation and screen shot?

## Configure OSPF Settings

➤ **To configure the OSPF 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 > OSPF > Advanced > OSPF Configuration**.

OSPF Configuration		
Router ID	<input type="text" value="0.0.0.0"/>	
Admin Mode	<input type="button" value="Enable"/> ▾	
ASBR Mode	<input type="button" value="Disable"/>	
RFC 1583 Compatibility	<input type="button" value="Enable"/> ▾	
ABR Status	<input type="button" value=""/>	
Opaque LSA Status	<input type="button" value="Enable"/> ▾	
Exit Overflow Interval (secs)	<input type="text" value="0"/>	(0 to 2147483647)
SPF Delay Time(secs)	<input type="text" value="5"/>	(0 to 65535)
SPF Hold Time(secs)	<input type="text" value="10"/>	(0 to 65535)
External LSA Count	<input type="button" value=""/>	
External LSA Checksum	<input type="button" value=""/>	
AS_OPAQUE LSA Count	<input type="button" value=""/>	
AS_OPAQUE LSA Checksum	<input type="button" value=""/>	
New LSAs Originated	<input type="button" value=""/>	
LSAs Received	<input type="button" value=""/>	
External LSDB Limit	<input type="text" value="-1"/>	(-1 to 2147483647)
Default Metric	<input type="text" value="0"/>	(0 to 16777214)
Maximum Paths	<input type="text" value="4"/>	(1 to 4)
AutoCost Reference Bandwidth	<input type="text" value="100"/>	(1 to 4294967)
Default Passive Setting	<input type="button" value="Disable"/> ▾	

8. In the **Router ID** field, enter the 32-bit integer in dotted-decimal format that uniquely identifies the router within the autonomous system (AS).

To change the router ID, you must first disable OSPF. After you set the new router ID, you must reenabling OSPF for the change to take effect. The default value is 0.0.0.0, although this is not a valid router ID.

9. In the **Admin Mode** field, select **Enable** or **Disable**.

If you select **Enable**, OSPF is activated for the switch. The default value is Enable. You must configure a router ID before OSPF can become operational. You do this on the IP Configuration screen, or by issuing the CLI command `config router id`. For more information, see [Configure the Router IP](#) on page 325.

10. In the **RFC 1583 Compatibility** field, select **Enable** or **Disable**.

This specifies the preference rules that are used when choosing among multiple AS-external-LSAs advertising the same destination. If you select **Enable**, the preference rules are those defined in Section 16.4.1 of the OSPF-2 standard (RFC 2328), which prevents routing loops when AS-external-LSAs for the same destination originated from different areas. The default value is Enable. All routers in the OSPF domain must be

configured the same. If all OSPF routers are capable of operating according to RFC 2328, **RFC 1583 Compatibility** must be disabled.

11. Set the **Opaque LSA Status** to **Enable** if OSPF will store and flood opaque LSAs.

An opaque LSA is used for flooding user-defined information within an OSPF router domain.

12. When the number of nondefault external LSAs exceeds a configured limit, the router enters an overflow state as defined in RFC 1765.

Use the **Exit Overflow Interval** field to specify how long in seconds OSPF must wait before attempting to leave overflow state. In overflow state, OSPF cannot originate nondefault external LSAs. If the Exit Overflow Interval is 0, OSPF does not leave the overflow state until it is disabled and reenabled. The range is 0 to 2,147,483,647 seconds. The default is 0.

13. Configure the **SPF Delay Time**.

This is the number of seconds from when OSPF receives a topology change to the start of the next SPF calculation. Delay Time is an integer from 0 to 65535 seconds. The default is 5 seconds. A value of 0 means that there is no delay; that is, the SPF calculation is started upon a topology change.

14. Configure the **SPF Hold Time**.

This is the minimum time in seconds between two consecutive SPF calculations. The range is 0 to 65,535 seconds. The default time is 10 seconds. A value of 0 means that there is no delay; that is, two SPF calculations can be done, one immediately after the other.

15. Use the **External LSDB Limit** field to set the number of the external LSDB limit for OSPF.

If the value is -1, then there is no limit. When the number of nondefault AS-external-LSAs in a router's link state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit none-default AS-external-LSAs in the database. The external LSDB limit must be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area. The range for the External LSDB Limit field is -1 to 2147483647. The default value is -1.

16. Use the **Default Metric** field to set a default for the metric of redistributed routes.

This field is blank if a default metric was not configured. The range of valid values is 1 to 16777214. The default value is 0.

17. Use the **Maximum Paths** field to set the number of paths that OSPF can report for a given destination.

The range of valid values is 1 to 16. The default value is 4.

18. Configure the **AutoCost Reference Bandwidth** to control how OSPF calculates link cost.

Specify the reference bandwidth in megabits per second. Unless a link cost is configured, the link cost is computed by dividing the reference bandwidth by the interface bandwidth. The range is 1 to 4294967. The default is 100.

19. In the **Default Passive Setting** field, select **Enable** or **Disable** from the list to configure the global passive mode setting for all OSPF interfaces.

Configuring this field overwrites any present interface level passive mode setting. OSPF does not form adjacencies on passive interfaces, but does advertise attached networks as stub networks. The default is Disabled.

20. Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 145. OSPF Configuration**

Field	Description
ASBR Mode	The router is an autonomous system boundary router if it is configured to redistribute routes from another protocol, or if it is configured to originate an external LSA advertising the default route.
ABR Status	The router is an autonomous system boundary router if it is configured to redistribute routes from another protocol, or if it is configured to originate an external LSA advertising the default route.
External LSA Count	The number of external (LS type 5) LSAs (link state advertisements) in the link state database.
External LSA Checksum	The sum of the LS checksums of the external LSAs (link state advertisements) contained in the link state database. This sum can be used to determine if there was a change in a router's link state database, and to compare the link state databases of two routers. This value is in hexadecimal.
AS_OPAQUE LSA Count	The number of opaque LSAs with domain-wide flooding scope.
AS_OPAQUE LSA Checksum	The sum of the LS checksums of the opaque LSAs with domain wide flooding scope. This sum can be used to determine if there was a change in a router's link state database, and to compare the link state databases of two routers. This value is in hexadecimal.
New LSAs Originated	In any given OSPF area, a router originates several LSAs. Each router originates a router-LSA. If the router is also the designated router for any of the area's networks, it originates network LSAs for those networks. This value represents the number of LSAs originated by this router.
LSAs Received	The number of LSAs (link state advertisements) received that were determined to be new instantiations. This number does not include newer instantiations of self-originated LSAs.

## Configure the OSPF Common Area ID

➤ **To configure the area ID:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > OSPF > Advanced > Common Area Configuration**.

OSPFv3 Common Area Configuration							
<input type="checkbox"/>	Area ID	External Routing	SPF Runs	Area Border Router Count	Area LSA Count	Area LSA Checksum	Import Summary LSAs
	<input type="text"/>						

8. Enter the OSPF **Area ID**.

An area ID is a 32-bit integer in dotted-decimal format that uniquely identifies the area to which a router interface connects.

9. Click the **Add** button.

The area ID is added.

10. To delete a selected area ID, click the **Delete** button.



The following table describes the nonconfigurable data that is displayed.

**Table 146. OSPF Common Area Configuration**

Field	Description
External Routing	A definition of the router's capabilities for the area, including whether or not AS-external-LSAs are flooded into/throughout the area. If the area is a stub area, then these are the possible options for which you can configure the external routing capability; otherwise, the only option is <i>Import External LSAs</i> . <ul style="list-style-type: none"> <li>• Import External LSAs. Import and propagate external LSAs.</li> <li>• Import No LSAs. Do not import and propagate external LSAs.</li> </ul>
SPF Runs	The number of times that the intra-area route table was calculated using this area's link state database. This is typically done using Dijkstra's algorithm.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.
Area LSA Count	The total number of link state advertisements in this area's link state database, excluding AS external LSAs.
Area LSA Checksum	The 32-bit unsigned sum of the link state advertisements' LSA checksums contained in this area's link state database. This sum excludes external (LSA type 5) link state advertisements. The sum can be used to determine if there was a change in a router's link state database, and to compare the link state database of two routers.
Flood List Length	This is the number of LSAs on this area's flood list.
Import Summary LSAs	The summary LSAs are imported into this area.

## Configure the OSPF Stub Area

### ➤ To configure the OSPF stub area:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > OSPF > Advanced > Stub Area Configuration**.

Area ID	SPF Runs	Area Border Router Count	Area LSA Count	Area LSA Checksum	Import Summary LSAs	Default Cost	Type of Service
<input type="text"/>					<input type="text" value="v"/>	<input type="text"/>	

8. Enter the OSPF **Area ID**.

An area ID is a 32-bit integer in dotted-decimal format that uniquely identifies the area to which a router interface connects.

9. Configure the **Import Summary LSAs** by selecting **Enable** or **Disable** from the list.

If you select **Enable**, summary LSAs are imported into stub areas.

10. Configure the **Default Cost** by entering the metric value to be applied for the default route advertised to the stub area.

The valid values range from 1 to 16,777,215.

11. Click the **Add** button.

The area is configured as a stub area.

12. To delete the stub area designation, click the **Delete** button.

The area is returned to normal state.

13. Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 147. OSPF Stub Area Configuration**

Field	Description
SPF Runs	The number of times that the intra-area route table was calculated using this area's link state database. This is typically done using Dijkstra's algorithm.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.
Area LSA Count	The total number of link state advertisements in this area's link state database, excluding AS external LSAs.

Table 147. OSPF Stub Area Configuration (continued)

Field	Description
Area LSA Checksum	The 32-bit unsigned sum of the link state advertisements' LSA checksums contained in this area's link state database. This sum excludes external (LSA type 5) link state advertisements. The sum can be used to determine if there was a change in a router's link state database, and to compare the link state database of two routers.
Type of Service	This field is the normal ToS associated with the stub metric.

## Configure the OSPF NSSA Area

### ➤ To configure the NSSA area:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > OSPF > Advanced > NSSA Area Configuration**.

OSPF NSSA Area Configuration						
<input type="checkbox"/>	Area ID	SPF Runs	Area Border Router Count	Area LSA Count	Area LSA Checksum	Import Summary LSAs
	<input type="text"/>					<input type="text" value="v"/>

Default Information Originate			Translator Role	Translator Stability Interval	Redistribute Mode	Translator State
Admin Mode	Metric Value	Metric Type				
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

**8. Enter the OSPF Area ID.**

An area ID is a 32-bit integer in dotted-decimal format that uniquely identifies the area to which a router interface connects.

**9. Configure the Import Summary LSAs by selecting Enable or Disable from the list.**

If you select **Enable**, summary LSAs are imported into NSSA areas.

**10. Configure the Default Information Originate.**

This option permits you to advertise a default route into the NSSA when Import Summary LSAs is disabled. This can also be applied by the CLI command **area (area-id) NSSA default-info-originate** in the IP router OSPF config mode.

- a. In the **Admin Mode** list, select to **Enable** or **Disable** the default information originate.
- b. In the **Metric Value** field, set the default metric value for default information originate. The value range of values is 1 to 16777214.
- c. In the **Metric Type** field, select the type of metric specified in the Metric Value field. Options are as follows:
  - **Comparable Cost.** External type 1 metrics that are comparable to the OSPF metric.
  - **Non-comparable Cost.** External type 2 metrics that are assumed to be larger than the cost of the OSPF metric.

**11. Select the Translator Role of the NSSA.**

Options are as follows:

- a. **Always.** Cause the router to assume the role of the translator the instant it becomes a border router.
- b. **Candidate.** Cause the router to participate in the translator election process when it attains border router status.

**12. In the Translator Stability Interval field, configure the translator of the NSSA.**

The value is the period of time that an elected translator continues to perform its duties after it determines that its translator status was deposed by another router. The valid range is 0 to 3600.

**13. In the Redistribute Mode field, select Enable or Disable from the list.**

This configures the NSSA ABR so that learned external routes are redistributed to the NSSA.

**14. Click the Add button.**

The area is configured as an NSSA area.

15. To delete the NSSA area designation, click the **Delete** button.

The area is returned to normal state.

16. Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 148. OSPF NSSA Area Configuration**

Field	Description
SPF Runs	The number of times that the intra-area route table was calculated using this area's link state database. This is typically done using Dijkstra's algorithm.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.
Area LSA Count	The total number of link state advertisements in this area's link state database, excluding AS external LSAs.
Area LSA Checksum	The 32-bit unsigned sum of the link state advertisements' LSA checksums contained in this area's link state database. This sum excludes external (LSA type 5) link state advertisements. The sum can be used to determine if there was a change in a router's link state database, and to compare the link state database of two routers.
Translator State	This field displays if and how the NSSA border router translates Type 7 into Type 5. Possible options are as follows: <ul style="list-style-type: none"> <li>• <b>Enabled.</b> The NSSA border router's translator role is set to always.</li> <li>• <b>Elected.</b> The candidate NSSA border router is translating Type 7 LSAs into Type 5.</li> <li>• <b>Disabled.</b> The candidate NSSA border router is not translating Type 7 LSAs into Type 5.</li> </ul>

## Configure the OSPF Area Range

### ➤ Configure the OSPF area range:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > OSPF > Advanced > Area Range Configuration**.

OSPF Area Range Configuration					
<input type="checkbox"/>	Area ID	IP Address	Subnet Mask	LSDB Type	Advertise
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="Network Summary"/>	<input type="text" value="Enable"/>

8. Enter the OSPF **Area ID**.

An area ID is a 32-bit integer in dotted-decimal format that uniquely identifies the area to which a router interface connects.

9. Enter the **IP Address** for the address range for the selected area.
10. Enter the **Subnet Mask** for the address range for the selected area.
11. From the list in the **LSDB Type** field, select the type of link advertisement associated with the specified area and address range.

Options are as follows: **Network Summary** or **NSSA External**. The default type is Network Summary.

12. In the **Advertise** list, select **Enable** or **Disabl**.

If you select **Enable**, the address range is advertised outside the area through a network summary LSA. The default is Enable.

13. Click the **Add** button.

The new address range is added.

14. To remove the specified address range from the area configuration, click the **Delete** button.

15. Click the **Apply** button.

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

## Configure the OSPF Interface

### ➤ To configure the OSPF 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 **Routing > OSPF > Advanced > Interface Configuration**.

OSPF Interface Configuration

1 2 3 VLANs All

<input type="checkbox"/>	Interface	IP Address	Subnet Mask	Area ID	Admin Mode	Router Priority	Retransmit Interval	Hello Interval
<input type="checkbox"/>	1/0/1	0.0.0.0	0.0.0.0	0	Disable	1	5	10
<input type="checkbox"/>	1/0/2	0.0.0.0	0.0.0.0	0	Disable	1	5	10
<input type="checkbox"/>	1/0/3	0.0.0.0	0.0.0.0	0	Disable	1	5	10

Dead Interval	ltransit Delay Interval	LSA Ack Interval (secs)	MTU Ignore	Passive Mode	Network Type	Authentication Type	Authentication Key
40	1	1	Disable	Disable	Broadcast	None	
40	1	1	Disable	Disable	Broadcast	None	
40	1	1	Disable	Disable	Broadcast	None	
40	1	1	Disable	Disable	Broadcast	None	
40	1	1	Disable	Disable	Broadcast	None	

Go To Interface

Authentication Key ID	State	Designated Router	Backup Designated Router	Number of Link Events	Local Link LSAs	Local Link LSA Checksum	Metric Cost
							1
							1
							1
							1
							1

8. In the **Go To Interface** field, enter the interface in unit/slot/port format and click the **Go** button.

The entry corresponding to the specified interface is selected.

9. Select the check box next to the **Interface**.

10. In the OSPF **Area ID** field, enter the 32-bit integer in dotted-decimal format.

This ID uniquely identifies the OSPF area to which the selected router interface connects. If you assign an area ID that does not exist, the area is created with default values.

**11. In the Admin Mode list, select Enable or Disable.**

The default value is **Disable**. You can configure OSPF parameters without enabling OSPF admin mode, but the change does not take effect until you enable admin mode. The following information is displayed only if admin mode is enabled:

- State
- Designated router
- Backup designated router
- Number of link events
- LSA Ack interval
- Metric cost

For OSPF to be fully functional, you must enter a valid ID address and subnet mask using either the **IP Interface Configuration** screen or the CLI command **config ip interface network**. For more information, see [Configure the IP Interface](#) on page 336.

**Note:** Once OSPF is initialized on the router, it remains initialized until the router is reset.

**12. In the Router Priority field, enter the OSPF priority for the selected interface.**

The priority of an interface is specified as an integer from 0 to 255. The default is 1, which is the highest router priority. A value of 0 indicates that the router is not eligible to become the designated router on this network.

**13. Configure the Retransmit Interval by entering the OSPF retransmit interval for the specified interface.**

This is the number of seconds between link state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link state request packets. The valid values range from 1 to 3600 seconds (1 hour). The default is 5 seconds.

**14. Configure the Hello Interval by entering the OSPF hello interval for the specified interface in seconds.**

This parameter must be the same for all routers attached to a network. Values range from 1 to 65,535. The default is 10 seconds.

**15. Enter the OSPF Dead Interval for the specified interface in seconds.**

This specifies how long a router waits to see a neighbor router's hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value must be a multiple of the hello interval (for example, 4). The valid values range from 1 to 65,535. The default is 40 seconds.

**16. In the Iftransit Delay Interval field, enter the OSPF transit delay for the specified interface.**

This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. The valid values range from 1 to 3600 seconds (1 hour). The default value is 1 second.



17. Configure **MTU Ignore** by selecting **Enable** or **Disable** from the list.

MTU Ignore disables OSPF MTU mismatch detection on received database description packets. The default value is Disable (MTU mismatch detection is enabled).

18. Configure **Passive Mode** by selecting **Enable** or **Disable** from the list.

Make an interface passive to prevent OSPF from forming an adjacency on an interface. OSPF advertises networks attached to passive interfaces as stub networks. Interfaces are not passive by default, meaning that the passive mode default is Disable.

19. In the OSPF **Network Type** list, select **Broadcast** or **Point-to-Point**.

OSPF selects a designated router and originates network LSAs only for broadcast networks. No more than two OSPF routers can be present on a point-to-point link. The default network type for Ethernet interfaces is broadcast.

20. Select an **Authentication Type** other than **None** by selecting from the list.

The choices are as follows:

- **None.** This is the initial interface state. If you select this option from the list, no authentication protocols are run. The default is None.
- **Simple.** You are prompted to enter an authentication key. This key is included, in the clear, in the OSPF header of all packets sent on the network. All routers on the network must be configured with the same key.
- **Encrypt.** You are prompted to enter an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.

21. Enter the **Authentication Key ID** to be used for authentication.

You are prompted to enter an ID only if you select Encrypt as the authentication type. The ID is a number between 0 and 255, inclusive.

22. In the **Metric Cost** field, enter the link cost.

OSPF uses this value in computing shortest paths. The range is from 1 to 65,535. The default is 1.

23. Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 149. OSPF Interface Configuration**

Field	Description
IP Address	The IP address of the interface.
Subnet Mask	The network mask, indicating the portion of the IP address that identifies the attached network.

Table 149. OSPF Interface Configuration (continued)

Field	Description
LSA Ack Interval (secs)	The number of seconds to wait before sending a delayed acknowledgement.
State	<p>The state of the selected router interface. State is one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Down.</b> This is the initial interface state. The lower-level protocols indicated that the interface is unusable. Interface parameters are set to their initial values. All interface timers are disabled, and there are no adjacencies associated with the interface.</li> <li>• <b>Loopback.</b> The router's interface to the network is looped back either in hardware or software. The interface is unavailable for regular data traffic. You can get information on the quality of this interface by sending ICMP pings to the interface or through something like a bit error test. For this reason, IP packets can still be addressed to an interface in loopback state. To facilitate this, such interfaces are advertised in router- LSAs as single host routes, whose destination is the IP interface address.</li> <li>• <b>Waiting.</b> The router is trying to determine the identity of the backup designated router for the network by monitoring received hello packets. The router cannot elect a backup designated router or a designated router until it transitions out of the waiting state. This prevents unnecessary changes of the backup designated router.</li> <li>• <b>Designated Router.</b> This router is the designated router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network LSA for the network node. The network LSA contains links to all routers (including the designated router) attached to the network.</li> <li>• <b>Backup Designated Router.</b> This router is the backup designated router on the attached network. It is promoted to designated router if the present designated router fails. The router establishes adjacencies to all other routers attached to the network. The backup designated router performs slightly different functions during the LSA flooding, as compared to the designated router.</li> <li>• <b>Other Designated Router.</b> The interface is connected to a broadcast on which other routers are the designated router and backup designated router. The router attempts to form adjacencies to both the designated router and the backup designated router.</li> </ul>
Designated Router	The identity of the designated router for this network, in the view of the advertising router. The designated router is identified here by its router ID. The value 0.0.0.0 means that there is no designated router. This field displays only if the OSPF admin mode is enabled.
Backup Designated Router	The identity of the backup designated router for this network, in the view of the advertising router. The backup designated router is identified here by its router ID. Set to 0.0.0.0 if there is no backup designated router.
Number of Link Events	The number of times the specified OSPF interface changed its state.
Local Link LSAs	The number of opaque LSAs whose flooding scope is the link on this interface.
Local Link LSA Checksum	The sum of the checksums of local link LSAs for this link.

## View OSPF Statistics for an Interface

If OSPF is enabled, you can view statistics for the selected interface.

➤ **To view OSPF statistics 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 **Routing > OSPF > Advanced > Interface Statistics**.

The screenshot shows two side-by-side panels from a web management interface.

**Left Panel: OSPF Interface Selection**

- Interface: 1/0/1 (dropdown menu)
- OSPF Interface Statistics** (Section Header)
- OSPF Area ID
- Area Border Router Count
- AS Border Router Count
- Area LSA Count
- IP Address
- Interface Events
- Virtual Events
- Neighbor Events
- Sent Packets
- Received Packets
- Discards
- Bad Version
- Source Not On Local Subnet
- Virtual Link Not Found
- Area Mismatch
- Invalid Destination Address
- Wrong Authentication Type
- Authentication Failure
- No Neighbor at Source Address
- Invalid OSPF Packet Type
- Hellos Ignored
- Hellos Sent
- Hellos Received
- DD Packets Sent

**Right Panel:**

- DD Packets Received
- LS Requests Sent
- LS Requests Received
- LS Updates Sent
- LS Updates Received
- LS Acknowledgements Sent
- LS Acknowledgements Received

8. In the OSPF Interface Selection area of the screen, from the list in the **Interface** field, select the interface for which data is to be displayed.

To clear all the statistics of the OSPF interface, click the **Clear** button.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable OSPF Interface Statistics data that is displayed.

**Table 150. OSPF Interface Statistics**

Field	Description
OSPF Area ID	The OSPF area to which the selected router interface belongs. An OSPF area ID is a 32 bit integer in dotted-decimal format that uniquely identifies the area to which the interface connects.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.
AS Border Router Count	The total number of autonomous system border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.
Area LSA Count	The total number of link state advertisements in this area's link state database, excluding AS external LSAs.
IP Address	The IP address of the interface.
Interface Events	The number of times the specified OSPF interface changed its state, or an error occurred.
Virtual Events	The number of state changes or errors that occurred on this virtual link.
Neighbor Events	The number of times this neighbor relationship changed state, or an error occurred.
Sent Packets	The number of OSPF packets transmitted on the interface.
Received Packets	The number of valid OSPF packets received on the interface.
Discards	The number of received OSPF packets discarded because of an error in the packet or an error in processing the packet.
Bad Version	The number of received OSPF packets whose version field in the OSPF header does not match the version of the OSPF process handling the packet.
Source Not on Local Subnet	The number of received packets discarded because the source IP address is not within a subnet configured on a local interface.
Virtual Link Not Found	The number of received OSPF packets discarded where the ingress interface is in a non-backbone area and the OSPF header identifies the packet as belonging to the backbone, but OSPF does not have a virtual link to the packet's sender.

Table 150. OSPF Interface Statistics (continued)

Field	Description
Area Mismatch	The number of OSPF packets discarded because the area ID in the OSPF header is not the area ID configured on the ingress interface.
Invalid Destination Address	The number of OSPF packets discarded because the packet's destination IP address is not the address of the ingress interface and is not the AllDrouters or AllSpfRouters multicast addresses.
Wrong Authentication Type	The number of packets discarded because the authentication type specified in the OSPF header does not match the authentication type configured on the ingress interface.
Authentication Failure	The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor.
No Neighbor at Source Address	The number of OSPF packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor.
Invalid OSPF Packet Type	The number of OSPF packets discarded because the packet type field in the OSPF header is not a known type.
Hellos Ignored	The number of received hello packets that were ignored by this router from the new neighbors after the limit was reached for the number of neighbors on an interface or on the system as a whole.
Hellos Sent	The number of hello packets sent on this interface by this router.
Hellos Received	The number of hello packets received on this interface by this router.
DD Packets Sent	The number of database description packets sent on this interface by this router.
DD Packets Received	The number of database description packets received on this interface by this router.
LS Requests Sent	The number of LS requests sent on this interface by this router.
LS Requests Received	The number of LS requests received on this interface by this router.
LS Updates Sent	The number of LS updates sent on this interface by this router.
LS Updates Received	The number of LS updates received on this interface by this router.
LS Acknowledgements Sent	The number of LS acknowledgements sent on this interface by this router.
LS Acknowledgements Received	The number of LS acknowledgements received on this interface by this router.

## View the OSPF Neighbor Table

You can view the OSPF neighbor table list. When a particular neighbor ID is specified, detailed information about a neighbor is given. The information is displayed only if OSPF is enabled.

➤ **To view the OSPF 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 **Routing > OSPF > Advanced > Neighbor Table**.

OSPF Neighbor Table													
Search By Interface													Go
Interface	Neighbor IP Address	Neighbor Interface Index	Router ID	Area ID	Options	Router Priority	State	Events	Permanence	Hellos Suppressed	Retransmission Queue length	Up Time	Dead Time

To refresh the screen with the latest information on the switch, click the **Update** button.

To clear all the neighbors in the table, click the **Clear** button.

The following table describes the nonconfigurable data that is displayed.

**Table 151. OSPF Neighbor Table**

Field	Description
Interface	The interface for which data is to be displayed or configured. Slot 0 is the base unit.

Table 151. OSPF Neighbor Table (continued)

Field	Description
Neighbor IP Address	The IP address of the neighboring router's interface to the attached network. It is used as the destination IP address when protocol packets are sent as unicasts along this adjacency. Also used in router LSAs as the link ID for the attached network if the neighboring router is selected to be designated router. The neighbor IP address is learned when hello packets are received from the neighbor. For virtual links, the neighbor IP address is learned during the routing table build process.
Neighbor Interface Index	A unit/slot/port identifying the neighbor interface index.
Router ID	A 32-bit integer in dotted-decimal format representing the neighbor interface.
Area ID	The area ID of the OSPF area associated with the interface.
Options	An integer value that indicates the optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its hello packets. This enables received hello packets to be rejected (for example, neighbor relationships do not even start to form) if there is a mismatch in certain crucial OSPF capabilities.
Router Priority	The OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of 0 indicates that the router is not eligible to become the designated router on this network.
State (continued on the following page)	<p>The state of a neighbor can be the following:</p> <ul style="list-style-type: none"> <li>• <b>Down.</b> This is the initial state of a neighbor conversation. It indicates that no recent information was received from the neighbor. On NBMA networks, hello packets can still be sent to <i>Down</i> neighbors, although at a reduced frequency.</li> <li>• <b>Attempt.</b> This state is valid only for neighbors attached to NBMA networks. It indicates that no recent information was received from the neighbor, but that a more concerted effort must be made to contact the neighbor. This is done by sending the neighbor hello packets at hello intervals.</li> <li>• <b>Init.</b> A hello packet was recently seen from the neighbor. However, bidirectional communication was not yet established with the neighbor (for example, the router did not appear in the neighbor's hello packet). All neighbors in this state (or greater) are listed in the hello packets sent from the associated interface.</li> <li>• <b>2-Way.</b> Communication between the two routers is bidirectional. This was assured by the operation of the hello protocol. This is the most advanced state short of beginning adjacency establishment. The backup designated router is selected from the set of neighbors in state 2-way or greater.</li> <li>• <b>Exchange Start.</b> This is the first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial DD sequence number. Neighbor conversations in this state or greater are called adjacencies.</li> <li>• <b>Exchange.</b> The router is describing its entire link state database by sending database description packets to the neighbor. The link state request packets can also be sent asking for the neighbor's more recent LSAs. All adjacencies in the exchange state or greater are used by the flooding procedure. These adjacencies are fully capable of transmitting and receiving all types of OSPF routing protocol packets.</li> </ul>

Table 151. OSPF Neighbor Table (continued)

Field	Description
State (continued)	<ul style="list-style-type: none"> <li>• <b>Loading.</b> Link state request packets are sent to the neighbor asking for the more recent LSAs that were discovered (but not yet received) in the exchange state.</li> <li>• <b>Full.</b> The neighboring routers are fully adjacent. These adjacencies now appear in router LSAs and network LSAs.</li> </ul>
Events	The number of times this neighbor relationship changed state, or an error occurred.
Permanence	This variable displays the status of the entry. <b>Dynamic</b> and <b>Permanent</b> refer to how the neighbor became known.
Hellos Suppressed	This indicates whether hellos are being suppressed to the neighbor.
Retransmission Queue Length	An integer representing the current length of the retransmission queue of the specified neighbor router ID of the specified interface.
Up Time	Neighbor uptime; how long since the adjacency last reached the Full state.
Dead Time	The amount of time, in seconds, to wait before the router assumes the neighbor is unreachable.

## View the OSPF Link State Database

### ➤ To view the OSPF link state database:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > OSPF > Advanced > Link State Database**.



Link State Database							
Router ID	Area ID	LSA Type	LS ID	Age	Sequence	Checksum	Options
External LSDB Table							
Router ID	LSA Type	LS ID	Age	Sequence	Checksum		
AS Opaque LSDB Table							
Router ID	LSA Type	LS ID	Age	Sequence	Checksum		

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 152. OSPF Link State Database**

Field	Description
Router ID	The 32-bit integer in dotted-decimal format that uniquely identifies the router within the autonomous system (AS). The router ID is set on the IP Configuration screen. To change the router ID you must first disable OSPF. After you set the new router ID, you must reenble OSPF for the change to take effect. The default value is 0.0.0.0, although this is not a valid router ID.
Area ID	The ID of an OSPF area to which one of the router interfaces is connected. An area ID is a 32-bit integer in dotted-decimal format that uniquely identifies the area to which an interface is connected.

Table 152. OSPF Link State Database (continued)

Field	Description
LSA Type	<p>The format and function of the link state advertisement. LSA Type is one of the following:</p> <ul style="list-style-type: none"> <li>• Illegal</li> <li>• Router Links</li> <li>• Network Links</li> <li>• Network Summary</li> <li>• ASBR Summary</li> <li>• AS-external</li> <li>• Group Member</li> <li>• NSSA</li> <li>• TMP2</li> <li>• Link Opaque</li> <li>• Area Opaque</li> <li>• AS Opaque</li> <li>• Unknown</li> </ul>
LS ID	The link state ID identifies the piece of the routing domain that is being described by the advertisement. The value of the LS ID depends on the advertisement's LS type.
Age	The time since the link state advertisement was first originated, in seconds.
Sequence	The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement.
Checksum	The checksum is used to detect data corruption of an advertisement. This corruption can occur while an advertisement is being flooded, or while it is being held in a router's memory. This field is the checksum of the complete contents of the advertisement, except the LS age field.
Options	<p>The Options field in the link state advertisement header indicates which optional capabilities are associated with the advertisement. The options are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Q</b>. This enables support for QoS traffic engineering.</li> <li>• <b>E</b>. This describes the way AS external LSAs are flooded.</li> <li>• <b>MC</b>. This describes the way IP multicast datagrams are forwarded according to the standard specifications.</li> <li>• <b>O</b>. This describes whether opaque LSAs are supported.</li> <li>• <b>V</b>. This describes whether OSPF++ extensions for VPN/COS are supported.</li> </ul>

## External Link State Database Table

The following table describes the nonconfigurable data that is displayed in the External Link State Database (LSDB) table.

**Table 153. OSPF External Link State Database Table**

Field	Description
Router ID	The 32-bit integer in dotted-decimal format that uniquely identifies the router within the autonomous system (AS). The router ID is set on the IP Configuration screen. To change the router ID you must first disable OSPF. After you set the new router ID, you must reenable OSPF for the change to take effect. The default value is 0.0.0.0, although this is not a valid router ID.
LSA Type	The format and function of the link state advertisement. LSA Type is one of the following: <ul style="list-style-type: none"> <li>ASBR Summary</li> <li>AS-external</li> <li>NSSA</li> <li>TMP2</li> </ul>
LS ID	The link state ID identifies the piece of the routing domain that is being described by the advertisement. The value of the LS ID depends on the advertisement's LS type.
Age	The time since the link state advertisement was first originated, in seconds.
Sequence	The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement.
Checksum	The checksum is used to detect data corruption of an advertisement. This corruption can occur while an advertisement is being flooded, or while it is being held in a router's memory. This field is the checksum of the complete contents of the advertisement, except the LS age field.

## AS Opaque Link State Database Table

The following table describes the nonconfigurable data that is displayed in the AS Opaque Link State Database (LSDB) table.

**Table 154. OSPF AS Opaque Link State Database Table**

Field	Description
Router ID	The 32-bit integer in dotted-decimal format that uniquely identifies the router within the autonomous system (AS). The router ID is set on the IP Configuration screen. To change the router ID you must first disable OSPF. After you set the new router ID, you must reenable OSPF for the change to take effect. The default value is 0.0.0.0, although this is not a valid router ID.

Table 154. OSPF AS Opaque Link State Database Table (continued)

Field	Description
LSA Type	The format and function of the link state advertisement. LSA Type is one of the following: <ul style="list-style-type: none"> <li>• Area Opaque</li> <li>• AS Opaque</li> <li>• Link Opaque</li> </ul>
LS ID	The link state ID identifies the piece of the routing domain that is being described by the advertisement. The value of the LS ID depends on the advertisement's LS type.
Age	The time since the link state advertisement was first originated, in seconds.
Sequence	The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement.
Checksum	The checksum is used to detect data corruption of an advertisement. This corruption can occur while an advertisement is being flooded, or while it is being held in a router's memory. This field is the checksum of the complete contents of the advertisement, except the LS age field.

## Configure the OSPF Virtual Link

### ➤ To configure the OSPF virtual 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 **Routing > OSPF > Advanced > Virtual Link Configuration**.

OSPF Virtual Link Configuration					
Area ID	Neighbor Router ID	Hello Interval	Dead Interval	Iftransit Delay Interval	Retransmit Interval
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Authentication Type	Authentication Key	Authentication ID	Neighbor State	State	Metric
<input type="text" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

8. In the **Area ID** field, enter the OSPF area ID.

An area ID is a 32-bit integer in dotted-decimal format that uniquely identifies the area to which a router interface connects.

Virtual links can be configured between any pair of area border routers having interfaces to a common (non-backbone) area.

9. Configure the **Neighbor Router ID** by entering the neighbor portion of a virtual link specification.

Virtual links can be configured between any pair of area border routers having interfaces to a common (non-backbone) area.

10. In the **Hello Interval** field, enter the OSPF hello interval for the specified interface in seconds.

This parameter must be the same for all routers attached to a network. The valid values range from 1 to 65,535. The default is 10 seconds.

11. In the **Dead Interval** field, enter the OSPF dead interval for the specified interface in seconds.

This specifies how long a router waits to see a neighbor router's hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value must be a multiple of the hello interval (for example, 4). The valid values range from 1 to 65,535. The default is 40.

12. In the **Iftransit Delay Interval** field, enter the OSPF transit delay for the specified interface.

This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. The valid values range from 1 to 3600 seconds (1 hour). The default value is 1 second.

13. In the **Retransmit Interval** field, enter the OSPF retransmit interval for the specified interface.

This is the number of seconds between link state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link state request packets. The valid values range from 1 to 3600 seconds (1 hour). The default is 5 seconds.

14. From the **Authentication Type** menu, select one of the following authentication types:

- **None.** This is the initial interface state.
- **Simple.** If you select Simple, you are prompted to enter an authentication key. This key is included, in the clear, in the OSPF header of all packets sent on the network. All routers on the network must be configured with the same key.
- **Encrypt.** If you select Encrypt you are prompted to enter both an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.

15. In the **Authentication Key** field, enter the OSPF authentication key for the specified interface.

If you do not select authentication, you are not prompted to enter a key.

- If you select **Simple** authentication, you cannot use a key of more than 8 octets.
- If you select **Encrypt**, the key can be up to 16 octets long.

The key value is displayed only if you are logged on with read/write privileges; otherwise, it is displayed as asterisks.

16. In the **Authentication ID** field, enter the ID to be used for authentication.

You are prompted to enter an ID only when you select **Encrypt** as the authentication type. The ID is a number between 0 and 255, inclusive.

17. Click the **Add** button

The new virtual link is added.

18. To remove the specified virtual link from the switch configuration, click the **Delete** button.

19. Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 155. OSPF Virtual Link Configuration**

Field	Description
Neighbor State continued on the next page)	<p>The OSPF interface state can be one of these values:</p> <ul style="list-style-type: none"> <li>• <b>Down.</b> This is the initial interface state. The lower-level protocols indicated that the interface is unusable. Interface parameters are set to their initial values. All interface timers are disabled, and there are no adjacencies associated with the interface.</li> <li>• <b>Waiting.</b> The router is trying to determine the identity of the backup designated router by monitoring received hello packets. The router is not allowed to elect a backup designated router or a designated router until it transitions out of Waiting state. This prevents unnecessary changes of backup designated router.</li> </ul>

Table 155. OSPF Virtual Link Configuration (continued)

Field	Description
Neighbor State (continued)	<ul style="list-style-type: none"> <li>• <b>Point-to-Point.</b> The interface is operational, and is connected either to the virtual link. On entering this state the router attempts to form an adjacency with the neighboring router. hello packets are sent to the neighbor every hello interval seconds.</li> <li>• <b>Designated Router.</b> This router is the designated router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA contain links to all routers (including the designated router) attached to the network.</li> <li>• <b>Backup Designated Router.</b> This router is the backup designated router on the attached network. It is promoted to designated router if the present designated router fails. The router establishes adjacencies to all other routers attached to the network. The backup designated router performs slightly different functions during the flooding procedure, as compared to the designated router.</li> <li>• <b>Other Designated Router.</b> The interface is connected to a broadcast or NBMA network on which other routers were selected to be the designated router and backup designated router either. The router attempts to form adjacencies to both the designated router and the backup designated router.</li> </ul>
State (continued on the next page)	<p>The state of the interface. It takes one the following values:</p> <ul style="list-style-type: none"> <li>• <b>Down.</b> This is the initial interface state. The lower-level protocols indicated that the interface is unusable. Interface parameters are set to their initial values. All interface timers are disabled, and there are no adjacencies associated with the interface.</li> <li>• <b>Waiting.</b> The router is trying to determine the identity of the backup designated router by monitoring received hello packets. The router is not allowed to elect a backup designated router or a designated router until it transitions out of waiting state. This prevents unnecessary changes of backup designated router.</li> <li>• <b>Point-to-Point.</b> The interface is operational, and is connected either to the virtual link. On entering this state the router attempts to form an adjacency with the neighboring router. hello packets are sent to the neighbor every hello interval seconds.</li> <li>• <b>Designated Router.</b> This router is the designated router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA contain links to all routers (including the designated router) attached to the network.</li> <li>• <b>Backup Designated Router.</b> This router is the backup designated router on the attached network. It is promoted to designated router if the present designated router fails. The router establishes adjacencies to all other routers attached to the network. The backup designated router performs slightly different functions during the flooding procedure, as compared to the designated router.</li> </ul>

Table 155. OSPF Virtual Link Configuration (continued)

Field	Description
State (continued)	<ul style="list-style-type: none"> <li><b>Other Designated Router.</b> The interface is connected to a broadcast or NBMA network on which other routers were selected to be the designated router and backup designated router either. The router attempts to form adjacencies to both the designated router and the backup designated router.</li> </ul>
Metric	The metric value used by the Virtual Link.

## Configure the OSPF Route Redistribution

You can configure the OSPF Route Redistribution parameters. The allowable values for each field are displayed next to the field. If any invalid values are entered, an alert message is displayed with the list of all the valid values.

### ➤ Configure the OSPF route redistribution:

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

OSPF Route Redistribution							
<input type="checkbox"/>	Source	Redistribute Option	Metric	Metric Type	Tag	Subnets	Distribute List
<input type="checkbox"/>	Connected	Disable					
<input type="checkbox"/>	Static	Disable					
<input type="checkbox"/>	RIP	Disable					
<input type="checkbox"/>	OSPF	Disable					
<input type="checkbox"/>	BGP	Disable					



8. From the **Source** menu, select from the list of available source routes that were not previously configured for redistribution by OSPF.

The valid values are as follows:

- BGP
- Connected
- OSPF
- RIP
- Static

9. In the **Redistribute** list, select to **Enable** or **Disable** the redistribution for the selected source protocol.

10. Set the **Metric** value to be used as the metric of redistributed routes.

This field displays the metric if the source was preconfigured and can be modified. The valid values are 0 to 16777214.

11. From the **Metric Type** list, select the OSPF metric type of redistributed routes.

12. Set the **Tag** field in routes redistributed.

This field displays the tag if the source was preconfigured; otherwise, the tag is 0 and can be modified. The valid values are 0 to 4294967295.

13. From the **Subnets** list, select whether the subnetted routes will be redistributed (Enable) or not (Disable).

14. In the **Distribute List** field, set the access list that filters the routes to be redistributed by the destination protocol.

Only permitted routes are redistributed. If this command refers to a nonexistent access list, all routes are permitted. The valid values for access list IDs are 1 to 199.

When used for route filtering, the only fields in an access list that get used are as follows:

- Source IP address and netmask
- Destination IP address and netmask
- Action (permit or deny)

All other fields (source and destination port, precedence, ToS, and so on) are ignored.

The source IP address is compared to the destination IP address of the route. The source IP netmask in the access list rule is treated as a wildcard mask, indicating which bits in the source IP address must match the destination address of the route.

**Note:** A 1 in the mask indicates a *do not care* in the corresponding address bit.

When an access list rule includes a destination IP address and netmask (an extended access list), the destination IP address is compared to the network mask of the destination of the route. The destination netmask in the access list serves as a wildcard mask, indicating which bits in the route's destination mask are significant for the filtering operation.

15. Click the **Apply** button.

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

## View the NSF OSPF Summary

You can view the NSF OSPF summary. The allowable values for each field are displayed next to the field. If any invalid values are entered, an alert message is displayed with the list of all the valid values.

### ➤ To configure the NSF OSPF 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 **Routing > OSPF > Advanced > NSF OSPF Summary**.

NSF OSPF Summary	
Support Mode	Disabled ▾
Restart Interval	120 (0-1800)
Restart Status	
Restart Age (secs)	
Restart Exit Reason	
Helper Support Mode	Always ▾
Helper Strict LSA Checking	Enable ▾

8. From the **Support Mode** list, configure how the unit performs graceful restarts by selecting from the following possible values:

- **Always.** Indicates that OSPF performs a graceful restart for all planned and unplanned warm restart events.
- **Disabled.** Disables OSPF performing graceful restarts.
- **Planned.** Indicates that OSPF performs a graceful restart only when a restart is planned (for example, due to an **initiate failover** command).

The default is Disabled.

9. Configure the **Restart Interval**. The valid values are 0 to 1800 in seconds.

The default is 120 seconds.

10. Use the **Helper Support Mode** field to configure how the unit acts when a neighbor performs a warm restart.

The possible values are as follows:

- **Always.** Indicates that OSPF helps a restarting neighbor only during all planned and unplanned warm restart events.
- **Disabled.** Disables OSPF acting as a helpful neighbor.
- **Planned.** Indicates that OSPF helps a restarting neighbor only during planned events.

The default is Always.

11. Configure **Helper Strict LSA Checking** by selecting **Enable** or **Disable**.

When enabled, the unit exits helper mode whenever the topology changes.

12. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 156. NSF OSPF Summary**

Field	Description
Restart Status	<p>The restart status of OSPF Helper feature. The possible values are as follows:</p> <ul style="list-style-type: none"> <li>• Not Restarting</li> <li>• Planned Restart</li> <li>• Unplanned Restart</li> </ul>

Table 156. NSF OSPF Summary (continued)

Field	Description
Restart Age (seconds)	The amount of time since the last restart occurred.
Restart Exit Reason	Displays how the master unit on the chassis last started up. The possible values are as follows: <ul style="list-style-type: none"> <li>• <b>Not Attempted.</b> Graceful restart was not attempted.</li> <li>• <b>In Progress.</b> Restart is in progress.</li> <li>• <b>Completed.</b> The previous graceful restart completed successfully.</li> <li>• <b>Timed Out.</b> The previous graceful restart timed out.</li> <li>• <b>Topology Changed.</b> The previous graceful restart terminated prematurely because of a topology change.</li> </ul>

## OSPFv3

Only the following switches support OSPFv3:

- M6100
- M5300-28G3
- M5300-52G3
- M5300-28GF3

The following switches support OSPFv3 with an L3 license:

- M5300-28G
- M5300-52G
- M5300-28G-POE+
- M5300-52G-POE+

## Configure Basic OSPFv3 Settings

### ➤ To configure the basic OSPFv3 settings:

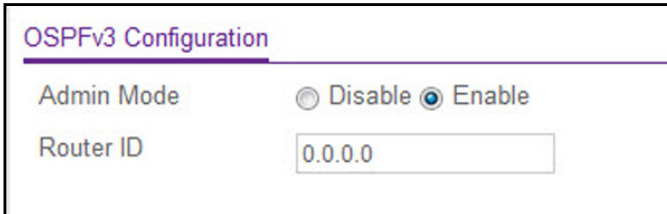
1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address 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 > OSPFv3 > Basic > OSPFv3 Configuration**.



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

If you select **Enable**, OSPFv3 is activated for the switch. By default, OSPFv3 is enabled. You must configure a router ID before OSPFv3 can become operational. This can also be done by issuing the CLI command **config router id** in IPv6 router OSPF mode. For more information, see [Configure the Router IP](#) on page 325.

**Note:** Once OSPFv3 is initialized on the router, it remains initialized until the router is reset.

9. Enter the **Router ID** as a 32-bit integer in dotted-decimal format that uniquely identifies the router within the autonomous system (AS).

To change the router ID, you must first disable OSPFv3. After you set the new router ID, you must reenabling OSPFv3 for the change to take effect. The default value is 0.0.0.0, although this is not a valid router ID.

10. Click the **Apply** button.

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

## Configure OSPFv3 Default Route Advertise Settings

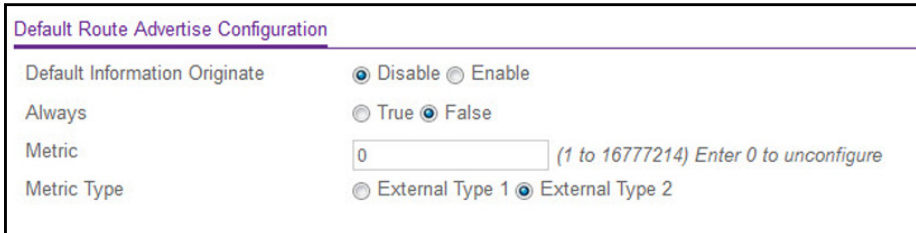
1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address 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 > OSPFv3 > Advanced > OSPFv3 Configuration**.



8. Select the Default Information Originate **Enable** radio button.

Selecting Enable makes it possible to specify the other settings in this screen. Selecting Disable returns the other fields in this screen to their default values.

9. Select the **Always True** or **False** radio button.

When set to True, this field sets the router advertise. The default is False.

10. In the **Metric** field, specify the metric of the default route.

The valid values range from 0 to 16777214. The default is 0.

11. Select the **Metric Type External Type 1** or **External Type 2** radio button.

This sets the OSPFv3 metric type of the default route. The default is External Type 2.

12. Click the **Apply** button.

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

## Configure the Advanced OSPFv3 Settings

### ➤ To configure the advanced OSPFv3 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 > OSPFv3 > Advanced > OSPFv3 Configuration**.

OSPFv3 Configuration	
Router ID	0.0.0.0
Admin Mode	Enable
ASBR Mode	Disable
ABR Status	Disable
Exit Overflow Interval (secs)	0 (0 to 2147483647)
External LSA Count	0
External LSA Checksum	0
New LSAs Originated	0
LSAs Received	0
External LSDB Limit	-1 (-1(No Limit) to 2147483647)
Default Metric	0 (1 to 16777214) Enter 0 to unconfigure
Maximum Paths	4 (1 to 4)
AutoCost Reference Bandwidth	100 (1 to 4294967)
Default Passive Setting	Disable
Helper Support Mode	Always
Helper Strict LSA Checking	Enable

8. Enter the **Router ID** in 32-bit integer, dotted-decimal format that uniquely identifies the router within the autonomous system (AS).

To change the router ID you must first disable OSPFv3. After you set the new router ID, you must reenabling OSPFv3 for the change to take effect. The default value is 0.0.0.0, although this is not a valid router ID.

9. In the **Admin Mode** field, select **Enable** or **Disable**.

If you select **Enable**, OSPFv3 is activated for the switch. The default value is Enable. You must configure a router ID before OSPFv3 can become operational. You do this on the IP Configuration screen, or by issuing the CLI command **config router id** in IPv6 router OSPF mode. For more information, see [Configure the Router IP](#) on page 325.

**Note:** Once OSPFv3 is initialized on the router, it remains initialized until the router is reset.

10. In the **Exit Overflow Interval** field, specify the number of seconds that, after entering overflow state, the router must wait before attempting to leave overflow state.

Because OSPFv3 cannot originate nondefault external LSAs while in overflow state, this allows the router to again originate nondefault AS-external-LSAs. If you enter an exit overflow interval of 0, the router does not leave the overflow state until it is restarted. The range is 0 to 2,147,483,647 seconds. The default is 0.

When the number of nondefault external LSAs exceeds a configured limit, the router enters an overflow state as defined in RFC 1765.

11. Enter the **External LSDB Limit**. This is the maximum number of AS-external-LSAs that can be stored in the database.

A value of –1 implies there is no limit on the number that can be saved. The valid range of values is –1 to 2147483647. The default is –1 (no limit).

12. Use the **Default Metric** field to set a default for the metric of redistributed routes.

This field displays the default metric if one was already set, or blank if one was not configured earlier. The valid values are 1 to 16777214. The default is 0 (unconfigured).

13. Use the **Maximum Paths** field to configure the maximum number of paths that OSPFv3 can report to a given destination.

The valid values are 1 to 4.

14. Configure the **AutoCost Reference Bandwidth** to control how OSPF calculates default metrics for the interface.

The valid values are 1 to 4294967. The default is 100.

15. In the **Default Passive Setting**, select the **Enable** or **Disable** option to configure the global passive mode setting for all OSPF interfaces.

Configuring this field overwrites any present interface-level passive mode setting. OSPF does not form adjacencies on passive interfaces, but does advertise attached networks as stub networks.

16. Use **Helper Support Mode** to configure how the unit acts when a neighbor performs a warm restart.

The possible values are as follows:

- **Planned**. OSPF helps a restarting neighbor only during planned events.
- **Always**. OSPF helps a restarting neighbor during all planned and unplanned warm restart events.
- **Disabled**. OSPF does not act as a helpful neighbor.

17. Configure **Helper Strict LSA Checking** by selecting the **Enable** or **Disable** option.

When enabled, the unit exits helper mode whenever the topology changes.

18. Click the **Apply** button.

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



The following table describes the nonconfigurable data that is displayed.

**Table 157. Advanced OSPFv3 Configuration**

Field	Description
ASBR Mode	Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learned from other protocol.
ABR Status	The values of this are Enabled or Disabled. Enabled implies that the router is an area border router. Disabled implies that it is not an area border router.
External LSA Count	The number of external (LS type 5) link state advertisements (LSAs) in the link state database.
External LSA Checksum	The sum of the LS checksums of the external LSAs contained in the link state database. This sum can be used to determine if there was a change in a router's link state database, and to compare the link state databases of two routers.
New LSAs Originated	In any given OSPFv3 area, a router originates several LSAs. Each router originates a router-LSA. If the router is also the designated router for any of the area's networks, it originates network-LSAs for those networks. This value represents the number of LSAs originated by this router.
LSAs Received	The number of LSAs received that were determined to be new instantiations. This number does not include newer instantiations of self-originated LSAs.

## Configure the OSPFv3 Common Area

### ➤ To configure the OSPFv3 common area 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 > OSPFv3 > Advanced > Common Area Configuration**.

OSPFv3 Common Area Configuration							
<input type="checkbox"/>	Area ID	External Routing	SPF Runs	Area Border Router Count	Area LSA Count	Area LSA Checksum	Import Summary LSAs
	<input type="text"/>						

8. In the **Area ID** field, enter the OSPF area ID.

An area ID is a 32-bit integer in dotted-decimal format that uniquely identifies the area to which a router interface connects.

9. Click the **Add** button.

The area is configured as a common area.

10. To delete the common area designation, click the **Delete** button.

The area is returned to normal state.

The following table describes the nonconfigurable data that is displayed.

**Table 158. Advanced OSPFv3 Common Area Configuration**

Field	Description
External Routing	A definition of the router's capabilities for the area, including whether or not AS-external-LSAs are flooded into or throughout the area.
SPF Runs	The number of times that the intra-area route table was calculated using this area's link state database. This is done using Dijkstra's algorithm.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.
Area LSA Count	The total number of link state advertisements in this area's link state database, excluding AS external LSAs.
Area LSA Checksum	The 32-bit unsigned sum of the link state advertisements' LSA checksums contained in this area's link state database. This sum excludes external (LSA type 5) link state advertisements. The sum can be used to determine if there was a change in a router's link state database, and to compare the link state database of two routers.
Import Summary LSAs	The summary LSAs are enabled or disabled imported into this area.

## Configure an OSPFv3 Stub Area

- **To configure the OSPFv3 stub area:**

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

3. Launch a web browser.
4. Enter 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 > OSPFv3 > Advanced > Stub Area Configuration**.

Area ID	SPF Runs	Area Border Router Count	Area LSA Count	Area LSA Checksum	Import Summary LSAs	Default Cost	Type of Service
<input type="text"/>					<input type="text" value="v"/>	<input type="text"/>	

8. In the **Area ID** field, enter the OSPF area ID.  
An area ID is a 32-bit integer in dotted-decimal format that uniquely identifies the area to which a router interface connects.
9. In the **Import Summary LSAs** list, select the **Enable** or **Disable** option.  
If you select **Enable**, summary LSAs are imported into areas. The default is Enable.
10. In the **Default Cost** field, enter the metric value to be applied for the default route advertised into the stub area.  
The valid values range from 1 to 16,777,215. This value is applicable only to stub areas.
11. Click the **Add** button.  
The area is configured as a stub area.
12. To delete the stub area designation, click the **Delete** button.  
The area is returned to normal state.
13. Click the **Apply** button.  
The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable data that is displayed.

**Table 159. Advanced OSPFv3 Stub Area Configuration**

Field	Description
SPF Runs	The number of times that the intra-area route table was calculated using this area's link state database. This is done using Dijkstra's algorithm.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF Pass.
Area LSA Count	The total number of link state advertisements in this area's link state database, excluding AS External LSAs.
Area LSA Checksum	The 32-bit unsigned sum of the link state advertisements' LSA checksums contained in this area's link state database. This sum excludes external (LSA type 5) link state advertisements. The sum can be used to determine if there was a change in a router's link state database, and to compare the link state database of two routers.
Type of Service	This field is the normal ToS associated with the stub metric.

## Configure the OSPFv3 NSSA Area

### ➤ To configure the OSPFv3 NSSA area:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > OSPFv3 > Advanced > NSSA Area Configuration**.

OSPFv3 NSSA Area Configuration						
<input type="checkbox"/>	Area ID	SPF Runs	Area Border Router Count	Area LSA Count	Area LSA Checksum	Import Summary LSAs
	<input type="text"/>					<input type="text"/>

Default Information Originate			Translator Role	Translator Stability Interval	Redistribute Mode	Translator State
Admin Mode	Metric Value	Metric Type				
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

8. In the **Area ID** field, enter the OSPF area ID.

An area ID is a 32-bit integer in dotted-decimal format that uniquely identifies the area to which a router interface connects.

9. Configure the **Import Summary LSAs** by selecting **Enable** or **Disable** from the list.

If you select **Enable**, summary LSAs are imported into stub areas.

10. Configure the **Default Information Originate**.

This option permits you to advertise a default route into the NSSA when import summary LSAs are disabled. This can also be applied by the CLI command **area (area-id) NSSA default-info-originate** in the IP router OSPF config mode.

- In the **Admin Mode** list, select to **Enable** or **Disable** the default information originate.
- In the **Metric Value** field, set the default metric value for default information originate. The value range of values is 1 to 16777214.
- In the **Metric Type** field, select the type of metric specified in the Metric Value field. Options are as follows:
  - Comparable Cost.** External type 1 metrics that are comparable to the OSPF metric.
  - Non-comparable Cost.** External type 2 metrics that are assumed to be larger than the cost of the OSPF metric.

11. Select the **Translator Role** of the NSSA.

Options are as follows:

- Always.** Cause the router to assume the role of the translator the instant it becomes a border router.
- Candidate.** Cause the router to participate in the translator election process when it attains border router status.

12. In the **Translator Stability Interval** field, configure the translator of the NSSA.

The value is the period of time that an elected translator continues to perform its duties after it determines that its translator status was deposited by another router. The valid range is 0 to 3600.

- 13.** In the **Redistribute Mode** field, select to **Enable** or **Disable**.

This configures the NSSA ABR so that learned external routes are redistributed to the NSSA.

- 14.** Click the **Add** button.

The area is configured as an NSSA area.

- 15.** To delete the NSSA area designation, click the **Delete** button.

The area is returned to normal state.

- 16.** Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 160. Advanced OSPFv3 NSSA Area Configuration**

Field	Description
SPF Runs	The number of times that the intra-area route table was calculated using this area's link state database. This is typically done using Dijkstra's algorithm.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.
Area LSA Count	The total number of link state advertisements in this area's link state database, excluding AS external LSAs.
Area LSA Checksum	The 32-bit unsigned sum of the link state advertisements' LSA checksums contained in this area's link state database. This sum excludes external (LSA type 5) link state advertisements. The sum can be used to determine if there was a change in a router's link state database, and to compare the link state database of two routers.
Translator State	<p>The field tells you if and how the NSSA border router translates Type 7 into Type 5. Possible values are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Enabled.</b> The NSSA border router's translator role was set to always.</li> <li>• <b>Elected.</b> The candidate NSSA border router is translating Type 7 LSAs into Type 5.</li> <li>• <b>Disabled.</b> The candidate NSSA border router is NOT translating Type 7 LSAs into Type 5.</li> </ul>

## Configure the OSPFv3 Area Range

### ➤ To configure the OSPFv3 area range:

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

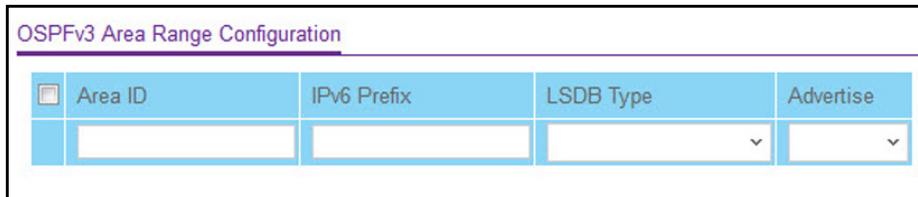
5. Enter the user name and password.

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 > OSPFv3 > Advanced > Area Range Configuration**.



Area ID	IPv6 Prefix	LSDB Type	Advertise
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

8. Enter the OSPFv3 **Area ID**.

An area ID is a 32-bit integer in dotted-decimal format that uniquely identifies the area to which a router interface connects.

9. Enter the **IPv6 Prefix** for the address range for the selected area.
10. From the list in the **LSDB Type** field, select the type of link advertisement associated with the specified area and address range.

Options are: **Network Summary** or **NSSA External**. The default type is **Network Summary**.

11. In the **Advertise** field, select the **Enable** or **Disable** option.

If you select Enable, the address range is advertised outside the area through a network summary LSA. The default is Enable.

12. Click the **Add** button.

The new address range is added to the switch.

13. To remove the specified address range from the area configuration, click the **Delete** button.

## Configure the OSPFv3 Interface

➤ **To configure the OSPFv3 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 **Routing > OSPFv3 > Advanced > Interface Configuration**.

OSPFv3 Interface Configuration

1 2 3 VLANs All

<input type="checkbox"/>	Interface	IPv6 Address	Area ID	Admin Mode	Router Priority	Retransmit Interval	Hello Interval	Dead Interval	LSA Ack Interval
<input type="checkbox"/>			<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	1/0/1		None	Disable	1	5	10	40	1
<input type="checkbox"/>	1/0/2		None	Disable	1	5	10	40	1
<input type="checkbox"/>	1/0/3		None	Disable	1	5	10	40	1

Go To Interface

lfransit Delay Interval	MTU Ignore	Passive Mode	Network Type	State	Designated Router	Backup Designated Router	Number of Link Events	Metric Cost
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>					<input type="text"/>
1	Disable	Disable	Broadcast					1
1	Disable	Disable	Broadcast					1
1	Disable	Disable	Broadcast					1
1	Disable	Disable	Broadcast					1
1	Disable	Disable	Broadcast					1

8. In the **Go To Interface** field, enter the interface in unit/slot/port format and click the **Go** button.

The entry corresponding to the specified interface is selected.

9. Select the check box next to the **Interface** for which data is to be displayed or configured.
10. In the **Area ID** field, enter the 32-bit integer in dotted-decimal format that uniquely identifies the OSPFv3 area to which the selected router interface connects.



If you assign an area ID that does not exist, the area is created with default values.

11. Configure the **Admin Mode** by selecting the **Enable** or **Disable** option from the list.

The default value is Disable. You can configure OSPFv3 parameters without enabling OSPFv3 admin mode, but the settings do not take effect until you enable admin mode. The following information is displayed only if admin mode is enabled:

- State
- Designated router
- Backup designated router
- Number of link events
- LSA Ack interval
- Metric cost

For OSPFv3 to be fully functional, you must enter a valid IPv6 prefix/prefix length. This can be done using the CLI **IPv6 address** command.

**Note:** Once OSPFv3 is initialized on the router, it remains initialized until the router is reset.

12. Configure the **Router Priority** by entering the OSPFv3 priority for the selected interface.

The priority of an interface is specified as an integer from 0 to 255. The default is **1**, which is the highest router priority. A value of 0 indicates that the router is not eligible to become the designated router on this network.

13. Configure the **Retransmit Interval** by entering the OSPFv3 retransmit interval for the specified interface.

This is the number of seconds between link state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link state request packets. The valid values range from 0 to 3600 seconds (1 hour). The default is 5 seconds.

14. Configure the **Hello Interval** by entering the OSPFv3 hello interval for the specified interface in seconds.

This parameter must be the same for all routers attached to a network. Value values range from 1 to 65,535. The default is 10 seconds.

15. Enter the OSPFv3 **Dead Interval** for the specified interface in seconds.

This specifies how long a router waits to see a neighbor router's hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value is a multiple of the hello interval (for example, 4). The valid values range from 1 to 65,535. The default is 40 seconds.

16. In the **lfrtransit Delay Interval** field, enter the OSPFv3 transit delay for the specified interface.

This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. The valid values range from 1 to 3600 seconds (1 hour). The default value is 1 second.

17. Configure **MTU Ignore** by selecting **Enable** or **Disable** from the list.

MTU Ignore disables OSPF MTU mismatch detection on receiving database description packets. The default value is **Disable** (MTU mismatch detection is enabled).

18. Configure **Passive Mode** by selecting **Enable** or **Disable** from the list.

Make an interface passive to prevent OSPF from forming an adjacency on an interface. OSPF advertises networks attached to passive interfaces as stub networks. Interfaces are not passive by default, meaning that the passive mode default is Disable.

19. Set the OSPFv3 **Network Type** on the interface by selecting either **Broadcast** or **Point-to-Point** Mode from the list.

OSPFv3 selects a designated router and originates network LSAs only for broadcast networks. No more than two OSPFv3 routers can be present on a point-to-point link. The default network type for Ethernet interfaces is Broadcast.

20. In the **Metric Cost** field, enter the value for the cost Type of Service (TOS).

OSPF uses this value in computing shortest paths. The range is from 1 to 65,535. The default is 1. Metric Cost is configurable only if OSPFv3 is initialized on the interface.

21. Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 161. Advanced OSPFv3 Interface Configuration**

Field	Description
IPv6 Address	The IPv6 address of the interface.
LSA Ack Interval (secs)	The number of seconds between LSA acknowledgment packet transmissions, which must be less than the retransmit interval.
State (continued on the next page)	<p>The current state of the selected router interface. State is one of the following:</p> <ul style="list-style-type: none"> <li><b>Down.</b> This is the initial interface state. The lower-level protocols indicate that the interface is unusable. Interface parameters are set to their initial values. All interface timers are disabled, and there are no adjacencies associated with the interface.</li> </ul>

Table 161. Advanced OSPFv3 Interface Configuration (continued)

Field	Description
State (continued.)	<ul style="list-style-type: none"> <li>• <b>Loopback.</b> The router's interface to the network is looped back in either the hardware or software. The interface is unavailable for regular data traffic. However, you might want to gain information about the quality of this interface, either through sending ICMP pings to the interface or through something like a bit error test. For this reason, IP packets can still be addressed to an interface in loopback state. To facilitate this, such interfaces are advertised in router LSAs as single host routes, whose destination is the IP interface address.</li> <li>• <b>Waiting.</b> The router is trying to determine the identity of the backup designated router for the network by monitoring received hello packets. The router is not allowed to elect a backup designated router or a designated router until it transitions out of waiting state. This prevents unnecessary changes of backup designated router.</li> <li>• <b>Designated Router.</b> This router is the designated router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network-LSA contains links to all routers (including the designated router) attached to the network.</li> <li>• <b>Backup Designated Router.</b> This router is the backup designated router on the attached network. It is promoted to designated router if the present designated router fails. The router establishes adjacencies to all other routers attached to the network. The backup designated router performs slightly different functions during the LSA flooding procedure, as compared to the designated router.</li> <li>• <b>Other Designated Router.</b> The interface is connected to a broadcast or NBMA network on which other routers were selected to be either the designated router or backup designated router. The router attempts to form adjacencies to both the designated router and the backup designated router.</li> </ul> <p><b>Note:</b> The state is displayed only if the OSPFv3 Admin mode is enabled.</p>
Designated Router	<p>The identity of the designated router for this network, in the view of the advertising router. The designated router is identified here by its router ID. The value 0.0.0.0 means that there is no designated router.</p> <p><b>Note:</b> This field displays only if the OSPFv3 admin mode is enabled.</p>
Backup Designated Router	<p>The identity of the backup designated router for this network, in the view of the advertising router. The backup designated router is identified here by its router ID. Set to 0.0.0.0 if there is no backup designated router.</p> <p><b>Note:</b> This field displays only if the OSPFv3 admin mode is enabled.</p>
Number of Link Events	<p>This is the number of times the specified OSPF interface changed its state.</p> <p><b>Note:</b> This field displays only if the OSPFv3 admin mode is enabled.</p>

## View OSPFv3 Interface Statistics

You can view statistics for the selected interface. The information is displayed only if OSPFv3 is enabled.

➤ **To view the OSPFv3 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.

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 > OSPFv3 > Advanced > Interface Statistics**.

OSPFv3 Interface Selection	
Interface	1/0/1

OSPFv3 Interface Statistics	
OSPFv3 Area ID	
Area Border Router Count	
AS Border Router Count	
Area LSA Count	
IPv6 Address	
Interface Events	
Virtual Events	
Neighbor Events	
Sent Packets	
Received Packets	
Discards	
Bad Version	
Virtual Link Not Found	
Area Mismatch	
Invalid Destination Address	
No Neighbor at Source Address	
Invalid OSPF Packet Type	
Hellos Ignored	
Hellos Sent	
Hellos Received	
DD Packets Sent	
DD Packets Received	

LS Requests Sent
LS Requests Received
LS Updates Sent
LS Updates Received
LS Acknowledgements Sent
LS Acknowledgements Received

8. In the OSPFv3 Interface Selection area of the screen, in the **Interface** list, select the interface.

To clear all the statistics of the OSPFv3 interface, click the **Clear** button.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable OSPF Interface Statistics data that is displayed.

**Table 162. Advanced OSPFv3 Interface Statistics**

Field	Description
OSPFv3 Area ID	The OSPFv3 area to which the selected router interface belongs. An OSPFv3 area ID is a 32-bit integer in dotted-decimal format that uniquely identifies the area to which the interface connects.
Area Border Router Count	The total number of area border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.
AS Border Router Count	The total number of autonomous system border routers reachable within this area. This is initially zero, and is calculated in each SPF pass.
Area LSA Count	The total number of link state advertisements in this area's link state database, excluding AS External LSAs.
IPv6 Address	The IPv6 address of the interface.
Interface Events	The number of times the specified OSPFv3 interface changed its state, or an error occurred.
Virtual Events	The number of state changes or errors that occurred on this virtual link.
Neighbor Events	The number of times this neighbor relationship changed state, or an error occurred.
Sent Packets	The number of OSPFv3 packets transmitted on the interface.
Received Packets	The number of valid OSPFv3 packets received on the interface.
Discards	The number of received OSPFv3 packets discarded because of an error in the packet or an error in processing the packet.
Bad Version	The number of received OSPFv3 packets whose version field in the OSPFv3 header does not match the version of the OSPFv3 process handling the packet.
Virtual Link Not Found	The number of received OSPFv3 packets discarded where the ingress interface is in a non-backbone area and the OSPFv3 header identifies the packet as belonging to the backbone, but OSPFv3 does not have a virtual link to the packet's sender.
Area Mismatch	The number of OSPFv3 packets discarded because the area ID in the OSPFv3 header is not the area ID configured on the ingress interface.

**Table 162. Advanced OSPFv3 Interface Statistics (continued)**

Field	Description
Invalid Destination Address	The number of OSPFv3 packets discarded because the packet's destination IP address is not the address of the ingress interface and is not the AllDrouters or AllSpfRouters multicast address.
No Neighbor at Source Address	The number of OSPFv3 packets dropped because the sender is not an existing neighbor or the sender's IP address does not match the previously recorded IP address for that neighbor.
Invalid OSPF Packet Type	The number of OSPFv3 packets discarded because the packet type field in the OSPFv3 header is not a known type.
Hellos Ignored	The number of received hello packets that were ignored by this router from the new neighbors after the limit was reached for the number of neighbors on an interface or on the system as a whole.
Hellos Sent	The number of hello packets sent on this interface by this router.
Hellos Received	The number of hello packets received on this interface by this router.
DD Packets Sent	The number of database description packets sent on this interface by this router.
DD Packets Received	The number of database description packets received on this interface by this router.
LS Requests Sent	The number of LS requests sent on this interface by this router.
LS Requests Received	The number of LS requests received on this interface by this router.
LS Updates Sent	The number of LS updates sent on this interface by this router.
LS Updates Received	The number of LS updates received on this interface by this router.
LS Acknowledgements Sent	The number of LS acknowledgements sent on this interface by this router.
LS Acknowledgements Received	The number of LS acknowledgements received on this interface by this router.

## View the OSPFv3 Neighbor Table

This screen displays the OSPFv3 neighbor table list. This information is displayed only if OSPFv3 is enabled, and there exists at least one OSPFv3-enabled interface having a valid neighbor.

### ➤ To view the OSPFv3 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 **Routing > OSPFv3 > Advanced > Neighbor Table**.

Interface	Interface Identifier	Router ID	Area ID	Options	Router Priority	State	Dead Time(secs)	Events	Retransmission Queue length
-----------	----------------------	-----------	---------	---------	-----------------	-------	-----------------	--------	-----------------------------

To refresh the screen with the latest information on the switch, click the **Update** button.

To clear all the neighbors in the table, click the **Clear** button.

The following table describes the nonconfigurable data that is displayed.

**Table 163. Advanced OSPFv3 Neighbor Table**

Field	Description
Interface	The interface for which data is to be displayed or configured. Slot 0 is the base unit.
Interface Identifier	The interface ID that the neighbor advertises in its hello packets on this link.
Router ID	A 32-bit integer in dotted-decimal format representing the router ID of the neighbor on the selected interface.
Area ID	A 32-bit integer in dotted-decimal format representing the area common to the neighbor selected.
Options	A bit mask corresponding to the neighbor's options field.
Router Priority	The priority of this neighbor in the designated router election algorithm. A value of 0 signifies that the neighbor is not eligible to become the designated router on this particular network.
State	The state of the relationship with this neighbor.
Dead Time	The amount of time, in seconds, since the last hello was received from adjacent neighbors. Set to 0 for neighbors in a state less than or equal to Init.

Table 163. Advanced OSPFv3 Neighbor Table (continued)

Field	Description
Events	The number of times this neighbor relationship changed state, or an error occurred.
Retransmission Queue Length	An integer representing the current length of the selected neighbor's retransmit queue.

## View the OSPFv3 Link State Database

### ➤ To view the OSPF link state database:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > OSPFv3 > Advanced > Link State Database**.

OSPFv3 Link State Database

Router ID	Area ID	LSA Type	LS ID	Age	Sequence	Checksum	Options	Router Options
-----------	---------	----------	-------	-----	----------	----------	---------	----------------

OSPFv3 External LSA Database

Router ID	LSA Type	LS ID	Age	Sequence	Checksum
-----------	----------	-------	-----	----------	----------

To refresh the screen with the latest information on the switch, click the **Update** button.



The following table describes the nonconfigurable data that is displayed.

**Table 164. Advanced OSPFv3 Link State Database**

Field	Description
Router ID	The 32-bit integer in dotted-decimal format that uniquely identifies the router within the autonomous system (AS). The router ID is set on the OSPFv3 Configuration screen. To change the router ID you must first disable OSPFv3. After you set the new router ID, you must reenale OSPFv3 for the change to take effect. The default value is 0.0.0.0, although this is not a valid router ID.
Area ID	The ID of an OSPFv3 area to which one of the router interfaces is connected. An area ID is a 32-bit integer in dotted-decimal format that uniquely identifies the area to which an interface is connected.
LSA Type	<p>The format and function of the link state advertisement. LSA Type is one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Router LSA.</b> A router can originate one or more router LSAs for a given area. Each router LSA originated in an area describes the collected states of all the router's interfaces to the area.</li> <li>• <b>Network LSA.</b> A network LSA is originated for every link having two or more attached routers, by the designated router. It lists all the routers attached to the link.</li> <li>• <b>Inter-Area Router LSA.</b> This type describes a prefix external to the area, yet internal to the autonomous system. It is originated by an area border router.</li> <li>• <b>AS-External LSA.</b> This LSA type describes a path to a prefix external to the autonomous system and is originated by an autonomous system border router.</li> <li>• <b>Link LSA.</b> A router originates a separate Link LSA for each attached link. It provides router's link local address to routers attached to the link and also inform them of a list of IPv6 prefixes to associate with the link.</li> <li>• <b>Intra-Area-Prefix LSA.</b> A link's designated router originates one or more intra-area prefix lsas to advertise the link's prefixes throughout the area. A router can originate multiple intra-area-prefix lsas for a given area to advertise its own prefixes and those of its attached stub links.</li> </ul>
LS ID	The link state ID identifies the piece of the routing domain that is being described by the advertisement. The value of the LS ID depends on the advertisement's LS type.
Age	The time since the link state advertisement was first originated, in seconds.
Sequence	The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement.
Checksum	The checksum is used to detect data corruption of an advertisement. This corruption can occur while an advertisement is being flooded, or while it is being held in a router's memory. This field is the checksum of the complete contents of the advertisement, except the LS age field.

Table 164. Advanced OSPFv3 Link State Database (continued)

Field	Description
Options	<p>The Options field in the link state advertisement header indicates which optional capabilities are associated with the advertisement. The options are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Q.</b> This enables support for QoS traffic engineering.</li> <li>• <b>E.</b> This describes the way AS-external LSAs are flooded.</li> <li>• <b>MC.</b> This describes the way IP multicast datagrams are forwarded according to the standard specifications.</li> <li>• <b>O.</b> This describes whether opaque LSAs are supported.</li> <li>• <b>V.</b> This describes whether OSPF++ extensions for VPN/COS are supported.</li> </ul>
Router Options	The router-specific options.

The following table describes the nonconfigurable data that is displayed in the External Link State Database (LSDB) table.

Table 165. Advanced OSPFv3 External Link State Database Table

Field	Description
Router ID	<p>The 32-bit integer in dotted-decimal format that uniquely identifies the router within the autonomous system (AS). The router ID is set on the OSPFv3 Configuration screen. To change the router ID you must first disable OSPFv3. After you set the new router ID, you must reenable OSPFv3 for the change to take effect. The default value is 0.0.0.0, although this is not a valid router ID.</p>
LSA Type	<p>The format and function of the link state advertisement. LSA Type is one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Router LSA.</b> A router can originate one or more router LSAs for a given area. Each router LSA originated in an area describes the collected states of all the router's interfaces to the area.</li> <li>• <b>Network LSA.</b> A network LSA is originated for every link having two or more attached routers, by the designated router. It lists all the routers attached to the link.</li> <li>• <b>Inter-Area Router LSA.</b> This type describes a prefix external to the area, yet internal to the autonomous system. It is originated by an area border router.</li> <li>• <b>AS-External LSA.</b> This LSA type describes a path to a prefix external to the autonomous system and is originated by an autonomous system border router.</li> <li>• <b>Link LSA.</b> A router originates a separate link LSA for each attached link. It provides router's link local address to routers attached to the link and also inform them of a list of IPv6 prefixes to associate with the link.</li> <li>• <b>Intra-Area-Prefix LSA.</b> A link's designated router originates one or more intraarea-prefix LSAs to advertise the link's prefixes throughout the area. A router can originate multiple intra-area-prefix LSAs for a given area to advertise its own prefixes and those of its attached stub links.</li> </ul>

Table 165. Advanced OSPFv3 External Link State Database Table (continued)

Field	Description
LS ID	The link state ID identifies the piece of the routing domain that is being described by the advertisement. The value of the LS ID depends on the advertisement's LS type.
Age	The time since the link state advertisement was first originated, in seconds.
Sequence	The sequence number field is a signed 32-bit integer. It is used to detect old and duplicate link state advertisements. The larger the sequence number, the more recent the advertisement.
Checksum	The checksum is used to detect data corruption of an advertisement. This corruption can occur while an advertisement is being flooded, or while it is being held in a router's memory. This field is the checksum of the complete contents of the advertisement, except the LS age field.

## Configure the OSPFv3 Virtual Link

### ➤ To configure the OSPFv3 virtual 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 **Routing > OSPFv3 > Advanced > Virtual Link Configuration**.

OSPFv3 Virtual Link Configuration									
<input type="checkbox"/>	Area ID	Neighbor Router ID	Hello Interval	Dead Interval	lfransit Delay Interval	Retransmit Interval	Neighbor State	State	Metric
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>			

8. Enter the **Area ID** of the OSPF area.

An area ID is a 32-bit integer in dotted-decimal format that uniquely identifies the area to which a router interface connects. Virtual links can be configured between any pair of area border routers with interfaces to a common (non-backbone) area.

9. Configure the **Neighbor Router ID** by entering the neighbor portion of a virtual link specification.

Virtual links can be configured between any pair of area border routers having interfaces to a common (non-backbone) area.

10. In the **Hello Interval** field, enter the OSPFv3 hello interval for the specified interface in seconds.

This parameter must be the same for all routers attached to a network. The valid values range from 1 to 65,535. The default is 10 seconds.

11. In the **Dead Interval** field, enter the OSPFv3 dead interval for the specified interface in seconds.

This specifies how long a router waits to see a neighbor router's hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. This value is a multiple of the hello interval (for example, 4). The valid values range from 1 to 65,535. The default is 40.

12. In the **Iftransit Delay Interval** field, enter the OSPFv3 transit delay for the specified interface.

This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. The valid values range from 1 to 3600 seconds (1 hour). The default value is 1 second.

13. In the **Retransmit Interval** field, enter the OSPFv3 retransmit interval for the specified interface.

This is the number of seconds between link state advertisements for adjacencies belonging to this router interface. This value is also used when retransmitting database descriptions and link state request packets. The valid values range from 1 to 3600 seconds (1 hour). The default is 5 seconds.

14. Click the **Add** button

The new virtual link is added to the switch.

15. To remove the specified virtual link from the switch configuration, click the **Delete** button.

16. Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 166. Advanced OSPFv3 Virtual Link Configuration**

Field	Description
Neighbor State	<p>The state of the virtual neighbor relationship. The OSPFv3 interface state can be any of these values:</p> <ul style="list-style-type: none"> <li>• <b>Down.</b> This is the initial interface state. The lower-level protocols indicated that the interface is unusable. Interface parameters are set to their initial values. All interface timers are disabled, and there are no adjacencies associated with the interface.</li> <li>• <b>Waiting.</b> The router is trying to determine the identity of the (backup) designated router by monitoring received hello packets. The router is not allowed to elect a backup designated router or a designated router until it transitions out of the waiting state. This prevents unnecessary changes of the (backup) designated router.</li> <li>• <b>Point-to-Point.</b> The interface is operational, and is connected to the virtual link. On entering this state the router attempts to form an adjacency with the neighboring router. The interface sends hello packets to the neighbor at every hello interval seconds.</li> <li>• <b>Designated Router.</b> This router is the designated router on the attached network. adjacencies are established to all other routers attached to the network. The router must also originate a network LSA for the network node. The network-LSA contains links to all routers (including the designated router) attached to the network.</li> <li>• <b>Backup Designated Router.</b> This router is the backup designated router on the attached network. It is promoted to designated router if the present designated router fails. The router establishes adjacencies to all other routers attached to the network. The backup designated router performs slightly different functions during the flooding procedure, compared to the designated router.</li> <li>• <b>Other Designated Router.</b> The interface is connected to a broadcast or NBMA network on which other routers were selected to be the designated router and backup designated router. The router attempts to form adjacencies to both the designated router and the backup designated router.</li> </ul>
State (continued on the next page)	<p>The state of the interface. It takes one the following values:</p> <ul style="list-style-type: none"> <li>• <b>Down.</b> This is the initial interface state. The lower-level protocols indicated that the interface is unusable. Interface parameters are set to their initial values. All interface timers are disabled, and there are no adjacencies associated with the interface.</li> <li>• <b>Waiting.</b> The router is trying to determine the identity of the backup designated router by monitoring received hello packets. The router is not allowed to elect a backup designated router or a designated router until it transitions out of waiting state. This prevents unnecessary changes of backup designated router.</li> <li>• <b>Point-to-Point.</b> The interface is operational, and is connected either to the virtual link. On entering this state the router attempts to form an adjacency with the neighboring router. hello packets are sent to the neighbor every hello interval seconds.</li> </ul>

Table 166. Advanced OSPFv3 Virtual Link Configuration (continued)

Field	Description
State (continued)	<ul style="list-style-type: none"> <li>• <b>Designated Router.</b> This router is the designated router on the attached network. Adjacencies are established to all other routers attached to the network. The router must also originate a network-LSA for the network node. The network- LSA contains links to all routers (including the designated router) attached to the network.</li> <li>• <b>Backup Designated Router.</b> This router is the backup designated router on the attached network. It is promoted to designated router if the present designated router fails. The router establishes adjacencies to all other routers attached to the network. The backup designated router performs slightly different functions during the flooding procedure, as compared to the designated router.</li> <li>• <b>Other Designated Router.</b> The interface is connected to a broadcast or NBMA network on which other routers were selected to be the designated router and backup designated router either. The router attempts to form adjacencies to both the designated router and the backup designated router.</li> </ul>
Metric	The metric value used by the virtual link.

## Configure OSPFv3 Route Redistribution

You can configure the OSPFv3 Route Redistribution parameters. The allowable values for each field are displayed next to the field. If any invalid values are entered, an alert message is displayed with the list of all the valid values.

### ➤ To configure the OSPFv3 route redistribution:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > OSPFv3 > Advanced > Route Redistribution**.

OSPFv3 Route Redistribution					
<input type="checkbox"/>	Source	Redistribute Option	Metric	Metric Type	Tag
<input type="checkbox"/>		▼		▼	
<input type="checkbox"/>	Connected	Disable	0	External Type 2	0
<input type="checkbox"/>	Static	Disable	0	External Type 2	0

8. From the **Source** menu, select from the list of available source routes that were not previously configured for redistribution by OSPFv3. The valid values are as follows:

- Connected
- Static

9. In the **Redistribute Option** list, select to **Enable** or **Disable** the redistribution for the selected source protocol.

10. Set the **Metric** value to be used as the metric of redistributed routes.

This field displays the metric if the source was preconfigured; otherwise, the tag is 0 and can be modified. The valid values are 0 to 16777214.

11. From the **Metric Type** list, select the OSPFv3 metric type of redistributed routes.

12. Set the **Tag** field in routes redistributed.

This field displays the tag if the source was preconfigured; otherwise, the tag is 0 and can be modified. The valid values are 0 to 4294967295.

13. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

## View the NSF OSPFv3 Summary

You can view the NSF OSPFv3 summary. The allowable values for each field are displayed next to the field. If any invalid values are entered, an alert message is displayed with the list of all the valid values.

### ➤ To view the NSF OSPF 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.

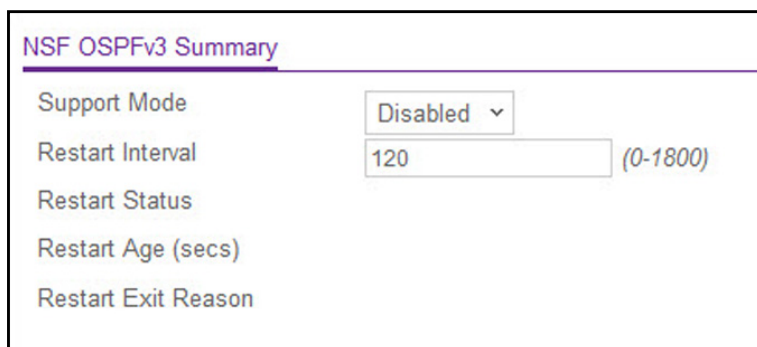
5. Enter the user name and password.

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 **Routing > OSPFv3 > Advanced > NSF OSPFv3 Summary**.



8. From the **Support mode** list, select one of the following values:
  - **Always**. OSPF performs a graceful restart for all planned and unplanned warm restart events.
  - **Disabled**. Prevents OSPF from performing graceful restarts.
  - **Planned**. OSPF performs a graceful restart only when a restart is planned (for example, due to an **initiate failover** command).

The default is Disabled. This setting configures how the unit performs graceful restarts.

9. Configure the **Restart Interval**.

The valid values are 0 to 1800 in seconds. The default is 120 seconds.

10. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.



The following table describes the nonconfigurable data that is displayed.

**Table 167. Advanced NSF OSPFv3 Summary**

Field	Description
Restart Status	<p>The restart status of OSPF helper feature. The possible values are as follows:</p> <ul style="list-style-type: none"> <li>• Not Restarting</li> <li>• Planned Restart</li> <li>• Unplanned Restart</li> </ul>
Restart Age (seconds)	The amount of time since the last restart occurred.
Restart Exit Reason	<p>Displays how the master unit on the chassis last started up. The possible values are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Not Attempted.</b> Graceful restart was not been attempted.</li> <li>• <b>In Progress.</b> Restart is in progress.</li> <li>• <b>Completed.</b> The previous graceful restart completed successfully.</li> <li>• <b>Timed Out.</b> The previous graceful restart timed out.</li> <li>• <b>Topology Changed.</b> The previous graceful restart terminated prematurely because of a topology change.</li> </ul>

# Multicast Routing

---

# 7

This chapter covers the following topics:

- *Multicast Overview*
- *Configure Multicast IGMP Settings*
- *Configure PIM Settings*
- *Configure Multicast Static Routes*
- *Configure the Multicast Admin Boundary*
- *Configure IPv6 Multicast Settings*

## Multicast Overview

Only the following switches support multicast:

- M6100
- M5300-28G3
- M5300-52G3
- M5300-28GF3

The following switches support multicast with an L3 license:

- M5300-28G
- M5300-52G
- M5300-28G-POE+
- M5300-52G-POE+

The NETGEAR ProSafe Managed Multicast component is best suited for video and audio traffic requiring multicast packet control for optimal operation. The Multicast component includes support for IGMPv2 and IGMPv3. Communication from point to multipoint is called multicasting. The source host (point) transmits a message to a group of zero or more hosts (multipoint) that are identified by a single IP destination address. Although the task can be accomplished by sending unicast (point-to-point) messages to each of the destination hosts, multicasting is the more desirable method for this type of transmission. A multicast message is delivered to all members of its destination host group with the same best-efforts reliability as regular unicast IP messages. The message is not guaranteed to arrive intact at all members of the destination group or in the same order relative to other messages.

## View the Multicast Mroute Table

### ➤ To view the Mroute 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 > Multicast > Mroute Table**.

Mroute Table									
Group IP	Source IP	Incoming Interface	Outgoing Interfaces	Up Time(hh:mm:ss)	Expiry Time(hh:mm:ss)	RPF Neighbor	Protocol	Flags	

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 168. Multicast Mroute Table**

Field	Description
Group IP	The destination group IP address.
Source IP	The IP address of the multicast packet source to be combined with the group IP to fully identify a single route whose Mroute table entry.
Incoming Interface	The incoming interface on which multicast packets for this source/group arrive.
Outgoing Interfaces	The list of outgoing interfaces on which multicast packets for this source/group are forwarded.
Up Time (hh:mm:ss)	The time in seconds since the entry was created.
Expiry Time (hh:mm:ss)	The time in seconds before this entry ages out and is removed from the table.
RPF Neighbor	The IP address of the reverse path forwarding (RPF) neighbor.
Protocol	The multicast routing protocol which created this entry. The possible values are as follows: <ul style="list-style-type: none"> <li>PIM-DM</li> <li>PIM-SM</li> <li>DVMRP</li> </ul>
Flags	The value displayed in this field is valid if the multicast routing protocol running is PIM-SM. The possible values are <b>RPT</b> or <b>SPT</b> . For other protocols a "-----" is displayed.

## Configure Global Multicast Settings

➤ **To configure global multicast 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 > Multicast > Global Configuration**.

Global Configuration	
Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Protocol State	Non-Operational
Table Maximum Entry Count	2048
Protocol	No Protocol Enabled
Table Entry Count	0

8. In the **Admin Mode** field, select the **Enable** or **Disable** option to set the administrative status of multicast forwarding in the router.

The default is **Disable**.

9. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

The following describes the nonconfigurable data that is displayed.

**Table 169. Multicast Global Configuration**

Field	Description
Protocol State	The operational state of the multicast forwarding module.
Table Maximum Entry Count	The maximum number of entries in the IP multicast routing table.
Protocol	The multicast routing protocol presently activated on the router, if any.
Table Entry Count	The number of multicast route entries currently present in the multicast route table.

## Configure the Multicast Interface

➤ **To configure the multicast 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 **Routing > Multicast > Interface Configuration**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance				
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast

Multicast							
• Mroute Table	Configuration						
• Global Configuration	1 2 3 VLANs All Go To Interface <input type="text"/> <input type="button" value="Go"/>						
• <b>Interface Configuration</b>	<table border="1"> <thead> <tr> <th>Interface</th> <th>TTL Threshold</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> 1/0/1</td> <td>1</td> </tr> <tr> <td><input type="checkbox"/> 1/0/2</td> <td>1</td> </tr> </tbody> </table>	Interface	TTL Threshold	<input type="checkbox"/> 1/0/1	1	<input type="checkbox"/> 1/0/2	1
Interface	TTL Threshold						
<input type="checkbox"/> 1/0/1	1						
<input type="checkbox"/> 1/0/2	1						
• DVMRP							
• IGMP							

8. In the **Go To Interface** field, enter the interface in unit/slot/port format and click the **Go** button.

The entry corresponding to the specified interface is selected.

9. Select the check box next to the routing interface.
10. Enter the **TTL Threshold** below which a multicast data packet is not forwarded from the selected interface.

Enter a number between 0 and 255. The default is 1. If you enter **0**, all multicast packets for the selected interface are forwarded. You must configure at least one router interface before you see this field.

11. Click the **Apply** button.

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

## Configure Global Multicast DVMRP Settings

➤ **To configure global multicast DVMRP 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 > Multicast > DVMRP > Global Configuration**.

DVMRP Global Configuration	
Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Version	3
Total Number of Routes	0
Reachable Routes	0

8. Select the **Admin Mode Disable** or **Enable** radio button.  
This sets the administrative status of DVMRP to active or inactive. The default is Disable.
9. Click the **Apply** button.  
The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable data that is displayed.

**Table 170. DVMRP Global Configuration**

Field	Description
Version	The current value of the DVMRP version string.
Total Number of Routes	The number of routes in the DVMRP routing table.
Reachable Routes	The number of routes in the DVMRP routing table that use a non-infinite metric.

## Configure the DVMRP Interface

### ➤ To configure the multicast DVMRP 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 **Routing > Multicast > DVMRP > Interface Configuration**.

System									
Switching		Routing		QoS		Security		Monitoring	
Routing Table		IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery
Multicast		IPv6 Multicast							
DVMRP Interface Configuration									
1 2 3 VLANs All									
Go To Interface <input type="text"/> <input type="button" value="Go"/>									
Interface		Interface Mode	Protocol State	Local Address	Interface Metric	Generation ID	Received Bad Packets	Received Bad Routes	Sent Routes
<input type="checkbox"/>	1/0/1	Disable	Non-Operational		1		0	0	0
<input type="checkbox"/>	1/0/2	Disable	Non-Operational		1		0	0	0
<input type="checkbox"/>	1/0/3	Disable	Non-Operational		1		0	0	0

8. In the **Go To Interface** field, enter the interface in unit/slot/port format and click the **Go** button.
9. Select the check box next to the **Interface** for which data is to be displayed or configured.
10. In the **Interface Mode** field, select the **Enable** or **Disable** option to set the administrative mode of the selected DVMRP routing interface.

The default is Disable.

11. In the **Interface Metric** field, enter the DVMRP metric for the selected interface.

This value is sent in DVMRP messages as the cost to reach this network. Valid values are 1 to 31. The default value is 1.

12. Click the **Apply** button.



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

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 171. DVMRP Interface Configuration**

Field	Description
Protocol State	The operational state of the DVMRP protocol on the selected interface, either Operational or Non-Operational.
Local Address	The IP address used as a source address in packets sent from the selected interface.
Generation ID	The DVMRP generation ID used by the router for the selected interface. This value is reset every time an interface is started and is placed in prune messages. A change in generation ID informs the neighbor routers to discard any previous information about this router.
Received Bad Packets	The number of invalid packets received on the selected interface.
Received Bad Routes	The number of invalid routes received on the selected interface.
Sent Routes	The number of routes sent on the selected interface.

## View the DVMRP Neighbor

### ➤ To view the multicast DVMRP neighbor :

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

8. Use the **Search** menu to search for neighbor entries by MAC **Interface** or **Neighbor IP**.

- Select **Search > Interface** from the list, enter the interface in unit/slot/port format, for example 1/0/13, then click the **Go** button. If the neighbor entry exists, the entry is displayed as the first entry, followed by the remaining entries.
- Select **Search > Neighbor IP** from the list, enter the neighbor IP, then click the **Go** button. If the entry with the matching neighbor IP exists, that entry is displayed as the first entry, followed by the remaining entries. An exact match is required.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 172. DVMRP Neighbor**

Field	Description
Interface	Select the interface for which data is to be displayed, or all the interfaces are displayed.
Neighbor IP	The IP address of the neighbor whose information is displayed
State	The state of the specified neighbor router on the selected interface, either active or down.
Up Time	The DVMRP uptime for the specified neighbor on the selected interface. This is the time since the neighbor entry was learned.
Expiry Time	The DVMRP expiry time for the specified neighbor on the selected interface. This is the time left before this neighbor entry ages out, and is not applicable if the neighbor router's state is down.
Generation ID	The DVMRP generation ID for the specified neighbor on the selected interface.
Major Version	The DVMRP major version for the specified neighbor on the selected interface.
Minor Version	The DVMRP minor version for the specified neighbor on the selected interface.
Capabilities	The DVMRP capabilities of the specified neighbor on the selected interface.
Received Routes	The number of routes received for the specified neighbor on the selected interface.

Table 172. DVMRP Neighbor (continued)

Field	Description
Received Bad Packets	The number of invalid packets received for the specified neighbor on the selected interface.
Received Bad Routes	The number of invalid routes received for the specified neighbor on the selected interface.

## View the DVMRP Next Hop Settings

➤ **To view the multicast DVMRP Next Hop 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.

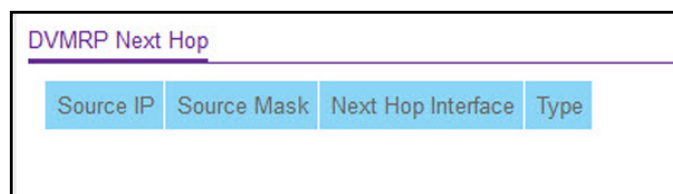
5. Enter the user name and password.

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 > Multicast > DVMRP > DVMRP Next Hop**.



DVMRP Next Hop			
Source IP	Source Mask	Next Hop Interface	Type

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

Table 173. DVMRP Next Hop

Field	Description
Source IP	The IP address used with the source mask to identify the source network for this table entry.
Source Mask	The network mask used with the source IP address.

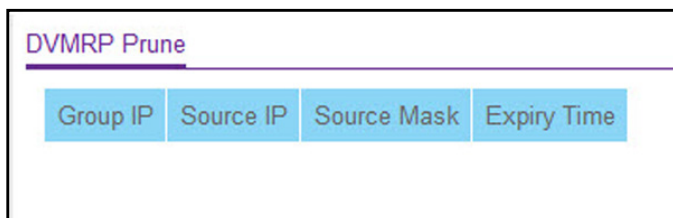
Table 173. DVMRP Next Hop (continued)

Field	Description
Next Hop Interface	The outgoing interface for this next hop.
Type	The next hop type. <b>Leaf</b> means that no downstream dependent neighbors exist on the outgoing interface. Otherwise, the type is <b>branch</b> .

## View the Multicast DVMRP Prune

### ➤ To view the multicast DVMRP prune:

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



DVMRP Prune			
Group IP	Source IP	Source Mask	Expiry Time

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 174. DVMRP Prune**

Field	Description
Group IP	The group address that was pruned.
Source IP	The IP address used with the source mask to identify the source network for this table entry.
Source Mask	The network mask used with the source IP address.
Expiry Time	The amount of time remaining before this prune will expire at the upstream neighbor. If no prune messages were received from downstream neighbors, this is set to the value of the default prune lifetime timer; otherwise, it is set to the smallest received value or the default timer, whichever is less.

## View the DVMRP Route

### ➤ To view the multicast DVMRP route:

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

DVMRP Route						
Source Address	Source Mask	Upstream Neighbor	Interface	Metric	Expiry Time	Up Time

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 175. DVMRP Route**

Field	Description
Source Address	The network address that is combined with the source mask to identify the sources for this entry.
Source Mask	The network subnet mask used with the source IP address to identify the sources for this entry.
Upstream Neighbor	The address of the upstream neighbor (for example, RPF neighbor) from which IP datagrams from these sources are received.
Interface	The interface on which IP datagrams sent by these sources are received. A value of 0 typically means the route is an aggregate for which no next-hop interface exists.
Metric	The distance in hops to the source subnet.
Expiry Time	The amount of time remaining before this prune expires at the upstream neighbor. If no prune messages were received from downstream neighbors, this is set to value of the default prune lifetime timer, otherwise it is set to the smallest received value or the default timer, whichever is less.
Up Time	The time since the route represented by this entry was learned by the router.

## Configure Multicast IGMP Settings

You can configure IGMP settings and view IGMP statistics.

### Configure IGMP Global Settings

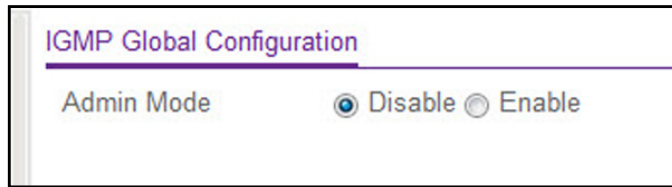
➤ **To configure the IGMP global settings:**

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 **Routing > Multicast > IGMP > Global Configuration**.



8. In the **Admin Mode** field, select the **Enable** or **Disable** option.

This sets the administrative status of IGMP in the router to active or inactive. The default is Disable.

9. Click the **Apply** button.

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

## Configure the IGMP Routing Interface

### ➤ To configure the IGMP routing 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 the **Routing > Multicast > IGMP > Routing Interface Configuration**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index			
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast

IGMP Routing Interface Configuration											
1 2 3 VLANs All											
Interface	Admin Mode	Version	Robustness	Query Interval	Query Max Response Time	Startup Query Interval	Startup Query Count	Last Member Query Interval	Last Member Query Count	Go To Interface <input type="text"/> <input type="button" value="Go"/>	
<input type="checkbox"/> 1/0/1	Disable	V3	2	125	100	31	2	10	2		
<input type="checkbox"/> 1/0/2	Disable	V3	2	125	100	31	2	10	2		
<input type="checkbox"/> 1/0/3	Disable	V3	2	125	100	31	2	10	2		
<input type="checkbox"/> 1/0/4	Disable	V3	2	125	100	31	2	10	2		
<input type="checkbox"/> 1/0/5	Disable	V3	2	125	100	31	2	10	2		
<input type="checkbox"/> 1/0/6	Disable	V3	2	125	100	31	2	10	2		

8. In the **Go To Interface** field, enter the interface in unit/slot/port format and click the **Go** button.

The entry corresponding to the specified interface is selected.

9. Select the check box beside the interface for which data is to be displayed or configured.

10. In the **Admin Mode** field, select the **Enable** or **Disable** option to set the administrative status of IGMP on the selected routing interface.

The default is Disable.

11. In the **Version** field, enter the version of IGMP to configure for the selected interface.

Valid values are 1 to 3. The default value is 3. This field is configurable only when IGMP Interface mode is enabled.

12. In the **Robustness** field, enter the robustness value.

This variable allows tuning for the expected packet loss on a subnet. If you expect the subnet to be lossy, enter a higher number for this parameter. IGMP is robust to robustness variable –1 packet losses. Valid values are 1 to 255. The default value is 2.

13. In the **Query Interval** field, enter the frequency in seconds at which IGMP host-query packets are to be transmitted on this interface.

Valid values are 1 to 3600. The default value is 125.

14. In the **Query Max Response Time** field, enter the maximum query response time, in tenths of a second, to be advertised in IGMPv2 queries on this interface.

The default value is 100. Valid values are 0 to 255.

15. In the **Startup Query Interval** field, enter the number of seconds between the transmission of startup queries on the selected interface.

Valid values are 1 to 300. The default value is 31.

16. In the **Startup Query Count** field, enter the number of queries to be sent on startup.

The valid values are 1 to 20. The default value is 2.

17. In the **Last Member Query Interval** field, enter the last member query interval in tenths of a second.



This is the maximum response time to be inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. Valid values are from 0 to 255. The default value is 10. This value is not used for IGMP version 1.

18. In the **Last Member Query Count** field, enter the number of queries to be sent on receiving a leave group report.

Valid values are from 1 to 20. The default value is 2.

19. Click the **Apply** button.

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

## View IGMP Routing Interface Statistics

- To view the IGMP routing 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.

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 > Multicast > IGMP > Routing Interface Statistics**.

System	Switching		Routing		QoS		Security	Monitoring	Maintenance	Help	Index
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast

Multicast

• Mroute Table

• Global Configuration

• Interface Configuration

• DVMRP

• IGMP

• Global Configuration

• Routing Interface Configuration

• Routing Interface Statistics

• IGMP Groups

1

2

3

VLANs

All

Interface	IP Address	Subnet Mask	Protocol State	Querier IP	Querier Status	Querier Up Time	Querier Expiry Time	Wrong Version Queries Received	Number of Joins Received	Number of Groups
1/0/1	20.10.10.10	255.255.255.0	Non-Operational							
1/0/2	0.0.0.0	0.0.0.0	Non-Operational							
1/0/3	0.0.0.0	0.0.0.0	Non-Operational							
1/0/4	0.0.0.0	0.0.0.0	Non-Operational							
1/0/5	0.0.0.0	0.0.0.0	Non-Operational							
1/0/6	0.0.0.0	0.0.0.0	Non-Operational							
1/0/7	0.0.0.0	0.0.0.0	Non-Operational							
1/0/8	0.0.0.0	0.0.0.0	Non-Operational							
1/0/9	0.0.0.0	0.0.0.0	Non-Operational							

To refresh the screen with the latest information on the switch, click the **Update** button. The following table describes the nonconfigurable data that is displayed.

**Table 176. Multicast IGMP Routing Interface Statistics**

Field	Description
Interface	The interface on which the IGMP is enabled.
IP Address	The IP address of the selected interface.
Subnet Mask	The subnet mask for the IP address of the selected interface.
Protocol State	The operational state of IGMP on the selected interface, either Operational or Non-Operational.
Querier IP	The address of the IGMP querier on the IP subnet to which the selected interface is attached.
Querier Status	Indicates whether the selected interface is in querier or non-querier mode.
Querier Up Time	The time in seconds since the IGMP interface querier was last changed.
Querier Expiry Time	The time in seconds remaining before the other querier present timer expires. If the local system is the querier, this is zero.
Wrong Version Queries Received	The number of queries that were received on the selected interface with an IGMP version that does not match the IGMP version configured for the interface, over the lifetime of the entry. IGMP requires that all routers on a LAN be configured to run the same version of IGMP. Therefore, a configuration error is indicated if any queries are received with the wrong version number.
Number of Joins Received	The number of times a group membership was added on the selected interface; that is, the number of times an entry for this interface was added to the cache table. This gives an indication of the amount of IGMP activity on the interface.
Number of Groups	The current number of entries for the selected interface in the cache table.

## View the IGMP Groups

➤ **To view the IGMP 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 **Routing > Multicast > IGMP > IGMP Groups**.

Interface	Multicast Group IP	Last Reporter	Up Time	Expiry Time	Version 1 Host Timer	Version 2 Host Timer	Compatibility	Filter Mode
-----------	--------------------	---------------	---------	-------------	----------------------	----------------------	---------------	-------------

8. Use the **Search** menu to search for multicast entries by **Interface** or **Group**.
  - Select **Interface** from the **Search** list, enter the interface in unit/slot/port format, for example 1/0/13, then click the **Go** button. If the entry exists, the entry is displayed as the first entry, followed by the remaining entries.
  - Select **Group** from the **Search** list, enter the multicast group IP, then click the **Go** button. If the entry exists, that entry with the matching group is displayed as the first entry, followed by the remaining entries. An exact match is required.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 177. Multicast IGMP Groups**

Field	Description
Interface	The interface for which data is to be displayed.
Multicast Group IP	The IP multicast group address for which data is to be displayed.
Last Reporter	The IP address of the source of the last membership report received for the IP multicast group address on the selected interface.
Up Time	The time elapsed since this entry was created.
Expiry Time	The minimum amount of time remaining before this entry is aged out.

Table 177. Multicast IGMP Groups (continued)

Field	Description
Version 1 Host Timer	The time remaining until the local router assumes that no IGMP version 1 members are on the IP subnet attached to this interface. When an IGMPv1 membership report is received, this timer is reset to the group membership timer. While this timer is non-zero, the local router ignores any IGMPv2 leave messages for this group that it receives on the selected interface. This field is displayed only if the interface is configured for IGMP version 1.
Version 2 Host Timer	The time remaining until the local router assumes that no IGMP version 2 members are on the IP subnet attached to this interface. When an IGMPv2 membership report is received, this timer is reset to the group membership timer. While this timer is non-zero, the local router ignores any IGMPv1 and IGMPv3 leave messages for this group that it receives on the selected interface. This field is displayed only if the interface is configured for IGMP version 2.
Compatibility	This parameter shows group compatibility mode (v1, v2, and v3) for this group on the specified interface.
Filter Mode	The source filter mode ( <b>Include</b> , <b>Exclude</b> , or <b>NA</b> ) for the specified group on this interface. When NA mode is active, the field is blank.

## View the IGMP Membership

### ➤ To view the IGMP 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 **Routing > Multicast > IGMP > IGMP Membership**.

8. Use the **Search By** list to search for multicast entries by **Interface** or **Group IP**.
- Select **Interface** from the **Search** list, enter the interface in unit/slot/port format, for example, 1/0/13, then click the **Go** button. If the entry exists, the entry is displayed as the first entry, followed by the remaining entries.
  - Select **Group IP** from the **Search** list, enter the multicast group IP, then click the **Go** button. If the entry exists, that entry with the matching group IP is displayed as the first entry, followed by the remaining entries. An exact match is required.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 178. Multicast IGMP Membership**

Field	Description
Interface	The interface on which multicast packets are forwarded.
Group IP	The IP multicast group address for which data is to be displayed.
Compatibility Mode	This parameter shows group compatibility mode (v1, v2, and v3) for this group on the specified interface.
Source Filter Mode	The source filter mode ( <b>Include</b> , <b>Exclude</b> , or <b>NA</b> ) for the specified group on this interface. When NA mode is active, the field is blank.
Source Hosts	This parameter shows source addresses that are members of this multicast address.
Expiry Time	This parameter shows expiry time interval against each source address that are members of this multicast group. This is the amount of time after which the specified source entry is aged out.

## Configure the IGMP Proxy Interface

### ➤ To configure the IGMP proxy 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.

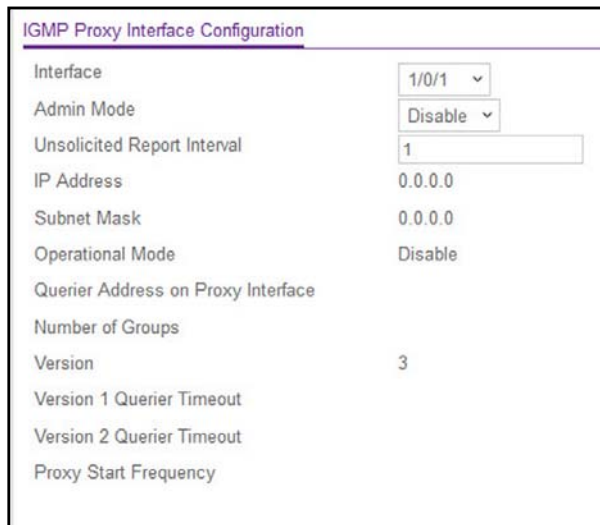
5. Enter the user name and password.

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 **Routing > Multicast > IGMP > Proxy Interface Configuration**.



8. Use the **Interface** list to select the port.

At least one router interface must be configured before you configure or display data for an IGMP proxy interface, and it must not be an IGMP routing interface.

9. Select **Enable** or **Disable** from the Admin Mode list.

This sets the administrative status of IGMP proxy on the selected interface. The default is Disable. Routing, IGMP and Multicast global admin modes must be enabled to enable IGMP proxy interface mode.

10. In the **Unsolicited Report Interval** field, enter the unsolicited time interval value in seconds.

The unsolicited report interval is the time between repetitions of a host's initial report of membership in a group. Valid values are from 1 to 260. The default value is 1.

11. Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 179. Multicast IGMP Proxy Interface Configuration**

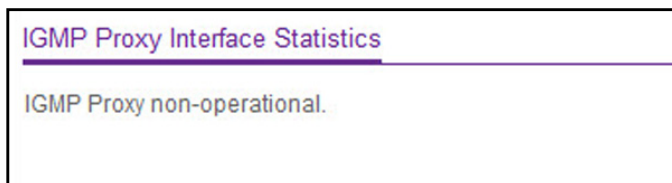
Field	Description
IP Address	The IP address of the IGMP proxy interface.
Subnet Mask	The subnet mask for the IP address of the IGMP proxy interface.
Operational Mode	The operational state of IGMP proxy interface.
Querier Address on Proxy Interface	The querier address on the proxy interface.
Number of Groups	The current number of multicast group entries for the IGMP proxy interface in the cache table.
Version	Enter the version of IGMP to configure on the selected interface. Valid values are 1 to 3; the default value is 3. This field is configurable only when IGMP proxy Interface mode is enabled.
Version 1 Querier Timeout	The older IGMP version 1 querier time-out value in seconds. The older version querier Interval is the time-out for transitioning a host back to IGMPv3 mode, once an older version query is heard. When an older version query is received, hosts set their older version querier present timer to older version querier Interval.
Version 2 Querier Timeout	The older IGMP version 2 querier time-out value in seconds.
Proxy Start Frequency	The number of times the proxy was brought up.

## View the IGMP Proxy Interface Statistics

### ➤ To view the IGMP proxy 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.  
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 > Multicast > IGMP > Proxy Interface Statistics**.



To refresh the screen with the latest information on the switch, click the **Update** button.

The following describes the nonconfigurable data that is displayed.

**Table 180. Multicast IGMP Proxy Interface Statistics**

Field	Description
Proxy Interface	The interface on which IGMP packets are received.
Version	The version of IGMP packets received.
Queries Received	The number of IGMP queries received.
Report Received	The number of IGMP reports received.
Reports Sent	The number of IGMP reports sent.
Leaves Received	The number of IGMP leaves received.
Leaves Sent	The number of IGMP leaves sent.

## View the IGMP Proxy Membership

➤ **To view the IGMP proxy 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 **Routing > Multicast > IGMP > Proxy Membership**.



IGMP Proxy Membership

Search By Group IP

Proxy Interface	Group IP	Source Hosts	Last Reporter	Up Time	Expiry Time	State	Filter Mode	Number of Sources
-----------------	----------	--------------	---------------	---------	-------------	-------	-------------	-------------------

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 181. Multicast IGMP Proxy Membership**

Field	Description
Proxy Interface	The interface on which IGMP proxy is enabled.
Group IP	The IP multicast group address.
Source Hosts	This parameter shows source addresses that are members of this multicast address.
Last Reporter	The IP address of the source of the last membership report received for the IP multicast group address on the IGMP proxy interface.
Up Time	The time elapsed since this entry was created.
Expiry Time	This parameter shows expiry time interval against each source address that is a member of this multicast group. This is the amount of time after which the specified source entry is aged out.
State	The state of the host entry. A host can be in one of the state. Non-member state - does not belong to the group on the interface. Delaying member state - host belongs to the group on the interface and report timer running. The report timer is used to send out the reports. Idle member state - host belongs to the group on the interface and no report timer running.
Filter Mode	The group filter mode (Include/Exclude/None) for the specified group on the IGMP proxy interface.
Number of Sources	The number of source hosts present in the selected multicast group.

## Configure PIM Settings


You can configure PIM settings and view PIM statistics.

## Configure the Multicast PIM Global Settings

Protocol-Independent Multicast (PIM) is a standard multicast routing protocol that provides scalable interdomain multicast routing across the Internet, independent of the mechanisms provided by any particular unicast routing protocol.

➤ **To configure the PIM 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 **Routing > Multicast > PIM > Global Configuration**.



PIM Global Configuration

Admin Mode ☒ Disable ☐ PIM-SM ☐ PIM-DM

8. In the **Admin Mode** field, select the protocol of PIM in the router.  
Possible values are **Disable**, **PIM-SM**, or **PIM-DM**. The default is **Disable**.
9. Click the **Apply** button.  
The updated configuration is sent to the switch. Configuration changes take effect immediately.

## Configure PIM SSM Settings

While PIM employs a specially configured rendezvous point (RP) router that serves as a meeting junction for multicast senders and listeners, Protocol-Independent Multicast Single-Source Multicast (PIM-SSM) does not use an RP. It supports only source route delivery trees. It is used between routers so that they can track which multicast packets to forward to each other and to their directly connected LANs. The SSM service model can be

implemented with a strict subset of the PIM protocol mechanisms. Both regular IP multicast and SSM semantics can coexist on a single router, and both can be implemented using the PIM protocol. A range of multicast addresses, currently 232.0.0.0/8 in IPv4 and FF3x::/32 in IPv6, is reserved for SSM.

➤ **To configure PIM SSM 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.

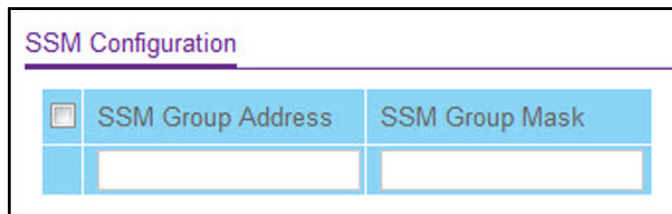
5. Enter the user name and password.

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 > Multicast > PIM > SSM Configuration**.



	SSM Group Address	SSM Group Mask
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

8. In the **SSM Group Address** field, enter the source-specific multicast group IP address.
9. In the **SSM Group Mask** field, enter the source-specific multicast group IP address mask.
10. Click the **Add** button.  
The source-specific group is added.
11. To delete the selected source-specific group., click the **Delete** button.

## Configure PIM Interface

➤ **To configure the multicast PIM 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 **Routing > Multicast > PIM > Interface Configuration**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index			
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast

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

The following table describes the nonconfigurable data that is displayed.

**Table 182. Multicast PIM Interface Configuration**

Field	Description
Protocol State	The state of PIM in the router. either Operational or Non-Operational.
IP Address	The IP address of the selected PIM interface. If you enter an IPv6 address, the format is prefix/prefix length.
Designated Router	The designated router on the selected PIM interface.
Neighbor Count	The number of PIM neighbors on the selected interface.

## View the PIM Neighbor

### ➤ To view the PIM neighbor:

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

PIM Neighbor

Search Interface  Go

Interface	Neighbor IP	Up Time(hh:mm:ss)	Expiry Time(hh:mm:ss)
-----------	-------------	-------------------	-----------------------

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 183. Multicast PIM Neighbor**

Field	Description
Interface	The interface on which the neighbor is displayed.
Neighbor IP	The IP address of the PIM neighbor for this entry.
Up Time (hh:mm:ss)	The time since this PIM neighbor (last) became a neighbor of the local router.
Expiry Time (hh:mm:ss)	The minimum time remaining before this PIM neighbor is aged out.

## View the PIM Candidate Rendezvous Point

### ➤ To view the multicast PIM candidate rendezvous point (RP):

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > Multicast > PIM > Candidate RP Configuration**.

**PIM Interface Selection**

Interface

**PIM Candidate RP Configuration**

<input type="checkbox"/>	Group Address	Group Mask	C-RP Advertisement Interval
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

The following table describes the nonconfigurable data that is displayed.

**Table 184. Multicast PIM Neighbor**

Field	Description
Field	Description
Interface	The interface on which the neighbor is displayed.
Neighbor IP	The IP address of the PIM neighbor for this entry.
Up Time (hh:mm:ss)	The time since this PIM neighbor (last) became a neighbor of the local router.
Expiry Time (hh:mm:ss)	The minimum time remaining before this PIM neighbor is aged out.

## View the PIM Neighbor

### ➤ To view the multicast PIM neighbor:

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

PIM Neighbor

Search Interface  Go

Interface	Neighbor IP	Up Time(hh:mm:ss)	Expiry Time(hh:mm:ss)
-----------	-------------	-------------------	-----------------------

To refresh the screen with the latest information on the switch, click the **Update** button.

**Table 185. Multicast PIM Neighbor**

Field	Description
Interface	The interface on which the neighbor is displayed.
Neighbor IP	The IP address of the PIM neighbor for this entry.
Up Time (hh:mm:ss)	The time since this PIM neighbor (last) became a neighbor of the local router.
Expiry Time (hh:mm:ss)	The minimum time remaining before this PIM neighbor is aged out.

## Configure the PIM Candidate Rendezvous Point

### ➤ To configure the PIM candidate rendezvous point (RP):

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > Multicast > PIM > Candidate RP Configuration**.

**PIM Interface Selection**

Interface

**PIM Candidate RP Configuration**

<input type="checkbox"/>	Group Address	Group Mask	C-RP Advertisement Interval
	<input type="text"/>	<input type="text"/>	<input type="text"/>



8. From the list of interfaces, select the **Interface**.
9. Enter the **Group Address** transmitted in candidate-RP-advertisements.  
If you enter an IPv6 address, the format is prefix/prefix length.
10. In the **Group Mask** field, enter the group address mask transmitted in candidate-RP-advertisements
11. In the **C-RP Advertisement Interval** field, specify the duration in seconds at which the C-RP messages are unicast to the bootstrap router (BSR).  
The range is from 1 to 16383 seconds. The default value is 60 seconds. If this field is submitted without any value, the default value is used.
12. Click the **Add** button.  
The candidate-RP address is added for the PIM router.
13. To delete the selected candidate-RP address for the PIM router, click the **Delete** button.

## Configure the PIM Bootstrap Router Candidate

- **To configure the multicast PIM bootstrap router (BSR) candidate:**
  1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
  2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
  3. Launch a web browser.
  4. Enter 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 > Multicast > PIM > BSR Candidate Configuration**.

PIM BSR Candidate Configuration	
Interface	1/0/1 ▾
Hash Mask Length	30 (0 to 32)
BSR Expiry Time (hh:mm:ss)	
Priority	0 (0 to 255)
IP Address	
Next bootstrap Message(hh:mm:ss)	
Next Candidate RP Advertisement(hh:mm:ss)	
Advertisement Interval (secs)	60 (1 to 16383)

8. From the list of interfaces, select the **Interface**.
9. Enter the C-BSR **Hash Mask Length** to be advertised in bootstrap messages.  
This hash mask length is used in the hash algorithm for selecting the RP for a particular group. The valid values are from 0 to 32. The default value is 30.
10. In the **Priority** field, enter the priority of C-BSR.
11. Enter the **Advertisement Interval** value of the C-BSR in seconds.  
The default value is 60.
12. Click the **Apply** button.  
The updated configuration is sent to the switch. Configuration changes take effect immediately.
13. Click the **Delete** button to remove the configured Hash Mask Length and Priority values and restore them to the default values.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 186. Multicast BSR Candidate Configuration**

Field	Description
BSR Expiry Time (hh:mm:ss)	Time (in hours, minutes and seconds) in which the learned elected bootstrap router (BSR) expires.
IP Address	The IP address of the elected BSR.
Next bootstrap Message (hh:mm:ss)	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.
Next Candidate RP Advertisement (hh:mm:ss)	Time (in hours, minutes, and seconds) in which the next candidate RP advertisement is sent.

## Configure the PIM Static Rendezvous Point

You can statically configure the rendezvous point (RP) address for one or more multicast groups.

➤ **To configure the PIM static RP:**

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

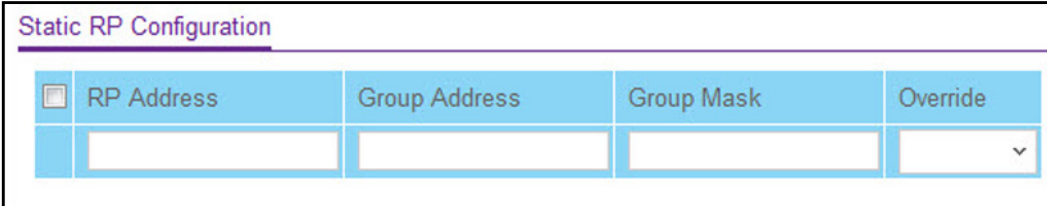
5. Enter the user name and password.

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 > Multicast > PIM > Static RP Configuration**.



Static RP Configuration				
<input type="checkbox"/>	RP Address	Group Address	Group Mask	Override
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="v"/>

8. In the **RP Address** field, enter the IP address for one or more multicast groups.
9. In the **Group Address** field, enter the group address of the RP.
10. Enter the **Group Mask** of the RP to be created or deleted.
11. In the **Override** field, select **Enable** or **Disable**.

**Enable** indicates that, if there is a conflict, the RP configured with this option prevails over the RP learned by BSR.

12. Click the **Add** button.

The static RP address is added for one or more multicast groups

13. To remove the selected RP address, click the **Delete** button.

14. Click the **Apply** button.

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

## Configure Multicast Static Routes

➤ **To configure multicast static 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.

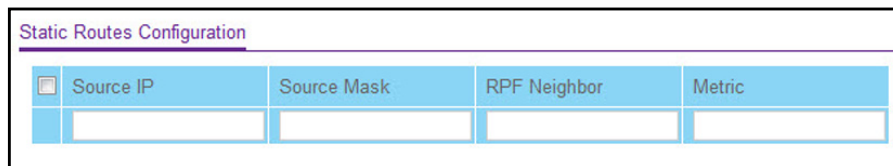
5. Enter the user name and password.

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 > Multicast > Static Routes Configuration**.



Static Routes Configuration				
<input type="checkbox"/>	Source IP	Source Mask	RPF Neighbor	Metric
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

8. In the **Source IP** field, enter the IP address that identifies the multicast packet source for the entry you are creating.
9. In the **Source Mask** field, enter the subnet mask to be applied to the source IP address.
10. In **RPF Neighbor** field, enter the IP address of the neighbor router on the path to the source.
11. In the **Metric** field, enter the link state cost of the path to the multicast source.

The range is 0 to 255, the default is 1. You can change the metric for a configured route by selecting the static route and editing this field.

12. Click the **Add** button.

The static route is added to the switch.

13. To delete the selected multicast static route, click the **Delete** button.

14. Click the **Apply** button.

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

## Configure the Multicast Admin Boundary

The definition of an administratively scoped boundary is a mechanism to stop the ingress and egress of multicast traffic for a given range of multicast addresses on a given routing interface.

➤ **To configure the multicast admin boundary:**

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

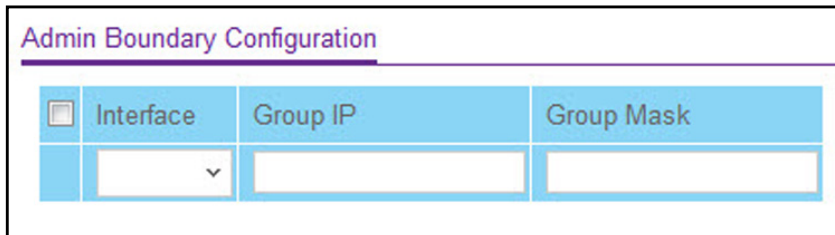
5. Enter the user name and password.

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 > Multicast > Admin Boundary Configuration**.



<input type="checkbox"/>	Interface	Group IP	Group Mask
	<input type="text" value="v"/>	<input type="text"/>	<input type="text"/>

8. In the **Interface** list, select the router interface for which the administratively-scoped boundary is to be configured.
9. In the **Group IP** field, enter the multicast group address for the start of the range of addresses to be excluded.

The address must be in the range of 239.0.0.0 through 239.255.255.255.

10. In the **Group Mask** field, enter the mask to be applied to the multicast group address.

The combination of the mask and the group IP gives the range of administratively scoped addresses for the selected interface.

11. Click the **Add** button.

The administratively scoped boundary is added.

12. To delete the selected administratively scoped boundary, click the **Delete** button.

## Configure IPv6 Multicast Settings

Only the following switches support IPv6 multicast:

- M6100
- M5300-28G3
- M5300-52G3
- M5300-28GF3

The following switches support IPv6 with an L3 license:

- M5300-28G
- M5300-52G
- M5300-28G-POE+
- M5300-52G-POE+

## View the IPv6 Multicast Mroute Table

You can view the contents of the Mroute Table in tabular format.

### ➤ To view the Mroute 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 > IPv6 Multicast > Mroute Table**.

Mroute Table								
Group IP	Source IP	Incoming Interface	Outgoing Interfaces	Up Time(hh:mm:ss)	Expiry Time(hh:mm:ss)	RPF Neighbor	Protocol	Flags

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 187. Multicast Mroute Table**

Field	Description
Group IP	The destination group IP address.
Source IP	The IP address of the multicast packet source to be combined with the group IP to fully identify a single route whose Mroute table entry.
Incoming Interface	The incoming interface on which multicast packets for this source/group arrive.
Outgoing Interfaces	The list of outgoing interfaces on which multicast packets for this source/group are forwarded.
Up Time (hh:mm:ss)	The time in seconds since the entry was created.
Expiry Time (hh:mm:ss)	The time in seconds before this entry ages out and is removed from the table.
RPF Neighbor	The IP address of the reverse path forwarding (RPF) neighbor.
Protocol	The multicast routing protocol which created this entry. The possible values are as follows: <ul style="list-style-type: none"> <li>PIM-DM</li> <li>PIM-SM</li> </ul>
Flags	The value displayed in this field is valid if the multicast routing protocol running is PIM-SM. The possible values are <b>RPT</b> or <b>SPT</b> . For other protocols a – (hyphen) is displayed.

## Configure the IPv6 PIM Global Settings

### ➤ To configure the IPv6 PIM 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.

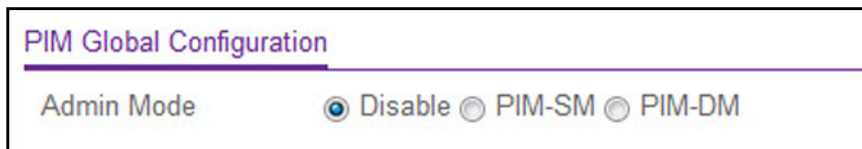
5. Enter the user name and password.

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 **Routing > IPv6 Multicast > IPv6 PIM > Global Configuration**.



8. Select an Admin Mode radio button.

The options are **Disable**, or the protocol variant of PIM option, dense mode (**PIM-DM**) or sparse mode (**PIM-SM**).

By default, this setting is disabled. The **Disable** option sets the administrative status of PM in the router to active or inactive.

9. Click the **Apply** button.

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

## Configure IPv6 PIM SSM

While PIM employs a specially-configured rendezvous point (RP) router that serves as a meeting junction for multicast senders and listeners, Protocol-Independent Multicast Single-Source Multicast (PIM-SSM) does not use an RP. It supports only source route delivery trees. It is used between routers so that they can track which multicast packets to forward to each other and to their directly connected LANs. The SSM service model can be implemented with a strict subset of the PIM protocol mechanisms. Both regular IP multicast and SSM semantics can coexist on a single router, and both can be implemented using the PIM protocol. A range of multicast addresses, currently 232.0.0.0/8 in IPv4 and FF3x::/32 in IPv6, is reserved for SSM.

### ➤ To configure the IPv6 PIM SSM 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.

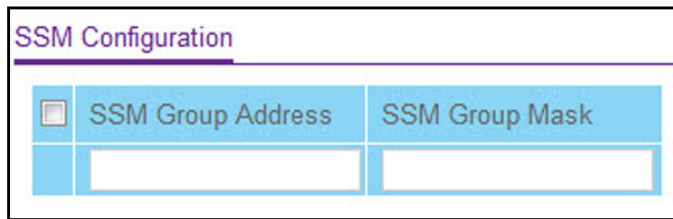
5. Enter the user name and password.

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 > IPv6 Multicast > IPv6 PIM > SSM Configuration**.



	SSM Group Address	SSM Group Mask
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

8. In the **SSM Group Address** field, enter the source-specific multicast group IP address.

9. In the **SSM Group Mask** field, enter the source-specific multicast group IP address mask.

10. Click the **Add** button.

The source-specific group is added.

11. To delete an existing source-specific group, click the **Delete** button.

## Configure the IPv6 PIM Interface

### ➤ To configure the IPv6 PIM 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 **Routing > IPv6 Multicast > IPv6 PIM > Interface Configuration**.

PIM Interface Configuration

1 All Go To Interface

<input type="checkbox"/>	Interface	Admin Mode	Protocol State	IPv6 Prefix/Length	Hello Interval	Join/Prune Interval	BSR Border	DR Priority	Designated Router	Neighbor Count
<input type="checkbox"/>	1/0/1	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/>	1/0/2	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/>	1/0/3	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/>	1/0/4	Disable	Non-Operational		30	60	Disable	1		
<input type="checkbox"/>	1/0/5	Disable	Non-Operational		30	60	Disable	1		

8. In the **Go To Interface** field, enter the interface in unit/slot/port format and click the **Go** button.

The entry corresponding to the specified interface is selected.

9. Select the check box beside the **Interface**.

10. In the **Admin Mode** field, select **Enable** or **Disable**.

This sets the administrative status of PIM-SM in the router. The default is Disable.

11. In the **Hello Interval** field, enter the time in seconds between the transmission of PIM hello messages on this interface.

The valid values are from 0 to 18000. The default value is 30.

12. In the **Join/Prune Interval** field, enter the frequency at which PIM Join/Prune messages are transmitted on this PIM interface.

The valid values are from 0 to 18000. The default value is 60.

13. In the **BSR Border** field, select the **Enable** or **Disable** option to set the bootstrap router (BSR) border status on the selected interface.

14. Enter the **DR Priority** for the selected interface.

The valid values are from 0 to 2147483647. The default value is 1.

15. Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 188. IPv6 PIM Interface Configuration**

Field	Description
Protocol State	The state of PIM in the router. either Operational or Non-Operational.
IPv6 Prefix/Length	The IPv6 address prefix and the length of the selected interface.
Designated Router	The designated router on the selected PIM interface.
Neighbor Count	The number of PIM neighbors on the selected interface.

## View the IPv6 PIM Neighbor

➤ **To view the IPv6 PIM neighbor:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > IPv6 Multicast > IPv6 PIM > PIM Neighbor**.

The screenshot shows the 'PIM Neighbor' web interface. At the top, there's a search bar with a dropdown menu currently set to 'Interface' and a 'Go' button. Below the search bar, there's a table with four columns: 'Interface', 'Neighbor IP', 'Up Time(hh:mm:ss)', and 'Expiry Time(hh:mm:ss)'.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 189. IPv6 PIM Neighbor**

Field	Description
Interface	The interface on which the neighbor is displayed.
Neighbor IP	The IP address of the PIM neighbor for this entry.
Up Time (hh:mm:ss)	The time since this PIM neighbor (last) became a neighbor of the local router.
Expiry Time (hh:mm:ss)	The minimum time remaining before this PIM neighbor is aged out.

## Configure the IPv6 PIM Candidate Rendezvous Point

➤ **To configure the IPv6 PIM candidate rendezvous point:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > IPv6 Multicast > IPv6 PIM > Candidate RP Configuration**.

PIM Interface Selection			
Interface		1/0/1	
PIM Candidate RP Configuration			
<input type="checkbox"/>	Group Address	Prefix Length	C-RP Advertisement Interval
	<input type="text"/>	<input type="text"/>	<input type="text"/>

8. From the list of interfaces, select the **Interface**.
9. In the **Group Address** field, enter the group IPv6 address prefix transmitted in candidate-RP-advertisements.
10. In the **Prefix Length** field, enter the group IPv6 Prefix Length transmitted in candidate-RP-advertisements.
11. In the **C-RP Advertisement Interval**, specify the duration in seconds at which the C-RP messages are unicast to the bootstrap router (BSR).  
The range is from 1 to 16383 seconds. The default value is 60 seconds. If this field is submitted without any value, the default value is used.
12. Click the **Add** button.  
The candidate-RP address is added for the PIM router.
13. To delete an existing candidate-RP address for the PIM router, click the **Delete** button.

## Configure the IPv6 PIM Bootstrap Router Candidate Settings

➤ **To configure the IPv6 PIM BSR Candidate 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 > IPv6 Multicast > IPv6 PIM > BSR Candidate Configuration**.

PIM BSR Candidate Configuration	
Interface	1/0/1 <input type="button" value="v"/>
Hash Mask Length	<input type="text" value="126"/> (0 to 128)
BSR Expiry Time (hh:mm:ss)	
Priority	<input type="text" value="0"/> (0 to 255)
IP Address	
Next bootstrap Message(hh:mm:ss)	
Next Candidate RP Advertisement(hh:mm:ss)	
Advertisement Interval (secs)	<input type="text" value="60"/> (1 to 16383)

8. From the list of interfaces, select the **Interface**.
9. Enter the C-BSR **Hash Mask Length** to be advertised in bootstrap messages.  
This hash mask length is used in the hash algorithm for selecting the RP for a particular group. The valid values are from 0 to 128. The default value is 126.
10. In the **Priority** field, enter the priority of the C-BSR.
11. Enter the **Advertisement Interval** value of the C-BSR in seconds.  
The default value is 60.  
To remove the configured Hash Mask Length, and Priority values and restore them to the default values, click the **Delete** button.

12. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 190. IPv6 PIM BSR Candidate Configuration**

Field	Description
BSR Expiry Time (hh:mm:ss)	Time (in hours, minutes and seconds) in which the learned elected bootstrap router (BSR) expires.
IP Address	The IP address of the elected BSR.
Next bootstrap Message (hh:mm:ss)	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.
Next Candidate RP Advertisement (hh:mm:ss)	Time (in hours, minutes, and seconds) in which the next candidate RP advertisement is sent.

## Configure the IPv6 PIM Static Rendezvous Point

You can statically configure the rendezvous point (RP) address for one or more multicast groups.

➤ **To configure the IPv6 PIM static RP:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > IPv6 Multicast > IPv6 PIM > Static RP Configuration**.

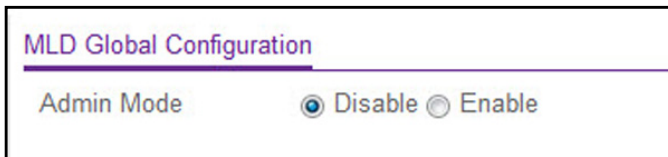
Static RP Configuration				
<input type="checkbox"/>	RP Address	Group Address	Prefix Length	Override
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="v"/>

8. In the **RP Address** field, enter the IP address of the RP.
9. In the **Group Address** field, enter the address of the RP.
10. In the **Prefix Length** field, enter the group address prefix length.
11. In the **Override** field, select **Enable** or **Disable**.  
**Enable** indicates that, if there is a conflict, the RP configured with this option prevails over the RP learned by BSR.
12. Click the **Add** button.  
The static RP address is added for one or more multicast groups.
13. To remove the selected RP address, click the **Delete** button.
14. Click the **Apply** button.  
The updated configuration is sent to the switch. Configuration changes take effect immediately.

## Configure IPv6 MLD Global Settings

### ➤ To configure the IPv6 PIM 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 **Routing > IPv6 Multicast > MLD > Global Configuration**.



MLD Global Configuration

Admin Mode ☒ Disable ☐ Enable

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

This sets the administrative status of MLD in the router to active or inactive. The default is Disable.

9. Click the **Apply** button.

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

## Configure the IPv6 MLD Routing Interface

### ➤ To configure the IPv6 MLD routing 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.

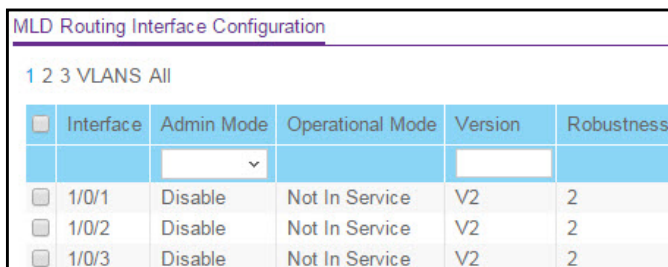
5. Enter the user name and password.

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 **Routing > IPv6 Multicast > MLD > Routing Interface Configuration**.



MLD Routing Interface Configuration

1 2 3 VLANs All

<input type="checkbox"/>	Interface	Admin Mode	Operational Mode	Version	Robustness
<input type="checkbox"/>	1/0/1	Disable	Not In Service	V2	2
<input type="checkbox"/>	1/0/2	Disable	Not In Service	V2	2
<input type="checkbox"/>	1/0/3	Disable	Not In Service	V2	2



Query Interval	Query Max Response Time	Startup Query Interval	Startup Query Count	Last Member Query Interval	Last Member Query Count
125	10000	31	2	1000	2
125	10000	31	2	1000	2
125	10000	31	2	1000	2
125	10000	31	2	1000	2
125	10000	31	2	1000	2

8. In the **Go To Interface** field, enter the interface in unit/slot/port format and click the **Go** button.

The entry corresponding to the specified interface is selected.

9. Select the check box beside the **Interface**.

10. In the **Admin Mode** field, select **Enable** or **Disable**.

This sets the administrative status of MLD on the selected routing interface. The default is Disable.

11. In the **Version** field, enter the version to configure for the selected interface.

Valid values are 1 to 2. The default value is 2.

12. In the **Query Interval** field, enter the frequency in seconds at which MLD host-query packets are to be transmitted on this interface.

Valid values are 1 to 3600. The default value is 125.

13. In the **Query Max Response Time** field, enter the maximum query response time, in milliseconds, to be advertised in MLDv2 queries on this interface.

Valid values are 0 to 65535. The default value is 10000 milliseconds.

14. In the **Startup Query Interval** field, enter the configured interval in seconds between general queries sent by a querier on startup.

The default value is 31.

15. Enter the **Startup Query Count** value to indicate the configured number of queries sent out on startup, separated by the startup query interval.

The default value is 2.

16. In the **Last Member Query Interval** field, enter the last member query interval in milliseconds.

This is the maximum response time to be inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. Valid values are from 0 to 65535. The default value is 1000 milliseconds.

17. In the **Last Member Query Count** field, enter the number of queries to be sent on receiving a leave group report.

Valid values are from 1 to 20. The default value is 2.

18. Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 191. IPv6 MLD Routing Interface Configuration**

Field	Description
Operational Mode	The operational status of MLD on the Interface.
Robustness	The robustness parameter for the selected interface. This variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the robustness variable can be increased. MLD is robust to robustness variable –1 packet losses. The default value is 2.

## View IPv6 MLD Routing Interface Statistics

### ➤ To view the IPv6 multicast MLD routing 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.

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 > IPv6 Multicast > MLD > Routing Interface Statistics**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index			
Routing Table	IP	IPv6	VLAN	ARP	RIP	OSPF	OSPFv3	Router Discovery	VRRP	Multicast	IPv6 Multicast
IPv6 Multicast											
MLD Routing Interface Statistics											
1 2 3 VLANs All											
• IPv6 PIM											
• MLD											
• Global Configuration											
• Routing Interface Configuration											
• Routing Interface Statistics											
• MLD Groups											
	Interface	Querier Status	Querier IP	Querier Up Time	Querier Expiry Time	Wrong Version Queries Received	Number of Joins Received	Number of Groups			
	1/0/1										
	1/0/2										
	1/0/3										
	1/0/4										
	1/0/5										
	1/0/6										
	1/0/7										

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

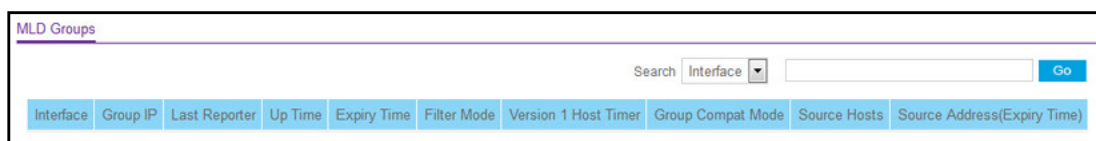
**Table 192. IPv6 MLD Routing Interface Statistics**

Field	Description
Interface	The interface for which data is to be displayed.
Querier Status	Indicates whether the selected interface is an MLD querier or non-querier on the subnet it is associated with.
Querier IP	The address of the MLD querier on the IP subnet to which the selected interface is attached.
Querier Up Time	The time in seconds since the MLD interface querier was last changed.
Querier Expiry Time	The time in seconds remaining before the other querier present timer expires. If the local system is the querier, this is zero.
Wrong Version Queries Received	The number of queries received whose MLD version does not match the MLD version of the interface.
Number of Joins Received	The number of times a group membership was added on the selected interface.
Number of Groups	The current number of membership entries for the selected interface in the cache table.

## View the IPv6 MLD Groups

### ➤ To view the IPv6 MLD 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 **Routing > IPv6 Multicast > MLD > MLD Groups**.



8. Use the **Search By** list to search for multicast entries by **Interface** or **Group**:

- Select **Interface** from the **Search** list, enter the interface in unit/slot/port format, for example 1/0/13, then click the **Go** button.

If the entry exists, it is displayed as the first entry, followed by the remaining entries.

- Select **Group** from the **Search** list, enter the MLD group IP, then click the **Go** button.

If the entry exists, it is displayed as the first entry, followed by the remaining entries. An exact match is required.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 193. IPv6 Multicast MLD Groups**

Field	Description
Interface	The interface for which data is to be displayed.
Group IP	The address of the MLD members.
Last Reporter	The IP address of the source of the last membership report received for this multicast group address on the selected interface.
Up Time	The time elapsed in seconds since the multicast group was known.
Expiry Time	Time left in seconds before the entry is removed from the MLD membership table of this interface.
Filter Mode	The filter mode of the multicast group on this interface. Possible values are <b>Include</b> and <b>Exclude</b> .
Version 1 Host Timer	The time remaining until the router assumes that there are no longer any MLD version 1 hosts on the specified interface.
Group Compat Mode	The compatibility mode of the multicast group on the interface. The values it can take are MLDv1 and MLDv2.
Source Hosts	This parameter shows source addresses that are members of this multicast address.
Source Address (Expiry Time)	This parameter shows expiry time interval against each source address that is a member of this multicast group. This is the amount of time after which the specified source entry is aged out.

## View IPv6 MLD Traffic

➤ **To view the IPv6 MLD traffic:**

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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 > IPv6 Multicast > MLD > MLD Traffic**.

MLD Traffic	
Valid MLD Packets Received	0
Valid MLD Packets Sent	0
Queries Received	0
Queries Sent	0
Reports Received	0
Reports Sent	0
Leaves Received	0
Leaves Sent	0

To clear all the MLD traffic, click the **Clear** button.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 194. IPv6 Multicast MLD Traffic**

Field	Description
Valid MLD Packets Received	The number of valid MLD packets received by the router.
Valid MLD Packets Sent	The number of valid MLD packets sent by the router.

Table 194. IPv6 Multicast MLD Traffic (continued)

Field	Description
Queries Received	The number of valid MLD queries received by the router.
Queries Sent	The number of valid MLD queries sent by the router.
Reports Received	The number of valid MLD reports received by the router.
Reports Sent	The number of valid MLD reports sent by the router.
Leaves Received	The number of valid MLD leaves received by the router.
Leaves Sent	The number of valid MLD leaves sent by the router.

## Configure the IPv6 MLD Proxy Interface

### ➤ To configure the IPv6 multicast MLD proxy 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 **Routing > IPv6 Multicast > MLD > Proxy Interface Configuration**.

MLD Proxy Interface Configuration	
Interface	1/0/1 ▾
Admin Mode	Disable ▾
Unsolicited Report Interval	1
IPv6 Prefix	
Prefix Length	
Operational Mode	Disable
Querier Address on Proxy Interface	
Number of Groups	
Version	V2
Version 1 Querier Timeout	
Proxy Start Frequency	

8. In the **Interface** list, select the interface.
9. In the **Admin Mode** list, select **Enable** or **Disable**.

This sets the administrative status of MLD proxy on the selected interface. The default is Disable. Routing, MLD, and Multicast global admin modes must be enabled to enable MLD proxy interface mode.

10. In the **Unsolicited Report Interval** field, enter the unsolicited time interval value in seconds.

The unsolicited report interval is the time between repetitions of a host's initial report of membership in a group. Valid values are 1 to 260. The default value is 1.

11. Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 195. IPv6 Multicast MLD Proxy Interface Configuration**

Field	Description
IPv6 Prefix	The IPv6 address of the MLD proxy interface.
Prefix Length	The prefix length for the IPv6 address of the MLD proxy interface.
Operational Mode	The operational state of MLD proxy interface.
Querier Address on Proxy Interface	The querier address on the proxy interface.
Number of Groups	The current number of multicast group entries for the MLD proxy interface in the cache table.
Version	This field is configurable only when MLD proxy interface mode is enabled. Enter the version of MLD to configure on the selected interface. Valid values are 1 to 2. The default version is 3.

**Table 195. IPv6 Multicast MLD Proxy Interface Configuration (continued)**

Field	Description
Version 1 Querier Timeout	The older MLD version 1 querier time-out value in seconds. The older version querier Interval is the time-out for transitioning a host back to MLDv2 mode once an older version query is heard. When an older version query is received, hosts set their older version querier present timer to Older Version querier Interval.
Proxy Start Frequency	The number of times the proxy was brought up.

## View IPv6 MLD Proxy Interface Statistics

➤ **To view the IPv6 multicast MLD proxy 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.

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 > IPv6 Multicast > MLD > Proxy Interface Statistics**.

MLD Proxy Interface Statistics					
Proxy Interface		1/0/42			
Version	Queries Received	Reports Received	Reports Sent	Leaves Received	Leaves Sent
1	0	0	0	0	0
2	0	0	0	-	-

To refresh the screen with the latest information on the switch, click the **Update** button.



The following table describes the nonconfigurable data that is displayed.

**Table 196. IPv6 Multicast MLD Proxy Interface Statistics**

Field	Description
Proxy Interface	The interface on which MLD proxy packets received.
Version	The version of MLD proxy packets received.
Queries Received	The number of MLD proxy queries received.
Reports Received	The number of MLD proxy reports received.
Reports Sent	The number of MLD proxy reports sent.
Leaves Received	The number of MLD proxy leaves received.
Leaves Sent	The number of MLD proxy leaves sent.

## View the IPv6 MLD Proxy Membership

### ➤ To view the IPv6 multicast MLD proxy 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 **Routing > IPv6 Multicast > MLD > Proxy Membership**.

MLD Proxy Membership

Search Group

Proxy Interface	Group IP	Source Hosts	Last Reporter	Up Time	Expiry Time	State	Filter Mode	Number of Sources
-----------------	----------	--------------	---------------	---------	-------------	-------	-------------	-------------------

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 197. IPv6 Multicast MLD Proxy Membership**

Field	Description
Proxy Interface	The interface on which the MLD proxy is enabled.
Group IP	The IPv6 multicast group address.
Source Hosts	Source addresses that are members of this multicast address.
Last Reporter	The IPv6 address of the source of the last membership report received for the IPv6 multicast group address on the MLD proxy interface.
Up Time	The time elapsed since this entry was created.
Expiry Time	The expiry time interval against each source address that is a member of this multicast group. This is the amount of time after which the specified source entry is aged out.
State	The state of the host entry. A host can be in one of the following states: <ul style="list-style-type: none"> <li>• Non-member state. Does not belong to the group on the interface.</li> <li>• Delaying member state. Host belongs to the group on the interface and report timer running. The report timer is used to send out the reports.</li> <li>• Idle member state. Host belongs to the group on the interface and no report timer is running.</li> </ul>
Filter Mode	The group filter mode (Include/Exclude/None) for the specified group on the MLD proxy interface. Possible modes are as follows: <ul style="list-style-type: none"> <li>• Include</li> <li>• Exclude</li> <li>• None</li> </ul>
Number of Sources	The number of source hosts present in the selected multicast group.

## Configure IPv6 Multicast Static Routes

### ➤ To configure IPv6 multicast static routes 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 > IPv6 Multicast > Static Routes Configuration**.

Static Routes Configuration					
<input type="checkbox"/>	Source IP	Prefix Length	RPF Neighbor	Metric	RPF Interface
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="v"/>

8. In the **Source IP** field, enter the IP address that identifies the multicast packet source for the entry you are creating.
9. In the **Prefix Length** field, enter the prefix length to be applied to the Source IPv6 address.
10. In the **RPF Neighbor** field, enter the IP address of the neighbor router on the path to the source.
11. In the **Metric** field, enter the link state cost of the path to the multicast source.

The range is 0 to 255; the default is 1. You can change the metric for a configured route by selecting the static route and editing this field.

12. Select the interface number from the **RPF Interface** list.

This is the interface that connects to the neighbor router for the given source IP address.

13. Click the **Add** button.

The static route is added to the switch.

14. To delete the selected multicast static route, click the **Delete** button.

15. Click the **Apply** button.

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

## 8. Configure Quality of Service

---

This chapter covers the following topics:

- *QoS Overview*
- *Class of Service*
- *Differentiated Services Overview*

## QoS Overview

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.

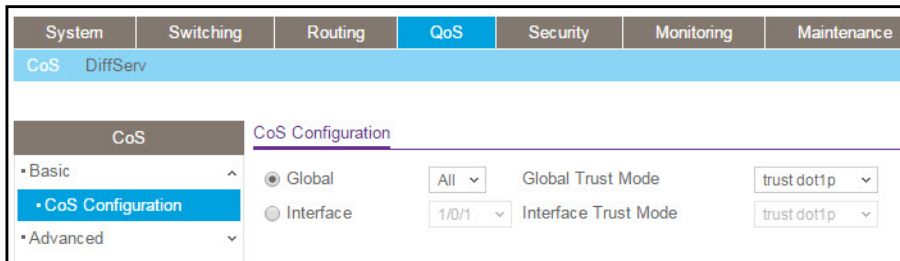
Use CoS to set the Class of Service trust mode of an interface. Each port in the switch can be configured to trust one of the packet fields (802.1p or IP DSCP), or to not trust any packet's priority designation (untrusted mode). If the port is set to a trusted mode, it uses a mapping table appropriate for the trusted field being used. This mapping table indicates the CoS queue to which the packet is 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 port(s), in accordance with the configured default priority of the ingress port. This process is also used for cases where a trusted port mapping cannot be honored, such as when a non-IP packet arrives at a port configured to trust the IP DSCP value.

## Configure Global CoS Settings

➤ **To configure global CoS 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 **QoS > CoS > Basic > CoS Configuration**.



**Note:** You can also navigate to this screen by selecting **QoS > CoS > Advanced > 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 per-interface.
10. Use **Global Trust Mode** to specify whether to trust a particular packet marking at ingress.

Global Trust Mode can be 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 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

The 802.1p to Queue Mapping screen also displays the Current 802.1p Priority Mapping table.

### ➤ 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**.

Interface Selection

Interface

1/0/1 ▾

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 select interfaces.

You can specify CoS configuration settings per-interface or for 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.

The updated configuration is sent to the switch.

## Map DSCP Values to Queues

You can specify which internal traffic class to map 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	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 ▾

The **IP DSCP** field displays an IP DSCP value from 0 to 63.

- For each DSCP value, specify which internal traffic class to map the corresponding IP DSCP value.

The queue number depends on specific hardware.

- Click the **Apply** button.

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

## Configure CoS Interface 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:

- 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 **QoS > CoS > Advanced > CoS Interface Configuration**.

**CoS Interface Configuration**

1 LAGS All      Go To Interface  **Go**

<input type="checkbox"/>	Interface	Interface Trust Mode	Interface Shaping Rate
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	1/0/1	802.1p	0
<input type="checkbox"/>	1/0/2	802.1p	0
<input type="checkbox"/>	1/0/3	802.1p	0
<input type="checkbox"/>	1/0/4	802.1p	0
<input type="checkbox"/>	1/0/5	802.1p	0

8. Select **LAG** to show the list of all LAG interfaces.
9. Select **All** to show the list of all physical as well as LAG interfaces.
10. Select an interface from the **Interface** list of all CoS configurable interfaces.
11. Use the **Go To Interface** field to enter the interface in unit/slot/port format and click the **Go** button.

The entry corresponding the specified interface is selected.

12. Use **Interface Trust Mode** to specify whether or not to trust a particular packet marking at ingress.

Interface Trust Mode can be one of the following:

- Untrusted
- 802.1p
- IP DSCP

The default value is 802.1p.

13. Use **Interface Shaping Rate** to specify the maximum bandwidth allowed.

This is 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. Valid Range is 0 to 100 in increments of 1. The value 0 means that the maximum is unlimited.

14. Click the **Apply** button.

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

## Configure CoS Queue Settings for an Interface

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 CoS queue 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 **QoS > CoS > Advanced > Interface Queue Configuration**.

Interface	Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
<input type="checkbox"/> 1/0/1	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/2	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/3	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/4	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/5	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/6	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/7	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/8	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/9	0	0	Weighted	TailDrop
<input type="checkbox"/> 1/0/10	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. Use the **Queue ID** menu to select the queue to be configured (platform based).
10. 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. Valid Range is 0 to 100 in increments of 1. The value 0 means no guaranteed minimum. Sum of individual Minimum Bandwidth values for all queues in the selected interface cannot exceed defined maximum (100).
11. **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. From the Queue Management Type menu, select either **TailDrop** or **WRED**. The default value is **TailDrop**.
12. Click the **Apply** button.  
 Your changes are applied to the system.

## Configure CoS Drop Precedence Settings

### ➤ To configure CoS Drop Precedence 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 **QoS > CoS > Advanced > CoS Queue Drop Precedence Configuration**.

**CoS Interface Queue Drop Precedence Configuration**

Interface:

Queue ID:

Drop Precedence Level:

WRED Minimum Threshold:  (0 to 100)

WRED Maximum Threshold:  (0 to 100)

WRED Drop Probability Scale:  (0 to 100)

**CoS Interface Queue Drop Precedence Status**

Interface	Queue ID	Drop Precedence Level	WRED Minimum Threshold	WRED Maximum Threshold	WRED Drop Probability Scale
1/0/1	0	1	40	100	10
1/0/1	1	1	40	100	10
1/0/1	2	1	40	100	10
1/0/1	3	1	40	100	10
1/0/1	4	1	40	100	10
1/0/1	5	1	40	100	10
1/0/1	6	1	40	100	10

8. Use **Interface** to specify all CoS configurable interfaces.
9. Use **Queue ID** to specify all the available queues.  
Valid values are 0 to 6. The default is 0.
10. Use **Drop Precedence Level** to specify all the available drop precedence levels.  
Valid values are 1 to 4. The default is 1.
11. Use **WRED Minimum Threshold** to specify the weighted RED minimum queue threshold below which no packets are dropped for the current drop precedence level.  
The range is 0 to 100. The default is 40.
12. Use **WRED Maximum Threshold** to specify the weighted RED maximum queue threshold above which all packets are dropped for the current drop precedence level.  
The range is 0 to 100. The default is 100.
13. Use **WRED Drop Probability Scale** to determine the packet drop probability for the current drop precedence level.  
The range is 0 to 100. The default is 10.
14. Click the **Apply** button.  
The updated configuration is sent to the switch. Configuration changes take effect immediately.

The following table describes the nonconfigurable data that is displayed.

**Table 198. CoS Interface Queue Drop Precedence Status**

Field	Description
Interface	The CoS configurable interface.
Queue ID	The queue ID.

Table 198. CoS Interface Queue Drop Precedence Status (continued)

Field	Description
Drop Precedence Level	The drop precedence level.
WRED Minimum Threshold	The weighted RED minimum queue threshold value.
WRED Maximum Threshold	The weighted RED maximum queue threshold value.
WRED Drop Probability Scale	The packet drop probability value.

## Differentiated Services Overview

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 there is no guarantee. 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.

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

The DiffServ Wizard enables DiffServ on the switch by creating a traffic class, adding the traffic class to a policy, and then adding the policy to the ports that you select. 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 follows:

- **VOIP.** Sets the match criteria to UDP protocol.
- **HTTP.** Sets the match criteria to HTTP destination port.
- **FTP.** Sets match criteria to FTP destination port.
- **Telnet.** Sets the match criteria to Telnet destination port.
- **Every.** Sets the match criteria for all traffic.
- Create a **Diffserv Policy** and add it to the **DiffServ Class** created.
- If **Policing** is set to **YES**, then **DiffServ Policy** style is set to **Simple**. Traffic which 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 the policing action to markdscp ef.
  - **Med.** Sets the policing action to markdscp af31.
  - **Low.** Sets the policing action to send.
- If **Policing** is set to **NO**, then all traffic is marked as follows:
  - **High.** Sets the policy mark to ipdscp ef.
  - **Med.** Sets the policy mark to ipdscp af31.
  - **Low.** Sets the policy mark to pdscp 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**.

Traffic type options are: **VOIP**, **HTTP**, **FTP**, **Telnet**, and **Every**.

9. Ports displays the ports which can be configured to support a **DiffServ** policy.

The **DiffServ** policy is added to selected ports.

10. Use **Enable Policing** to add policing to the **DiffServ** policy.

The policing rate to be applied.

11. 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.

12. 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 the action to markdscp af31, and **Low** sets the action to send.
- When **Policing** is disabled, **Outbound Priority** defines the policy where: **High** sets the policy to mark ipdscp ef, **Med** sets policy to mark ipdscp af31, and **Low** sets the policy to mark ipdscp be.

## Configure Basic DiffServ Settings

Packets are filtered and processed based on defined criteria. The filtering criteria is 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 specifies 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 basic DiffServ 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 **QoS > DiffServ > Basic > DiffServ Configuration**.

### DiffServ Configuration

DiffServ Admin Mode ☐ Disable ☒ Enable

#### Status

MIB Table	Current Size	Max Size
Class Table	0	32
Class Rule table	0	416
Policy table	0	64
Policy Instance table	0	1792
Policy Attributes table	0	5376
Service table	0	226

The following table describes the nonconfigurable data that is displayed.

**Table 199. 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	The number of configured DiffServ classes out of the total allowed on the switch.
Class Rule table	The number of configured class rules out of the total allowed on the switch.
Policy table	The number of configured policies out of the total allowed on the switch.
Policy Instance table	The number of configured policy class instances out of the total allowed on the switch.
Policy Attributes table	The number of configured policy attributes (attached to the policy class instances) out of the total allowed on the switch.
Service table	The number of configured services (attached to the policies on specified interfaces) out of the total allowed on the switch.

## Configure the Global DiffServ Settings

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 specifies 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.

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 > Diffserv Configuration**.

DiffServ Configuration		
DiffServ Admin Mode <input type="radio"/> Disable <input checked="" type="radio"/> Enable		
Status		
MIB Table	Current Size	Max Size
Class Table	0	32
Class Rule table	0	416
Policy table	0	64
Policy Instance table	0	1792
Policy Attributes table	0	5376
Service table	0	226

8. Select the administrative mode for DiffServ:
  - **Enable**. Differentiated Services are active.
  - **Disable**. The DiffServ configuration is retained and can be changed, but it is not active.
9. Click the **Apply** button.

Your settings are applied to the system.

The following table describes the information displayed in the Status table on the DiffServ Configuration screen.

**Table 200. DiffServ Status**

Field	Description
<b>Class Table</b>	The number of configured DiffServ classes out of the total allowed on the switch.
<b>Class Rule table</b>	The number of configured class rules out of the total allowed on the switch.
<b>Policy table</b>	The number of configured policies out of the total allowed on the switch.

Table 200. DiffServ Status (continued)

Field	Description
<b>Policy Instance table</b>	The number of configured policy class instances out of the total allowed on the switch.
<b>Policy Attributes table</b>	The number of configured policy attributes (attached to the policy class instances) out of the total allowed on the switch.
<b>Service table</b>	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. You can also 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, click the class link to 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**.

System		Switching		Routing		QoS		Security		Monitoring							
CoS		DiffServ															
<div> <div>DiffServ</div> <div> <div>DiffServ Wizard</div> <div>Basic</div> <div>Advanced</div> <div>DiffServ Configuration</div> <div><b>Class Configuration</b></div> <div>IPv6 Class Configuration</div> </div> </div> <div> <div>Class Name</div> <table border="1"> <thead> <tr> <th>Class Name</th> <th>Class Type</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> <input type="text"/></td> <td><input type="text"/></td> </tr> <tr> <td><input type="checkbox"/> <a href="#">Class4</a></td> <td>All</td> </tr> </tbody> </table> </div>												Class Name	Class Type	<input type="checkbox"/> <input type="text"/>	<input type="text"/>	<input type="checkbox"/> <a href="#">Class4</a>	All
Class Name	Class Type																
<input type="checkbox"/> <input type="text"/>	<input type="text"/>																
<input type="checkbox"/> <a href="#">Class4</a>	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 is 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 the class is created, the Class Type field becomes nonconfigurable.

9. To rename an existing class, select the check box next to the configured class, update the name.
10. Click the **Apply** button.

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

11. To remove a class, select the class name check box and click the **Delete** button.

To refresh the screen with the latest information on the switch, click the **Update** button.

12. After creating a class, click the class link to the Class screen.

13. Click the **class name** for an existing class.

Class Name	
<input type="checkbox"/> Class Name	Class Type
<input type="text"/>	<input type="text"/>
<input type="checkbox"/> <a href="#">Class4</a>	All

The class name is a hyperlink. The following figure shows the configuration fields for the class.

14. To configure the class details, complete the fields:

- **Class Name** - The name for the configured DiffServ class.
- **Class Type** - The DiffServ class type.

You can select the class type only when you are creating a new class. After you create the class, this field displays the class type, but you cannot change it.

15. 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 0–4093.
- **Secondary Class of Service.** Select this option to require the Class of Service (CoS) value in an Ethernet frame header to match the specified CoS value.
- **Secondary VLAN.** Select this option to require a packet's VLAN ID to match a secondary VLAN ID or a secondary VLAN ID within a continuous range. If you configure a range, a match occurs if a packet's secondary VLAN ID is the same as any secondary VLAN ID within the range. After you select this option, use the following fields to configure the secondary VLAN match criteria:
  - **Secondary VLAN ID Start.** The secondary VLAN ID to match or the secondary VLAN ID with the lowest value within a range of VLANs.
  - **Secondary VLAN ID End.** The secondary VLAN ID with the highest value within the range of VLANs. This field is not required if the match criteria is a single VLAN ID.

- **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 a MAC address indicating which part(s) 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 a MAC address indicating which part(s) 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 part(s) 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 part(s) 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 00 to ff to compare against.
  - **ToS Mask.** This indicates which ToS bits are subject to comparison against the Service Type value.

**16.** 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 in the Class Summary at the bottom of the DiffServ Advanced Class Configuration screen.

**Table 201. DiffServ Class Configuration - Class Summary**

Field	Description
Match Criteria	The configured match criteria for the specified class.
Values	The values of the configured match criteria.

## Configure DiffServ IPv6 Class Settings

You can add a new IPv6 DiffServ class name, or to rename or delete an existing class. You can also 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, click the class link to the Class screen.

### ➤ To configure DiffServ IPv6 class 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 **QoS > DiffServ > Advanced > IPv6 Class Configuration**.

Class Name	Class Type
<input type="text"/>	<input type="button" value="v"/>
<a href="#">class1</a>	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 is satisfied for a packet match. All signifies the logical AND of all the match criteria. Only when a new class is created, this field is a selector field. After class creation 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, and update the name
10. Click the **Apply** button.

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

11. To remove a class, select the **Class Name** check box and then click the **Delete** button.  
To refresh the screen with the latest information on the switch, click the **Update** button.
12. After creating a class, click the **class name** for an existing class.

IPv6 Class Name	
<input type="checkbox"/> Class Name	Class Type
<input type="text"/>	<input type="text"/>
<input type="checkbox"/> <a href="#">class1</a>	All
<input type="checkbox"/> <a href="#">Class2</a>	All

The class name is a hyperlink. The following figure shows the configuration fields for the class.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index				
CoS DiffServ												
DiffServ		IPv6 Class Information										
<ul style="list-style-type: none"> <li>DiffServ Wizard</li> <li>Basic</li> <li>Advanced               <ul style="list-style-type: none"> <li>DiffServ Configuration</li> <li>Class Configuration</li> <li><b>IPv6 Class Configuration</b></li> <li>Policy Configuration</li> <li>Service Interface Configuration</li> <li>Service Statistics</li> </ul> </li> </ul>		Class Name <input type="text" value="Class1"/> Class Type <input type="text" value="All"/>										
		IPv6 DiffServ Class Configuration										
		<input checked="" type="radio"/> Match Every <input type="text" value="Any"/> <input type="radio"/> Reference Class <input type="text" value="Class4"/> <input type="radio"/> Protocol Type <input type="text" value="ICMPv6"/> <input type="text" value="(0 to 255)"/> <input type="radio"/> Source Prefix/Length <input type="text" value="domain"/> <input type="text" value="(0 to 65535)"/> <input type="radio"/> Source L4 Port <input type="text" value="domain"/> <input type="text" value="(0 to 65535)"/> <input type="radio"/> Destination Prefix/Length <input type="text" value="domain"/> <input type="text" value="(0 to 65535)"/> <input type="radio"/> Destination L4 Port <input type="text" value="domain"/> <input type="text" value="(0 to 65535)"/> <input type="radio"/> Flow Label <input type="text" value=""/> <input type="text" value="(0 to 1048575)"/> <input type="radio"/> IP DSCP <input type="text" value="af11"/> <input type="text" value="(0 to 63)"/>										
		Class Summary										
		<table border="1"> <thead> <tr> <th>Match Criteria</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>							Match Criteria	Values		
Match Criteria	Values											

13. To configure the IPv6 class, complete the fields:

- **Class Name** - The name for the configured DiffServ class.
- **Class Type** - The DiffServ class type.

Options: All

You can specify the class type only when you are creating a new class. After the class is created, this field displays the class type, but you cannot change it.

14. 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. 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: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: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. The flow label can be specified in the range of 0 to 1048575.
- **IP DSCP** - You can select a keyword for the known DSCP values. The list includes Other as an option for the remaining values.

15. **Match Criteria** - Displays the configured match criteria for the specified class.

16. **Values** - Displays the values of the configured match criteria.

17. 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 in the Class Summary at the bottom of the DiffServ Advanced IPv6 Class Configuration screen.

**Table 202. DiffServ IPv6 Class Configuration - Class Summary**

Field	Description
Match Criteria	The configured match criteria for the specified class.
Values	The values of the configured match criteria.

## Configure DiffServ Policy

You can associate a collection of classes with one or more policy statements. After creating a policy, click the policy link to the Policy screen.

### ➤ To configure 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**.

<input type="checkbox"/>	Policy Name	Policy Type	Member Class
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="v"/>	<input type="text" value="v"/>

8. Use **Policy Name** to uniquely identify a policy using a case-sensitive alphanumeric string from 1 to 31 characters.
9. In the **Member Class** list, select a DiffServ class.

This lists all existing 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. This field is a selector field only when an existing policy class instance is to be removed. After removal of the policy class instance this becomes a nonconfigurable field.

**10. Policy Type** - Indicates the type is specific to inbound traffic direction.

**11.** Click the **Add** button.

The new policy is added to the switch.

**12.** Click the **Delete** button to delete the currently selected policy from the switch.

**13.** To configure the policy attributes, click the name of the policy.

	Policy Name	Policy Type	Member Class
	<input type="text"/>	<input type="text"/>	<input type="text"/>
	<a href="#">Class2</a>	In	

The policy name is a hyperlink. The following figure shows the configuration fields for the policy.

**Class Information**

Policy Name:   
Policy Type:   
Member Class Name:

**Policy Attribute**

Policy Attribute

☐ Assign Queue   
☐ Drop  
☐ Mark VLAN CoS   
☐ Mark CoS As Secondary CoS  
☐ Mark IP Precedence   
☐ Mirror   
☐ Redirect   
☐ Mark IP DSCP   
☐ Simple Policy

Color Mode  
Comitted Rate  
Comitted Burst Size  
Conform Action

Color Blind  
  
  
☒ Send  
☐ Drop  
☐ Mark CoS   
☐ Mark CoS As Secondary CoS  
☐ Mark IP Precedence   
☐ Mark IP DSCP    
☒ Send  
☐ Drop

Color Mode

Violate Action

**14.** Select the **Assign Queue** to which packets of this policy-class are assigned.

This is an integer value in the range 0 to 6.

**15.** 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 CoS as Secondary Cos** - This option marks outer VLAN tag priority bits of all packets as the inner VLAN tag priority. This essentially means that the inner VLAN tag CoS is copied to the outer VLAN tag CoS.
- **Mark IP Precedence** - This is an IP precedence value in the range from 0 to 7.
- **Mirror**
- **Redirect**
- **Two Rate Policy** - With the two-rate policer, you can enforce traffic policing according to two separate rates: Committed Rate and Peak Rate.
- **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).

16. 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, non-excluded 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 according to 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 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 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 field be set.

17. If you select **Two Rate**, you can configure additional fields (same fields as for a simple policy).

18. 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 203. DiffServ Policy Configuration - Policy Attribute**

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 the DiffServ Service Interface

### ➤ To configure the DiffServ service 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

1 LAGS All Go To Interface  Go

	Interface	Policy In Name	Policy Out Name	Direction	Operational Status
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>		
<input type="checkbox"/>	1/0/1				
<input type="checkbox"/>	1/0/2				
<input type="checkbox"/>	1/0/3				
<input type="checkbox"/>	1/0/4				
<input type="checkbox"/>	1/0/5				

8. Use **Interface** to select the interface for the DiffServ service.

9. **Policy Name** - Lists all the policy names from which one can be selected.

This field is not shown for read/write users where the inbound service policy attachment is not supported by the platform.

**Table 204. 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 DiffServ Service Statistics

This screen displays class-oriented statistical information for the policy, which is specified by the interface and direction. The Member Class list 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 the DiffServ 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.

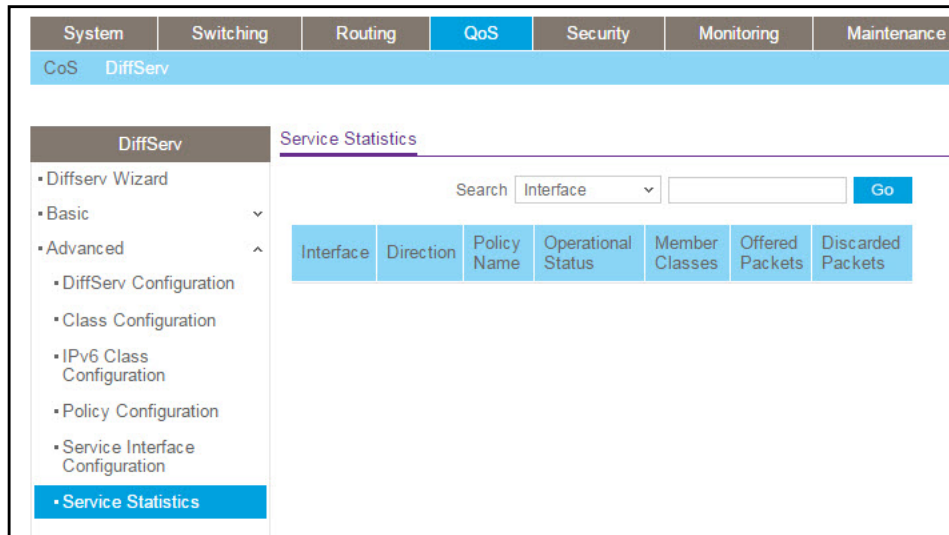
5. Enter the user name and password.

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**.



8. Use the **Search** menu to search for neighbor entries by MAC Interface, or Neighbor IP.

9. To search by interface, select **Interface**, enter the interface in unit/slot/port format, for example, 1/0/13. Then click the **Go** button.

If the neighbor entry exists, the entry is displayed as the first entry, followed by the remaining entries.

10. To search by member class, select **Member Class**, enter the Member Class, then click the **Go** button.

If the entry with a matching Member Class exists, that entry is displayed as the first entry, followed by the remaining entries. An exact match is required.

To refresh the screen with the latest information on the switch, click the **Update** button.



The following table describes the information available on the Service Statistics screen.

**Table 205. DiffServ Service Statistics**

Field	Description
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. Shows only 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. Select a member class name to display its statistics. If no class is associated with the selected policy, then nothing is populated in the list.
Offered Packets	A count of the total number of packets 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	A count of the total number of packets 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. The discarded packets are supported in the inbound direction but not in the outbound direction.

## 9. Manage Device Security

---

This chapter covers the following topics:

- *Management Security Settings*
- *TACACS Overview*
- *Configure Management Access*
- *Port Authentication*
- *Traffic Control*
- *Port Security*
- *DHCP Snooping*
- *Configure Access Control Lists*

## 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, the password is blank for both of these accounts. The names are not case-sensitive.

If you log on to a user account with read/write privileges (as admin), you can assign passwords and set security parameters for the default accounts and add and delete accounts (other than admin), up to a maximum of six. Only a user with read/write privileges can modify data on the web interface screens, and only one account can be created with 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**.

Manage Users							
	User Name	Edit Password	Password	Confirm Password	Access Mode	Lockout Status	Password Expiration Date
<input type="checkbox"/>	<input type="text"/>	Disable ▾	••••••••	••••••••	<input type="text"/>		
<input type="checkbox"/>	admin	Disable	••••••••	••••••~••••	READ_WRITE	FALSE	
<input type="checkbox"/>	guest	Disable	••••••~••••	••••••~••••	READ_ONLY	FALSE	

8. In the **User Name** field, enter the name for the new account.

You can enter a new user name only when you are creating an account. User names are up to 64 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. Set the **Edit Password** field to **Enable** only when you are changing the password.

The default value is Disable.

10. In the **Password** field, enter the password for the account.

The characters do not display as they are typed; only asterisks (\*) show. Passwords are up to eight alphanumeric characters in length, and are case-sensitive.

11. In the **Confirm Password** field, enter the password again, to confirm that you entered it correctly.

This field does not display the password as it is typed, but shows asterisks (\*).

The **Access Mode** field displays the user's access mode. The admin account always has read/write access, and all other accounts are assigned read-only access. The default value is read-only.

The **Lockout Status** field indicates whether the user account is locked out (TRUE or FALSE).

The **Password Expiration Date** field indicates the current password expiration date.

12. Click the **Add** button.

The user account is added.

13. To delete the selected user account, click the **Delete** button.

You cannot delete the admin read/write user.

## Configure a User Password

- To configure a user 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 > Local User > User Password Configuration**.

Password Configuration		
Password Minimum Length	<input type="text" value="8"/>	(0 to 64)
Password Aging (days)	<input type="text" value="0"/>	(0 to 365)
Password History	<input type="text" value="0"/>	(0 to 10)
Lockout Attempts	<input type="text" value="0"/>	(0 to 5)

8. In the **Password Minimum Length** field, type the minimum character length of all new local user passwords.
9. In the **Password Aging (days)** field, type 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. In the **Password History** field, type 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. In the **Lockout Attempts** field, specify the number of allowable failed local authentication attempts before the user's account is locked.

A value of 0 indicates that user accounts are never locked.

## Enable Password Configuration

You can change the privileged EXEC password. Passwords are a maximum of 64 alphanumeric characters. The password is case-sensitive.

➤ **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**.

The screenshot shows a web interface titled 'Enable Password Configuration'. Below the title, there are two input fields. The first field is labeled 'Password' and the second is labeled 'Confirm Password'. Both fields contain masked characters (dots) indicating that a password has been entered.

8. In the **Password** field, type the password.  
Passwords are a maximum of 64 alphanumeric characters.
9. In the **Confirm Password** field, type the password again, to confirm that you entered it correctly.

## 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.

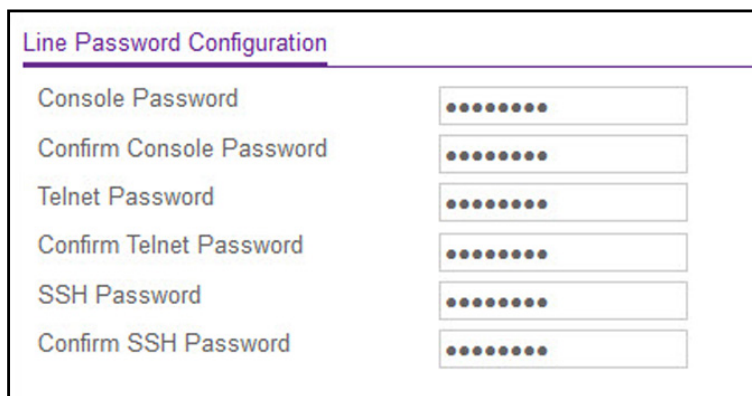
5. Enter the user name and password.

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**.

A screenshot of the 'Line Password Configuration' web interface. The title 'Line Password Configuration' is at the top left. Below it are six input fields, each with a label and a password mask (dots). The labels are: 'Console Password', 'Confirm Console Password', 'Telnet Password', 'Confirm Telnet Password', 'SSH Password', and 'Confirm SSH Password'. Each field is a rectangular box with a light gray border and a series of dots representing the password characters.

8. In the **Console Password** field, enter the console password.  
Passwords are a maximum of 64 alphanumeric characters.
9. In the **Confirm Console Password** field, type the password again to confirm that you typed it correctly.
10. In the **Telnet Password** field, type the Telnet password.  
Passwords are a maximum of 64 alphanumeric characters.
11. In the **Confirm Telnet Password** field, type the password again to confirm that you entered it correctly.
12. In the **SSH Password** field, type the SSH password.  
Passwords are a maximum of 64 alphanumeric characters.
13. In the **Confirm SSH Password** field, type the password again, to confirm that you entered it correctly.

## RADIUS Overview

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)

## Configure Global RADIUS Server Settings

You can add information about one or more RADIUS servers on the network.

### ➤ To configure global RADIUS 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.

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**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance
Management Security   Access   Port Authentication   Traffic Control   Control   ACL						
<div> <div>Management Security</div> <div> <div>Local User</div> <div>Enable Password</div> <div>Line Password</div> <div>RADIUS</div> <div><b>Radius Configuration</b></div> <div>Server Configuration</div> <div>Accounting Server Configuration</div> <div>TACACS</div> <div>Authentication List</div> <div>Login Sessions</div> </div> </div> <div> <div>Radius Configuration</div> <div> <div>Current Server Address</div> <div>Source Interface</div> <div>Number of Configured Authentication Servers</div> <div>Number of Configured Accounting Servers</div> <div>Number of Named Authentication Server Groups</div> <div>Number of Named Accounting Server Groups</div> <div>Max Number of Retransmits</div> <div>Timeout Duration (secs)</div> <div>Accounting Mode</div> <div>Radius Attribute 4 Mode</div> </div> </div>						



The **Current Server IP Address** field is blank if no servers are configured (see [Configure a RADIUS Server](#) on page 548). The switch supports up to three configured RADIUS servers. If more than one RADIUS servers is configured, the current server is 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 **Source Interface** list, select the interface to use for RADIUS.

Possible values are as follows:

- **None**
- **Routing interface**
- **Routing VLAN**
- **Routing loopback interface**
- **Service Port**

By default, VLAN 1 is used as source interface.

9. In the **Max Number of Retransmits** field, specify 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.

Consider the maximum delay time when you configure the RADIUS maximum retransmit and RADIUS time-out. 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 passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the retransmit times the 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. 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.

Consider the maximum delay time when you configure RADIUS maximum retransmit and RADIUS time-out. 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 passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the retransmit times the 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.

11. Select the Accounting Mode **Disable** or **Enable** radio button.

This specifies whether the RADIUS accounting mode is enabled or disabled on the current server.

12. Select the RADIUS Attribute 4 **Disable** or **Enable** radio button.

This enables or disables 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.

**Table 206. 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	The number of configured authentication RADIUS servers. The value can range from 0 to 32.
Number of Configured Accounting Servers	The number of RADIUS accounting servers configured. The value can range from 0 to 32.
Number of Named Authentication Server Groups	The number of Named RADIUS server authentication groups configured.
Number of Named Accounting Server Groups	The number of named RADIUS server accounting groups configured.

## Configure a RADIUS Server

### ➤ 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									
<input type="checkbox"/>	Radius Server IP Address	Radius Server Name	Current	Port	Secret Configured	Secret	Primary Server	Message Authenticator	Server Type
	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	*****	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>

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

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. Click the **Add** button.

The server is added to the switch.

This button is available only when you log in with the admin user name, which has read-write permission. These changes are not retained across a power cycle unless a save is performed.

10. To remove the selected server from the configuration, click the **Delete** button.

This button is available only when you log in with the admin user name, which has read-write permission. These changes are not retained across a power cycle unless a save is performed.

The **Current** field indicates if this server is currently in use as the authentication server.

To reset the authentication server and RADIUS statistics to their default values, click the **Clear Counters** button at the bottom of the screen.

The following table describes the RADIUS server statistics displayed on the screen.

**Table 207. RADIUS statistics**

Field	Description
Radius Server	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 to 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 RADIUS Accounting Servers

### ➤ 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 IP Address	Accounting Server Name	Port	Secret Configured	Secret	Accounting Mode
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Statistics										
Accounting Server	Round Trip Time	Accounting Requests	Accounting Retransmissions	Accounting Responses	Malformed Accounting Responses	Bad Authenticators	Pending Requests	Timeouts	Unknown Types	Packets Dropped

8. In the **Accounting Server IP Address** field, specify the IP address of the RADIUS accounting server.
9. In the **Accounting Server Name** field, enter the name of the accounting server.
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** list, 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 is 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 208. RADIUS Accounting Server Statistics**

Field	Description
Accounting Server Address	The accounting server associated with the statistics.
Round Trip Time(secs)	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	The number of RADIUS accounting-request packets sent not including retransmissions.
Accounting Retransmissions	The number of RADIUS accounting-request packets retransmitted to this RADIUS accounting server.
Accounting Responses	The number of RADIUS packets received on the accounting port from this server.
Malformed Accounting Responses	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	The number of RADIUS accounting-response packets that contained invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS accounting-request packets sent to this server that did not yet time out or receive a response.
Timeouts	The number of accounting time-outs to this server.
Unknown Types	The number of RADIUS packets of unknown type that were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets that were received from this server on the accounting port and dropped for some other reason.

## TACACS Overview

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 configure 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**.

System	Switching	Routing	QoS	Security	Monitoring
Management Security	Access	Port Authentication	Traffic Control	Control	ACL

Management Security	TACACS Configuration
• Local User	Key String <input type="text"/> (0 to 128)
• Enable Password	Connection Timeout <input type="text"/> (1 to 30)
• Line Password	Source Interface <input type="text"/> (vlan 1)
• RADIUS	
• TACACS	
• TACACS Configuration	
• TACACS Server Configuration	

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. 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. In the **Source Interface** list, select the source for TACACS.

Possible values are as follows:

- None
- Routing interface
- Routing VLAN
- Routing loopback interface
- Service port

By default VLAN 1 is used as source interface.

**11. Click the **Apply** button.**

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

## Configure TACACS Server Settings

You can configure up to five TACACS servers with which the switch can communicate.

➤ **To configure TACACS 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.

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					
<input type="checkbox"/>	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" value="*****"/>	<input type="text"/>

8. Use **TACACS Server** to configure the TACACS server IP address.
9. Use **Priority** to specify the order in which the TACACS servers are used.

The valid range is 0–65535.



10. Use **Port** to specify the authentication port. It must be within the range 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. 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 1–30.
13. Click the **Add** button.  
The server is added to the switch.  
This button is available only to read/write users. These changes are not retained across a power cycle unless a save is performed.
14. To delete the selected server from the configuration, click the **Delete** button.

## Configure a Login Authentication List

A login list specifies the authentication methods 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 configure 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						
List Name	1	2	3	4	5	6
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> defaultList	Local	N/A	N/A	N/A	N/A	N/A
<input type="checkbox"/> networkList	Local	N/A	N/A	N/A	N/A	N/A

8. To create a new login list, enter 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, 6) 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. Click the **Add** button.

The login list is added to the switch.

11. To remove the selected authentication login list from the configuration, click the **Delete** button.

The delete fails if the selected login list is assigned to any user (including the default user) for system login. You can use this button only if you logged in as the admin user, which has read/write access. The change is not retained across a power cycle unless you perform a save.

## Configure an Enable Authentication List

An enable list specifies the authentication methods 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 an 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**.

List Name	1	2	3	4	5
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> enableList	Enable	None	N/A	N/A	N/A
<input type="checkbox"/> enableNetList	Enable	None	N/A	N/A	N/A

8. To create a new enable list, enter the name in the **List Name** field.  
It can be up to 15 alphanumeric characters long and is not case-sensitive.
9. In the numbered lists (1, 2, 3, 4, 5, 6) 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. Click the **Add** button.  
The login list is added to the switch.
11. To remove the selected authentication enable list from the configuration, click the **Delete** button.

You can use this button only if you have read/write access. The change is not retained across a power cycle unless you perform a save.

## Configure the Dot1x Authentication List

You can configure a dot1x list. A dot1x list specifies the authentication methods 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 the 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.

The Login screen displays.

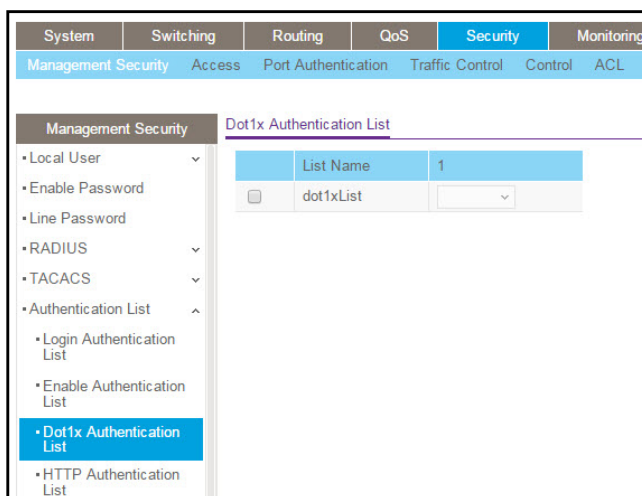
5. Enter the user name and password.

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 > Dot1x Authentication List**.



8. In the **List Name** field, select the dot1x list name.

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 is 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 authenticated without a user name and password.

## Configure an HTTP Authentication List

You can configure an HTTP list. An HTTP list specifies the authentication methods 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**.

The screenshot shows the configuration web interface for a switch. The top navigation bar includes tabs for System, Switching, Routing, QoS, Security, Monitoring, and Maintenance. The Security tab is active, and the sub-tab is HTTP Authentication List. On the left, a sidebar menu shows various security options, with 'HTTP Authentication List' selected. The main content area displays a table for configuring the authentication list.

List Name	1	2	3	4
httpList	Local			

8. Use **List Name** to select the HTTP list name.
9. In the numbered lists (1, 2, 3, 4) 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.
- **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.

## Configure an HTTPS Authentication List

You can configure an HTTPS list. A login list specifies the authentication methods 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.

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 > HTTPS Authentication List**.

The screenshot shows the web management interface with the following structure:

- Top Navigation Bar:** System, Switching, Routing, QoS, **Security**, Monitoring, Maintenance.
- Sub-Navigation Bar:** Management Security, Access, Port Authentication, Traffic Control, Control, ACL.
- Left Sidebar (Management Security):**
  - Local User
  - Enable Password
  - Line Password
  - RADIUS
  - TACACS
  - Authentication List (expanded)
    - Login Authentication List
    - Enable Authentication List
    - Dot1x Authentication List
    - HTTP Authentication List
    - HTTPS Authentication List** (selected)
    - Login Sessions
- Main Content Area (HTTPS Authentication List):**

List Name	1	2	3	4
<input type="checkbox"/> httpsList	Local			

8. Select the **List Name** check box for the HTTPS list name.
9. In the numbered lists (1, 2, 3, 4, 5, 6) 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.
- **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.

## 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**.

Login Sessions					
ID	User Name	Connection From	Idle Time	Session Time	Session Type
0	admin	EIA-232	01:29:48	25:02:49	Serial
11	admin	10.27.65.107	00:00:00	00:16:01	HTTP

Table 209. Login Sessions

Field	Description
ID	Identifies the ID of this row.
User Name	The user's name whose session is open.
Connection From	The machine from which the user is connected.
Idle Time	The idle session time.
Session Time	The total session time.
Session Type	The type of session: Telnet, Serial, or SSH

## Configure Management Access

You can configure HTTP and Secure HTTP access to the switch's management interface.

### Configure HTTP Server Settings

To access the switch using a web browser, 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

Once you establish in-band connectivity, you can change the IP information using a web-based management.

➤ **To configure the 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.

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 > HTTP > HTTP Configuration**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help
Management Security Access Port Authentication Traffic Control Control ACL							
Access		HTTP Configuration					
• HTTP ^		HTTP Access		<input type="radio"/> Disable <input checked="" type="radio"/> Enable			
• HTTP Configuration		HTTP Port		80 (1025 to 65535)   Default: 80			
• HTTPS v		Java Mode		<input type="radio"/> Disable <input checked="" type="radio"/> Enable			
• SSH v		HTTP Session Soft Timeout (Minutes)		60 (1 to 60)			
• Telnet		HTTP Session Hard Timeout (Hours)		24 (1 to 168)			
• Console Port		Maximum Number of HTTP Sessions		16 (0 to 16)			
• Denial of Service Configuration		Authentication List		HttpList			

8. Select the HTTP Access **Disable** or **Enable** radio button.

This specifies whether the switch can be accessed from a web browser. If you enable web mode, you can manage the switch from a web browser. The factory default is Enable.

9. In the **HTTP Port** field, enter the HTTP port number.

The valid range is 80 and 1025 to 65535. The default value is 80.

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

This enables or disables the Java applet, which 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.

11. In the **HTTP Session Soft Timeout (Minutes)** field, to set the inactivity time-out for HTTP sessions.

The value must be in the range of 1 to 60 minutes. The default value is 5 minutes. The currently configured value displays.

12. 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 displayed.

13. 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 displayed.

The **Authentication List** field displays the list that HTTP is using.

## HTTPS Configuration

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 to 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**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help
Management Security Access Port Authentication Traffic Control Control ACL							
Access		HTTPS Configuration					
• HTTP		Admin Mode <input checked="" type="radio"/> Disable <input type="radio"/> Enable					
• HTTPS		SSL Version 3 <input type="radio"/> Disable <input checked="" type="radio"/> Enable					
• HTTPS Configuration		TLS Version 1 <input type="radio"/> Disable <input checked="" type="radio"/> Enable					
• Certificate Management		HTTPS Port <input type="text" value="443"/> (1025 to 65535)   Default: 443					
• Certificate Download		HTTPS Session Soft Timeout (Minutes) <input type="text" value="5"/> (1 to 60)					
• SSH		HTTPS Session Hard Timeout (Hours) <input type="text" value="24"/> (1 to 168)					
• Telnet		Maximum Number of HTTPS Sessions <input type="text" value="16"/> (0 to 16)					
• Console Port		Authentication List <input type="text" value="HttpsList"/>					

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

This enables or disables the administrative mode of Secure HTTPS. The currently configured value is displayed. The default value is Disable. You can download SSL certificates only when the HTTPS admin mode is disabled. HTTPS admin mode can be enabled only if a certificate is present on the device.

9. Select the SSL Version 3 **Disable** or **Enable** radio button.

This enables or disables Secure Sockets Layer version 3.0. The currently configured value is displayed. The default value is Enable.

10. Select the TLS Version 1 **Disable** or **Enable** radio button

This enables or disables Transport Layer Security version 1.0. The currently configured value is displayed. The default value is Enable.

11. In the **HTTPS Port** field, type the HTTPS port number.

The value must be in the range of 1025 to 65535. Port 443 is the default value. The currently configured value is displayed.

12. In the **HTTPS Session Soft Timeout (Minutes)** field, enter the inactivity time-out for HTTPS sessions.

The value must be in the range of 1 to 60 minutes. The default value is 5 minutes. The currently configured value is displayed.

13. In the **HTTPS Session Hard Timeout (Hours)** field, 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 displayed.

14. In the **Maximum Number of HTTPS Sessions** field, enter 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 displayed.

The **Authentication List** field displays the authentication list for HTTPS.

## 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**.

Certificate Management	
Certificate Present	No
<input checked="" type="radio"/> None <input type="radio"/> Generate Certificates <input type="radio"/> Delete Certificates	
Certificate Generation Status	
Certificate Generation Status	No certificate generation in progress

The **Certificate Present** field displays whether there is a certificate present on the device.

8. Select one of the following radio buttons:

- **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.

The **Certificate Generation Status** field displays the SSL certificate generation status.

## Download Certificates

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, offline) 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 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 Download**.

8. In the **File Type** list, specify the type of file to transfer:
  - **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** list, 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** list, 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, enter 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 Settings

You can view and modify the Secure Shell (SSH) server settings on the device. SSH is a network protocol that enables access to the CLI management interface by using an SSH client on a remote administrative system. SSH is a more secure access method than Telnet

because it encrypts communication between the administrative system and the device. You can download or generate SSH host keys for secure CLI-based management.

➤ **To configure SSH 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 > SSH > SSH Configuration**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index
Management Security Access Port Authentication Traffic Control Control ACL								
Access		SSH Configuration						
• HTTP	▼	SSH Admin Mode		<input checked="" type="radio"/> Disable <input type="radio"/> Enable				
• HTTPS	▼	SSH Version 1		<input type="radio"/> Disable <input checked="" type="radio"/> Enable				
• SSH	^	SSH Version 2		<input type="radio"/> Disable <input checked="" type="radio"/> Enable				
• SSH Configuration		SSH Session Timeout		5 minutes				
• Host Keys Management		Maximum Number of SSH Sessions		5				
• Host Keys Download		Current Number of SSH Sessions		0				
• Telnet		Keys Present		Yes				
• Console Port		Login Authentication List		networkList				
• Denial of Service Configuration		Enable Authentication List		enableList				
• Access Control	▼	SSH Port		22 (1 to 65535)				

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

This enables or disables the SSH server administrative mode. When this mode is enabled, the device can be accessed by using an SSH client on a remote system. The currently configured value is displayed. The default value is Disable.

9. Select the SSH Version 1 **Disable** or **Enable** radio button.

This enables or disables Protocol Level 1 for SSH. When Enable is selected, the SSH server on the device can accept connections from an SSH client using Protocol Level 1

for SSH (SSH-1). When Disable is selected, the device does not allow connections from clients using the SSH-1 protocol. The currently configured value is displayed. The default value is Enable.

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

This enables or disables Protocol Level 2 for SSH. When Enable is selected, the SSH server on the device can accept connections from an SSH client using Protocol Level 2 for SSH (SSH-2). When Disable is selected, the device does not allow connections from clients using the SSH-2 protocol. The currently configured value is displayed. The default value is Enable.

- 11.** Use **SSH Session Timeout** to configure the SSH session inactivity time-out value for incoming SSH sessions to the switch.

A connected user that does not exhibit any SSH activity for this amount of time is automatically disconnected from the device. The acceptable range for this field is 1-5 minutes.

- 12.** Use **Maximum Number of SSH Sessions** to configure the maximum number of inbound SSH sessions that can be connected to the device simultaneously.

The currently configured value is displayed. The acceptable range for this field is 0–5.

- 13.** Use **Login Authentication List** to select an authentication list.

This list is used to authenticate users who try to login to the switch.

- 14.** Use **Enable Authentication List** to select an authentication list.

This list is used to authenticate users who try to get *enable* level privilege.

- 15.** Use **SSH Port** to enter the port range from 1 to 65535.

The default value is 22.

- 16.** Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

**Table 210. SSH Configuration**

Field	Description
Current Number of SSH Sessions	The number of active SSH sessions between remote SSH clients and the SSH server on the device.
Keys Present	Displays <b>Yes</b> or <b>No</b> whether one or both (if any) of the following keys are present on the device: <ul style="list-style-type: none"> <li>SSH-1 Rivest-Shamir-Adelman (RSA) key file or SSH-2 RSA key file (PEM encoded)</li> <li>SSH-2 Digital Signature Algorithm (DSA) key file (PEM encoded)</li> </ul>



## 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.

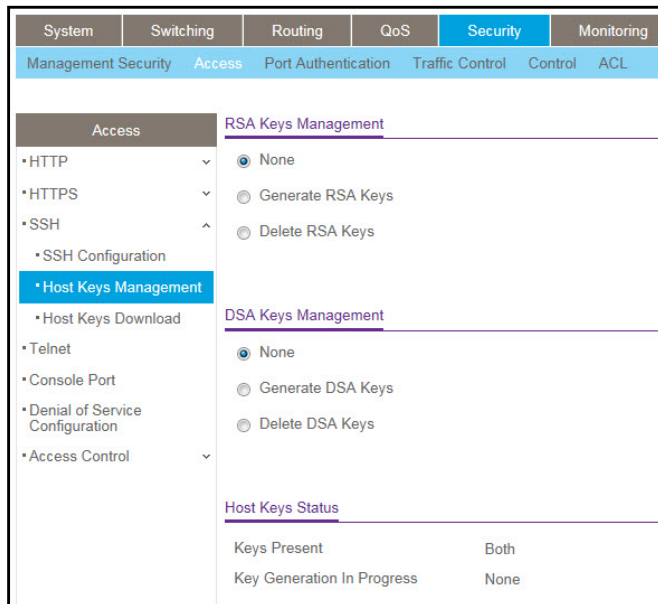
5. Enter the user name and password.

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**.



8. Select an RSA Keys Management radio button:
  - **None.** This is the default selection.
  - **Generate RSA Keys.** 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.** 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.** 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.** Delete the corresponding DSA key file, if it is present.

10. Click the **Apply** button.

The host key file starts downloading. To download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.

To refresh the screen with the latest information on the switch, click the **Update** button.

**Table 211. RSA Key Management**

Field	Description
Keys Present	Displays which of the following keys or both (if any) are present on the device: <ul style="list-style-type: none"> <li>• SSH-1 Rivest-Shamir-Adelman (RSA) key file or SSH-2 RSA key file (PEM Encoded)</li> <li>• SSH-2 Digital Signature Algorithm (DSA) key file (PEM Encoded)</li> </ul>
Key Generation In Progress	Displays which key is being generated (if any), RSA, DSA, or None.

## Download Host Keys

You can download an SSH-1 RSA, SSH-2 RSA, or SSH-2 DSA key file from a remote system to the device.

➤ **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** list, select the type of file to transfer:
  - **SSH-1 RSA Key File.** SSH-1 Rivest-Shamir-Adelman (RSA) key file
  - **SSH-2 RSA Key PEM File.** SSH-2 Rivest-Shamir-Adelman (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** list, select 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**.  
 This specifies the format of the TFTP/SFTP/SCP Server Address field. The factory default is IPv4.
11. In the **Server Address** field, 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. 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, 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. To download SSH key files SSH must be administratively disabled and there can be no active SSH sessions.

## Configure Telnet Settings

### ➤ To configure Telnet 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 > Telnet**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance
Management Security	Access	Port Authentication	Traffic Control	Control	ACL	

**Access**

- HTTP
- HTTPS
- SSH
- **Telnet**
- Console Port
- Denial of Service Configuration
- Access Control

### Authentication List

Login Authentication List networkList

Enable Authentication List enableList

### Inbound Telnet

Telnet Server Admin Mode ☐ Disable ☒ Enable

Allow new telnet sessions ☐ Disable ☒ Enable

Session Timeout (Minutes)  (1 to 160)

Maximum Number of Sessions  (0 to 5)

Current Number of Sessions

### Outbound Telnet

Allow new telnet sessions ☐ Disable ☒ Enable

Session Timeout (Minutes)  (1 to 160)

Maximum Number of Sessions  (0 to 5)

Current Number of Sessions

## Configure the Telnet Authentication List

You can select the Login and Enable authentication list available. The login list specifies the authentication methods to use to validate switch or port access for the users associated with

the list. The enable list specifies the authentication methods to use 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 the 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**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance
Management Security	Access	Port Authentication	Traffic Control	Control	ACL	

**Access**

- HTTP
- HTTPS
- SSH
- Telnet**
- Console Port
- Denial of Service Configuration
- Access Control

### Authentication List

Login Authentication List:

Enable Authentication List:

### Inbound Telnet

Telnet Server Admin Mode: ☐ Disable ☒ Enable

Allow new telnet sessions: ☐ Disable ☒ Enable

Session Timeout (Minutes):  (1 to 160)

Maximum Number of Sessions:  (0 to 5)

Current Number of Sessions:

### Outbound Telnet

Allow new telnet sessions: ☐ Disable ☒ Enable

Session Timeout (Minutes):  (1 to 160)

Maximum Number of Sessions:  (0 to 5)

Current Number of Sessions:

8. Use **Login Authentication List** to specify which authentication list to use log in through Telnet.

The default value is networkList.

9. Use **Enable Authentication List** to specify which authentication list you are using when going into the privileged EXEC mode.

The default value is enableNetList.

10. To configure inbound Telnet settings, specify the following:

- Select the Telnet Server Admin Mode **Disable** or **Enable** radio button.  
This enables or disables the administrative mode of the Telnet server. The default value is Enabled.
- Select the Allow New Telnet Sessions **Disable** or **Enable** radio button.  
This specifies whether the new inbound Telnet session is enabled or disabled. The default value is Enabled so that new inbound Telnet sessions can be established until there are no more sessions available. If it 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.
- Use **Session Timeout** to specify how many minutes of inactivity 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 minutes.
- Use **Maximum Number of Sessions** to specify how many simultaneous Telnet sessions are allowed. The maximum is 5, which is also the factory default.

The **Current Number of Sessions** field displays the number of current sessions.

11. To configure outbound Telnet settings, specify the following:

- Select the **Allow New Telnet Sessions Disable** or **Enable** radio button.  
This specifies whether the new outbound Telnet sessions are enabled or disabled. The default value is Enabled so that 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.
- Use **Session Timeout** to specify the outbound Telnet login inactivity time-out in minutes.  
The default value is 5 minutes. Valid range is 1 to 160.
- Use **Maximum Number of Sessions** to specify the maximum number of outbound Telnet sessions allowed.  
The default value is 5. The valid range is 0 to 5.

The **Current Number of Sessions** field 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**.

Access		Console Port	
• HTTP	▼	Serial Port Login Timeout (minutes)	5 (0 to 160)
• HTTPS	▼	Baud Rate (bps)	115200 ▼
• SSH	▼	Character Size (bits)	8
• Telnet	▼	Flow Control	Disable
• <b>Console Port</b>		Stop Bits	1
• Denial of Service Configuration		Parity	None
• Access Control	▼	Login Authentication List	defaultList ▼
		Enable Authentication List	enableList ▼

8. In the **Serial Port Login Timeout (minutes)** field, specify how many minutes of inactivity 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.
9. In the **Baud Rate (bps)** list, 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** list, select which authentication list to use when you log in through Telnet.

The default value is defaultList.

11. In the **Enable Authentication List** list, select which authentication list to use when going into the privileged EXEC mode.

The default value is enableList

The following table describes the nonconfigurable data that is displayed.

**Table 212. 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 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 > Denial of Service Configuration**.



System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help
Management Security	Access	Port Authentication	Traffic Control	Control	ACL		
<div> <div>Access</div> <div>Denial of Service Configuration</div> </div>							
• HTTP		Denial of Service Min TCP Header Size		20 (0 to 255)			
• HTTPS		Denial of Service ICMPv4		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
• SSH		Denial of Service Max ICMPv4 Packet Size		512 (0 to 16376)			
• Telnet		Denial of Service ICMPv6		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
• Console Port		Denial of Service Max ICMPv6 Packet Size		512 (0 to 16376)			
• Denial of Service Configuration		Denial of Service First Fragment		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
• Access Control		Denial of Service ICMP Fragment		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
		Denial of Service SIP=DIP		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
		Denial of Service SMAC=DMAC		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
		Denial of Service TCP FIN&URG&PSH		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
		Denial of Service TCP Flag&Sequence		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
		Denial of Service TCP Fragment		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
		Denial of Service TCP Offset		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
		Denial of Service TCP Port		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
		Denial of Service TCP SYN		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
		Denial of Service TCP SYN&FIN		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			
		Denial of Service UDP Port		<input checked="" type="radio"/> Disable <input type="radio"/> Enable			

8. In the **Denial of Service Min TCP Header Size** field, specify the minimum TCP header 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. Select the Denial of Service ICMPv4 **Disable** or **Enable** radio button.

Enabling 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 packet size. The factory default is Disable.

10. Specify the **Denial of Service Max ICMPv4 Packet Size**.

This is the maximum 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 packet size. Its range is 0 to 16376. The default value is 512.

11. Use **Denial of Service ICMPv6** to enable ICMPv6 DoS prevention.

This 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 Disable.

12. Use **Denial of Service Max ICMPv6 Packet Size** to specify the maximum IPv6 ICMP packet size allowed.

If ICMPv6 DoS prevention is enabled, the switch drops IPv6 ICMP ping packets with a size greater than the configured maximum ICMPv6 packet size. Its range is 0 to 16376. The default value is 512.

13. Select the Denial of Service First Fragment **Disable** or **Enable** radio button.

This enables First Fragment DoS prevention, which causes the switch to check DoS options on first fragment IP packets when switch are receiving fragmented IP packets. Otherwise, switch ignores the first fragment IP packages. The factory default is Disable.

14. Select the Denial of Service ICMP Fragment **Disable** or **Enable** radio button.

Enabling ICMP Fragment DoS prevention causes the switch to drop ICMP Fragmented packets. The factory default is Disable.

15. Select the Denial of Service SIP=DIP **Disable** or **Enable** radio button.

Enable SIP=DIP DoS prevention causes the switch to drop packets with a source IP address equal to the destination IP address. The factory default is Disable.

16. Select the Denial of Service SMAC=DMAC **Disable** or **Enable** radio button.

Enabling SMAC=DMAC DoS prevention causes the switch to drop packets with a source MAC address equal to the destination MAC address. The factory default is Disable.

17. Select the Denial of Service TCP FIN&URG&PSH **Disable** or **Enable** radio button.

Enabling TCP FIN & URG & PSH DoS prevention causes the switch to drop packets with TCP Flags FIN, URG, and PSH set and TCP Sequence Number=0. The factory default is Disable.

18. Select the Denial of Service TCP Flag&Sequence **Disable** or **Enable** radio button.

Enabling TCP Flag DoS prevention causes the switch to drop packets with TCP control flags set to 0 and TCP sequence number set to 0. The factory default is Disable.

19. Select the Denial of Service TCP Fragment **Disable** or **Enable** radio button.

Enabling TCP Fragment DoS prevention causes the switch to drop packets as follows:

First TCP fragments with a TCP payload:  $IP\_Payload\_Length - IP\_Header\_Size < Min\_TCP\_Header\_Size$ .

The factory default is Disable.

20. Select the Denial of Service TCP Offset **Disable** or **Enable** radio button.

Enabling TCP Offset DoS prevention causes the switch to drop packets with a TCP header Offset=1. The factory default is Disable.

21. Select the Denial of Service TCP Port **Disable** or **Enable** radio button.

Enabling TCP Port DoS prevention causes the switch to drop packets with TCP source port equal to TCP destination port. The factory default is Disable.

22. Select the Denial of Service TCP SYN **Disable** or **Enable** radio button.

Enabling TCP SYN DoS prevention causes the switch to drop packets with TCP flags SYN set. The factory default is Disable.

23. Select the Denial of Service TCP SYN & FIN **Disable** or **Enable** radio button.

Enabling TCP SYN & FIN DoS prevention causes the switch to drop packets with TCP flags SYN and FIN set. The factory default is Disable.

24. Select the **Denial of Service UDP Port Disable** or **Enable** radio button.

Enabling UDP Port DoS prevention causes the switch to drop packets with UDP source port equal to UDP destination port. The factory default is Disable.

## Configure an Access Control Profile

### ➤ To configure the access profile 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 > Access Control > Access Profile Configuration**.

**Access Profile Configuration**

Access Profile Name

Activate Profile ☐

Deactivate Profile ☐

Remove Profile ☐

Packets Filtered 0

**Profile Summary**

Rule Type	Service Type	Source IP Address	Mask	Priority
-----------	--------------	-------------------	------	----------

8. In the **Access Profile Name** field, enter the name of the access profile to be added.

The maximum length is 32 characters.

9. To activate an access profile, select the **Activate Profile** check box.
10. To deactivate an access profile, select the **Deactivate Profile** check box.
11. To remove an access profile, select the **Remove Profile** check box.

NETGEAR recommends that you deactivate the access profile before removing it.

The **Packets Filtered** field displays the number of packets filtered.

12. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 213. Access Profile Configuration Profile Summary**

Field	Description
Rule Type	The action performed when the rules are matched.
Service Type	The service type chosen. The policy is restricted by the service type chosen.
Source IP Address	Source IP address of the client originating the management traffic.
Mask	The subnet mask of the IP Address.
Priority	The priority of the rule.

## Configure Access Rule Settings

### ➤ To configure the access rule 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 > Access Control > Access Rule Configuration**.

Rule Type	Service Type	Source IP Address	Mask	Priority
	TELNET TFTP HTTP Secure HTTP(SSL) SNMP Secure Telnet(SSH) JAVA			

You can apply changes to the access rule only when the access profile is in a deactivated state.

**Note:** Make sure that the access profile is created before adding the rules.

8. From the **Rule Type** list, select to either **Permit** or **Deny** access when the rules selected are matched.
9. The policy is restricted by the **Service Type** you select from the list.

Possible management methods are as follows:

- HTTP
- JAVA
- Secure HTTP (SSL)
- Secure Telnet (SSH)
- SNMP
- Telnet
- TFTP

10. Enter the **Source IP Address** of the client originating the management traffic.
11. Enter the source IP address **Mask** of the client originating the management traffic.
12. Configure the **Priority** for the rule.

The rules are validated against the incoming management request in ascending order of their priorities. If a rule matches, the action is performed and subsequent rules below that are ignored. For example, if a source IP 10.10.10.10 is configured with priority 1 to permit, and source IP 10.10.10.10 is configured with priority 2 to deny, then access is permitted if the profile is active, and the second rule is ignored.

13. Click the **Add** button.

The access rule is added.

14. To delete the selected access rule, click the **Delete** button.

You can delete an access rule only if the access profile is deactivated.

15. Click the **Apply** button.

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

## Port Authentication

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.** The port that is authenticated before permitting system access.
- **Supplicants.** The host connected to the authenticated port requesting access to the system services.
- **Authentication Server.** 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

### ➤ 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**.

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

This enables or disables 802.1X administrative mode on the switch.

- **Enable.** Port-based authentication is permitted on the switch.

If 802.1X is enabled, authentication is performed by a RADIUS server. This means 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 Login Authentication List](#) on page 555.

- **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. Use **Dynamic VLAN Creation Mode** to select **Disable** or **Enable**.

The default value is Disable.

12. Use **Monitor Mode** to 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.

13. Use **Users** to select the user name for the selected login list for 802.1x port security.

14. Use **Login** to select the login list to apply to the specified user.

All configured login lists are displayed. The Authentication List field displays the authentication list that is used by 802.1X

## Configure 802.1X Settings

You can enable or disable 802.1X access control on the system.

➤ **To configure 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 > Advanced > 802.1X Configuration**.

System	Switching	Routing	QoS	Security	Monitoring
Management Security	Access	Port Authentication	Traffic Control	Control	ACL

Port Authentication
802.1X Configuration

- Basic
- Advanced
- 802.1X Configuration**
  - Port Authentication
  - Port Summary
  - Client Summary

Administrative Mode: ☒ Disable ☐ Enable  
VLAN Assignment Mode: ☒ Disable ☐ Enable  
EAPOL Flood Mode: ☒ Disable ☐ Enable  
Dynamic VLAN Creation Mode:   
Monitor Mode:   
Users:   
Login:   
Authentication List:

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. Use Dynamic VLAN Creation Mode to select Disable or Enable.**

The default value is Disable.

**12. Use Monitor Mode to 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.

**13. Use Users to select the user name for the selected login list for 802.1x port security.**

**14. Use Login to select the login list to apply to the specified user.**

All configured login lists are displayed. The **Authentication List** field displays the list that is used by 802.1X.

## Configure 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**.

**Note:** Use the horizontal scroll bar at the bottom of the screen to view all the fields.

Port Authentication															
1 All															
	Port	Control Mode	MAB	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
															Max Users
<input type="checkbox"/>	1/0/1	Auto	Disable	60	30	0	90	0	30	30	2	Authenticator	Disable	3600	admin.guest
<input type="checkbox"/>	1/0/2	Auto	Disable	60	30	0	90	0	30	30	2	Authenticator	Disable	3600	admin.guest
<input type="checkbox"/>	1/0/3	Auto	Disable	60	30	0	90	0	30	30	2	Authenticator	Disable	3600	admin.guest
<input type="checkbox"/>	1/0/4	Auto	Disable	60	30	0	90	0	30	30	2	Authenticator	Disable	3600	admin.guest
<input type="checkbox"/>	1/0/5	Auto	Disable	60	30	0	90	0	30	30	2	Authenticator	Disable	3600	admin.guest

8. Select the check box next to the port to configure.

You can also 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 ports, specify the following settings:

- **Control Mode.** Select an option for the 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 MAC-based. The default selection is Disable. 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.
- **Quiet Period.** This input field allows you 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 and 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 you click the **Apply** button.
- **Transmit Period.** This input field allows you 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 and 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 you to configure guest VLAN ID on the interface. The valid range is 0–4093. 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 for guest VLAN authentication. The guest VLAN time-out must be a value from 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.** 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 **Apply** button is clicked. Enter 0 to clear the unauthenticated VLAN ID on the interface.
  - **Supplicant Timeout.** 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 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.** 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 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.** 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.** Select the port access entity (PAE) functionality of the selected port. Possible values are Authenticator or Supplicant.
  - **Periodic Reauthentication.** 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.** Enter the reauthentication period for the selected port. The reauthentication period is the value, in seconds, of the timer for 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.** Add the specified user to the list of users with access to the specified port or all ports.
  - **Max Users.** Enter the limit to the number of supplicants on the specified interface.
10. To begin the initialization sequence on the selected port, click the **Initialize** button.

The initialization sequence begins.

You can click this button only if the control mode is auto. If the button is not available, it is grayed out. Once this button is clicked, the action is immediate. You do not need to click the **Apply** button for the action to occur.

## 11. Click the **Reauthentication** button.

The reauthentication sequence begins on the selected port.

You can click this button only if the control mode is auto. If the button is not available, it is grayed out. Once you click this button, the action is immediate. You do not need to click the **Apply** button 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														
1 All														
Port	Control Mode	Operating Control Mode	Reauthentication Enabled	Control Direction	Protocol Version	PAE Capabilities	Authenticator PAE State	Backend State	VLAN Assigned	VLAN Assigned Reason	Key Transmission Enabled	Session Timeout	Session Termination Action	Port Status
1/0/1	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A
1/0/2	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A
1/0/3	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A
1/0/4	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A
1/0/5	Auto	N/A	FALSE	Both	Version1	Authenticator	Initialize	Initialize	0	Not Assigned	FALSE	0	Default	N/A

The following table describes the fields on the Port Summary screen.

**Table 214. Port Summary**

Field	Description
Port	The port whose settings are displayed in the current table row.
Control Mode	<p>This field indicates the configured control mode for the port. Possible values are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Force Unauthorized.</b> The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized.</li> <li>• <b>Force Authorized.</b> The authenticator PAE unconditionally sets the controlled port to authorized.</li> <li>• <b>Auto.</b> 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>• <b>MAC Based.</b> 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	<p>The control mode under which the port is actually operating. Possible values are as follows:</p> <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	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	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	The port access entity (PAE) functionality of the selected port. Possible values are Authenticator or Supplicant. This field is not configurable.

**Table 214. Port Summary (continued)**

Field	Description
Authenticator PAE State	<p>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>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>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>The 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>The session rimeout 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 214. Port Summary (continued)

Field	Description
Session Termination Action	<p>The 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:</p> <ul style="list-style-type: none"> <li>• Default</li> <li>• Reauthenticate</li> </ul> <p>If the termination action is set to default, then at the end of the session, the client details are initialized. Otherwise re-authentication is attempted.</p>
Port Status	<p>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.</p>

## 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**.

Client Summary								
1 All								
Port	User Name	Supplicant MAC Address	Session Time	Filter ID	VLAN ID	VLAN Assigned	Session Timeout	Termination Action
1 All								

**Table 215. Client Summary**

Field	Description
Port	The port to be displayed.
User Name	The user name representing the identity of the supplicant device.
Supplicant Mac Address	The supplicant's device MAC address.
Session Time	The time since the supplicant as logged in seconds.
Filter ID	The policy filter ID assigned by the authenticator to the supplicant device.
VLAN ID	The VLAN ID assigned by the authenticator to the supplicant device.
VLAN Assigned	The reason for the VLAN ID assigned by the authenticator to the supplicant device.
Session Timeout	The session time-out set by the RADIUS server to the supplicant device.
Termination Action	The 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.

### Configure MAC Filtering

You can create MAC filters that limit the traffic allowed into and out of specified ports on the system.

➤ **To configure MAC filter settings:**

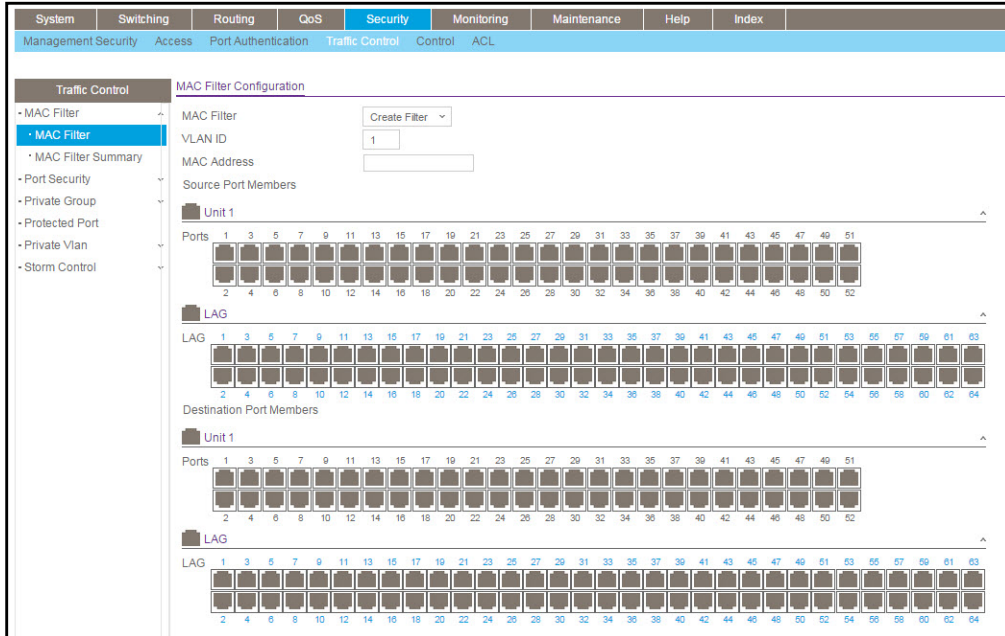
1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address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



This is the list of MAC address and VLAN ID pairings for all configured filters.

8. To change the port masks for an existing filter, select the entry.
9. To add a new filter, select **Create Filter** from the **MAC Filter** list.
10. From the **VLAN ID** list, select the VLAN to use with the MAC address to fully identify packets to be filtered.

You can change this field only when **Create Filter** is selected from the **MAC Filter** list.

11. In the **MAC Address** field, 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:

- 00:00:00:00:00:00
- 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

12. Use **Source Port Members** to list the ports to be 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.

13. 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 are transmitted only from ports that are in the list. Destination ports can be included only in the multicast filter.

**14.** To delete a configured MAC filter, select it, and then click the **Delete** button.

**15.** Click the **Apply** button.

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

## MAC Filter Summary

### ➤ 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.

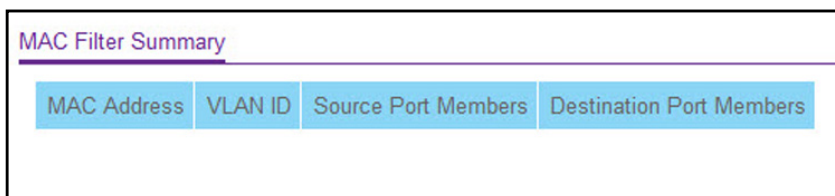
5. Enter the user name and password.

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**.



MAC Filter Summary			
MAC Address	VLAN ID	Source Port Members	Destination Port Members

The following table describes the information displayed on the screen.

**Table 216. MAC Filter Summary**

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 216. MAC Filter Summary (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.

## Port Security

You can configure port security settings.

### Configure the Global Port Security Mode

You can 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**.

**Port Security Settings**

Port Security Mode ☒ Disable ☐ Enable

**Port Security Violations**

Port	Last Violation MAC	VLAN ID
------	--------------------	---------

8. Select the Port Security Mode **Disable** or **Enable** radio button.

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 217. Port Security Violations**

Field	Description
Port	The physical interface.
Last Violation MAC	The source MAC address of the last packet that was discarded at a locked port.
VLAN ID	The VLAN ID corresponding to the last violation MAC address.

## Configure a Port Security Interface

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 was not 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**.

Interface Configuration

1 LAGS All Go To Port

<input type="checkbox"/>	Port	Security Mode	Max Allowed Dynamically Learned MAC	Max Allowed Statically Locked MAC	Violation Trap
<input type="checkbox"/>		<input type="text" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="v"/>
<input type="checkbox"/>	1/0/1	Disable	4096	48	Disable
<input type="checkbox"/>	1/0/2	Disable	4096	48	Disable
<input type="checkbox"/>	1/0/3	Disable	4096	48	Disable
<input type="checkbox"/>	1/0/4	Disable	4096	48	Disable
<input type="checkbox"/>	1/0/5	Disable	4096	48	Disable

8. 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.
9. 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 Learned MAC Addresses to Static Addresses

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**.

**Port Security Settings**

Convert Dynamic Address to Static ☒

Number Of Dynamic MAC Addresses Learned: 0

**Dynamic MAC Address Table**

Port List: 1/0/1 ▼

VLAN ID	MAC Address
---------	-------------

8. Use **Port List** to select the physical interface.
9. Use the **Convert Dynamic Address to Static** check box to convert a dynamically learned MAC address to a statically locked address.

The dynamic MAC address entries are converted to static MAC address entries in a numerically ascending order until the static limit is reached.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table shows the MAC addresses and their associated VLANs learned on the selected port. Use the **Port List** menu to select the interface.

**Table 218. Dynamic MAC Address**

Field	Description
Number of Dynamic MAC Addresses Learned	The number of dynamically learned MAC addresses on a specific port.
VLAN ID	The VLAN ID corresponding to the MAC address.
MAC Address	The MAC addresses learned on a specific port.

## Configure a Static MAC Address

### ➤ To configure a static 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 **Security > Traffic Control > Port Security > Static MAC Address**.

The screenshot shows the web management interface for configuring static MAC addresses. At the top, under the 'Port List' heading, there is a label 'Interface' followed by a dropdown menu currently showing '1/0/1'. Below this, under the 'Static MAC Address Table' heading, there is a table with two columns: 'Static MAC Address' and 'VLAN ID'. The 'Static MAC Address' column contains an empty text input field. The 'VLAN ID' column contains a dropdown menu with a downward arrow.

8. Use **Interface** to select the physical interface.

9. **Static MAC Address.** Accepts user input for the MAC address to be added.
10. Use **VLAN ID** to select the VLAN ID corresponding to the MAC address being added.
11. Click the **Add** button.

The static MAC address is added to the switch.

12. To delete a existing static MAC address from the switch, click the **Delete** button.

## Configure a Private Group

### ➤ To configure a traffic control 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		
Private Group Configuration		
Group Name	Group ID	Group Mode
<input type="text"/>	<input type="text"/>	<input type="text" value="v"/>

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** list, select the mode of private group.



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 that each member port can forward traffic to other members in the same group, but not to members in other groups.

11. Click the **Add** button.

The private group is created in the switch.

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.

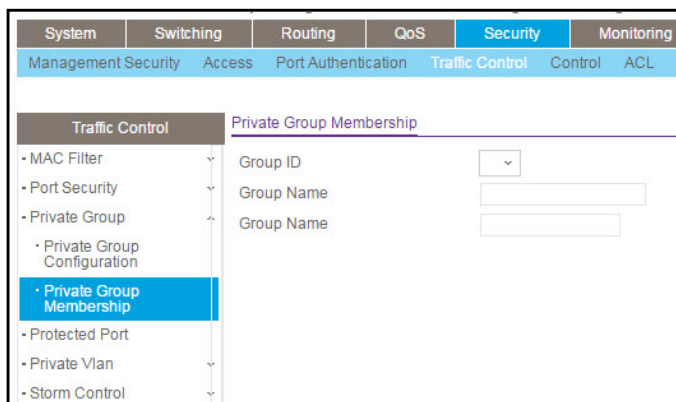
5. Enter the user name and password.

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** list, select the group ID.
9. Use **Port List** to add the ports you selected to this private group.

The port list displays when at least one group is configured.

**10.** 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 219. Private Group Membership**

Field	Description
Group Name	The name for the private group that you selected. It can be up to 24 non-blank characters long.
Group Mode	<p>The mode of the private group that you selected. The modes are as follows:</p> <ul style="list-style-type: none"> <li>community</li> <li>isolated</li> </ul> <p>When in <b>isolated</b> 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 <b>community</b> 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 does forward 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**.

Protected Ports Configuration

Group ID: 0

Group Name:

Unit 1

Ports: 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47

2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48

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 list includes all the possible protected port group IDs supported for the current platform. The valid range of the gGroup 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 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 **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

## Configure a Private VLAN

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.

### ➤ 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**.

<input type="checkbox"/>	VLAN ID	Private VLAN Type
<input type="checkbox"/>	1	Unconfigured

8. Use **Private VLAN Type** to select the type of private VLAN.  
The factory default is Unconfigured.
9. Click the **Apply** button.  
The updated configuration is sent to the switch. Configuration changes take effect immediately.  
The VLAN ID field specifies the VLAN ID for which the private VLAN type is being set. The factory default is Unconfigured.

## Configure Private VLAN Association Settings

- **To configure 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.  
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 Association Configuration**.

8. Use **Primary VLAN** to select the primary VLAN ID of the domain.

This is used to associate secondary VLANs with the domain.

9. Use **Secondary VLAN(s)** to display all the statically created VLANs (excluding the primary and default VLANs).

This control is used to associate VLANs with the selected primary VLAN.

10. To delete the IP subnet-based VLAN from the switch, click the **Delete** button.

11. 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 220. Private VLAN Association**

Field	Description
Isolated VLAN	The isolated VLAN associated with the selected primary VLAN.
Community VLAN(s)	The list of community VLANs 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**.

Private Vlan Port Mode Configuration	
1 LAGS All Go To Interface <input type="text"/> <input type="button" value="Go"/>	
<input type="checkbox"/> Interface	Port Vlan Mode
<input type="checkbox"/>	<input type="text" value="v"/>
<input type="checkbox"/> 1/0/1	General
<input type="checkbox"/> 1/0/2	General
<input type="checkbox"/> 1/0/3	General
<input type="checkbox"/> 1/0/4	General
<input type="checkbox"/> 1/0/5	General

8. Use **Switch Port Mode** to select the switch port mode.
  - **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.

The factory default is General.

9. Click the **Apply** button.

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

## Configure a 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**.

Private VLAN Host Interface Configuration				
1 LAG All		Go To Interface	Go	
<input type="checkbox"/>	Interface	Host Primary VLAN	Host Secondary VLAN	Operational VLAN(s)
<input type="checkbox"/>	1/0/1	0	0	
<input type="checkbox"/>	1/0/2	0	0	
<input type="checkbox"/>	1/0/3	0	0	
<input type="checkbox"/>	1/0/4	0	0	
<input type="checkbox"/>	1/0/5	0	0	

8. In the **Host Primary VLAN** field, 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 updated configuration is sent to the switch. Configuration changes take effect immediately.

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

**Table 221. Private VLAN Host Interface Configuration**

Field	Description
Interface	Select the physical or LAG interface.
Operational VLAN(s)	The operational VLANs.

## Configure a Private VLAN Promiscuous Interface

➤ **To configure a private VLAN promiscuous 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 Promiscuous Interface Configuration**.

Interface	Promiscuous Primary VLAN (2 to 4093)	Promiscuous Secondary VLAN(s) Range[2-4093]	Operational VLAN(s)
<input type="checkbox"/> 1/0/1	0		
<input type="checkbox"/> 1/0/2	0		
<input type="checkbox"/> 1/0/3	0		
<input type="checkbox"/> 1/0/4	0		
<input type="checkbox"/> 1/0/5	0		

8. Use **Promiscuous Primary VLAN** to set the primary VLAN ID for Promiscuous Association mode.

The range of the VLAN ID is 2–4093.

9. Use **Promiscuous Secondary VLAN ID(s)** to set the secondary VLAN ID list for Promiscuous Association mode.

This field can accept single VLAN ID or range of VLAN IDs or a combination of both in sequence separated by ','. You can specify individual VLAN ID, such as 10. You can specify the VLAN range values separated by a hyphen, for example, 10-13. You can specify the combination of both separated by commas, for example:

12,15,40–43,1000–1005, 2000. The range of the VLAN ID is 2–4093.



**Note:** The VLAN ID List given in this control replaces the configured secondary VLAN list in the association.

10. Click the **Delete** button to delete the IP subnet-based VLAN from the switch.

11. 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 222. Private VLAN Promiscuous Interface Configuration**

Field	Description
Interface	Select the physical or LAG interface
Operational VLAN(s)	The operational VLANs.

## Storm Control

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 Global Storm Control Settings

### ➤ To configure global storm control 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**.

Port Settings	
Broadcast Storm Control All	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Multicast Storm Control All	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Unknown Unicast Storm Control All	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

The following three 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.

8. Select the Broadcast Storm Control All **Disable** or **Enable** radio button.

This enables or disables Broadcast Storm Recovery mode on all ports. When you specify Enable and the broadcast traffic on any Ethernet port exceeds the configured threshold, the switch blocks (discards) the broadcast traffic. The factory default is Enable.

9. Select the Multicast Storm Control All **Disable** or **Enable** radio button.

This enables or disables Multicast Storm Recovery mode on all ports. When you specify Enable, and the multicast traffic on any Ethernet port exceeds the configured threshold, the switch blocks (discards) the multicast traffic. The factory default is Disable.

10. Select the Unknown Unicast Storm Control All **Disable** or **Enable** radio button.

This enables or disables Unicast Storm Recovery mode on all ports. When you specify Enable, and the unicast traffic on any Ethernet port exceeds the configured threshold, the switch blocks (discards) the unicast traffic. The factory default is Disable.

## Configure a Storm Control Interface

### ➤ To configure a storm control 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										
1 All										
Go To Port <input type="text"/> <input type="button" value="Go"/>										
Port	Broadcast Storm				Multicast Storm			Unicast Storm		
	Recovery Mode	Recovery Level Type	Recovery Level	Control Action	Recovery Mode	Recovery Level Type	Recovery Level	Recovery Mode	Recovery Level Type	Recovery Level
<input type="checkbox"/> 1/0/1	Enable	Percent	5	RateLimit	Disable	Percent	5	Disable	Percent	5
<input type="checkbox"/> 1/0/2	Enable	Percent	5	RateLimit	Disable	Percent	5	Disable	Percent	5
<input type="checkbox"/> 1/0/3	Enable	Percent	5	RateLimit	Disable	Percent	5	Disable	Percent	5
<input type="checkbox"/> 1/0/4	Enable	Percent	5	RateLimit	Disable	Percent	5	Disable	Percent	5
<input type="checkbox"/> 1/0/5	Enable	Percent	5	RateLimit	Disable	Percent	5	Disable	Percent	5

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

**Table 223. Storm Control Interface Configuration**

Field	Description
Broadcast Storm Recovery Mode	Enable or disable this option by selecting the corresponding line on the drop-down 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	Specify the broadcast storm recovery level as a percentage of link speed or as packets per second.
Broadcast Storm Recovery Level	Specify the threshold at which storm control activates. The factory default is 5 percent of port speed for pps type.
Broadcast Storm Control Action	Provides configurability to shut down the port when the configured threshold of the broadcast storm recovery feature gets breached. Select the option to either ShutDown or RateLimit mode. The default is RateLimit.
Multicast Storm Recovery Mode	Enable or disable this option by selecting the corresponding line on the list. 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 Disable.
Multicast Storm Recovery Level Type	Specify the multicast storm recovery level as a percentage of link speed or as packets per second.
Multicast Storm Recovery Level	Specify 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. 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 Disable.

Table 223. Storm Control Interface Configuration (continued)

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.

## DHCP Snooping

You can configure DHCP snooping global and interface settings.

### Configure DHCP Snooping Global Settings

➤ **To configure DHCP snooping 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 > Control > DHCP Snooping > Global Configuration**.

DHCP Snooping Global Configuration					
DHCP Snooping Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable				
MAC Address Validation	<input type="radio"/> Disable <input checked="" type="radio"/> Enable				
VLAN Configuration					
<input type="checkbox"/>	<table border="1"> <thead> <tr> <th>VLAN ID</th> <th>DHCP Snooping Mode</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text" value="v"/></td> </tr> </tbody> </table>	VLAN ID	DHCP Snooping Mode	<input type="text"/>	<input type="text" value="v"/>
VLAN ID	DHCP Snooping Mode				
<input type="text"/>	<input type="text" value="v"/>				

8. Select the DHCP Snooping Mode **Disable** or **Enable** radio button.  
The factory default is Disable.
9. Select the MAC Address Validation **Disable** or **Enable** radio button.  
This enables or disables the validation of sender MAC address for DHCP snooping. The factory default is Enable.
10. 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 Disable.
12. Click the **Apply** button.  
The updated configuration is sent to the switch. These changes are not retained across a power cycle unless a save configuration is performed.

## Configure a DHCP Snooping Interface

- **To configure a 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**.

<input type="checkbox"/>	Interface	Trust Mode	Invalid Packets	Rate Limit(pps)	Burst Interval(secs)
<input type="checkbox"/>	1/0/1	Disable	Disable	None	N/A
<input type="checkbox"/>	1/0/2	Disable	Disable	None	N/A
<input type="checkbox"/>	1/0/3	Disable	Disable	None	N/A
<input type="checkbox"/>	1/0/4	Disable	Disable	None	N/A
<input type="checkbox"/>	1/0/5	Disable	Disable	None	N/A

8. Use the **Interface** check boxes to select the interface.
9. If **Trust Mode** is enabled, DHCP snooping application considers the port as trusted.  
The factory default is Disable.
10. If **Invalid Packets** is enabled, DHCP snooping application logs invalid packets on this interface.  
The factory default is Disable.
11. Use **Rate Limit (pps)** to specify rate limit value for DHCP snooping purposes.  
If the incoming rate of DHCP packets exceeds the value of this 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 value -1, which means N/A. The range of rate limit is 0 to 300.
12. Use **Burst Interval (secs)** to specify the burst interval value for rate limiting purpose on this interface.  
If the rate limit is N/A, burst interval has no meaning and it is N/A. The default value is N/A. It can be set to -1, which means N/A. The range of Burst Interval is 1 to 15.

## Configure DHCP Snooping Binding

### ➤ To configure snooping 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				
<input type="checkbox"/>	Interface	MAC Address	VLAN ID	IP Address
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<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. To configure static binding, specify the following:
  - a. Use the **Interface** check boxes to select the interface.
  - b. Use **MAC Address** to specify the MAC address for the binding entry to be added.  
This is the key to the binding database.
  - c. Use **VLAN ID** to select the VLAN from the list for the binding rule.  
The range of the VLAN ID is 1 to 4093.
  - d. Use **IP Address** to specify valid IP address for the binding rule.
  - e. Click the **Add** button.  
The DHCP snooping binding entry is added into the database.
  - f. To delete selected static entries from the database, click the **Delete** button.
9. To configure dynamic binding, specify the following:
  - a. Use the **Interface** check boxes to select the interface.
  - b. Use **MAC Address** to display the MAC address for the binding in the binding database.
  - c. 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.

- d. **IP Address.** Displays IP address for the binding entry in the binding database.
- e. **Lease Time.** The remaining lease time for the dynamic entries.
- f. To delete all DHCP snooping binding entries, click the **Clear** button.

## Configure Snooping Persistent Settings

### ➤ To configure snooping persistent 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 > Persistent Configuration**.

8. Select the Store **Local** or **Remote** radio button.  
Selecting **Local** disables the remote fields **Remote File Name** and **Remote IP Address**.
9. If you are selected Remote, do the following:
  - a. In the **Remote IP Address** field, type the remote IP address on which the snooping database is stored.
  - b. In the **Remote File Name** field, enter the remote file name to store the database.



10. In the **Write Delay** field, enter the maximum write time to write the database into local or remote.

The range is 15 to 86400.

## View DHCP Snooping Statistics

### ➤ To view DHCP snooping 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 **Security > Control > DHCP Snooping > Statistics**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance
Management Security	Access	Port Authentication	Traffic Control	Control	ACL	

Control

• DHCP Snooping

• Global Configuration

• Interface Configuration

• Binding Configuration

• Persistent Configuration

• Statistics

• IP Source Guard

DHCP Snooping Statistics

123LAGAll

Interface	MAC Verify Failures	Client Ifc Mismatch	DHCP Server Msgs
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

To clear all interfaces statistics, click the **Clear** button.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the DHCP snooping statistics.

**Table 224. 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 because 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	The number of server messages that are dropped on an untrusted port.

## Configure an IP Source Guard Interface

You can configure IP source guard (IPSG) on each interface. IPSG is a security feature that filters IP packets based on source ID. This feature helps protect the network from attacks that use IP address spoofing to compromise or overwhelm the network. The source ID can be either the source IP address or a source IP address and source MAC address pair. The DHCP snooping bindings database, along with IPSG entries in the database, identify authorized source IDs. If you enable IPSG on a port where DHCP snooping is disabled or where DHCP snooping is enabled but the port is trusted, all IP traffic received on that port is dropped depending on the admin-configured IPSG entries. Additionally, IPSG interacts with port security, also known as port MAC locking, to enforce the source MAC address in received packets. Port security controls source MAC address learning in the Layer 2 forwarding database (the MAC address table). When a frame is received with a previously unlearned source MAC address, port security queries the IPSG feature to determine whether the MAC address belongs to a valid binding.

### ➤ To configure IP Source Guard 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 > Control > IP Source Guard > Interface Configuration**.

<input type="checkbox"/>	Interface	IPSG Mode	IPSG Port Security
<input type="checkbox"/>		<input type="text" value="v"/>	<input type="text" value="v"/>
<input type="checkbox"/>	1/0/1	Disable	Disable
<input type="checkbox"/>	1/0/2	Disable	Disable
<input type="checkbox"/>	1/0/3	Disable	Disable
<input type="checkbox"/>	1/0/4	Disable	Disable
<input type="checkbox"/>	1/0/5	Disable	Disable

8. Use the **Interface** check boxes to select the interface.
9. In the **IPSG Mode** list, select **Disable** or **Enable**.

This sets the administrative mode of IPSG on the interface. When IPSG mode is enabled, the sender IP address on this interface is validated against the DHCP snooping binding database. If IPSG is enabled, packets are not forwarded if the sender IP address is not in DHCP snooping binding database. The factory default is Disable.

10. In the **IPSG Port Security** list, select **Disable** or **Enable**.

This enables or disables the administrative mode of IPSG port security on the selected interface. When this is enabled, the packets are not forwarded if the sender MAC address is not in forwarding database (FDB) table or the 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 cannot be enabled if IPSG is disabled. The factory default is Disable. Also, you cannot turn off IPv6SG port security while IPv6SG is enabled.

11. Click the **Apply** button.

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

## Configure IP Source Guard Binding Settings

- **To configure IP source guard static binding 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 > IP Source Guard > Binding Configuration**.

The screenshot displays the 'Static Binding Configuration' web page. At the top, there's a section titled 'Static Binding Configuration' with a table containing five columns: 'Interface', 'MAC Address', 'VLAN ID', 'IP Address', and 'Filter Type'. Each column has a corresponding input field below it. Below this section is another section titled 'Dynamic Binding Configuration' with the same five columns and input fields.

8. Use the **Interface** check boxes to select the interface.
9. In the **MAC Address** field, type the MAC address for the binding.
10. In the **VLAN ID** list, select the VLAN for the binding rule.
11. In the **IP Address** field, specify valid IP address for the binding rule.
12. Click the **Add** button.

The IPSG static binding entry is added into the database.

13. To delete selected static entries from the database, click the **Delete** button.

To clear all the dynamic binding entries, click the **Clear** button.

The following table describes the nonconfigurable IP Source Guard Dynamic Binding Configuration information that is displayed.

**Table 225. IP Source Guard Dynamic Binding Configuration**

Field	Description
Interface	The interface for which to add a binding into the IPSG database.
MAC Address	The MAC address for the binding entry.
VLAN ID	The VLAN for the binding entry.

Table 225. IP Source Guard Dynamic Binding Configuration (continued)

Field	Description
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, and the other is source IP address and MAC address filter type.

## Configure IPv6 Source Guard Interface Settings

### ➤ To configure IPv6 source guard 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.

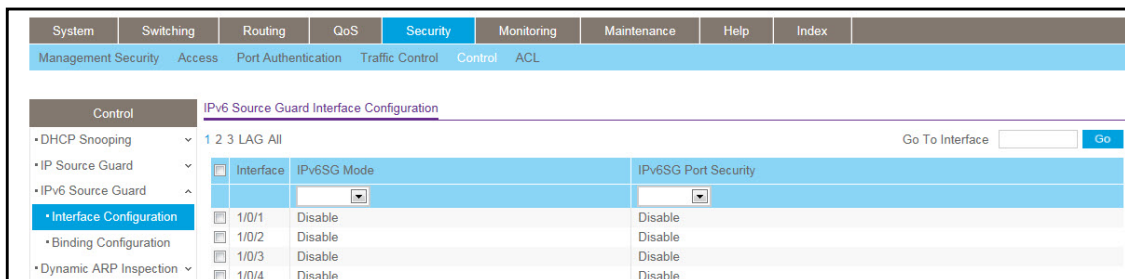
5. Enter the user name and password.

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 > Control > IPv6 Source Guard > Interface Configuration**.



8. Use **Interface** to select the interface.
9. Use **IPv6SG Mode** to enable or disable validation of sender IPv6 address on this interface.  
If IPv6SG is enabled, packets are not forwarded if the sender IPv6 address is not in the DHCP snooping binding database. The factory default is Disable.
10. Use **IPv6SG Port Security** to enable or disable the IPv6SG port security on the selected interface.

If IPv6SG port security is enabled, then the packets are not forwarded if the sender MAC address is not in FDB table and it is not in the 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.

IPv6SG port security cannot be enabled if IPv6SG is disabled. The factory default is Disable. Also, you are not allowed to turn off IPv6SG port security while IPv6SG is enabled.

**11. Click the **Apply** button.**

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

## Configure IPv6 Source Guard Binding

➤ **To configure IPv6 source guard 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 > IPv6 Source Guard > Binding Configuration**.

The screenshot shows the configuration interface for a switch. The top navigation bar includes System, Switching, Routing, QoS, Security, Monitoring, Maintenance, and Help. Under Security, there are sub-menus: Management Security, Access, Port Authentication, Traffic Control, Control, and ACL. The Control menu is expanded, showing options like DHCP Snooping, IP Source Guard, IPv6 Source Guard, Interface Configuration, Binding Configuration (highlighted), Dynamic ARP Inspection, and Captive Portal. The Binding Configuration section is active, displaying two tables: Static Binding Configuration and Dynamic Binding Configuration. Both tables have columns for Interface, MAC Address, VLAN ID, IPv6 Address, and Filter Type.

8. From the **Interface** list, select the interface to add a binding into the IPv6SG database.
9. Use **MAC Address** to specify the MAC address for the binding.
10. Use **VLAN ID** to select the VLAN from the list for the binding rule.
11. Use **IPv6 Address** to specify valid IP address for the binding rule.
12. Click the **Add** button.

The IPv6SG static binding entry is added to the database.

13. To delete the selected static entries from the database, click the **Delete** button.
14. To clear all the dynamic binding entries, click the **Clear** button.

The following table describes the nonconfigurable IPv6 Source Guard Dynamic Binding Configuration information that is displayed.

**Table 226. IPv6 Source Guard Dynamic Binding Configuration**

Field	Description
Interface	The interface to add a binding into the IPSG database.
MAC Address	The MAC address for the binding entry.
VLAN ID	The VLAN for the binding entry.
IPv6 Address	Displays valid IPv6 address for the binding entry.
Filter Type	Filter type used on the interface. One is source IPv6 address filter type, and the other is source IPv6 address and MAC address filter type.

## Configure Dynamic ARP Inspection

### ➤ To configure dynamic ARP inspection (DAI):

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

3. Launch a web browser.
4. Enter 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**.

Dynamic ARP Inspection Global Configuration	
Validate Source MAC	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Validate Destination MAC	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Validate IP	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

8. Select the Validate Source MAC **Disable** or **Enable** radio button.  
This specifies the DAI source MAC validation mode for the switch. 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. If you select **Enable**, IP address validation for the ARP packets is enabled. The factory default is Disable.

## Configure a DAI VLAN

### ➤ To configure a DAI 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 **Security > Control > Dynamic ARP Inspection > DAI VLAN Configuration**.

VLAN ID	Admin Mode	Invalid Packets	ARP ACL Name	Static Flag
1	Disable	Enable		Disable
	Disable	Enable		Disable

8. Use the **VLAN ID** check boxes to select the DAI capable VLANs.

9. In the **Admin Mode** list, select **Enable** or **Disable**.

This indicates whether the dynamic ARP inspection is enabled on this VLAN. If this is set to **Enable**, then dynamic ARP inspection is enabled. If this is set to **Disable**, then dynamic ARP inspection is disabled. The default is **Disable**.

10. Use **Invalid Packets** to indicate whether the dynamic ARP inspection logging is enabled on this VLAN.

If this is set to **Enable**, invalid ARP packets information is logged. If it is set to **Disable**, dynamic ARP inspection logging is disabled. The default is **Enable**.

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. The ARP ACL name is deleted if you specify N/A.

12. Use **Static Flag** to determine whether the ARP packet needs validation using the DHCP snooping database in case ARP ACL rules do not 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 by using the DHCP snooping entries. The factory default is **Disable**.

13. Click the **Apply** button.

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

## Configure the DAI Interface

➤ **To configure the DAI 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**.

<input type="checkbox"/>	Interface	Trust Mode	Rate Limit(pps)	Burst Interval(secs)
<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

8. Use the **Interface** check boxes to select the physical interface.
9. Use **Trust Mode** to indicate whether the interface is trusted for dynamic ARP inspection purposes.  
If this is set to Enable, the interface is trusted. ARP packets coming to this interface are forwarded without checking. If this is set to Disable, the interface is not trusted. ARP packets coming to this interface are subjected to ARP inspection. The factory default is Disable.
10. Use **Rate Limit (pps)** to specify rate limit value for dynamic ARP inspection purpose.  
If the incoming rate of ARP packets exceeds the value of this for consecutive burst interval seconds, ARP packets are dropped. If this value is N/A, there is no limit. The

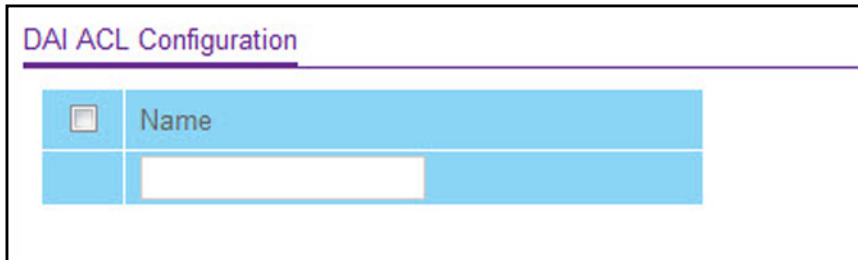
value can be set to -1, which means N/A. The range is 0– 300. The factory default is 15 pps (packets per second).

11. Use **Burst Interval (secs)** to specify the burst interval value for rate limiting purposes on this interface. If the rate limit is None, burst interval has no meaning shows it as N/A. The factory default is 1 second.

## Configure a DAI ACL

### ➤ To configure a DAI 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="text"/>

8. Use **Name** to create an ARP ACL for DAI.
9. Click the **Add** button.  
The DAI ACL is added to the switch configuration.
10. To remove the currently selected DAI ACL from the switch configuration, click the **Delete** button.

## Configure a DAI ACL Rule

➤ **To configure a DAI 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.  
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 Rule Configuration**.

Rules	
ACL Name	arpACL ▾
DAI Rule Table	
<input type="checkbox"/>	Source IP Address
	Source MAC Address

8. In the **ACL Name** field, select the DAI ARP ACL.
9. Click the **Add** button.  
The rule is added to the selected ACL.
10. To remove the currently selected rule from the selected ACL, click the **Delete** button.

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

**Table 227. DAI ACL Rule Configuration**

Field	Description
Source IP Address	This indicates sender IP address match value for the DAI ARP ACL.
Source MAC Address	This indicates sender MAC address match value for the DAI ARP ACL.

## View DAI Statistics

### ➤ To view the 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.
4. Enter 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 Statistics**.

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

To clear the DAI statistics, click the **Clear** button.

To refresh the screen with the latest information on the switch, click the **Update** button.

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

**Table 228. DAI 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.
Bad Source MAC	Number of ARP packets that were dropped by DAI because the sender MAC address in ARP packets 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 packets 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 ARP packets or the target IP address in ARP reply packets 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.

## Captive Portal

The captive portal feature allows you to prevent clients from accessing the network until user verification is established. You can configure captive portal verification to allow access for both guest and authenticated users. Authenticated users must be validated against a database of authorized captive portal users before access is granted. The database can be stored locally on the device or on a RADIUS server.

## Configure Captive Portal Global Settings

You can control the administrative state of the captive portal feature, and configure global settings that affect all captive portals configured on the switch.

➤ **To configure captive portal 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 > Control > Captive Portal > CP Global Configuration**.

Captive Portal Global Configuration	
Admin Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Operational Status	Disabled
Disabled Reason	Administrator Disabled
CP IP Address	0.0.0.0
Additional HTTP Port	<input type="text" value="0"/> (0 to 65535)
Additional HTTP Secure Port	<input type="text" value="0"/> (0 to 65535)
Authentication Timeout	<input type="text" value="300"/> (60 to 600)
Supported Captive Portals	10
Configured Captive Portals	1
Active Captive Portals	0
System Supported Users	1024
Local Supported Users	128
Configured Local Users	0
Authenticated Users	0

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

This sets the administrative mode of the captive portal feature. By default CP is disabled.

9. In the **Additional HTTP Port** field, enter a port number between 0–65535 (excluding port 80).

HTTP traffic uses standard port 80, but you can use the **Additional HTTP Port** field to configure an additional port for HTTP traffic. Enter 0 to unconfigure the additional HTTP port. The default is 0.

- 10.** In the **Additional HTTP Secure Port** field, enter a port number between 0–65535 (excluding port 443).

HTTP Secure traffic uses standard port 443, but you can configure an additional port for HTTP Secure traffic using the **Additional HTTP Secure Port** field. Enter 0 to unconfigure the additional HTTP Secure port. The default is 0.

- 11.** Use the **Authentication Timeout** field to enter the number of seconds that captive portal keeps the authentication session open with a client that is attempting to access the network through a portal.

To access the network through a portal, the client must first enter authentication information on an authentication web page. When the time-out expires, the switch disconnects any active TCP or SSL connection with the client. The valid range is 60 to 600 seconds. The default authentication time-out is 300 seconds.

- 12.** Click the **Apply** button.

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

The following table describes the nonconfigurable data that is displayed.

**Table 229. Captive Portal Global Configuration**

Field	Description
Operational Status	The operational status of the captive portal feature, which is either Enabled or Disabled. The default is Disabled.
Disabled Reason	If CP is disabled, this field displays the reason, which can be one of the following: <ul style="list-style-type: none"> <li>Administratively disabled</li> <li>IP address not configured</li> <li>No IP routing interface</li> <li>Routing disabled</li> </ul>
CP IP Address	The IP address that the captive portal uses.
Supported Captive Portals	The number of supported captive portals in the system.
Configured Captive Portals	Shows the number of captive portals configured on the switch.
Active Captive Portals	Shows the number of captive portal instances that are operationally enabled.
System Supported Users	Shows the number of authenticated users that the system can support.
Local Supported Users	Shows the number of entries that the local user database supports.



Table 229. Captive Portal Global Configuration

Field	Description
Configured Local Users	The number of local users configured.
Authenticated Users	Shows the number of users currently authenticated to all captive portal instances on this switch.

## Add a Captive Portal Instance

By default, the switch has one captive portal. You can change the settings for that captive portal, and you can also create and configure up to nine additional portals.

### ➤ To add a captive portal instance:

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

CP ID	CP Name	Admin Mode	Protocol	Verification	Block	Group	Idle Timeout	User Logout	Radius Auth Server
1	Default	Enable	http	Guest	Not Blocked	0	0	Disable	

Radius Auth Server	Redirect Mode	Redirect URL	Background Color	Foreground Color	Separator Color	Max Bandwidth Down	Max Bandwidth Up	Max Input	Max Output	Max Total
Disable	/cp_welcome.html	#BFBFBF	#999999	#B70024	0	0	0	0	0	

8. In the **CP Name** field, enter the name of the configuration.  
The name can contain 1 to 31 alphanumeric characters.
9. In the **Admin Mode** list, select **Enable** or **Disable**.

This sets the administrative mode of the captive portal feature. By default captive portal is disabled.

10. In the **Protocol** field, select either **HTTP** or **HTTPS** as the captive portal instances used for communication with clients during the verification process:
  - **HTTP** does not use encryption during verification.
  - **HTTPS** uses the Secure Sockets Layer (SSL), which requires a certificate to provide encryption. The certificate is presented to the user at connection time.
11. Select the type of user **Verification** that the captive portal instance performs with clients that attempt to connect:
  - **Guest**. The user does not need to be authenticated by a database.
  - **Local**. The device uses a local database to authenticate users.
  - **RADIUS**. The device uses a database on a remote RADIUS server to authenticate users.
12. Select the **Block** status.

If the CP is blocked, users cannot gain access to the network through the CP. Use this function to temporarily protect the network during unexpected events, such as denial of service attacks.
13. If the verification mode is Local or RADIUS, use the **Group** field to assign an existing user group to the captive portal.

All users who belong to the group are permitted to access the network through this portal. The User Group list is the same for all CP configurations on the switch.
14. In the **Idle Timeout** field, enter the number of seconds to wait before terminating a session.

A user is logged out once the session idle time-out is reached. If you set the value to 0, then the time-out is not enforced. The valid range is 0 to 900 seconds. The default value is 0.
15. In the **User Logout** list, select the **Enable** or **Disable** option to allow an authenticated client to deauthenticate from the network.

If this option is clear or the user does not specifically request logout, the client connection status remains authenticated until the captive portal deauthenticates the user, for example by reaching the idle time-out or session time-out values.
16. If the verification mode is RADIUS, use the **Radius Auth Server** field to enter the IP address of the RADIUS server to use for client authentication.

The device acts as the RADIUS client and performs all RADIUS transactions on behalf of the clients.
17. Select the **Redirect Mode** to specify whether the CP redirects the newly authenticated client to the configured URL (enabled).

If this mode is disabled, the default locale specific welcome is used.
18. Specify the **Redirect URL** to which the newly authenticated client is redirected.

The maximum length for the URL is 512 alphanumeric characters.

19. In the **Background Color** field, specify the value of the background color.  
For example, #BFBFBF.
20. In the **Foreground Color** field, specify the value of the foreground color.  
For example, #999999.
21. In the **Separator Color** field, specify the value of the separator color.  
For example, #46008F.
22. In the **Max Bandwidth Down** field, specify the maximum rate at which a client can receive data from the network.  
  
The rate is in bytes per seconds. 0 indicates the limit is not enforced. The range is 0 to 536870911.
23. In the **Max Bandwidth Up** field, specify the maximum rate in bytes per second at which a client can send data into the network.  
  
A value of 0 indicates the limit is not enforced. The range is 0 to 536870911.
24. In the **Max Input** field, specify the maximum number of octets that the user is allowed to transmit.  
  
After this limit is reached, the user is disconnected. 0 indicates that the limit is not enforced. The range is 0 to 4294967295.
25. In the **Max Output** field, specify the maximum number of octets that the user is allowed to receive.  
  
After this limit is reached, the user is disconnected. 0 indicates the limit is not enforced. The range is 0 to 4294967295.
26. In the **Max Total** field, specify the maximum number of octets that the user is allowed to transfer, meaning the sum of octets transmitted and received.  
  
After this limit is reached, the user is disconnected. 0 indicates the limit is not enforced. The range is 0 to 4294967295.
27. Click the **Add** button.  
  
The captive portal instance is added.
28. To change the settings for an existing captive portal instance:
  - a. Select the **CP ID** from the list.  
  
The ID is a unique value that identifies the captive portal instance. This value is automatically assigned to the instance when it is created and cannot be changed.
  - b. Update the configuration using the previous steps.
  - c. Click the **Apply** button.  
  
The updated configuration is sent to the switch. Configuration changes take effect immediately.
29. To delete an existing captive portal instance:
  - a. Select the **CP ID** from the list.

- b. Click the **Delete** button.

The currently selected CP instance is removed.

## Configure CP Binding

You can associate a configured captive portal with a specific network (SSID). The CP feature runs only on the interfaces you specify. Multiple interfaces can be associated with a CP, but an interface can be associated to only one CP at a time.

### ➤ To configure CP 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.

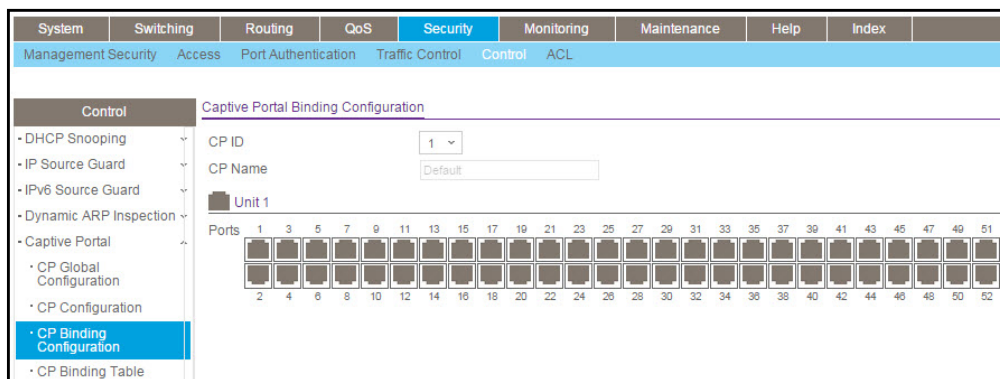
5. Enter the user name and password.

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 > Captive Portal > CP Binding Configuration**.



8. Select the **CP ID** from the list.

The ID is a unique value that identifies the captive portal instance. This value is automatically assigned to the instance when it is created and cannot be changed.

9. To create or update a captive portal instance, configure the following fields:
  - a. In the **CP Name** field, specify the name of the configuration.

The name can contain from 1 to 31 alphanumeric characters.

- b. Select the interface or interfaces from the **Port List**.
- c. Click the **Apply** button.

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

## View the Captive Portal Binding Table

### ➤ To view the captive portal binding 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 **Security > Control > Captive Portal > CP Binding Table**.

Captive Portal Binding Table					
<input type="checkbox"/>	Interface	CP ID	Operational Status	Block Status	Authenticated users

Click the **Delete** button to remove the currently selected interface.

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable data that is displayed.

**Table 230. Captive Portal Binding Table**

Field	Description
Interface	The interface.
CP ID	The ID of the captive portal instance.
Operational Status	Indicates whether the portal is active on the specified interface.
Block Status	Indicates whether the captive portal is temporarily blocked for authentication.
Authenticated Users	Shows the number of authenticated users using the captive portal instance on this interface.

## Configure a Captive Portal Group

### ➤ To configure a captive portal 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 > Control > Captive Portal > CP Group Configuration**.

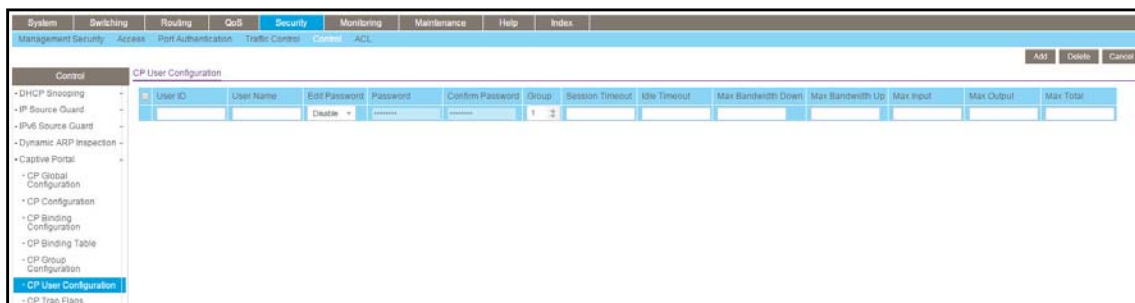
<input type="checkbox"/>	Group ID	Group Name
<input type="checkbox"/>	1	Default

8. Select the **Group ID** from the list.
9. In the **Group Name** field, specify the name of the user group.  
The name can contain from 1 to 31 alphanumeric characters.
10. Click the **Add** button.  
The group is added.
11. To remove the currently selected group, click the **Delete** button.
12. Click the **Apply** button.  
The updated configuration is sent to the switch. Configuration changes take effect immediately.

## Configure Captive Portal User Settings

### ➤ To configure captive portal user 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 > Captive Portal > CP User Configuration**.



8. Enter the local **User ID** to identify the name of the user.
9. In the **User Name** field, enter the name of the user.

The name can contain 1 to 31 alphanumeric characters. Once created, user names cannot be changed or modified.

10. In the **Edit Password** list, select **Enable** only when you are changing the password.

The default value is Disable.

11. In the **Password** field, enter a password for the user.

The password length can be from 8 to 64 characters.

12. In the **Confirm Password** field, enter the password for the user again.

13. Use the **Group** field to assign the user to a least one user group.

To assign a user to more than one group, press the **Ctrl** key and click each group. New users are assigned to the 1-Default user group by default.

14. In the **Session Timeout** field, enter the number of seconds a user is permitted to remain connected to the network.

Once the Session Timeout value is reached, the user is logged out automatically.

15. In the **Idle Timeout** field, enter the number of seconds to wait before terminating a session.

A user is logged out once the session idle time-out is reached. If the attribute is 0 or not present, then use the value configured for the captive portal.

16. In the **Max Bandwidth Down** field, enter the maximum rate, in bits per second, at which a client can receive data from the network.

A value of 0 indicates use global configuration. The range is 0 to 536870911 bps.

17. In the **Max Bandwidth Up** field, enter the maximum rate, in bits per second, at which a client can send data into the network.

A value of 0 indicates use the global limit. The range is 0 to 536870911 bps.

18. In the **Max Input** field, enter the number of octets the user is allowed to receive.

After this limit is reached, the user is disconnected. 0 means use the global limit. The range is 0 to 4294967295.

19. In the **Max Output** field, enter the number of octets the user is allowed to transmit.

After this limit is reached, the user is disconnected. 0 means use the global limit. The range is 0 to 4294967295.

20. In the **Max Total** field, enter the number of bytes the user is allowed to transmit and receive.

The maximum number of octets is the sum of octets transmitted and received. After this limit is reached, the user is disconnected. 0 means use the global limit. The range is 0 to 4294967295.

21. Click the **Add** button.

The user is added to the Local User database.

22. To delete the selected user from the Local User database, click the **Delete** button.

23. Click the **Apply** button.



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

## Configure the Captive Portal Trap Flag Settings

You can specify whether or not SNMP traps are sent from the captive portal and to specify captive portal events that generate a trap. All CP SNMP traps are disabled by default.

### ➤ To configure the captive portal trap flag 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.

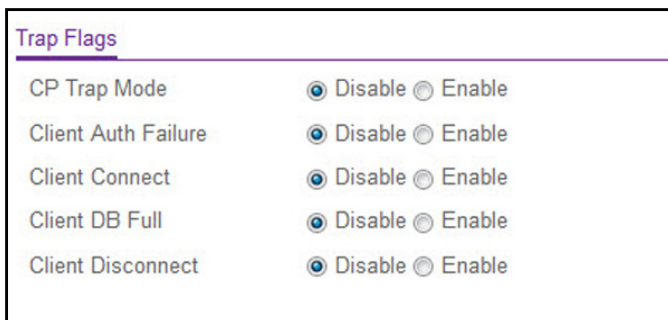
5. Enter the user name and password.

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 > Captive Portal > CP Trap Flags**.



Trap Flags	
CP Trap Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Client Auth Failure	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Client Connect	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Client DB Full	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Client Disconnect	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

8. Select the CP Trap Mode **Disable** or **Enable** radio button.

This sets the option to enable or disable the captive portal trap mode.

9. Select the Client Authentication Failure **Disable** or **Enable** radio button.

If you enable this, the SNMP agent sends a trap when a client attempts to authenticate with a captive portal but is unsuccessful.

10. Select the Client Connect **Disable** or **Enable** radio button..

If you enable this, the SNMP agent sends a trap when a client authenticates with, and connects to, a captive portal.

11. Select the Client Database Full **Disable** or **Enable** radio button..

If you enable this, the SNMP agent sends a trap each time an entry cannot be added to the client database because it is full.

12. Select the Client Disconnect **Disable** or **Enable** radio button.

If you enable this, the SNMP agent sends a trap when a client disconnects from a captive portal.

13. Click the **Apply** button.

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

## View the Captive Portal Client

You can view information about the traffic a client sent or received.

### ➤ To view the captive portal client:

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

Captive Portal Client											
Search By MAC Address										<input type="text"/>	Go
MAC Address	IP Address Drops	Protocol	Verification	Session Time	Interface	CP ID	User Name	Bytes Received	Bytes Transmitted	Packets Received	Packets Transmitted

To clear the information in the client table, click the **Clear** button.

To refresh the screen with the latest information on the switch, click the **Update** button.

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

**Table 231. Captive Portal Client**

Field	Description
MAC Address	Shows the client MAC address.
IP Address Drops	Identifies the IP address of the client (if applicable).
Protocol	Shows the current connection protocol, which is either HTTP or HTTPS.
Verification	Shows the current account type, which is Guest, Local, or RADIUS.
Session Time	Shows the amount of time that passed since the client was authorized.
Interface	Identifies the interface the client is using.
CP ID	The ID of the captive portal instance.
User Name	The user name (or guest ID) of the connected client.
Bytes Received	Total bytes the client received.
Bytes Transmitted	Total bytes the client transmitted.
Packets Received	Total packets the client received.
Packets Transmitted	Total packets the client transmitted.

## Configure 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 above all provide security for the network. ProSafe Managed switch's 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 to Create a Simple ACL

The ACL Wizard helps you create a simple ACL and apply it to the selected ports easily and quickly. You must select an ACL type to use when you create an ACL. Then add an ACL rule to this ACL and apply this ACL on the selected ports. The ACL Wizard allows you to create the ACL, but does not allow you to modify it. To modify the ACL, go to the ACL Configuration screen. See *Configure an IP ACL* on page 656.

➤ **To use the ACL Wizard to create a simple 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 > ACL Wizard**.

**ACL Type Selection**

ACL Type: ACL Based on Destination MAC

**ACL Based on Destination MAC**

Rule ID	Action	Match Every	Destination MAC	Destination MAC Mask	VLAN
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

**Binding Configuration**

Options: Direction: Inbound

**Unit 1**

**Ports**

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48

**LAG**

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51	53	55	57	59	61	63
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64

**Note:** The steps in this procedure describe creating an ACL based on the destination MAC address. If you select a different ACL type, for example, ACL based on a source IPv4, then what is shown on this screen varies, depending on the current step in the rule configuration process.

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 Layer 4 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.

---

**Note:** Two rules are created (one for TCP and one for UDP) in the case of L4 port options.

---

## Configure an ACL Based on Destination MAC Address

---

**Note:** Binding ACLs to interface fails when the system has no resources to bind a new ACL.

---

➤ **To configure a rule based on destination 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 **Security > ACL > ACL Wizard**.

The screenshot shows the 'ACL Type Selection' and 'Binding Configuration' sections of a web management interface.

**ACL Type Selection:**

- ACL Type: **ACL Based on Destination MAC** (selected from a dropdown menu).

**ACL Based on Destination MAC:**

Rule ID	Action	Match Every	Destination MAC	Destination MAC Mask	VLAN
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

**Binding Configuration:**

Options: Direction: **Inbound** (dropdown)

**Unit 1**

Ports: 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47  
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48

**LAG**

LAG: 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49 51 53 55 57 59 61 63  
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50 52 54 56 58 60 62 64

The steps in this procedure describe creating an ACL based on the

8. Use **Rule ID** to enter a whole number in the range of 1 to 1023 that is used to identify the rule.
9. Use **Action** to specify what action is taken if a packet matches the rule's criteria. The choices are Permit or Deny.
10. In the **Match Every** list, select either **True** or **False**:

- True signifies that all packets must match the selected ACL and rule and are 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 re-configure Match Every to False for the other match criteria to be visible.

11. Use **Destination MAC** to specify the destination MAC address to compare against an Ethernet frame.

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.

12. 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.

13. Specify the **VLAN ID** to compare against an Ethernet frame.

Valid range of values is 1 to 4093. Either a VLAN range or VLAN can be configured.

14. Click the **Add** button.

The rule is added to the ACL based on the Destination MAC.

15. To remove the currently selected rule from the ACL based on destination MAC address, click the **Delete** button.

16. Click the **Apply** button.

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

## Use the ACL Wizard to Complete the Destination MAC ACL

For information about the ACL Wizard, see [Use the ACL Wizard to Create a Simple ACL](#) on page 645.

To complete the destination MAC ACL using ACL wizard, you must do the following:

1. Select the destination MAC ACL as **ACL type**.
2. Enter the DMAC VLAN as the **ACL Rule**.
3. To select the direction and ports to bind the ACL, in the **Directions** field, select the packet filtering direction for an ACL.

The options are Inbound or Outbound.

The Port Selection Table specifies the list of all available valid interfaces for ACL mapping.

All non-routing physical interfaces and interfaces participating in LAG are listed.

## Configure a Basic MAC ACL

A MAC ACL consists of a set of rules which 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. Rules for the MAC ACL are specified/created using the MAC ACL Rule Configuration screen.

There are multiple steps involved in defining a MAC ACL and applying it to the switch:

1. Create the ACL Name.
2. Create rules for the ACL.
3. Assign the ACL by its name to a port.
4. Optionally, use the [View or Delete MAC ACL Bindings in the MAC Binding Table](#) screen to view the configurations.

➤ **To configure 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**.

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 number is equal to the number of configured IPv4 and IPv6 ACLs plus the number of configured MAC ACLs.

8. In the **Name** field, specify a name for the MAC ACL.

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.** The number of rules currently configured for the MAC ACL.
- **Direction.** The direction of packet traffic affected by the MAC ACL, which can be Inbound or blank.



9. Click the **Add** button.

The MAC ACL is added to the switch configuration.

10. To change the name of the MAC ACL, in the **Name** field, update the name, then click the **Apply** button.
11. To delete the selected MAC ACL, click the **Delete** button.

## Configure MAC ACL 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 ACL 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 > Basic > MAC Rules**.

ID	Action	Assign Queue Id	Mirror Interface	Redirect Interface	Match Every	CoS	Destination MAC	Destination MAC Mask	EtherType Key	EtherType User Value
1	Deny				False		01:80:C2:01:00:00	00:00:00:FF:FF:FF		

8. Use **ID** to enter a whole number in the range of 1 to 1023 to identify the rule.
9. Use **Action** to specify what action is taken if a packet matches the rule's criteria.  
The choices are Permit or Deny.
10. Use **Assign Queue ID** to specify the hardware egress queue identifier used to handle all packets matching this ACL rule.

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.

Valid values are as follows:

- **True.** Signifies that every packet is considered to match the selected ACL rule.
- **False.** Signifies that 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.

Valid range of values is 0 to 7.

15. Use **Destination MAC** to specify the destination MAC address to compare against an Ethernet frame. 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.

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.

Valid values are as follows:

- 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 you selected *User Value* as EtherType key, to compare against an Ethernet frame.

Valid range of values is 0x0600 to 0xFFFF.

19. Use **Source MAC** to specify the source MAC address to compare against an Ethernet frame.

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.

Valid format is xx:xx:xx:xx:xx:xx.

21. Use **VLAN** to specify the VLAN ID to compare against an Ethernet frame.

Valid range of values is 1 to 4095. Either VLAN range or VLAN can be configured.

22. Use **Logging** to enable or disable 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 only supported for a Deny action.

23. Use **Rate Limit Conform Data Rate** to specify the value of the conforming data rate of MAC ACL rule.

Valid values are 1 to 4294967295 in Kbps.

24. Use **Rate Limit Burst Size** to specify the burst size of MAC ACL rule.

Valid values are 1 to 128 in Kbytes.

25. Use **Time Range** to enter the name of the time range associated with the MAC ACL rule.

The **Rule Status** displays if the ACL rule is active or inactive. If this field is blank, no timer schedules are assigned to the rule.

26. To delete a rule, select the check box associated with the rule and click the **Delete** button.

27. To change a rule, select the check box associated with the rule and change the desired fields.

28. Click the **Apply** button.

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

## Configure MAC Binding

When an ACL is bound to an interface, all the rules that are defined are applied to the selected interface. Use the MAC Binding Configuration screen to assign MAC ACL lists to ACL priorities and interfaces.

➤ **To configure 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
1/0/1	Inbound	MAC ACL	ACL_Wizard_MAC_0	1

8. Select a MAC ACL from the **ACL ID** list.  
You can select one and bind it to the interfaces.  
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. 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 to save any changes to the running configuration.

The following table describes the information displayed in the **Interface Binding Status**.

**Table 232. Interface Binding Status**

Field	Description
Interface	The interface of the ACL assigned.
Direction	Displays selected packet filtering direction for ACL.
ACL Type	The type of ACL assigned to selected interface and direction.
ACL ID	The ACL number (in case of IP ACL) or ACL name (in case of MAC ACL) identifying the ACL assigned to selected interface and direction.
Sequence Number	The sequence number signifying the order of the specified ACL relative to other ACLs assigned to selected interface and direction.

## View or Delete MAC ACL Bindings in the MAC Binding Table

You can view or delete the MAC ACL bindings in the MAC Binding Table.

### ➤ To view or delete MAC 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.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > ACL > Basic > MAC Binding Table**.

MAC Binding Table					
<input type="checkbox"/>	Interface	Direction	ACL Type	ACL ID	Sequence Number
<input type="checkbox"/>	1/0/1	In Bound	MAC ACL	ACL_Wizard_MAC_0	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 233. MAC Binding Table**

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 selected interface and direction.
ACL ID	The ACL name identifying the ACL assigned to selected interface and direction.
Sequence Number	The sequence number signifying the order of the specified ACL relative to other ACLs assigned to selected interface and direction.

## Configure an IP ACL

An IP or 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 must specify the interfaces to which an IP ACL applies, as well as whether it applies to inbound or outbound traffic. Rules for the IP ACL are specified or created using the IPv6 ACL Rule Configuration screen.

### ➤ 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.
6. Click the **Login** button.  
The web management interface menu displays.
7. Select **Security > ACL > Advanced > IP ACL**.

System	Switching	Routing	QoS	Security	Monitoring
Management Security	Access	Port Authentication	Traffic Control	Control	ACL

**ACL**

- ACL Wizard
- Basic
- Advanced
- **IP ACL**
  - IP Rules
  - IP Extended Rules
  - IPv6 ACL
  - IPv6 Rules

**IP ACL Configuration**

Current Number of ACL: 
Maximum ACL:

**IP ACL Table**

IP ACL ID	Rules	Type
<input type="text"/>		

The IP ACL screen shows 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** field displays the current number of the all ACLs configured on the switch.

The **Maximum ACL** displays the maximum number of IP ACL can be configured on the switch, depending on the hardware.

8. In the **IP ACL** field, specify the ACL ID or IP ACL name, which depends on the IP ACL type. The IP ACL 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 an IPv4 ACL name string that includes up to 31 alphanumeric characters in length. The name must start with an alphabetic character.

Each configured ACL displays the following information:

- **Rules.** The number of rules currently configured for the IP ACL.
  - **Type.** Identifies the ACL as a basic IP ACL (with ID from 1 to 99), extended IP ACL (with ID from 100 to 199), or for named IP ACL.
9. To delete an IP ACL, select the check box next to the IP ACL ID field, then click the **Delete** button.
  10. Click the **Add** button.  
The IP ACL is added to the switch configuration.
  11. Click the **Apply** button.  
The updated configuration is sent to the switch. Configuration changes take effect immediately.

## Configure Rules for an IP ACL

You can display the rules for the IP access control lists (ACL) that you created. What is shown on this screen varies depending on the current step in the rule configuration process.

---

**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.  
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 Rules**.



IP Rules

ACL ID

Basic ACL Rule Table

	Rule ID	Action	Logging	Assign Queue Id	Match Every	Mirror Interface	Redirect Interface	Source IP Address	Source IP Mask	Rate Limit Conform Data Rate	Rate Limit Burst Size	Time Range	Rule Status
<input checked="" type="checkbox"/>	3	Permit		1	False	1/0/2		10.131.6.8	255.255.255.255	1	1		

8. To add an IP ACL rule, select the **ACL ID**, complete the fields described in the following list, and click the **Add** button.

(Displays only ACL IDs from 1 to 99.)

- **Rule ID.** Enter a whole number in the range of 1 to 1023 that is used to identify the rule. An IP ACL can have up to 1023 rules.
- **Action.** Specify what action is 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.** The hardware egress queue identifier used to handle all packets matching this IP ACL rule. Valid range of queue IDs is 0 to 6. This field is visible when Permit is chosen as the action.
- **Match Every.** Select **True** or **False**. True signifies that all packets must match the selected IP ACL and rule and are 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.
- **Mirror Interface.** 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.** 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.** Value of Rate Limit Conform Data Rate specifies the conforming data rate of IP ACL Rule. Valid values are 1 to 4294967295 in Kbps.
  - **Rate Limit Burst Size.** Value of Rate Limit Burst Size specifies burst size of the IP ACL rule. Valid values are 1 to 128 in Kbytes.
  - **Time Range.** Name of 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 rule check box, and then click the **Delete** button.
10. To update an IP ACL rule, select the rule check box, update the desired fields, and then click the **Apply** button.
- 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.
12. 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 Rules for an Extended IP ACL

You can view the rules for the IP access control lists that you created. What is shown on this screen varies depending on the current step in the rule configuration process.

---

**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 extended 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.

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	Established	Source IP Address	Source IP Mask	Source L4 Port Action	Source L4 Port	Source L4 Start Port	Source L4 End Port	Destination IP Address	Destination IP Mask
101	Deny	Disable				False	4 (IP)									10.27.64.129	255.255.255.255

8. **ACL ID/Name** - Select the IP ACL for which to create or update a rule.
9. **Configure Rule ID** by entering a whole number in the range of 1 to 1023 that is used to identify the rule.

An IP ACL can have up to 1023 rules.

10. In the **Action** list, specify the action to take if a packet matches the rule's criteria.

The choices are Permit or Deny.

11. Set **Logging** to **Enable**.

This enables 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.

12. In the **Assign Queue ID**, specify the hardware egress queue identifier used to handle all packets matching this IP ACL rule.

The valid range of queue IDs is 0 to 6.

13. Use the **Mirror Interface** field 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.

14. Use the **Redirect Interface** field 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 enabled for a *Permit* action.

15. In the **Match Every** list, select **True** or **False**.

True signifies that all packets must match the selected IP ACL and rule and are 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.

16. Use the **Protocol Type** field to 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, UDP, EIGRP, GRE, IPINIP, OSPF, and PIM.

17. In the **TCP Flag** field, 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, and FIN. Each TCP flag can be set separately. The possible values are as follows:

- **Ignore.** A packet matches this ACL rule whether the TCP flag in this packet is set or not.
- **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.

18. When **Established** is specified, a match occurs if either RST- or ACK-specified bits are set in the TCP header. These fields are enabled only when TCP protocol is selected.

19. In the **Src** field, enter a source 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:

- a. Select the **IP Address** option and enter an IP address with a relevant wildcard mask to apply this criteria. If this field is left empty, it means *any*.
- b. When you select the **Host** option, the wildcard mask is configured as 0.0.0.0. If this field is left empty, it means *any*.

The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that *none* of the bits are important. A wildcard of 255.255.255.255 indicates that *all* of the bits are important.

20. Use **Source L4 Port Action** to specify relevant matching conditions for L4 port numbers in the current extended ACL rule:

- **Equal.** IP ACL rule matches only if the Layer 4 source port number is equal to the specified port number or port key.
- **Less Than.** IP ACL rule matches if the Layer 4 source port number is less than the specified port number or port key.
- **Greater Than.** IP ACL rule matches if the Layer 4 source port number is greater than the specified port number or port key.
- **Not Equal.** IP ACL rule matches only if the Layer 4 source port number is not equal to the specified port number or port key.

21. **Src L4 Port** and **Src L4 Range** options are available only when protocol is set to TCP or UDP. When you select the **Port** option, choose *port key* from the list or enter the port number yourself.

- The source IP TCP port names are bgp, domain, echo, ftp, ftpdata, http, smtp, snmp, Telnet, www, pop2, pop3.

- The source IP UDP port names are domain, echo, ntp, rip, snmp, tftp, time, who.

Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.

Only when you select **Other** in the list of port keys, can you enter your own port number. If you leave the Other field empty, it means *any*.

- 22.** When you select the **Range** option, IP ACL rule matches only if the Layer 4 port number is within the specified port range.

The Start Port and End Port parameters identify the first and last ports that are part of the port range. They values can range from 0 to 65535.

The possibility of entering your own port number is available only when *Other* is selected in the list of port keys. The starting port, ending port, and all ports in between are a part of the Layer 4 port range. If these fields are left empty, it means *any*.

The wildcard mask determines which bits are used and which bits are ignored. A wildcard mask of 0.0.0.0 indicates that *none* of the bits are important. A wildcard of 255.255.255.255 indicates that *all* of the bits are important.

- 23.** In the **Dst** field, specify a destination IP address, using dotted-decimal notation, and with a relevant wildcard mask.

This is compared to a packet's destination IP address as a match criteria for the selected extended IP ACL rule.

- 24.** Select the **IP Address** option and enter an IP address with a relevant wildcard mask to apply this criteria.

If these fields are left empty, it means *any*.

- 25.** When you select the **Host** option, the wildcard mask is configured as 0.0.0.0.

If this field is left empty, it means *any*.

- 26.** In the **Destination IP Mask** field, specify the IP mask, in dotted-decimal notation, to be used with the destination IP address value.

- 27.** In the **Dst L4 Port** and **Dst L4 Range** fields, specify the Layer 4 destination port match condition for the selected extended IP ACL rule.

These options are available only when the protocol is set to TCP or UDP.

Only when you select **Other** in the list of port keys, can you enter your own port number. If you leave the Other field empty, it means *any*.

- The destination IP TCP possible port names are bgp, domain, echo, ftp, ftp-data, http, smtp, Telnet, www, pop2, pop3.
- The destination IP UDP possible port names are domain, echo, ntp, rip, snmp, tftp, time, who.

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.

- 28.** Use **Destination L4 Port Action** to specify relevant matching conditions for L4 port numbers in the current extended ACL rule:

- **Equal.** IP ACL rule matches only if the Layer 4 source port number is equal to the specified port number or port key.
- **Less Than.** IP ACL rule matches if the Layer 4 source port number is less than the specified port number or port key.
- **Greater Than.** IP ACL rule matches if the Layer 4 source port number is greater than the specified port number or port key.
- **Not Equal.** IP ACL rule matches only if the Layer 4 source port number is not equal to the specified port number or port key.

- 29.** When you select the **Range** option, IP ACL rule matches only if the Layer 4 port number is within the specified port range.

The Start Port and End Port parameters identify the first and last ports that are part of the port range. They values can range from 0 to 65535.

The possibility of entering your own port number is available only when *Other* is selected in the list of port keys. The destination L4 starting port, destination L4 ending port, and all ports in between are a part of the Layer 4 port range. If these fields are left empty, it means *any*.

- 30. IGMP Type** - When the IGMP type is specified, the IP ACL rule matches the specified IGMP message type.

Possible values are in the range 0 to 255. If this field is left empty, it means *any*.

- 31. ICMP Type and ICMP Code** - The ICMP Type and ICMP Code fields are enabled only if the protocol is ICMP. Use the ICMP Type and ICMP Code fields to specify a match condition for ICMP packets:

- When the ICMP Type option is selected, IP ACL rule matches the specified ICMP message type. Possible type numbers are in the range from 0 to 255.
- When the ICMP Code option is specified, IP ACL rule matches the specified ICMP message code. Possible values for Code could be in the range from 0 to 255.
- If these fields are left empty, it means *any*.
- When the *Message* option is selected, choose the type of the ICMP message to match with the selected IP ACL rule. Specifying Message implies that both ICMP type and ICMP code are specified. The ICMP message is decoded into the corresponding ICMP type and ICMP code within that ICMP type. IPv4 ICMP message types are: echo, echo-reply, host-redirect, mobile-redirect, net-redirect, net-unreachable, redirect, packet-too-big, port-unreachable, source-quench, router-solicitation, router-advertisement, time-exceeded, ttl-exceeded, and unreachable.

- 32. 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 a selection is made, the appropriate value can be specified.

- **IP DSCP.** Specify the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order 6 bits of the service type octet in the IP header. This is an optional configuration. Enter an integer from 0 to 63. To select the IP DSC, select one of the

DSCP keywords from the list. If a value is to be selected by specifying its numeric value, then select **Other** and a field displays where you can enter 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 8 bits of the service type octet in the IP header. The TOS Bits value is a hexadecimal number from 00 to 09 and to aa 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.

**33. Rate Limit Conform Data Rate** - Specify the conforming data rate of IP ACL rule.

Valid values are 1 to 4294967295 in Kbps.

**34. Rate Limit Burst Size** - Specify the burst size of the IP ACL rule. Valid values are 1 to 128 in Kbytes.

**35. Time Range** - Name of the time range associated with the IP extended ACL rule.

The **Rule Status** field displays if the ACL rule is active or inactive. Blank means that no timer schedules are assigned to the rule.

**36.** To modify an existing IP extended ACL rule, click the **Rule ID**.

The number is a hyperlink to the Extended ACL Rule Configuration 100-199 screen. Click the **Add** button on the IP Extended Rules screen.

**37.** For standard ACL Rule Configuration (1–99), click the **Add** button on the IP Rules screen.

**38.** To delete an IP ACL rule, select the rule's check box, and then click the **Delete** button.

## Configure IPv6 ACL

An IP or 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. On this screen the interfaces to which an IP ACL applies must be specified, as well as whether it applies to inbound or outbound traffic.

➤ **To configure IPv6 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**.

System	Switching	Routing	QoS	Security	Monitoring
Management Security	Access	Port Authentication	Traffic Control	Control	ACL

**ACL**

- ACL Wizard
- Basic
- Advanced
- IP ACL
- IP Rules
- IP Extended Rules
- **IPv6 ACL**
- IPv6 Rules
- IP Binding Configuration

**IPv6 Configuration**

Current Number of ACL:

Maximum ACL:

**IPv6 ACL Table**

	Rules	Type
<input type="checkbox"/> IPv6 ACL		IPv6 ACL
<input type="checkbox"/> <u>ACL</u>	0	IPv6 ACL

8. Specify the **IPv6 ACL**.

This is the IPv6 ACL name string, which includes up to 31 alphanumeric characters only. The name must start with an alphabetic character.

9. Click the **Add** button.

The IPv6 ACL is added to the switch configuration.

10. To remove the currently selected IPv6 ACL from the switch configuration, click the **Delete** button.

11. 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 234. IPv6 ACL**

Field	Description
Current Number of ACL	The current number of the 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.



Table 234. IPv6 ACL (continued)

Field	Description
Rules	The number of the rules associated with the IP ACL.
Type	The type is IPv6 ACL.

## Configure IPv6 Rules

Use these screens to display the rules for the IPv6 access control lists, which are created using the IPv6 Access Control List Configuration screen. By default, no specific value is in effect for any of the IPv6 ACL rules.

### ➤ Configure ACL 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 1023 that is used to identify the rule.  
An IP ACL can have up to 1023 rules.
9. Use **Action** to specify what action is taken 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.

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. In the **Match Every** field, select **True** or **False**.

True signifies that all packets must match the selected IPv6 ACL and rule and are 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.

15. There are two ways to configure IPv6 **Protocol Type**:

- Specify an integer ranging from 1 to 255 after selecting the protocol keyword other. This number represents the IP protocol.
- Select the name of the protocol from the existing list of Internet Protocols (IPv6), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMPv6).

16. Use **TCP Flag** to specify that a packet's TCP flag is a match condition for the selected IPv6 ACL rule.

The TCP flag values are URG, ACK, PSH, RST, SYN, FIN. Each TCP flag can be set separately. the possible values are as follows:

- **Ignore.** A packet matches this ACL rule whether the TCP flag in this packet is set or not.
- **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.
- When Established is specified, a match occurs if either RST or ACK specified bits are set in the TCP header.
- The following fields are enabled only when TCP protocol is selected:
  - **Protocol.** There are two ways to configure IPv6 protocol.

Specify an integer ranging from 1 to 255 after selecting protocol keyword *other*. This number represents the IP protocol.

Select 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).

- **Src.** Specify a source IPv6 address to match with the selected IPv6 ACL rule.

When the **IPv6 Address** radio button is selected, enter an IPv6 address with prefix length to match the IPv6 ACL rule. If these fields are left empty, it means *any*.

When the **Host** radio button is selected, enter a host source IPv6 address to match the specified IPv6 address. If this field is left empty, it means *any*.

This source IPv6 address argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

**17. Src L4 Port** options are enabled only for TCP or UDP protocols:

- Source L4 TCP port names are bgp, domain, echo, ftp, ftpdata, http, smtp, Telnet, www, pop2, pop3.
- Source L4 UDP port names are domain, echo, ntp, rip, snmp, tftp, time, who.

When the Port option is selected, select the port key from the list or enter a port number. You can enter your own port number only when **Other** is selected in the list of port keys. If this field is left empty, it means *any*.

**18. Src L4 Port Action** specifies the relevant matching condition for Layer 4 port numbers in the current extended rule:

- **Equal.** IPv6 ACL rule matches only if the Layer 4 source port number is equal to the specified port number or port key.
- **Less Than.** IPv6 ACL rule matches if the Layer 4 source port number is less than the specified port number or port key.
- **Greater Than.** IPv6 ACL rule matches if the Layer 4 source port number is greater than the specified port number or port key.
- **Not Equal.** IPv6 ACL rule matches only if the Layer 4 source port number is not equal to the specified port number or port key.

**19. Dst L4 Port** options are enabled only for TCP or UDP protocols:

- Destination L4 TCP port names are bgp, domain, echo, ftp, ftpdata, http, smtp, Telnet, www, pop2, pop3.
- Destination L4 UDP port names are domain, echo, ntp, rip, snmp, tftp, time, who.

When the Port option is selected, select the port key from the list or enter a port number. You can enter your own port number only when **Other** is selected in the list of port keys. If this field is left empty, it means *any*.

**20. Destination L4 Port Action** specifies the relevant matching condition for Layer 4 port numbers in the current extended ACL rule:

- **Equal.** IPv6 ACL rule matches only if the Layer 4 source port number is equal to the specified port number or port key.
- **Less Than.** IPv6 ACL rule matches if the Layer 4 source port number is less than the specified port number or port key.
- **Greater Than.** IPv6 ACL rule matches if the Layer 4 source port number is greater than the specified port number or port key.
- **Not Equal.** IPv6 ACL rule matches only if the Layer 4 source port number is not equal to the specified port number or port key.

**21. Fragments.** The rule to match the packets that are noninitial fragments (fragment bit asserted).

This option is not valid for rules that match L4 information such as TCP port number, since that information is carried in the initial packet.

**22. Routing.** The rule to match the packets that include a routing extension header.

**23. ICMPv6 Type.** Specifies a match condition for ICMPv6 packets.

When the *Type* radio button is selected, the IPv6 ACL rule matches the specified ICMPv6 message type. Possible type numbers are in range from 0 to 255. When ICMPv6 code is specified, IP ACL rule matches with the specified ICMPv6 message code. Possible values are in the range from 0 to 255. If this field is left empty, it means *any*.

**24.** When the *Message* radio button is selected, select the type of the ICMPv6 messages to match the selected IPv6 ACL rule.

Specifying Message implies that both ICMPv6 type and ICMPv6 code are specified. The ICMPv6 message is decoded into the corresponding ICMPv6 type and ICMPv6 code within that ICMPv6 type. IPv6 ICMPv6 message types are destination-unreachable, echo-reply, echo-request, header, hop-limit, mld-query, mld-reduction, mld-report, nd-na, nd-ns, next-header, no-admin, no-route, packet-too-big, port-unreachable, router-solicitation, router-advertisement, router-renumbering, time-exceeded, and unreachable.

---

**Note:** The following fields are enabled only if the protocol is ICMPv6.

---

**25. 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 specified within the range 0 to 1048575.

**26. 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. To select the IPv6 DSCP, select one of the DSCP keywords. If a value is to be selected by specifying its numeric value, then select **Other** and a field appears where you can enter the numeric value of the DSCP.

**27. Rate Limit Conform Data Rate.** Specify the conforming data rate of the IPv6 ACL rule.

Valid values are 1 to 4294967295 in Kbps.

- 28. Rate Limit Burst Size.** Specify the burst size of IPv6 ACL rule.

Valid values are 1 to 128 in Kbytes.

- 29. Time Range.** Name of time range associated with the IPv6 ACL rule.

- 30. Rule Status.** Displays if the ACL rule is active or inactive.

Blank means that no timer schedules are assigned to the rule.

- 31.** To modify an IP extended ACL rule, click the **Rule ID**.

The number is a hyperlink to the Extended IPv6 ACL Rule Configuration (100-199) screen. Click the **Add** button on the IP Extended Rules screen.

- 32.** For standard ACL rule configuration (1–99), click the **Add** button on the IPv6 Rules screen.

- 33.** To delete a rule, select its check box and click the **Delete** button.

## Configure IP ACL Interface Bindings

When an ACL is bound to an interface, all the rules that are defined are applied to the selected interface. You can assign ACL lists to ACL priorities and interfaces.

### ➤ To configure IP 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**.

8. In the **ACL ID** menu, select an IP ACL.

---

**Note:** Binding ACLs to interface fails when the system has no resources to bind a new ACL. IPv4 ACLs and IPv6 ACLs cannot be bound at the same time to an interface.

---

9. Select the packet filtering **Direction** for ACL.

Valid directions are Inbound or Outbound. The packet filtering direction for ACL is Inbound, which means the IP ACL rules are applied to traffic entering the port.

10. 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 (meaning that the value is 0), 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.

11. The **Port Selection Table** lists all available valid interfaces for ACL mapping.

All non-routing physical interfaces, and interfaces participating in LAGs, are listed. Click the appropriate unit name to expose the available ports or LAGs:

- 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.

12. Click the **Apply** button to save any changes to the running configuration.

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

**Table 235. IP Binding Configuration**

Field	Description
Interface	Displays the selected interface.
Direction	Displays 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 IP ACL) or ACL name (in the case of named IP ACL and IPv6 ACL) identifying the ACL assigned to selected interface and direction.
Sequence Number	The sequence number signifying the order of specified ACL relative to other ACLs assigned to selected interface and direction.

## View or Delete IP ACL Bindings in the IP ACL Binding Table

### ➤ To view or delete 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.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > ACL > Advanced > Binding Table**.

IP ACL Binding Table					
<input type="checkbox"/>	Interface	Direction	ACL Type	ACL ID/Name	Sequence Number

8. 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 236. IP ACL Binding Table**

Field	Description
Interface	Displays the selected interface.
Direction	Displays 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 the IP ACL) or ACL name (in the case of Named IP ACL and IPv6 ACL) identifying the ACL assigned to selected interface and direction.
Sequence Number	The sequence number signifying the order of the specified ACL relative to other ACLs assigned to selected interface and direction.

## View or Delete VLAN ACL Bindings in the VLAN Binding Table

### ➤ To view or delete VLAN 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.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Security > ACL > Advanced > VLAN Binding Table**.

VLAN Binding Configuration					
<input type="checkbox"/>	VLAN ID	Direction	Sequence Number	ACL Type	ACL ID
	<input type="text"/>	<input type="text" value="↓"/>	<input type="text" value="0"/>	<input type="text" value="↓"/>	<input type="text" value="↓"/>

8. Use **ACL Type** to specify the type of ACL.



Valid ACL Types include IP ACL, MAC ACL, and IPv6 ACL.

9. Use **ACL ID** to display all the ACLs configured, depending on the ACL type selected.
10. Click the **Add** button to add a VLAN ID to the selected ACL ID.
11. To delete a VLAN ACL-to-interface binding, select the check box for the interface and click the **Delete** button.

The following table describes the information displayed in the ACL VLAN Binding Table.

**Table 237. ACL VLAN Binding Table**

Field	Description
Direction	The packet filtering direction for 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 (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.

## 10. Monitor the System

---

# 10

This chapter covers the following topics:

- *View Port Statistics*
- *Manage Logs*
- *Configure Multiple Port Mirroring*
- *Configure RSPAN VLAN*
- *Configure sFlow*

## 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**.

Status										
1 LAGS All		Go To Interface <input type="text"/> <b>Go</b>								
<input type="checkbox"/>	Interface	Total Packets received without Errors	Packets received with Errors	Broadcast Packets received	Packets transmitted without Errors	Transmit Packet Errors	Collision Frames	Link down events	Link Flaps	Time since counters last cleared
<input type="checkbox"/>	1/0/1	0	0	0	0	0	0	0	0	1 day 4 hr 59 min 45 sec
<input type="checkbox"/>	1/0/2	0	0	0	0	0	0	0	0	1 day 4 hr 59 min 45 sec
<input type="checkbox"/>	1/0/3	0	0	0	0	0	0	0	0	1 day 4 hr 59 min 45 sec
<input type="checkbox"/>	1/0/4	0	0	0	0	0	0	0	0	1 day 4 hr 59 min 45 sec
<input type="checkbox"/>	1/0/5	0	0	0	0	0	0	0	0	1 day 4 hr 59 min 45 sec

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 for the port and click the **Clear** button.
- To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the per-port statistics displayed on the screen..

**Table 238. Port Statistics**

Field	Description
Interface	This object indicates 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. 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.
Number of Link Down Events	The total number of link down events on a physical port.
Link Flaps	The total number of occurrences of link down to link up events (makes one link flap) during debouncing time.
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

You can view a variety of per-port traffic 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 following figure shows some, but not all, of the fields on the Port Detailed Statistics screen.

Port Detailed Statistics	
Interface	1/0/1
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	Unknown
Link Status	Link Down
Link Trap	Enable
Packets RX and TX 64 Octets	0
Packets RX and TX 65-127 Octets	0
Packets RX and TX 128-255 Octets	0
Packets RX and TX 256-511 Octets	0
Packets RX and TX 512-1023 Octets	0

Use the buttons at the bottom of the screen to perform the following actions:

- To clear all the counters, click the **Clear** button. This resets all statistics for this port to the default values.
- To refresh the screen with the latest information on the switch, click the **Update** 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 239. Port Detailed Statistics**

Field	Description
MST ID	Display the MST instances associated with the interface.
ifIndex	This object indicates the ifIndex of the interface table entry associated with this port on an adapter.

Table 239. Port Detailed Statistics (continued)

Field	Description
Port Type	<p>For normal ports this field is normal. Otherwise the possible values are as follows:</p> <ul style="list-style-type: none"> <li>• <b>Mirrored.</b> This port is a participating in port mirroring as a mirrored port. Look at the Port Mirroring screens for more information.</li> <li>• <b>Probe.</b> This port is a participating in port mirroring as the probe port. Look at the Port Mirroring screens for more information.</li> <li>• <b>Trunk Member.</b> The port is a member of a link aggregation trunk. Look at the Port Channel screens for more information.</li> </ul>
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	<p>The Spanning Tree Protocol administrative mode associated with the port or port channel. The possible values are as follows:</p> <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	<p>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 states are defined in IEEE 802.1D:</p> <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 administrative 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.

**Table 239. Port Detailed Statistics (continued)**

Field	Description
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).
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 object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects must 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).

**Table 239. Port Detailed Statistics (continued)**

Field	Description
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).
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. 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 delivered to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
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). 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 with 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.



**Table 239. Port Detailed Statistics (continued)**

Field	Description
Rx FCS Errors	The total number of packets received with 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 because 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 that were discarded (that is, 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.
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 object can be used as a reasonable estimate of Ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects must 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 use, including Ethernet header, CRC, and payload. (1518 to 9216). The default maximum frame size is 1518.

**Table 239. Port Detailed Statistics (continued)**

Field	Description
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.
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.

**Table 239. Port Detailed Statistics (continued)**

Field	Description
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 display 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

1 2 3 All

Go To Interface  Go

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	0	00:00:00:00:00:00	0	0	0	0	0	0	
<input type="checkbox"/> 1/0/2	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	
<input type="checkbox"/> 1/0/3	Authenticator	0	0	0	0	0	00:00:00:00:00:00	0	0	0	0	0	0	

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. Clicking the button resets all statistics for all ports to default values.

- To clear the counters for a specific port, select the check box associated with the port and click the **Clear** button.
- To refresh the screen with the latest information on the switch.

The following table describes the EAP statistics displayed on the screen, click the **Update** button.

**Table 240. EAP Statistics**

Field	Description
Port	Selects the port to be displayed. When the selection is changed, a screen update 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 Received	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**.

Port	Cable Status	Cable Length	Failure Location
1/0/1	Untested		
1/0/2	Untested		
1/0/3	Untested		
1/0/4	Untested		
1/0/5	Untested		

8. **Port**. Indicates the interface to which the cable to be tested is connected.

9. Click the **Apply** button.

A cable test is performed on the selected interface. 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. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter then the cable status might 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 screen.

**Table 241. Cable Test**

Field	Description
Cable Status	<p>This displays the cable status as Normal, Open or Short.</p> <ul style="list-style-type: none"> <li>• Normal: the cable is working correctly.</li> <li>• Open: the cable is disconnected or there is a faulty connector.</li> <li>• Short: there is an electrical short in the cable.</li> <li>• Cable Test Failed: The cable status could not be determined. The cable might in fact be working.</li> <li>• Untested: The cable is not yet tested.</li> <li>• Invalid cable type: The cable type is unsupported.</li> </ul>
Cable Length	<p>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 only displayed if the cable status is Normal.</p>
Failure Location	<p>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.</p>

## Manage Logs

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 Buffered Logs

➤ **To view buffered logs:**

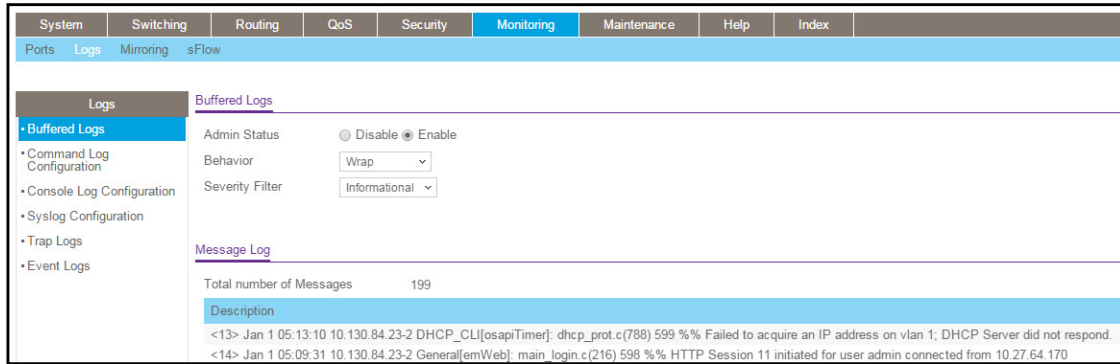
1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter the IP address of the switch in the web browser address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



## Configure Buffered Logs

This log stores messages in memory based upon the settings for message component and severity. On chassis systems, this log exists only on the top of chassis platform. Other platforms in the chassis forward their messages to the top of chassis log.

### ➤ To configure buffered logs:

1. Select the Admin Status **Enable** or **Disable** radio button.

A log that is disabled does not log messages.

2. Use **Behavior** to specify the behavior of the log when it is full.

It can either wrap around or stop when the log space is filled.

3. Select the severity option in the **Severity Filter** list.

A log records messages equal to or above a configured severity threshold. The severity levels are as follows:

- **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.

To refresh the screen with the latest information on the switch, click the **Update** button.

4. Click the **Clear** button to clear the buffered log in the memory.
5. Click the **Apply** button.

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

## Message Log Format

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:

- `<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 chassis 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 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 a chassis 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 syslog use a format identical to the previous message.
- **Total number of Messages:** For the message log, only the latest 200 entries are displayed on the screen.

## Enable or Disable the Command Log

### ➤ To enable or disable 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.

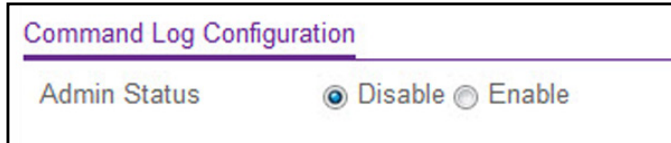
The default admin user name is **admin** and the default admin password is blank, that is, do not enter a password.



6. Click the **Login** button.

The web management interface menu displays.

7. Select **Monitoring > Logs > Command Log Configuration**.



8. Use **Admin Mode** to enable/disable the operation of the CLI command logging by selecting the corresponding radio button.

## Enable or Disable Console Logging

This allows logging to any serial device attached to the host.

### ➤ To enable or disable console logging:

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

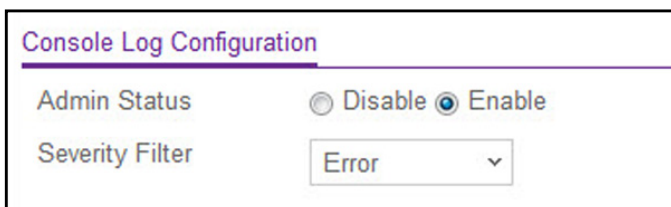
5. Enter the user name and password.

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**.



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

A log that is disabled does not log messages.

9. **Severity Filter.** A log records messages equal to or above a configured severity threshold. Select the severity option by selecting the corresponding line on the drop-down entry field. 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 Syslog Host Settings

### ➤ 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.  
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 > Syslog Configuration**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance	Help	Index										
Ports	Logs	Mirroring	sFlow															
<div> <div> <div>Logs</div> <ul style="list-style-type: none"> <li>• Buffered Logs</li> <li>• Command Log Configuration</li> <li>• Console Log Configuration</li> <li>• <b>Syslog Configuration</b></li> <li>• Trap Logs</li> <li>• Event Logs</li> </ul> </div> <div> <div>Syslog Configuration</div> <div> <div>Admin Status</div> <div> <input checked="" type="radio"/> Disable           <input type="radio"/> Enable         </div> </div> <div> <div>Local UDP Port</div> <div>514 (1 to 65535)</div> </div> <div> <div>Source Interface</div> <div>vlan 1</div> </div> <div> <div>Messages Received</div> <div>5925</div> </div> <div> <div>Messages Relayed</div> <div>0</div> </div> <div> <div>Messages Ignored</div> <div>0</div> </div> </div> </div> <div> <div>Host Configuration</div> <table border="1"> <thead> <tr> <th>IP Address Type</th> <th>Host Address</th> <th>Status</th> <th>Port</th> <th>Severity Filter</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> </div>									IP Address Type	Host Address	Status	Port	Severity Filter					
IP Address Type	Host Address	Status	Port	Severity Filter														

The **Status** field displays whether the host was configure to be actively logging or not.

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

This enables or disables logging to configured syslog hosts. Setting this to disable stops logging to all syslog hosts so that no messages are sent to any collectors or relays. Enable means messages are sent to configured collectors or relays using the values configured for each collector or relay.

9. Use **Local UDP Port** to specify the port on the local host from which syslog messages are sent.

The default port is 514.

10. Specify the **Source Interface** to use for syslog.

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.

11. Use **IP Address Type** to specify the address type of host.

It can be one of the following:

- IPv4
- IPv6
- DNS

12. In the **Host Address** - This is the address of the host configured for THE syslog.

13. In the **Port** field, specify the port on the host to which syslog messages are sent.

The default port is 514.

**14.** Select the severity option in the **Severity Filter** list.

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

The following table describes the nonconfigurable data.

**Table 242. Syslog Configuration**

Field	Description
Messages Received	The number of messages received by the log process. This includes messages that are dropped or ignored.
Messages Relayed	The count of syslog messages relayed.
Messages Ignored	The count of syslog messages ignored.

## View the Trap Logs

You can view the entries in the trap log. The information can be retrieved as a file.

➤ **View the 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.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Monitoring > Logs > Trap Logs**.

### Trap Logs

Number of Traps Since Last Reset	3
Trap Log Capacity	256
Number of Traps Since Log Last Viewed	3

### Trap Logs

Log	System Up Time	Trap
0	Jan 1 00:02:13 1970	Cold Start: Unit: 0
1	Jan 1 00:01:21 1970	Entity Database: Configuration Changed
2	Jan 1 00:01:16 1970	Power On Start has completed on unit 1.

The screen also displays information about the traps that were sent.

Click the **Clear** button to clear all the counters. This resets all statistics for the trap logs to the default values.

The following table describes the Trap Log information displayed on the screen.

**Table 243. 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.
System Up Time	The time when this trap occurred, expressed in days, hours, minutes and seconds, since the last reboot of the switch.
Trap	Information identifying the trap.

## View the Event Log

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 the event 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 > Event Logs**.

Event Logs						
Entry	Type	Filename	Line	Task ID	Code	Time
1	EVENT>	bootos.c	192	0	AAAAAAAA	0 0 0 28
2	EVENT>	unitmgr.c	6462	0	00000000	0 16 25 54
3	EVENT>	bootos.c	192	0	AAAAAAAA	0 0 0 28
4	EVENT>	unitmgr.c	6462	0	00000000	0 8 49 34
5	EVENT>	bootos.c	192	0	AAAAAAAA	0 0 0 28

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 with the latest information on the switch, click the **Update** button.

The following table describes the event log information displayed on the screen.

**Table 244. 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.

Table 244. Event Logs

Field	Description
Code	The event code.
Time	The time this event occurred.

## Configure Persistent Logs (M5300 and M7100 only)

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**.

**Persistent Logs**

Admin Mode ☒ Disable ☐ Enable

Behavior Error ▾

---

**Message Log**

Logs to be Displayed Current Logs ▾

Total number of Messages 0

Description

A log that is disabled does not log messages.

8. Select the Admin Mode **Disable** or **Enable** radio button.
9. In the **Behavior** list, select the 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

To refresh the screen with the latest information on the switch, click the **Update** button.

## Format of the Messages

- Total number of messages: 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 a chassis 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 syslog use a format identical to the previous message.



## Configure Multiple Port Mirroring

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, that 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.

➤ **To globally configure multiple 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.

6. Click the **Login** button.

The web management interface menu displays.

7. Select **Monitoring > Mirroring > Multiple Port Mirroring**.

**Global Configuration**

Session ID: 1

Admin Mode: ☐ True ☒ False

Destination Port: None

Filter Type: None

Filter Name:

**Source Interface Configuration**

1 2 3 LAG CPU VLANs All Go To Interface

Interface	Direction	Status
<input type="checkbox"/> 1/0/1	None	
<input type="checkbox"/> 1/0/2	None	

8. Select the number of the session from the **Session ID** list.

9. Select the Admin Mode **True** (enabled) or **False** (disabled) radio button.

Select the **True** option to enable Admin mode 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 disabled (**False**).

10. From the **Destination Port** list, select 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 ports. If the value is not configured, it is shown as None. The default value is None.

11. From the **Filter Type** list, select the IP or MAC ACL that can mirror traffic that matches a permit rule.

Possible values are as follows:

- **None.** No filter is configured for the session.
- **IP ACL.** Configure IP ACL.
- **MAC ACL.** Configure MAC ACL.

The default value is None.

12. In the **Filter Name** field, enter the name of the filter, if it is configured for the session.

13. Click the **Apply** button.

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

14. In the Source Interface Configuration section, use the following selection methods:

- Select **Unit ID** 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.
- Use **Interface** to specify the configured ports as mirrored ports. Traffic of the configured ports is sent to the probe port.

15. In the **Direction** field, specify the direction of the traffic to be mirrored from the configured mirrored ports.

If the value is not configured, it is shown as None. The default value is None. Direction options are as follows:

- **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.

**16.** Click the **Apply** button.

The settings are applied to the system. If the port is configured as a source port, the **Mirroring Port** field value is Mirrored.

The **Status** field indicates the interface status.

---

**Note:** In case of an error dialog having multiple error messages, resolve them to get the remaining set of errors, if any.

---

## Configure 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 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**.

System	Switching	Routing	QoS	Security	Monitoring									
Ports	Logs	Mirroring	sFlow											
<div> <div> Mirroring <ul style="list-style-type: none"> <li>Multiple Port Mirroring</li> <li><b>RSPAN VLAN</b></li> <li>RSPAN Source Switch Configuration</li> <li>RSPAN Destination Switch Configuration</li> </ul> </div> <div> RSPAN VLAN <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>VLAN ID</th> <th>Admin Mode</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td>1</td> <td>Disable</td> </tr> </tbody> </table> </div> </div>						<input type="checkbox"/>	VLAN ID	Admin Mode	<input type="checkbox"/>			<input type="checkbox"/>	1	Disable
<input type="checkbox"/>	VLAN ID	Admin Mode												
<input type="checkbox"/>														
<input type="checkbox"/>	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 updated configuration is sent to the switch. Configuration changes take effect immediately.

## Configure an RSPAN Source Switch

### ➤ To configure an 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 **Session ID** number from the list.
9. Select the Admin Mode **True** (enabled) or **False** (disabled) 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).

10. Select the **RSPAN Destination VLAN** from the list of available VLAN IDs.
11. Select the **RSPAN Reflector Port** from the list of reflector port interfaces.
12. Select from the **Filter Type** list to configure IP or MAC ACLs that can mirror traffic that matches a permit rule.

Possible values are as follows:

- **None.**
- **IP ACL.** Configure IP ACL.
- **MAC ACL.** Configure MAC ACL.

13. Enter the **Filter Name**, if a filter is configured for the session.
14. Click the **Apply** button.

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

➤ **To configure an RSPAN source interface:**

1. Select a Unit ID (**1, 2, 3**) to display a list of physical ports for the selected unit.
2. Select **LAG** to display LAGs only.
3. Select **CPU** to display CPUs only.
4. Select **VLAN** to display a list of available VLAN IDs.
5. Select **All** to display all physical ports, LAGs, CPUs, and VLANs.

6. Select an interface by entering the interface number in the **Go To Interface** field.
7. In the **Interface** list, select an interface to specify the configured ports as mirrored ports.  
Traffic of the configured ports is sent to the probe port.
8. Select from the **Direction** list to specify the direction of the traffic to be mirrored from the configured mirrored ports.  
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.

The **Status** field indicates the interface status.

## 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**.

System	Switching	Routing	QoS	Security	Monitoring														
Ports	Logs	Mirroring	sFlow																
<table border="1"> <thead> <tr> <th>Mirroring</th> <th>RSPAN Destination Switch Configuration</th> </tr> </thead> <tbody> <tr> <td>• Multiple Port Mirroring</td> <td>Session ID <input type="text" value="1"/></td> </tr> <tr> <td>• RSPAN VLAN</td> <td>Admin Mode <input type="radio"/> True <input checked="" type="radio"/> False</td> </tr> <tr> <td>• RSPAN Source Switch Configuration</td> <td>RSPAN Source VLAN <input type="text" value="None"/></td> </tr> <tr> <td>• RSPAN Destination Switch Configuration</td> <td>RSPAN Destination Port <input type="text" value="None"/></td> </tr> <tr> <td></td> <td>Filter Type <input type="text" value="None"/></td> </tr> <tr> <td></td> <td>Filter Name <input type="text"/></td> </tr> </tbody> </table>						Mirroring	RSPAN Destination Switch Configuration	• Multiple Port Mirroring	Session ID <input type="text" value="1"/>	• RSPAN VLAN	Admin Mode <input type="radio"/> True <input checked="" type="radio"/> False	• RSPAN Source Switch Configuration	RSPAN Source VLAN <input type="text" value="None"/>	• RSPAN Destination Switch Configuration	RSPAN Destination Port <input type="text" value="None"/>		Filter Type <input type="text" value="None"/>		Filter Name <input type="text"/>
Mirroring	RSPAN Destination Switch Configuration																		
• Multiple Port Mirroring	Session ID <input type="text" value="1"/>																		
• RSPAN VLAN	Admin Mode <input type="radio"/> True <input checked="" type="radio"/> False																		
• RSPAN Source Switch Configuration	RSPAN Source VLAN <input type="text" value="None"/>																		
• RSPAN Destination Switch Configuration	RSPAN Destination Port <input type="text" value="None"/>																		
	Filter Type <input type="text" value="None"/>																		
	Filter Name <input type="text"/>																		

8. From the **Session ID** list, select the session ID.
9. Select the Admin Mode **True** (enabled) or **False** (disabled) 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, the Admin mode is disabled.

10. Select the **RSPAN Source VLAN** from the list of available VLAN IDs.
11. Select the **RSPAN Destination VLAN** from the list of destination interfaces.
12. Configure the **Filter Type**.

IP or MAC ACLscan mirror traffic that matches a permit rule. Possible values are as follows:

- **None**. No filter is configured for the session.
- **IP ACL**. Configure IP ACL.
- **MAC ACL**. Configure MAC ACL.

13. Enter the **Filter Name**, if it is configured for the session.
14. Click the **Apply** button.

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

## Configure sFlow

You can configure basic or advanced sFlow settings.

### Configure Basic sFlow Agent Information

#### ➤ To configure basic 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**.

8. In the **Source Interface** list, select the management interface that is 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 the source interface.

9. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.



The following table describes the nonconfigurable information.

**Table 245. sFlow Basic Agent Information**

Field	Description
<b>Agent Version</b>	Uniquely identifies the version and implementation of this MIB. The version string must use the following structure: MIB Version;Organization;Software Revision where: <ul style="list-style-type: none"> <li>• MIB Version: For example, 1.3, the version of this MIB</li> <li>• Organization: NETGEAR Inc.</li> <li>• Revision: 1.0</li> </ul>
<b>Agent Address</b>	The IP address associated with this agent.

## Configure sFlow Agent Advanced Settings

### ➤ To configure sFlow agent advanced 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 Agent Information**.

The screenshot shows a web management interface with a top navigation bar containing tabs: System, Switching, Routing, QoS, Security, and Monitoring. The Monitoring tab is selected, and a sub-menu shows Ports, Logs, Mirroring, and sFlow. The sFlow sub-menu is expanded, showing a list of options: sFlow, sFlow Agent Source Interface, sFlow Agent Information, sFlow Receiver Configuration, and sFlow Interface Configuration. The sFlow Agent Information option is selected, displaying the following configuration details:

sFlow Agent Source Interface	
Source Interface	vlan 1

sFlow Agent Information	
Agent Version	1.3;Netgear Inc.;Q.2.15.1
Agent Address	10.130.84.23

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 the source interface.

9. Click the **Apply** button.

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

To refresh the screen with the latest information on the switch, click the **Update** button.

The following table describes the nonconfigurable information.

**Table 246. sFlow Advanced Agent Information**

Field	Description
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: <ul style="list-style-type: none"> <li>• MIB Version: '1.3', the version of this MIB</li> <li>• Organization: NETGEAR Inc.</li> <li>• Revision: 1.0</li> </ul>
Agent Address	The IP address associated with this agent.

## Configure an sFlow Receiver

### ➤ To configure an 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								
<input type="checkbox"/>	Receiver Index	Receiver Owner	Receiver Timeout	No Timeout	Maximum Datagram Size	Receiver Address	Receiver Port	Datagram Version
<input type="checkbox"/>	1		0	False	1400	0.0.0.0	6343	5
<input type="checkbox"/>	2		0	False	1400	0.0.0.0	6343	5
<input type="checkbox"/>	3		0	False	1400	0.0.0.0	6343	5
<input type="checkbox"/>	4		0	False	1400	0.0.0.0	6343	5
<input type="checkbox"/>	5		0	False	1400	0.0.0.0	6343	5

8. Specify the **Receiver Owner**

This is 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** to set the no time-out sampling for the receiver.

Sampling is not stopped until the 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. Default Value: 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.

The **Receiver Datagram Version** field displays the version of sFlow datagrams to be sent.

## Configure the sFlow Interface

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 the sFlow 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 > sFlow > Advanced > sFlow Interface Configuration**.

sFlow Interface Configuration					
1 All		Go To Interface		Go	
<input type="checkbox"/>	Interface	Poller		Sampler	
		Receiver Index	Poller Interval	Receiver Index	Maximum Header Size
<input type="checkbox"/>					
<input type="checkbox"/>	1/0/1	0	0	0	128
<input type="checkbox"/>	1/0/2	0	0	0	128
<input type="checkbox"/>	1/0/3	0	0	0	128
<input type="checkbox"/>	1/0/4	0	0	0	128
<input type="checkbox"/>	1/0/5	0	0	0	128

8. **Interface** displays the interface for this flow poller and sampler.

This agent supports physical ports only.

9. Use **Poller Receiver Index** to specify the allowed range for the sFlow receiver associated with this counter poller.

The allowed range is 1 to 8.

10. Use **Poller Interval** to 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 seconds.

11. Use **Sampler Receiver Index** to specify the sFlow receiver for this flow sampler.

If set to 0, the sampler configuration is set to default and the sampler is deleted.

Only active receivers can be set. If a receiver expires, then all samplers associated with the receiver also expires. The allowed range is 1 to 8.

12. Use **Sampling Rate** to 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.

13. Use **Maximum Header Size** to specify the maximum number of bytes to be copied from a sampled packet.

The allowed range is 20 to 256.

This chapter covers the following topics:

- *Save the Configuration*
- *Configure Auto Save Mode*
- *Reboot the Switch*
- *Power Cycle the Switch*
- *Reset the Switch to Its Factory Default Settings*
- *Reset All User Passwords to Their Default Settings*
- *Upload a File from the Switch*
- *Download a File to the Switch*
- *File Management*
- *Troubleshooting*

## Save the Configuration

When you save the configuration, changes that you made are retained by the switch when it is rebooted. You can manually save the configuration or you can set up autosave.

➤ **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.

The Login screen displays.

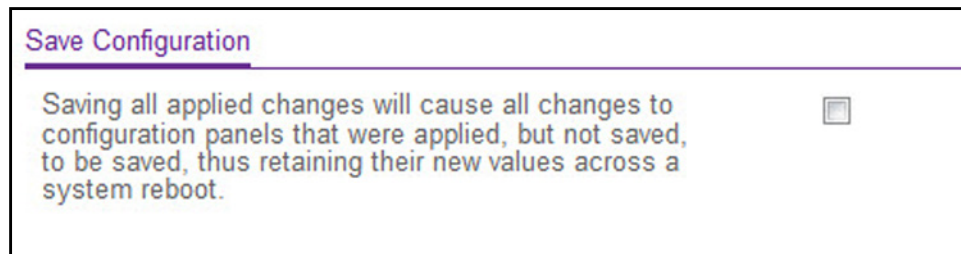
5. Enter the user name and password.

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 > Save Configuration**.



8. Select the check box.
9. Click the **Apply** button.

The 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.

## Configure Auto Save Mode

➤ **To configure auto save 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 **Maintenance > Save Config > Auto Install Configuration**.

Auto Install Configuration	
AutoInstall Mode	Stop ▾
AutoInstall Persistent Mode	Enabled ▾
AutoSave Mode	Disabled ▾
AutoInstall Retry Count	3 (1 to 3)
AutoInstall State	AutoInstall is completed.

The **Autoinstall State** field displays the current status of the Autoinstall process.

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. Use **AutoSave Mode** to select **Enabled** or **Disabled**.
11. Click the **Apply** button.

The configuration changes that you made are saved across a system reboot. All changes submitted since the previous save or system reboot are retained by the switch.

12. Use **AutoInstall Retry Count** to specify the number of times the unicast TFTP tries are made for the DHCP specified file before falling back for broadcast TFTP tries.

## Reboot the Switch

### ➤ To reboot 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.

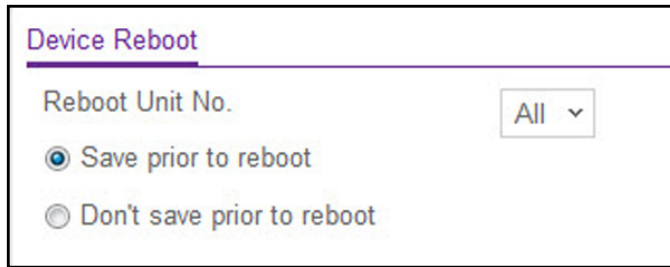
5. Enter the user name and password.

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.

7. Select **Maintenance > Reset > Device Reboot**.



Device Reboot

Reboot Unit No. All ▼

☒ Save prior to reboot

☐ Don't save prior to reboot

8. In the **Reboot Unit No.** field, select the unit to reset.

When multiple units are connected in a chassis, select **All** to reset all the units in the stack (in other words, the whole chassis) or select the unit number to reset only the specific unit.

9. Select a radio button:

- **Save prior to reboot.** The current configuration is saved and the switch reboots.
- **Don't save prior to reboot.** The switch will reboot without saving the current configuration

10. Click the **Apply** button.

If you selected the save option, the configuration is saved. The switch reboots.

## Power Cycle the Switch

You can use the power cycle feature to reboot the blade if it is not responding.

### ➤ To power cycle 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.

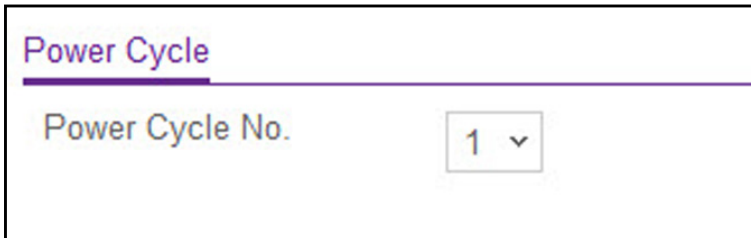
5. Enter the user name and password.

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.

7. Select **Maintenance > Reset > Power Cycle**.



8. Select the slot from the list.
9. Click the **Apply** button.

The switch performs a hardware reboot.

## Reset the Switch to Its Factory Default Settings

---

**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**.



8. Select the check box.

9. Click the **Apply** button.

A confirmation screen displays.

10. Click **Yes** to confirm.

All configuration parameters are reset to their factory default values. All changes you made are, even if you issued a save.

## Reset All User Passwords to Their Default Settings

### ➤ To reset all user passwords to their 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 > Password Reset**.

<b>Password Reset</b>
Check this box and click APPLY above to reset all user passwords. <input type="checkbox"/>

8. Select the check box.
9. Click the **Apply** button.

All user passwords are reset to their factory default values.

## Upload a File from the Switch

You can upload configuration (ASCII), log (ASCII), and image (binary) files from the switch to the TFTP server.

### Upload a File 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.

The Login screen displays.

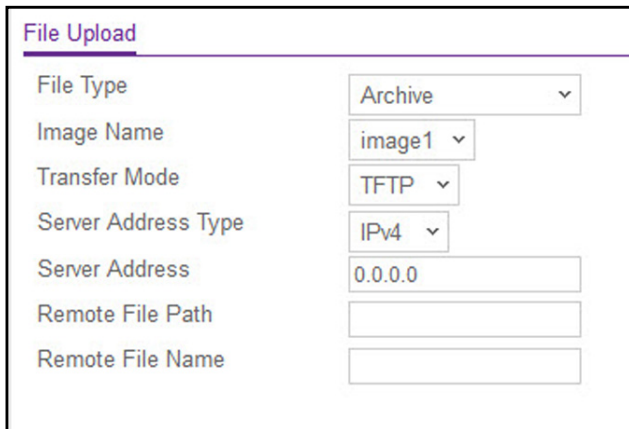
5. Enter the user name and password.

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 > File Upload**.



8. Use **File Type** to specify what type of file to upload:
  - **Archive.** Specify Archive (STK) code to retrieve from the operational flash.
  - **CLI Banner.** Specify CLI Banner to 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 trouble-shooting.
  - **Crash Logs.** Specify Crash Log to retrieve the crash logs.

The factory default is Archive.

9. The **Image Name** field is only visible when the selected File Type is Archive.

If you are uploading a switch image (Archive), use the **Image Name** list to select the software image on the switch to upload to the management system:

- **image1.** Select image1 to upload image1.
  - **image2.** Select image2 to upload image2.
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
    - **FTP.** File Transfer Protocol
  11. 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.

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 to upload the file.

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.

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 **Local File Name** to specify the local script file name to upload.

This field is visible only when File Type is Script File.

16. 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.

17. Use **Password** to enter the password for remote login to SFTP/SCP server where the file is sent.

This field is visible only when the SFTP or SCP transfer mode is selected.

The last row of the table is used to display information about the progress of the file transfer.

## HTTP File Upload

### ➤ To use HTTP file upload:

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

HTTP File Upload	
File Type	Archive ▼
Image Name	image1 ▼

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.** Specify the code image1 to retrieve.
    - **Image2.** Specify the code image2 to retrieve.
  - **CLI Banner.** Specify CLI Banner to 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.
  - **Crash Logs.** Specify Crash Logs to retrieve the system crash logs.

The factory default is Archive.

9. Use **Local File Name** to specify the local script file name to upload.

## Upload a File from the Switch to a USB Device

### ➤ To use upload a file from the switch 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 > Upload > USB File Upload**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance
Save Config	Reset	Upload	Download	File Management	Troubleshooting	

Upload	Upload File To USB
• File Upload	File Type: Archive
• HTTP File Upload	Image Name: image1
• <b>USB File Upload</b>	File Path:
	USB File:

8. Use **File Type** to specify what type of file to upload:
  - **Archive**. Archive (STK) code to retrieve from the operational flash:
  - **Text Configuration**. 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. In the **File Path** field, enter the path for the file to upload.  
You can use up to 146 characters. The default is blank.
11. 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.
12. Click the **Apply** button.

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

## Download a File to the Switch

The switch supports system file downloads from a remote system to the switch by using either TFTP or HTTP.



## Download a File

➤ **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.

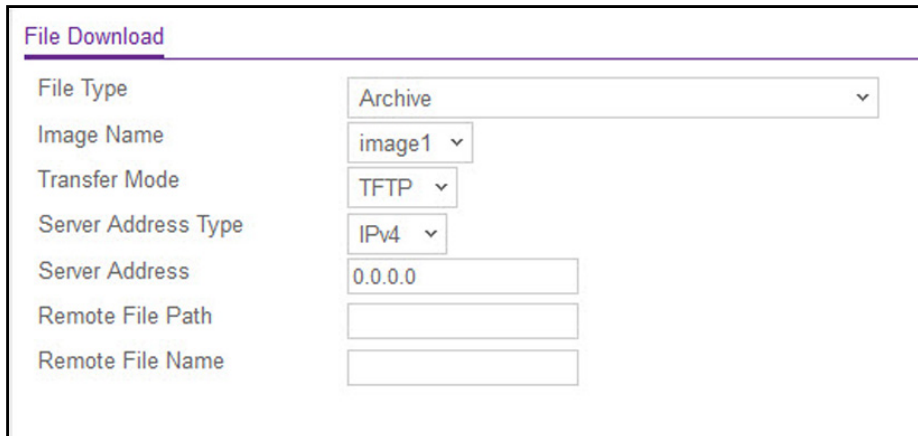
5. Enter the user name and password.

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 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 transfer.
  - **Archive.** Archive (STK) code to upgrade the operational flash.
  - **Text Configuration.** Configuration in text mode to update the switch's configuration. If the file has errors, the update is stopped.
  - **SSH-1 RSA Key File.** SSH-1 Rivest-Shamir-Adelman (RSA) Key File.
  - **SSH-2 RSA Key PEM File.** SSH-2 Rivest-Shamir-Adelman (RSA) Key File (PEM Encoded).
  - **SSH-2 DSA Key PEM File.** SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded).

- Use **SSL Trusted Root Certificate PEM File** to specify SSL Trusted Root Certificate File (PEM Encoded).
- Use **SSL Server Certificate PEM File** to specify SSL Server Certificate File (PEM Encoded).
- Use **SSL DH Weak Encryption Parameter PEM File** to specify SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded).
- Use **SSL DH Strong Encryption Parameter PEM File** to specify SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).
- Use **Script File** to specify script configuration file.
- **CLI Banner.** Specify CLI Banner if a banner will to be displayed before the login prompt.
- Use **IAS Users** to specify the Internal Authentication Server Users Database file.

The factory default is Archive.

---

**Note:** For you to download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.

---



---

**Note:** For you to download SSL PEM files, SSL must be administratively disabled and there can be no active SSH sessions.

---

The **Image Name** field is visible only when File Type **Archive** is selected.

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
  - **FTP.** File Transfer 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 TFTP server in accordance with the format indicated by the server address type, for example an IP address in the x.x.x.x format.  
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 160 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.

The file path cannot include the following symbols: ' \:.\*?"<>| '. 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.

The last row of the table displays information about the progress of the file transfer. It is displayed only after the process starts. The screen refreshes automatically until the file transfer completes.

17. Click the **Apply** button.

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

## Download a File to the Switch Using HTTP

You can download files of various types to the switch using an HTTP session (for example, through your web browser).

### ➤ To download a file to the switch 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**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance
Save Config	Reset	Upload	Download	File Management	Troubleshooting	
<div>Download</div> <div>File Download</div> <div> <div>File Download</div> <div>HTTP File Download</div> <div>USB File Download</div> </div> <div> <div>File Type</div> <div>Image Name</div> <div>Transfer Mode</div> <div>Server Address Type</div> <div>Server Address</div> <div>Remote File Path</div> <div>Remote File Name</div> </div> <div> <div>Archive</div> <div>image1</div> <div>TFTP</div> <div>IPv4</div> <div>0.0.0.0</div> <div></div> <div></div> </div>						

8. Use **File Type** to specify what type of file to transfer:

- **Archive.** Archive (STK) code to upgrade the operational flash.
- The **Image Name** field is visible only when File Type **Archive** is selected. Use **Image Name** to select one of the images from the list:
  - **Image1.** Specify the code image1 to download.
  - **Image2.** Specify the code image2 to download.
- **Text Configuration.** Configuration is in text mode to update the switch's configuration. If the file has errors, the update is stopped.
- Use **SSH-1 RSA Key File** to specify SSH-1 Rivest-Shamir-Adelman (RSA) Key File.
- Use **SSH-2 RSA Key PEM File** to specify SSH-2 Rivest-Shamir-Adelman (RSA) Key File (PEM Encoded).
- Use **SSH-2 DSA Key PEM File** to specify SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded).
- Use **SSL Trusted Root Certificate PEM File** to specify SSL Trusted Root Certificate File (PEM Encoded).
- Use **SSL Server Certificate PEM File** to specify SSL Server Certificate File (PEM Encoded).
- Use **SSL DH Weak Encryption Parameter PEM File** to specify SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded).
- Use **SSL DH Strong Encryption Parameter PEM File** to specify SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).
- Use **Config Script** to specify script configuration file.
- **CLI Banner.** Specify CLI Banner if a banner will be displayed before the login prompt.
- Use **IAS Users** to specify the Internal Authentication Server Users Database File.

The factory default is Archive.

**Note:** For you to download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.

**Note:** For you to download SSL PEM files, SSL must be administratively disabled and there can be no active SSH sessions.

9. Use **Select File** to browse and enter a name along with path for the file to download.

You can enter up to 80 characters. The factory default is blank.

10. Click **Browse** to locate the file to download.

The factory default is blank.

11. Click the **Apply** button.

The download begins.

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 from a USB Device

➤ **To download a file from 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 Download**.

System	Switching	Routing	QoS	Security	Monitoring	Maintenance
Save Config	Reset	Upload	Download	File Management	Troubleshooting	
<div> <div>Download</div> <div>Download File From USB</div> </div>						
<div> <div> • File Download  • HTTP File Download  • <b>USB File Download</b> </div> <div> File Type: <input type="text" value="Archive"/>  Image Name: <input type="text" value="image1"/>  File Path: <input type="text"/>  USB File: <input type="text"/> </div> </div>						

8. Use **File Type** to specify what type of file to download:
  - **Archive**. Archive (STK) code to download to the operational flash.
  - **Text Configuration**. Configuration s in text mode to update the switch's configuration (Startup-config).

If the file has errors, the update is stopped. The factory default is **Archive**.

9. Use **Image Name** to select one of the images from the list:
  - **Image1**. Select image1 to download to image1.
  - **Image2**. Select image2 to download to image2.

Only when File Type **Archive** is selected is the **Image Name** field visible.

10. Use the File Path field to give a path for the file to download.

You can enter up to 146 characters. The default is blank.

11. Use **USB File** to give a name along with path for the file to download.

You can enter up to 32 characters. The factory default is blank.

12. Click the **Apply** button.

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

**Download Status** displays the status of the file transfer to the switch. The last row of the table is used to display information about the progress of the file transfer. It is displayed only after the process starts. The screen refreshes automatically until the file transfer completes.

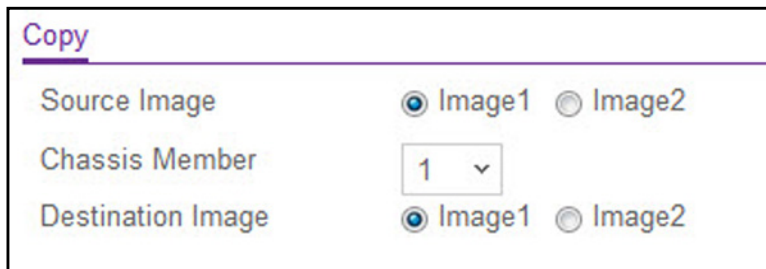
## File Management

The system maintains two versions of the M6100/M7100/M5300 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 you are upgrading or downgrading the M6100/M7100/M5300 software.

## Copy an Image

### ➤ To copy an image:

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



Copy	
Source Image	<input checked="" type="radio"/> Image1 <input type="radio"/> Image2
Chassis Member	1 ▼
Destination Image	<input checked="" type="radio"/> Image1 <input type="radio"/> Image2

8. Use **Source Image** to select the image1 or image2 as the source image (the image to be copied).
9. Use **Chassis Member** to select the destination unit to which you are going to copy from the supervisor.
10. Use **Destination Image** to select the image1 or image2 as the destination image.
11. Click the **Apply** button.

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

## Configure Dual Image Settings

The Dual Image feature allows the switch to retain two images in permanent storage. The administrator can designate image1 or image2 as the active image to be loaded during subsequent switch restarts. This feature reduces switch down time when you are upgrading or downgrading the software 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**.

Dual Image Configuration						
<input type="checkbox"/>	Unit	Image Name	Active Image	Next Active Image	Image Description	Version
<input type="checkbox"/>	1	image1	False	False		6.1.20.58
<input type="checkbox"/>	1	image2	True	True		6.2.13.24

8. Use **Unit** to select the unit ID whose code image to activate, update, or delete.
9. Use **Next Active Image** to make the selected image the next active image for subsequent reboots of this unit.
10. Use **Image Description** to specify the description for the image that you selected.
11. Click the **Delete** button 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 to run the new code.

---



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

**Table 247. Dual Image Configuration**

Field	Description
Image Name	This displays the image name for the selected unit.
Active Image	The current active image of the selected unit.
Version	The version of the image1 code file.

## Troubleshooting

You can use Ping or Traceroute and you can perform a memory dump.

### Ping IPv4

You can tell the switch to send a ping request to a specified IP address. You can check whether the switch can communicate with a particular IP station. When you click the **Apply** button, the switch sends a 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 message displays:

```
Reply From a.b.c.d: icmp_seq = 0. time= xyz usec.
Reply From a.b.c.d: icmp_seq = 1. time= abc usec.
Reply From a.b.c.d: icmp_seq = 2. time= 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	<input type="text"/>	(Max 255 characters/x.x.x.x)
Count	<input type="text" value="3"/>	(1 to 15)
Interval(secs)	<input type="text" value="3"/>	(1 to 60)
Datagram Size	<input type="text" value="0"/>	(0 to 65507)
Source	<input type="text" value="None"/>	
Results	<div></div>	

8. Use **IP Address/Host Name** to enter the IP address or host name of the station for the switch to ping.

The initial value is blank.

9. In the **Count field**, enter the number of echo requests to send.

The default value is 3. The range is 1 to 15.

10. Enter the **Interval** between ping packets in seconds.

The default value is 3 seconds. The range is 1 to 60.

11. Enter the **Datagram Size** of ping packet.

The default value is 0 bytes. The range is 0 to 65507.

12. Enter the **Source** IP address or interface to use when sending the echo request packets.

If source is not required, select **None** as the source option. Possible values are as follows:

- **None.** The source address of the ping packet would be the address of the default outgoing interface.
- **IP Address.** The source IP address to use when sending the echo request packets. This field is shown when **IP Address** is selected as the source option.
- **Interface.** The interface to use when sending the echo request packets. This field is shown when **Interface** is selected as the source option.

**Note:** Values configured in the fields on this screen are not saved to the switch. As a result, refreshing the screen sets these fields to the default values.

13. Click the **Apply** button.

The pings are sent to the specified address. The switch sends the number of pings specified in the **Count** field, and the results are displayed below the configurable data in the **Results** area.

To cancel the operation on the screen and reset the data on the screen to the latest value of the switch, click the **Cancel** button.

## Ping IPv6

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 a specified number of ping requests and the results are displayed below the configurable data. The output displays the following:

```
Send count=n, Receive count=n from (IPv6 Address). Average round trip
time = n ms.
```

### ➤ To use Ping IPv6:

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

3. Launch a web browser.

4. Enter 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**.

8. Select the **Ping** type from the list.

Possible values are as follows:

- **Global**. Ping a global IPv6 address.
- **Link Local**. Ping a link-local IPv6 address over the specified interface. This field is shown when Interface is selected as the ping option.

9. Use **IPv6 Address/Hostname** to enter the IPv6 address or host name of the station for the switch to ping.

The initial value is blank. The format is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx. The maximum number of characters is 255.

10. Use **Count** to enter the number of echo requests send.

The range is 1 to 15. The default value is 3.

11. Enter the **Interval** in seconds between ping packets.

The range is 1 to 60. The default value is 3.

12. Use **Datagram Size** to enter the datagram size.

The valid range is 0 to 13000. The default value is 0 bytes.

13. Enter the **Source** IP address or interface to use when sending the echo request packets.

If the source is not required, select None as the source option. Possible values are as follows:

- **None**. The source address of the ping packet would be the address of the default outgoing interface.
- **IPv6 Address**. The source IPv6 address to use when sending the echo request packets. This field is shown when **IPv6 Address** is selected as the source option.
- **Interface**. The interface to use when sending the echo request packets. This field is shown when **Interface** is selected as the source option.

**Note:** Values configured in the fields in this screen are not saved to the switch. As a result, refreshing the screen sets these fields to the default values.

14. Click the **Apply** button.

Pings are sent to the specified IPv6 address or host name. The switch sends the number of pings specified in the **Count** field, and the results are displayed below the configurable data in the **Results** area.

## 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. Once you click the **Apply** button, the switch sends traceroute and the results are displayed below the configurable data.

If a reply to the traceroute is received, the following message displays:

```
1 e.f.g.h 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 = j Last TTL = k Test attempt = m Test Success = n.
```

➤ **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.

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 IPv4**.

TraceRoute IPv4		
IP Address/Hostname	<input type="text"/>	(Max 255 characters/x.x.x.x)
Probes Per Hop	<input type="text" value="3"/>	(1 to 10)
Max TTL	<input type="text" value="30"/>	(1 to 255)
Init TTL	<input type="text" value="1"/>	(1 to 255)
MaxFail	<input type="text" value="5"/>	(1 to 255)
Interval(secs)	<input type="text" value="3"/>	(1 to 60)
Port	<input type="text" value="33434"/>	(1 to 65535)
Size	<input type="text" value="0"/>	(0 to 39936)
Source	<input type="text" value="None"/>	
<b>Results</b> <div></div>		

8. Use **IP Address/Hostname** to enter the IP address or host name of the station to which you want to discover a path.

The default value is blank.

9. Enter the number of **Probes Per Hop**.

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

10. Enter the **Maximum TTL** for the destination.

The default value is 30. The range is 1 to 255.

11. Enter the **Initial TTL** to be used.

The default value is 1. The range is 1 to 255.

12. Enter the **Maximum Failures** allowed in the session.

The default value is 5. The range is 1 to 255.

13. **Interval (secs)**. Enter the time between probes in seconds.

The default value is 3. The range is 1 to 60.

14. Enter the UDP Destination **Port** in probe packets.

The default value is 33434. The range is 1- 65535.

15. Enter the **Size** of the probe packets.

The default value is 0. The range is 0 to 39936.

16. Enter the **Source** IP address or interface to use when sending the echo request packets.

If source is not required, select None as the source option. Possible values are as follows:

- **None**. The source address of the ping packet would be the address of the default outgoing interface.
- **IP Address**. The source IP address to use when sending the echo request packets. This field is shown when **IP Address** is selected as the source option.
- **Interface**. The interface to use when sending the echo request packets. This field is shown when **Interface** is selected as the source option.

**Note:** Values configured in the fields in this screen are not saved to the switch. As a result, refreshing the screen sets these fields to the default values.

17. Click the **Apply** button.

A traceroute request is sent to the specified IP address or host name. The results are displayed below the configurable data in the TraceRoute Results area.

The **Results** field displays the traceroute IPv4 result after the switch sends a traceroute request to the specified IP address or host name.

## Traceroute IPv6

Use this screen to tell the switch to send a traceroute request to a specified IPv6 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 below the configurable data.

If a reply to the traceroute is received, the following message displays:

```
1 a:b:c:d:e:f:g 9869 usec 9775 usec 10584 usec
2 0:0:0:0:0:0:0:0 0 usec * 0 usec * 0 usec *
Hop Count = p Last TTL = q Test attempt = r Test Success = s.
```

### ➤ To use traceroute IPv6:

1. Prepare your computer with a static IP address in the 169.254.100.0 subnet, for example, 169.254.100.201.
2. Connect an Ethernet cable from an Ethernet port on your computer to an Ethernet port on the switch.
3. Launch a web browser.
4. Enter 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		
IPv6 Address/Host Name	<input type="text"/>	
Probes Per Hop	<input type="text" value="3"/>	(1 to 10)
Max TTL	<input type="text" value="30"/>	(1 to 255)
Init TTL	<input type="text" value="1"/>	(1 to 255)
MaxFail	<input type="text" value="5"/>	(1 to 255)
Interval(secs)	<input type="text" value="3"/>	(1 to 60)
Port	<input type="text" value="33434"/>	(1 to 65535)
Size	<input type="text" value="0"/>	(0 to 39936)
Source	<input type="text" value="None"/>	
<b>Results</b>		

8. In the **IPv6 Address/Hostname** field, enter the IPv6 address or host name of the station to which you want the switch to discover a path.

The initial value is blank. The IPv6 address or host name you enter is not retained across a power cycle.

9. Enter the **Probes Per Hop**.

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

10. Enter the **Maximum TTL** for the destination.

The default value is 30. The range is 1 to 255. The MaxTTL you enter is not retained across a power cycle.

11. Enter the **Initial TTL** to be used.

The default value is 1. The range is 1 to 255. The InitTTL you enter is not retained across a power cycle.

12. Enter the **Maximum Failures** allowed in the session.

The default value is 5. The range is 1 to 255. The MaxFail you enter is not retained across a power cycle.

13. **Interval (secs)** - Enter the time between probes in seconds.

The default value is 3. The range is 1 to 60. The interval that you enter is not retained across a power cycle.

14. Enter the UDP Destination **Port** in probe packets.

The default value is 33434. The range is 1- 65535. The port you enter is not retained across a power cycle.

15. Enter the **Size** of the probe packets.



The default value is 0. The range is 0 to 39936. The size you enter is not retained across a power cycle.

**16.** Enter the **Source** IP address or interface to use when sending the echo request packets.

If source is not required, select **None** as the source option. Possible values are as follows:

- **None.** The source address of the ping packet would be the address of the default outgoing interface.
- **IP Address.** The source IP address to use when sending the echo request packets. This field is shown when **IP Address** is selected as the source option.
- **Interface.** The interface to use when sending the echo request packets. This field is shown when **Interface** is selected as the source option.

**Note:** Values configured in the fields in this screen are not saved to the switch. As a result, refreshing the screen sets these fields to the default values.

**17.** Click the **Apply** button.

The traceroute begins. The results display in the TraceRoute area.

The **Results** field displays the traceroute IPv6 result after the switch sends a traceroute request to the specified IP address or host name.

## Perform a Full Memory Dump

You can perform a full memory dump to retrieve the core dump for troubleshooting.

➤ **To perform a full memory dump:**

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

The image shows a web-based configuration interface titled "Full Memory Dump Configuration". It contains several input fields and checkboxes:

- Protocol:** A dropdown menu with "USB" selected.
- File Path:** A text input field containing ".".
- File Name:** A text input field containing "core".
- Hostname:** A checkbox that is currently unchecked.
- Time-stamp:** A checkbox that is currently checked.
- Switch Register Dump:** A checkbox that is currently unchecked.
- Write Core Test:** A checkbox that is currently unchecked.
- Write Core:** A checkbox that is currently unchecked.
- Save Current Settings:** A checkbox that is currently checked.

8. From the **Protocol** menu, select the protocol used to store the core dump file.  
Possible values are as follows:
  - **None.** Disable core dump.
  - **TFTP.** Set TFTP protocol.
  - **NFS.** Set NFS protocol.
  - **USB.** Set USB protocol.
9. In the **File Path** field, enter the path to the location to store the core dump file.
10. In the **File Name** field, enter the core dump file name.
11. Select the **Hostname** option to append the host name to the core dump file name.
12. Select the **Time-stamp** option to append a time-stamp to the core dump file name.
13. Select the **Switch Register Dump** option to dump the switch chip register in case of an exception.
14. Select the **Write Core Test** option to test the core dump setup.
15. Select the **Write Core** option to create a core dump and store it to the previously configured external server.

Executing this procedure causes a reload of the device.

16. Select the **Save Current Settings** option to save the current settings of the system.
17. Click the **Apply** button.

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

## Default Settings

---

This appendix describes the default settings for many of the NETGEAR managed switch software features.

**Table 248. 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	None
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, SNMPv3)
SNMP Traps	Enabled
Auto Install	Enabled
Auto Save	Disabled

**Table 248. Default Settings (continued)**

Feature	Default
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
Captive Portal	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)	Disabled
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	Enabled
MAC table address aging	300 seconds (dynamic addresses)

**Table 248. Default Settings (continued)**

Feature	Default
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 RSTP
Optional STP features	Disabled
STP bridge priority	32768
Multiple Spanning Tree	Disabled
Link aggregation	No Link Aggregation Groups (LAGs) configured
LACP system priority	1
Routing mode	Disabled
IP helper and UDP relay	Disabled
Tunnel and loopback interfaces	None
DiffServ	Enabled
Auto VoIP	Disabled
Auto VoIP traffic class	6
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 (VLANs)*
- *Access Control Lists (ACLs)*
- *Differentiated Services (DiffServ)*
- *802.1X*
- *MSTP*

## Virtual Local Area Networks (VLANs)

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 PCs, 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 present 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 Settings](#) on page 204.
- 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 does not is not a member of the VLAN as 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 Configuration Examples

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 (see [Configure VLANs](#) on page 195), create the following VLANs:
  - A VLAN with VLAN ID 10.
  - A VLAN with VLAN ID 20.
2. In the VLAN Membership screen (see [Configure VLAN Membership](#) on page 201) 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).
3. In the Port PVID Configuration screen (see [Configure Port PVID Settings](#) on page 204), 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
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 (ACLs)

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.

M6100/M7100/M5300 allow 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 [Configure a Basic MAC ACL](#) on page 649).

By default, this ACL is bound on the inbound direction, which means the switch will examine 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 ACL Rules](#) on page 651.

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 MAC Binding](#) on page 654.)

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 ACL Bindings in the MAC Binding Table](#) on page 655).

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 Sample 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 656).
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 658.

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 IP ACL Interface Bindings](#) on page 671).  
  
 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 in the IP ACL Binding Table](#) on page 673).

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 there is no guarantee that it will. 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 cannot 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.

managed switch switches 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 (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 multi-field (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 (*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 three-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 (such as the DSCP or IP precedence value) definition to convey some QoS characteristics to downstream switches which 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 non-conformant. 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, follow these steps:

1. From the QoS Class Configuration screen, create a new class with the following settings:
  - Class Name: Class1
  - Class Type: All

For more information about this screen, see [Configure a DiffServ Class](#) on page 526.

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 about this screen, see [Configure a DiffServ Class](#) on page 526.

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 about this screen, see [Configure DiffServ Policy](#) on page 533.

6. Click the **Add** button.

The 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 about this screen, see [Configure DiffServ Policy](#) on page 533.

9. From the Service Configuration screen, select the check box next to interfaces g7 and g8 to attach the policy to these interfaces, and then click the **Apply** button. (See [Configure the DiffServ Service Interface](#) on page 536.)

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 include 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 you might want 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 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 switch 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/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 in 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 to ensure that access to its services is only permitted 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 when you 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 for you to complete an authentication exchange.

managed switch 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 will 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.

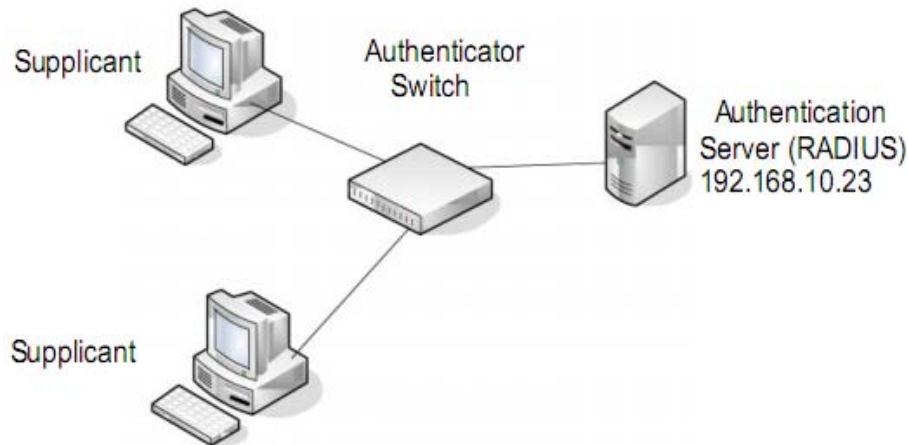


Figure 1. 802.1X Authentication Roles

## 802.1X Example 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 has been 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 be 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 [Configure a Port Security Interface](#) on page 598 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 the **Apply** button (See [Configure the Global Port Security Mode](#) on page 597).

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 Overview](#) on page 545.

7. Click the **Add** button.
8. From the Authentication List screen, configure the default List to use RADIUS as the first authentication method (See [Configure a Login Authentication List](#) on page 555).

This example enables 802.1X-based port security on M6100/M7100/M5300 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 Forwarding 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 provides 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 will transmit the appropriate BPDU depending on the received type of BPDU from a particular port.

An MST Region comprises of 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 a 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 has to be configured with an unambiguous assignment of VLAN IDs (VIDs) to spanning trees. This is achieved by:

1. Ensuring that the allocation of VIDs to FIDs is unambiguous.
2. Ensuring that 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.

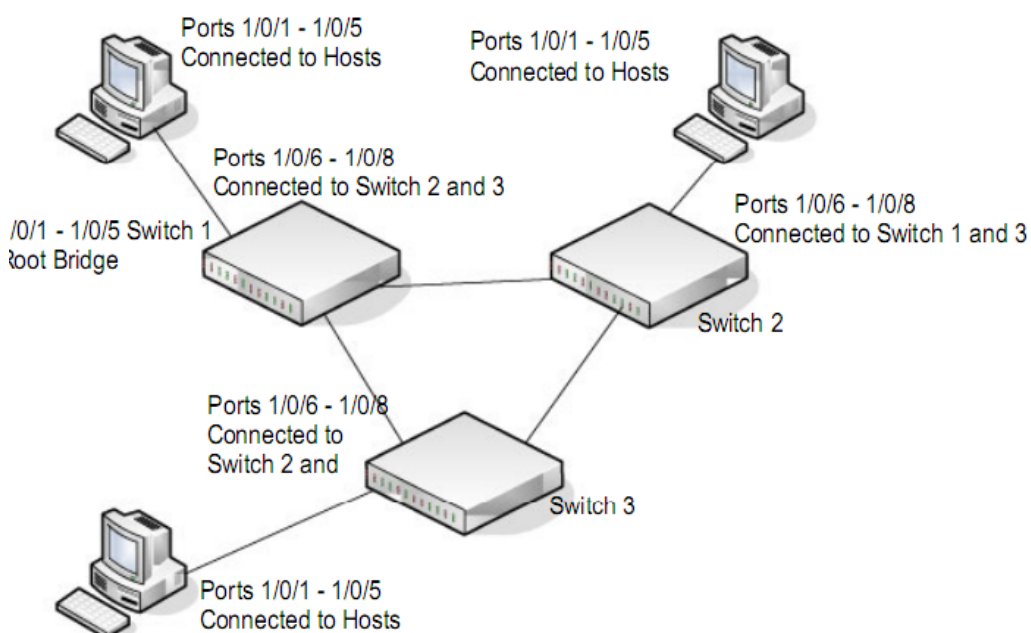
With this allocation we ensure that every VLAN is assigned to one and only one MSTI. The CIST is also an instance of spanning tree with a MSTID of 0.

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 Example Configuration

This example shows how to create an MSTP instance from the M6100/M7100/M5300 switch. The example network has three different M6100/M7100/M5300 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 sample configuration**

Perform the following procedures on each switch to configure MSTP:

1. Use the VLAN Configuration screen to create VLANs 300 and 500 (see [Configure Basic VLAN Settings](#) on page 195).
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 [Configure Basic VLAN Settings](#) on page 195).
3. From the STP Configuration screen, enable the Spanning Tree State option (see [Configure Advanced STP Settings](#) on page 231).

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.

4. 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 are assigned the same bridge priority value, the switch with the lowest MAC address is elected as the root bridge (see [Configure CST Settings](#) on page 234).

5. From the CST Port Configuration screen, select ports 1/0/1–1/0/8 and select **Enable** from the **STP Status** menu (see [Configure CST Port Settings](#) on page 236).
6. Click the **Apply** button.
7. 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.
8. Click the **Apply** button.

You can use the CST Port Status screen to view spanning tree information about each port.

9. From the MST Configuration screen, create a MST instances with the following settings:
  - MST ID: 1
  - Priority: Use the default (32768)
  - VLAN ID: 300

For more information, see [Configure MST Settings](#) on page 240.

10. Click the **Add** button.
11. Create a second MST instance with the following settings
  - MST ID: 2
  - Priority: 49152
  - VLAN ID: 500
12. Click the **Add** button.

In this example, assume that Switch 1 has become the Root bridge for the 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 include 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.

## c Acronyms and Abbreviations

---



In most cases, acronyms and abbreviations are defined on first use in this document. Acronyms and abbreviations are also defined in the following table.

**Table 249. Acronyms and Abbreviations**

Acronym	Definition
<b>802.1x</b>	IEEE 802.1x Authentication Protocol Standard
<b>ACE</b>	Access Control Entry
<b>ACL</b>	Access Control List
API	Application Programming Interface
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
CLI	Command Line Interface
CoS	Class of Service
Default Gateway	The IP address of a router that a host can use as its first hop when the host does not know a more specific route to a given destination.
Default Route	A manually configured ( <i>static</i> ) route whose destination is 0.0.0.0/0.0.0.0 and therefore matches every packet's destination. A router uses a default route to forward packets that do not match a more specific route.
DHCP	Dynamic Host Configuration Protocol (RFC 2131, RFC3315). A mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.
DHCP Server	Dynamic Host Configuration Protocol Servers are servers that grant the address and do parameter assignment to requested clients in the network. Current interest is that these servers provide TFTP server and boot file information.
DLL	Data Link Layer
DNS Server	Domain Name System servers that provide the IP address mapping to the name of the hosts.
DSCP	Differentiated Services Code Point

Table 249. Acronyms and Abbreviations (continued)

Acronym	Definition
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over LAN
ECMP	Equal Cost Multiple Paths
EEE	Energy Efficient Ethernet (from the IEEE 802.3az Energy Efficient Ethernet Task Force and IEEE 802.3az Energy Efficient Ethernet Study Group).
Host Interface	An IP interface that is not a routing interface. Only locally-originated packets are sent on a host interface. Only packets with a local destination are received. Host interfaces do not participate in dynamic routing protocols.
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAS	Internal Authentication Server
IGMP	Internet Group Management Protocol
In-band Interface	An IP interface that could be used for in-band management. Any IP interface other than the Out-of-Band port.
IP	Internet Protocol
IP Address Owner	The VRRP router that has the virtual router's IP address(es) as real interface address(es). This is the router that, when up, will respond to packets addressed to one of these IP addresses for ICMP pings, TCP connections, and so on
IP Interface	An interface configured as an IP interface rather than a Layer 2 switching interface. An IP interface must be assigned one or more IP addresses. Also called a <i>Layer 3 interface</i> .
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISDP	Industry Standard Discovery Protocol
ISID	Initiator-defined session identifier
L2	Layer 2 (networking)
L3	Layer 3 (networking)
LAG	Link Aggregation Group (IEEE standard)
LLDP	Link Layer Discovery Protocol
Local Route	A route to an attached subnet. A router creates a local route for each active, locally-configured IP address and uses the local route to reach other stations on the attached subnet.
LPI	Low-power Idle
MAB	MAC Authentication Bypass



**Table 249. Acronyms and Abbreviations (continued)**

Acronym	Definition
MAC	Media Access Control
Management Interface	An external IP interface used to send and receive IP packets to configure and monitor the device.
Management VLAN	A VLAN configured to be used for management rather than control or data traffic.
MFDB	Multicast Forwarding Database
MIB	Management Information Base
MLAG	Multi-chassis Link Aggregation
MPLS	Multiprotocol Label Switching: A standard involving IP quality.
MVR	Multicast VLAN Registration
N/A	not applicable
NSF	Nonstop Forwarding
PAE	Port Access Entity
PDU	Protocol Data Unit
PIM-DM	Protocol-Independent Multicast Dense mode
PIM-SM	Protocol-Independent Multicast Sparse mode
Primary IP Address	An IP address selected from the set of real interface addresses. One possible selection algorithm is to always select the first address. VRRP advertisements are always sent using the primary IP address as the source of the IP packet.
PoE	Power over Ethernet. Corresponds to the IEEE 802.3AF standard which supports power delivery of up to 15.4W per port.
PoE+	Power over Ethernet Plus. Corresponds to the IEEE 802.3AT standard which supports power delivery of up to 34.2W per port.
PSE	Power Sourcing Equipment
QoS	Quality of Service
RADIUS	Remote Authentication Dial-in User Service
Routing Interface	An IP interface whose physical ports are front panel ports and associated with a VLAN. Packets received on a routing interface can be transmitted on a different VLAN than they were received on.
SDM	Switch Database Management
Service Port	An IP interface on an Ethernet interface that is separate from the front panel ports. The service port is dedicated to management. The service port has its own independent interface to the IP stack. The service port is a host interface.
SM	state machine

**Table 249. Acronyms and Abbreviations (continued)**

Acronym	Definition
SMTP	Simple Mail Transfer Protocol
SNTP	Simple Network Time Protocol
TFTP	Trivial File Transfer Protocol
TFTP Server	Trivial File Transfer Protocol Servers are servers that hold the requested configuration and/or image files for requested clients.
TLV	Type-Length-Value
UDLD	Uni-Directional Link Detection
UI	User Interface
UPoE	Universal Power over Ethernet. No IEEE standard exists yet for UPoE. NETGEAR UPoE supports power delivery of up to 60W per port.
USB	Universal Serial Bus
Virtual Router	An abstract object managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a virtual router identifier and a set of associated IP address(es) across a common LAN. A VRRP router can backup one or more virtual routers
Virtual Router Backup	The set of VRRP routers available to assume forwarding responsibility for a virtual router if the current Master fails.
Virtual Router Master	The VRRP router that is assuming the responsibility of forwarding packets sent to the IP address(es) associated with the virtual router, and answering ARP requests for these IP addresses. Note that if the IP address owner is available, then it will always become the Master.
VLAN	Virtual Local Area Network
VRRP Router	A router running the Virtual Router Redundancy Protocol. It can participate in one or more virtual routers.